设备故障和人误数据分析评价方法

原子能出版社

内 容 简 介

本书以核电站、飞机等为例，系统地介绍了在定量安全评价工作中所需要的各种机电设备和部件的故障率、基本人误率和初因事件概率，详细地叙述了这些数据的收集、统计分析与评价的原则和方法。

本书可供从事安全系统分析的工程技术人员和负责劳动保护干部、设计、生产人员阅读，亦可供高等院校安全工程专业师生参考。

设备故障和人误数据
分析评价方法
阎凤文等　编译
刘雪涛　　审校
原子能出版社出版
（北京2108信箱）
原子能出版社印刷厂印刷
新华书店总店科技发行所发行·新华书店经售
☆
开本787×1092 1/32·印张5.75·字数125千字
1988年6月北京第一版·1988年6月北京第一次印刷
印数1—2200
ISBN 7-5022-01[illegible]
TL·45　定价：2.00元

序

为促进我国安全管理工作的科学化，对危险和事故进行预先分析研究，防止事故发生和对已发生的事故用科学分析方法找出原因，目前我国许多工矿、企业正在积极推广应用安全系统工程，并且已开始从定性分析向定量分析发展。但是，定量分析所必需的设备故障数据和人误数据在国内尚无完整的资料，为此，我们组织编译并审校了《设备故障和人误数据分析评价方法》这本书。

本书除核故障率数据外，还包括一般机械、电气、电子设备的故障率数据，而且包含有人员操作可靠性方面的数据，同时比较详尽地介绍了这些数据的统计、分析与评价的一般原则和方法。应用这些评价技术可对具体系统的经验数据进行分析，从而得出定量系统分析所需的设备故障率和人员失误率，作为故障树分析或事件树分析的输入参数。

本书第一章至第六章（阎凤文编译）取材于美国核管理委员会1975年发表的 WASH-1400 号报告附录 III "Failure Data"；附表 1 和附表 2（王朝贵、王劲松、肖峥、李涛、张炯编译）分别取材于美国电机电子工程师学会1984年发表的IEEE std-1984号报告和美国核管理委员会1982年发表的"Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application"一书的第20章；附表 3（李兆桓编译）取材于美国核管理委员会1985年发表的NURER/CR-2815号报告。

由于时间仓促，编译者水平有限，肯定有错误之处，敬请读者批评指正。

核工业部安全防护卫生局核安全防护处

核工业部西南反应堆研究设计院

一九八七年十二月二十日

目　录

第一章

术语和数据评价方法简介

在定量的系统概率估计中，需要把故障率和检修时间形式的部件行为数据作为系统模型的输入。对于风险评价来说，它与可靠性分析不同，在其定量结果中可容许有较大的误差（例如，一个量级的准确度），这对于处理现有数据有重要意义。在标准的可靠性分析中，为使系统模型定量化，数据和结果通常都采用点值（即“最佳估计值”）。

在风险评价中，由于结果准确到一个量级范围就足够了，故而能够有效地应用随机变量和概率统计方法来表示数据和结果。因此，可以大大地放宽故障率数据的基础，而且可以利用具有较大误差范围和不确定度的数据。本书给出的数据和有关材料是根据风险评价的需要而收集的，并且是应该按着随机变量的结构形式来使用的。但是，必须注意的是，在进行一般的定量可靠性分析时，这些数据可能是不够详细或准确的。

为了使读者便于了解本书的内容，我们先介绍一下本书中将出现的一些术语。

故障概率：系统、子系统或部件在指定的一段时间内发生故障的概率。对所定义的故障来说，故障概率相当于不可靠度。

无效度：系统、子系统或部件在某一具体时刻，处于故

障状态，即不能工作的概率。有效度是无效度的补充，这里把点无效度和区间无效度看成是等价的。

动态设备：像泵、阀和继电器等为了完成其预期的功能而运转、移动或改变状态的那些运行设备。

静态设备：像管道、容器和焊缝等通常是不活动的，但其故障会影响到系统行为的那些无活动能力的设备。

试验时间：试验一个系统、子系统或部件所需的全部在线时间，包括有效试验时间加上试验后重新组装所需的在线时间在内的全部时间。

维修时间：维修一个系统、子系统或设备所需的全部在线时间，与试验时间的定义类似，在线维修期包括实际维修时间加上与维修有关的任何安装或调试时间。①

试验间隔：系统、子系统和部件试验之间的时间长度。为了应用方便，常把试验间隔取作720小时（约一个月），不过也有例外，如根据每个部件得出合适的试验间隔，像进一步讨论的那样，把试验间隔看作是周期性的。

