全国系统可靠性分析方法学习班

讲义之二

故障树分析法(FTA法)
理论及应用

黄祥瑞　高金钟　许凤璋

全国系统可靠性学习班筹备组

1982.8

编　者　的　话

故障树分析法（ＦＴＡ）是系统可靠性研究中近几年发展起来的一种重要分析方法。在国外已广泛应用于工程技术领域中。它是工程技术人员研究系统可靠性的有效的得力工具。

根据我国可靠性研究工作迅速发展的需要。在数学学会可靠性专业委员会和军事系统工程委员会的大力支持下。我们为全国系统可靠性分析方法学习讨论会撰写了这本讲义。

本讲义是由清华大学核能研究所黄祥瑞同志和北京轻工业学院机械系许凤璋、高金钟同志编写。由于水平所限。错误及不当之处在所难免。敬望批评指正。

编　　者

一九八二年七月三十日

第一部分 FTA法理论基础

目 录

第二部分

第一章　故障树分析法概述

§1、1　历史的回顾

故障树分析法简称FTA法（Fault Tree Analysis）是一种近十年来发展起来的系统可靠性分析方法。它最为适合实际的工程系统中采用。最早使可靠性定量化的动力来自飞机工业。在第一次世界大战以后。由于空中交通和空中失事的增加。出现了有关飞机飞行的可靠性与安全性准则。从保证飞行成功出发对单发动机和多发动机飞机进行了比较。制订了每飞行小时事故率要求例如到1960年。曾经推断每百万次着陆大约有一次发生致命事故。于是就能够制订出这样的自动着陆系统设计准则：每10^7次着陆中发生致命的着陆风险少于1次。

四十年代：早期可靠性数学模型的推导是第二次世界大战期间在德国开始的。当时Werner Von Braun所领导的一个小组正在研制V－1导弹。第一批十枚导弹是完全不可靠的。它们都在发射台上爆炸或落于英吉利海峡。一位数学家Robert Lusser被请来作顾问。他肯定“一根链条不比它最薄弱的环节强”这句古谚对于串联系统是不适用的。因为这句话没有考虑随机失效的问题。然后Lusser 提出了串联组件的相乘律。即串联系统的可靠性等于组件可靠性的乘积$R_s = R_1 R_2 R_3 \cdots\cdots R_n$　或者$R_s = \prod_{i=1}^{n} R_i$

这就是现在常使用的公式。因此可见要使串联系统顺利工作。

各个组件的可靠性必须比系统可靠性高很多。

40年代美国致力于提高部件的可靠性。延长部件的使用寿命。例如更好的设计。更强的材料更好的检验手段等。在通用汽车公司的电动力分公司通过使用更好的绝缘。高温试验和改进锥一球形滚柱轴承等办法使汽车牵引马达的使用寿命从25000英里延长到100万英里。通过对曲轴和凸轮的轴承表面硬化处理大大延长了。柴油机的寿命。在设计方面考虑容易维修。事先维修。检查大大的提高了部件的可靠性。

五十年代：可靠性与安全性研究发展到航宇与核工业领域这时对元件可靠性研究已经用失效率。平均寿命。成功率等参量来描述。使可靠性学科更为科学化。

朝鲜战争中美国国防部发现不可靠设备的维护费用浩大。它发现各军种每年要花2美元去维护1美元的电子设备。向政府表明进行可靠性设计要比等待设备失效再去维修更为明智。从而美国开始了有关可靠性工作计划并应用于生产合同。销售各个方面美国国防部可靠性顾问团（AGREE)提出的有关对可靠性研究方面的报告得到了美国政府的重视。

六十年代。出现了新的可靠性方法并且应用的专业范围也扩大了早先的研究是集中于元件的效能。包括机械的。电气的。和液压的。现在扩大到元件效能对系统的失效的影响研究。即系统可靠性研究从洲际导弹的开发和其后“水星”“双子星座”等载人火前发展计划的时代加速了“首次试验成功”设计准则的必要性“航宇年代”在元件和系统的功能试验方面做了很多工作每次失效。失效分析和调查中所发现的缺陷检验记录都保留了记录对每种元件失效模式。机理。原因和失效对系统的影响都做了评估。