维修间隔：指系统、子系统或部件维修之间的时间长度。维修间隔取决于维修是否为周期性或非周期性，计划性或非计划性等特点。此处为了使用方便，通常把维修间隔看成是非计划性的，因此也是非周期性的。

需求概率：对于那些需要起动、改变状态或在发生事故时起作用的部件、设备而未能按需求起作用的概率。用Q_d表示需求概率，其贡献包括需求时刻的故障，需求以前的故障，以及足够时间的连续操作未能成功地响应需求的故障。

---

① 标准应用的术语"在线"，表示实际影响系统无效度或故障概率的时间。惯用语"在线"常被理解为仅仅对系统有实际影响的试验或维修时间。

有时，需求概率数据可能与标准的周期性数据有关，或者把它理解为一般的无效度。人误数据也可能同需求概率（即每次动作）有关，如6.1节所述。

运行故障率：对于需要在一定时期内运行或起作用的那些部件，故障概率（每小时）用λ_0表示。对于受到事故环境影响的那些部件，给出适合于相应事故环境的附加故障率。

待机故障率：对于那些被动型设备，像管道、导线等，通常处于静止或待机状态，一直到进行试验或事故发生时为止，其故障概率（每小时）用λ_s表示。

上述定义涉及到可靠性理论中所使用的专用词汇和概念。试验和维修数据通常包括试验和维修时间，以及试验和维修间隔；部件故障数据一般包括需求概率，运行故障率和待机故障率。这里给出的定义已能满足风险评价研究工作的需要。

下面再叙述一下本文用到的一些基本概念、研究中所用的概率法或随机变量法及与建立数据基础有关的结论。

系统的定量估计可能涉及到点估计和随机变量估计这两种计算方法中的一种，就主要目的和方法而论，点估计同随机变量估计是不同的，而且必须考虑怎样输入数据。应用点估计时，其一般目的是获取有关系统参数的最佳值，通常为系统的无效度或故障概率（不可靠度）。由于在点估计中，计算结果是表示精确型数值的，因此人们试图得到具有高度准确度的输入数据。当然，实际上，点估计值并非是准确的，只不过是尽可能计算得精确些罢了。

由于点估计需要高度准确的部件评价，所以一般需要多方面的输入数据，根据具体特性对每个部件进行分类，掌握部件的“演变过程”。这些特性的示例如下：

a. 部件的类型（继电器、马达等），

b. 部件的制造厂家，

c. 部件的故障模式（开、闭、破损等），

d. 部件的技术规范（电压、电流等），

e. 部件的环境（温度、湿度等）。

在点估计中，求出每个部件的单值故障率或需求概率，然后把这些精确数值代入可靠性方程，求出系统结果的点值。实际上，为了得到具体部件的单值故障率或需求概率，要用抽样的方法收集新的故障数据，并且应用统计学的点估计技术①。

实际上，演变过程特性的精确选配不是一定能办得到的，而故障率是从尽可能同问题的重要特性相匹配的数据中导出的。利用技术鉴定来确定各种数据的可利用性。点估计中所用的原始数据可从手册、现场经验或专门设计的抽样实验中取得。

第二种方法，随机变量技术通常不是在关于可靠性教科书中介绍和论述的，而是统计和概率模拟中的一种一般的标准方法。在随机变量法中，用一个点值作为输入参数来描述实际情况似乎是不够的，故需要求出区间值代替之，以便描述同参数相联系的可变性和随机性。把区间形式的数据参数（如故障率）输入计算，于是，可以把这些输入数据看作是随机变量，而数据的区间给出随机变量的各种可能性。最后一点是概率分布同随机变量相联系，被用来描述各种可能数值的概率。

获得随机变量法所需数据的最简单的方法之一，是估计

---

① 标准方法包括像最大似然估计那样的参数估计技术。

出所用的每部分数据的区间。在应用随机变量法做可靠性分析时，把故障率看作是随机变量。因此，估计包括求出每个部件故障率和每个需求概率的区间。

选用随机变量法进行故障数据评价有几种原因。由于计算出的可靠性结果是应用于核电站总体（100座）的，因此希望能对不同电站的部件故障可变性进行模拟。同时，现有数据不是精确的，而有很大的不确定性，所以希望能把这些不确定性和可变性包括在内。

在数据分布为先验的情况下，把数据作为随机变量处理，有时涉及到用贝叶斯方法处理。其次，把系统故障率及其无效度看作是条件概率，并且通过先验数据的积分得出总的边缘分布。由于数据分布是同总体（100座核电站）相联系的，所以通过研究现有的简单随机变量来处理数据和系统的特性，但是，当数据分布被认为是给定的贝叶斯先验时，也可以应用贝叶斯方法进行解释。

后面各章列出的故障率和需求概率是根据一些参考手册、报告、运行经验和核电站经验推导出来的。数据源包括美国国防部（国家航天和航空管理局、空军等）的资料，以及一般工业运行经验和核电站运行经验资料。为了得出最终区间，评价过程需要把这些信息混合起来，以使数据处在此区间范围之内的概率很高。

分析各种部件的数据源表明，在最终的数据基础评价中，一般达到一个数量级的准确度是可行的。对于风险概率估计，这样的准确度足够了，因为只要求数量级结果。下面给出直观的区间评价图示，区间型评价的优点是使计算和结果对任何个别少量数据的微小差别不敏感。

在用对数正态分布描述数据的可变性时，由于对数正态

有两个参数（比方说均值和标准偏差），应适当规定区间的两个端点以确定出唯一的对数正态。在评价中，选择90％区间，

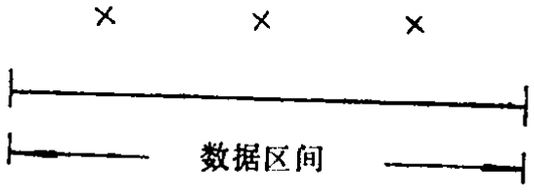

图1-1　数据源值区间评价示意图

区间下端点为5％界，而上端点为95％界。于是，每个故障率和需求概率的评价区间与90％的定义界相一致（这样，数据值可能处于此区间内的概率为90％）。

尽管所用的数据源体现不同的条件和用途，而某些源显然比另一些源更适合，但通常数据源在一至两个数量级准确度内是符合的。于是，最终评价出的区间一般为一至两个数量级宽度，反映出数据一致性的程度。根据这一数量级准确度，可以把区间和点值按指数标度确定到最接近的半整数，即故障率结果为10^{-1}或$10^{-1.5}$，等等。半整数指数标度与有效数字3或1相一致，即1×10^{-1}或3×10^{-2}，等等。

由于在评价时使用了不同的数据源，而且涉及到大量的部件，在获得实际的评价区间时，包括有一些重复，从各种数据源选择数据点（包括核电站经验在内），然后使区间相重叠，以便覆盖大约90％的点。该处理方法对90％定义界的精确度不敏感，例如，若区间实际上为85％或95％，几乎没有差别。区间的确定是根据每个源数据点的重要程度断然作出的，评价的判定是以可靠性和核电站运行经验中的个体经验为基础的。

鉴于这一数量级区间和准确度，通常只按一般的类型对

部件进行分类。当存在极端特性时，对部件故障的定义作了进一步的叙述。若有可能，用实际的核电站经验作为确定和检验最终评价区间的主要基准。可观察到的不同核电站部件的可变性同最终评价的区间宽度是不一致的（该可变性同所用的随机变量法也是不一致的）。

后面几章列出的有关数据表和进行的讨论，给出了基本数据，评价区间，和各评价区间的比较。希望这些能帮助读者有效地确定自己所用的数据区间。

在表和讨论中，可摘录出的故障模式是根据每个部件的类别给出的，故障率的单位为每小时（h^{-1}），而需求概率（无效度）的单位为每次需求（D^{-1}）。上下界与大约95%和5%区间端点相一致（至半整数标度）。可把区间和上下界理解为数据的置信度，但是，必须在随机变量(或贝叶斯法)范围内才能这样理解。