并提出了补救的措施当时系统的可靠性与安全性分析方法采用可靠性框图法（成功模型法）做为定量化的数学模型。随着更成熟的框图的出现。其复杂性不断增长因而有必要寻求其他途径。1961年。贝尔电话研究所H。A。Watson提出了故障树分析的方法。作为评估“民兵”导弹发射控制系统安全性的一项计划。后来波音公司修改了那个方案。使之便于利用计算机。

1965年 D。F Haasl 进一步发展了故障树建造技术。并把它推广应用到很宽范围的工业安全和可靠性问题中。

1962年在四个洲际导弹/地下井基地发生了灾难性的事故以后。按照美国空军的训令。第一次将系统的安全性问题作为一项独立的单项任务进行研究 1966年国防部采用了空军的标准。对一切国防合同都要求进行系统安全分析这些标准得到不断的扩大和修改。1969年国防部通过了MIL－STD－882：它是一份“对于系统。分系统及设备的系统安全性保障大钢”作为对一切国防合同承包商的标准通令。

国防部对各个硬件项目的可靠性。有效性。和可维护性的平行要求逐渐形成。如MIL－STD－471（有关可维修性标准）MIL－STD－781（有关指数分布可靠性试验标准）等。这些都是可靠性工程师和顾问工作的重要文件。从60年起初版发刊了不少可靠性方面的书籍。1961年出版的种子数科书”《可靠性理论与实践》著者是Igor Bazovsky 并在Rhlph Evans J ZW。Birnbaum。R Barlow。F。Proschan。 博士领导下创刊了《IEEE可靠性会刊》。

Esary 和W。Weibull等。在高级统计理论研究方面为可

可靠性和可维修性研究奠定了基础。

正是60年代起加速了对元件。系统和人失效的数据的搜集和编挡保存。逐渐各国形成了自己国家的数据库。

七十年代。由美国原子能委员会支持。1974年完成的“WASH—1400”反应堆安全性研究 毫不夸张地说它是划时代的广泛的核电站风险评价的重要报告。报告由MIT教授N·Rasmussen 领导。耗资300万美元。专家共60余人完成了压水堆沸水堆核电站中大量各类事故的分析与计算使事件树和故障树方法的应用得到重要的发展。“WASH—1400报告的主要内容有可能做为将来美核管理委员会（NRC）对核电站审批的补充标准这种研究方式已扩散到化工工业与其他工业。Rasmussen 式的研究正在欧洲。亚洲和美国迅速扩散。而报告中采取的主要方法就是事件树和故障树分析的方法。

随着科学技术迅速发展。大型系统工程（洲际导弹。宇航工程核电站等）的可靠性要求愈来愈高。因为它们的故障或失效都必将给社会带来严重的人身危害和巨大的经济损失。

系统可靠性研究学科是系统工程学科的重要分枝。研究和发展它必将对国民经济和我国四个现代化起到应有的作用。

§1。2 FTA法概论

60年代初人们对系统进行可靠性分析时。主要采用的方法是“真值表法”和“概率图法”。当系统部件较多。结构复杂时上述方法有一定困难。例如有10个部件组成的系统。每个元件都有正常和失效两种状态。那么需要对$2^{10}=1024$种状态进行分析。框图法在系统复杂时不易清楚表示人和环境对系统的

二次失效。为了深入地分析系统失效的因素是什么？在这么多的因素中哪些是主要的。以电子设备为例能导致电子设备失效的因素有物理的、化学的。环境的。人的影响。框图法就很难有层次的说明这些影响。故障树分析法到７０年代已被公认是对复杂系统可靠性。安全性的好方法。

1、2、1　故障树分析法的特点

（１）故障树分析法是一种图形演绎方法。是故障事件在一定条件下的逻辑推理方法。它不局限于对系统作一般的可靠性分析。它可以围绕一个或一些特定的失效状态。作层层深入的分析。因而在清晰地故障树图形下。表达了系统内在联系。并指出部件失效与系统失效之间的逻辑关系。