第二章

数据基础评价

2.1 综合数据列表

表2.1给出了反应堆安全研究所用的故障数据的最终评价区间和形成评价区间基础的主要原始输入数据。

2.2 数据评价的比较

表2.1比较明确地表示了最终评价的区间与可得到的核电站经验值的比较，以及与其他工业经验的界值的比较。核电站的数据是根据第三章所介绍的1975年的核电站经验估算的，工业经验的界值是从原始工业数据源输入值（为确定型界值）得出的最大值和最小值，并且同评价区间（按90%概率定义的）进行了比较。

表2.1 评价值与核经验值和工业经验值的比较

部件名称	主要故障			评价值		工业经验值		核电站经验值
	模式	符号	单位	下界	上界	下界	上界	
泵	启动失败	Q_d	1/次	3×10^{-4}	3×10^{-3}	5×10^{-5}	5×10^{-3}	1×10^{-3}
	停转（正常环境）	λ_0	1/小时	3×10^{-6}	3×10^{-4}	1.4×10^{-7}	1.4×10^{-4}	3×10^{-6}①
	停转（异常环境）	λ_0	1/小时	1×10^{-4}	1×10^{-2}	3×10^{-4}	1×10^{-3}	
电动阀	未起作用	Q_d	1/次	3×10^{-4}	3×10^{-3}	2×10^{-4}	7×10^{-2}⑤	1×10^{-3}
	堵塞	Q_d	1/次	3×10^{-5}	3×10^{-4}	6×10^{-5}	3×10^{-4}	3×10^{-5}②
电磁阀	未起作用	Q_d	1/次	3×10^{-4}	3×10^{-3}	2×10^{-5}	6.5×10^{-3}	1×10^{-3}
	堵塞	Q_d	1/次	3×10^{-5}	3×10^{-4}			3×10^{-5}③

续表

部件名称	主要故障			评价值		工业经验值		核电站经验值
	模式	符号	单位	下界	上界	下界	上界	
气动阀	未起作用	Q_d	1/次	1×10^{-4}	1×10^{-3}	1×10^{-6}	2×10^{-2}⑥	1×10^{-4}
	堵塞	Q_d	1/次	3×10^{-5}	3×10^{-4}			3×10^{-5}②
真空阀	未起作用	Q_d	1/次	1×10^{-5}	1×10^{-4}	1×10^{-5}	1×10^{-4}	
闸阀	未能打开	Q_d	1/次	3×10^{-5}	3×10^{-4}	2×10^{-5}	3×10^{-4}	1×10^{-4}
	内部渗漏	λ_0	1/小时	1×10^{-7}	1×10^{-6}	1×10^{-7}	1×10^{-6}	
溢流阀	未能打开	Q_d	1/次	3×10^{-6}	3×10^{-5}	1.4×10^{-5}	3.5×10^{-5}	1×10^{-5}
手动阀	堵塞	Q_d	1/次	3×10^{-5}	3×10^{-4}	3×10^{-4}	3×10^{-4}	3×10^{-5}
管道	堵塞/破裂 直径≤3英寸	λ_0	1/小时	3×10^{-11}	3×10^{-8}	2×10^{-9}	5×10^{-6}⑦	2×10^{-9}
	直径>3英寸	λ_0	1/小时	3×10^{-12}	3×10^{-9}	3×10^{-10}	1×10^{-6}⑦	1×10^{-10}
机械离合器	未能联接或脱开	Q_d	1/次	1×10^{-4}	1×10^{-3}	1×10^{-4}	4×10^{-3}	3×10^{-4}

电动离合器	未起作用	Q_d	1/次	1×10^{-4}	1×10^{-3}	2×10^{-4}	4×10^{-3}	3×10^{-4}
电机	启动失败	Q_d	1/次	1×10^{-4}	1×10^{-3}	7×10^{-5}	3×10^{-3}⑧	3×10^{-4}
	停转（正常环境）	λ_0	1/小时	3×10^{-6}	3×10^{-5}	5×10^{-7}	1×10^{-4}	1×10^{-6}⑧
	停转（异常环境）	λ_0	1/小时	1×10^{-4}	1×10^{-2}	1×10^{-4}	1×10^{-3}	
变压器	断路/短路	λ_0	1/小时	3×10^{-7}	3×10^{-6}	1×10^{-7}	1×10^{-6}	1×10^{-6}
继电器	没有激磁	Q_d	1/次	3×10^{-5}	3×10^{-4}	4×10^{-5}	1×10^{-3}⑧	3×10^{-5}
断路器	未能转换	Q_d	1/次	3×10^{-4}	3×10^{-3}	2×10^{-5}	3×10^{-3}	1×10^{-3}
限位开关	未起作用	Q_d	1/次	1×10^{-4}	1×10^{-3}	1×10^{-5}	7×10^{-4}	
扭转开关	未起作用	Q_d	1/次	3×10^{-5}	3×10^{-4}	2×10^{-5}	1×10^{-4}	1×10^{-4}
压力开关	未起作用	Q_d	1/次	3×10^{-5}	3×10^{-4}	5×10^{-5}	1×10^{-3}	1×10^{-4}

部件名称	主要故障			评价值		工业经验值		核电站经验值
	模式	符号	单位	下界	上界	下界	上界	
手动开关	未起作用	Q_d	1/次	3×10^{-6}	3×10^{-5}	3×10^{-6}	1×10^{-4}⑩	3×10^{-5}
蓄电池	输出不正常	λ_0	1/小时	1×10^{-6}	1×10^{-5}	1×10^{-7}	6×10^{-6}	3×10^{-7}④
固体组件	功能失效(高功率)	λ_0	1/小时	3×10^{-7}	3×10^{-5}	2×10^{-6}	1×10^{-4}⑪	1×10^{-6}
	功能失效(低功率)	λ_0	1/小时	1×10^{-7}	1×10^{-5}	2×10^{-7}	2×10^{-6}	
柴油机	启动失败	Q_d	1/次	1×10^{-2}	1×10^{-1}	1×10^{-3}	1×10^{-1}	3×10^{-2}
	停转（应急负荷）	λ_0	1/小时	3×10^{-4}	3×10^{-2}	1×10^{-4}	1×10^{-3}	1×10^{-3}
仪器仪表	未起作用	λ_0	1/小时	1×10^{-7}	1×10^{-5}	3×10^{-7}	6×10^{-5}⑫	1×10^{-6}

表 2.1注：①根据泵的平均数据导出的，包括待机时间和运行时间在内。②根据已发现的堵塞事件估计的。③根据待机和运行数据导出的。④根据蓄电池不带负荷的待机试验导出的。⑤根据高温钠介质条件导出的。⑥包括气源不合适引起的故障。⑦由于不同数据源的管道长度单位不同，每英尺、每段、每座电站等，所以工业源的故障率区间极宽。至于管道故障率的详细比较见第六章的专门评价部分。⑧是从高温液态金属试验堆的应用中得出的。⑨本数据是继电器所有故障模式的平均值。⑩本数据是开关所有故障模式的平均值。⑪该数据是从实验反应堆经验推导的。⑫该数据取自化学工业，

第三章

核电站经验

美国于1975年对它当时的商用反应堆运行经验进行了研究，目的是检验有关反应堆部件的故障率数据。因为当时很少采用定量估价的观点对反应堆的历史进行记录，所以要获得这方面的有用的数据有一定的困难。对于故障现象，一般没有记录到足够的定量特性，也几乎没有按统计的和行为的趋势估价进行区别和分类，而且几乎没有系统地贮存用于定量估价和检索的资料。

即便得到了一些比较准确的核数据，数据基础中评定的区间也是比较窄的。因为不可能得到精确而详细的部件资料数据，所以只能以粗略的统计平均值代替。但是，由于采用了随机变量法，能把统计平均数据包括进去，并能把该统计平均值作为评定区间的重要资料。

在评价程序中，包括数据基础在内，把评定的区间同核电站数据作了比较，以确保核电站数据同确定的区间相一致，并且核电站数据值与区间评价值是不矛盾的。平均核电站数据值是通过分析核电站的运行历史和人为选取的数据估计值（即故障率、需求概率等）应用标准可靠性估计技术得出的。在表2.1中已给出了核电站数据与评定区间的比较。本章对获得核电站数据值而做的估价重新进行了审查，并将提供估价中所用的原始数据汇总表。同时给出某些附加的趋势分析，这种分析是同数据评价一起进行的，并在区间