（２）由于故障树能把系统故障的各种因素连系起来。因此有利于提高系统的可靠性。找出系统的薄弱环节和系统的故障谱。

（３）故障树建成后。对不曾参与系统设计的管理与维修人员来说是相当于一个形象的管理。维修指南。因此对培训长期使用的大系统人员更有意义。

（４）通过故障树可以定量的求出复杂系统的失效概率和其他可靠性参量。为改善和评估系统可靠性提供定量数据。

（５）故障树分析的发展是和电子计算机技术和软件发展紧密相关的。图象信息技术也已经应用在故障树分析之中不能想象分析一株大型故障树不使用计算程序。因此编制计算程序是故障树分析中不可缺少的一部分。

（６）故障树分析法的理论基础是概率论布尔代数和数理统计等数学工具。其他在可靠性数学中用到的数学基础。在故障树分析的定量化中同样需要。故障树分析方法不仅应用于解决工程

技术问题，而且也开始用于社会经济管理的系统工程问题之中。

1、2、2 故障树的应用范围

FTA法用途很广一般讲可用于以下几个方面：

（1）系统的可靠性分析。可靠性参数定性与定量计算。

（2）系统的安全分析和事故分析

（3）系统的风险评价

（4）系统的重要度分析（灵敏度分析）

（5）故障诊断与检修表的制定

（6）系统最佳探测器的配置

（7）故障树摸拟

1、2、3 故障树分析法的不足处：

（1）建树过程复杂。需要具有丰富经验的技术人员参加。而且不同人所建造的故障不会完全相同。有时不可避免会发生错误和遗漏

（2）工作量大而且耗费人力、物力复杂系统更困难。有的故障树要建造数年。

（3）收集数据困难。而且进行区间估计时。用蒙台卡罗法在计算上和理论上都存在一定的困难。

1、2、4 FTA法及其步骤

所谓故障树分析法是把系统最不希望发生的失效状态（一般对可维修系统丧失机能称故障状态。而对不可维修系统丧失机能称失效以下所提到的故障和失效不作严格的区分）作为故障分析的目标（在故障树中定义为项事件）。因而找出导致这一故障状态所有可能发生的直接因素（在故障树中定义为中间故障事件）

再跟踪追迹找出导致这些中间故障事件所有可能发生的直接原因。直追寻到引起部件发生故障的全部原因（在故障树中定义为底事件）。用相应的代表符号及逻辑门把顶事件、中间故障事件、底事件联结成树形图。称此树形图为故障树（Fault Tree以下简称为FT）。以FT对系统的失效进行定性分析及定量计算。也就是说。以故障树为工具对系统的失效进行评价的方法。称故障树分析法。

FTA法的步骤。通常因评价对象、分析目的、精细程度等而不同。但一般可按如下步骤进行。

（1）故障树的建造。

（2）故障树的数学表达。

（3）定性分析。

（4）定量计算。

第二章　故障树的建造

§2.1　概述

故障树建造是FTA法的关键。因为FT建造的完善程度将直接影响定性分析和定量计算结果的准确性。此外这一工作十分庞大烦杂。机理交错多变。所以要求建树者必须慎重。仔细。并广泛的掌握设计、运行、安全分析等各方面的经验和知识。如能有多方面有关技术人员参加。共同研究等树是最为理想的。

建树一般可按照下步骤进行。

（1）广泛收集并分析有关技术资料

（2）选择顶事件

（3）建树

（4）FT简化

事实上建树过程也就是对系统仔细。透彻分析的过程。不同的人。从不同的角度所建造的故障树不会相同。目前还没有一种有效地统一建树方法。

建树过程常常也是一种反复过程。经过多次讨论。逐步完善使所建造的故障树趋于统一。

一般建树方法可分为两大类　I演绎法：

一般来说。故障树是由各种事件以及连接它的逻辑门所构成。建树就是找出导致顶事件发生的各种可能因素及其与顶事件之间的各种可能的因果关系。用符号和逻辑门把它们与顶事件联结成树枝状的逻辑树形图。具体建法是。先写出顶事件表示符号作为第一行。（称第一级）。在其下面并列的写出导致顶事件发生的