

可靠性技术丛书— 7

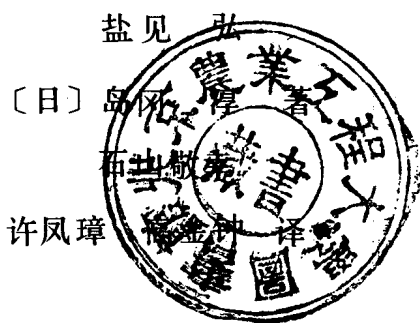
故障模式和影响分析 与故障树分析的应用

盐见 弘
〔日〕 岛冈 淳 著
石山敬幸

机械工业出版社

可靠性技术丛书—7

故障模式和影响分析 与 故障树分析的应用



机械工业出版社

3462062

本书是日本科技连可靠性技术丛书第7册的中译本。全书共分六章,前五章对可靠性的重要分析方法FMEA(故障模式和影响分析)与FTA(故障树分析)的基本概念及使用方法做了浅显易懂的介绍,并提供了具体而丰富的实例。第六章概要地介绍了系统可靠性分析的其他几种方法。

本书既是学习FMEA、FTA的入门书,也是一本实用手册性参考书。可供从事产品设计、质量保证、可靠性研究的专业技术人员、管理干部、部门领导人员和工科院校有关专业师生学习和参考。

日科技連信頼性工学シリーズ 第7卷

FMEA、FTAの活用

塩見 弘, 島岡 淳, 石山敬幸 著

日科技連出版社

1983年

可靠性技术丛书—7

故障模式与影响分析与故障树分析的应用

〔日〕 盐见 弘 岛冈 淳 石山敬幸 著

许凤璋 高金钟 译

责任编辑: 王正琼 封面设计: 方芬

机械工业出版社出版(北京阜成门外百万庄南里一号)

(北京市书刊出版业营业许可证出字第117号)

北京通县电子外文印刷厂印刷

新华书店北京发行所发行·新华书店经售

开本 $787 \times 1092^{1/32}$ 印张 $7^{1/4}$ 字数 153 千字

1987年11月北京第一版·1987年11月北京第一次印刷

印数 0,001—2,800 定价: 1.95 元

统一书号: 15033·7261

译者序

可靠性是衡量机电产品质量的一项重要标准。随着工业技术的发展,产品性能参数日益提高,结构日趋复杂,产品的使用场所更加广泛,环境更为严酷,因而,产品的可靠性问题越来越突出。从50年代起,国外就兴起了可靠性技术的研究。可靠性技术的观点和方法,目前已经成为产品质量保证、安全性研究和产品责任预防措施不可缺少的依据和手段。

日本开展可靠性技术的研究和应用已有近30年的历史。其可靠性技术着重应用在民用工业产品上,尤其是和TQC(全面质量管理)结合,形成实用化的特点,使产品的可靠性有显著提高。日本专家认为高可靠的优质产品的实现,是长期积累的可靠性技术和严格的生产管理制度相结合的结晶,必须强调从设计、制造、管理到使用、维修的全过程的管理。

这套丛书总结了日本推广可靠性技术的经验,通俗易懂,实用性强。它是为指导日本的技术人员和管理人员应用可靠性技术而编写的一套工具书。全书共分15册,包括可靠性、维修性总论、数理基础、设计、试验、数据采集和处理、故障诊断、维修和管理等诸方面内容。

为了配合国内普及和推广可靠性技术,我们决定翻译出版这套丛书,供从事产品设计、试验、管理、维修以及产品开发研究的各种专业人员和各级管理干部借鉴和应用。这套

丛书同时也可作为国内高等院校可靠性课程的教材，并且对从事可靠性研究的高等院校教师、科研人员和研究生也有参考价值。丛书由国家机械工业委员会机械科学研究院组织翻译、校审。全套丛书将陆续与读者见面，希望能对各单位开展可靠性活动有所裨益。

由于我们水平有限，难免有不足和谬误之处，欢迎批评指正。

在此，对日本科技连的慷慨赠书表示感谢。

国家机械工业委员会 科 技 司
机械科学研究院
一九八七年二月

《可靠性技术丛书》出版序言

1958年日本科技连内设立了可靠性研究会，至今已经历了近四分之一世纪的岁月。在这个期间，通过各种研究班和专题讨论会等普及活动，以及由于有关协会、学会及企业的努力，已经发表了大量有关可靠性的应用报告和研究成果。可靠性的观点和方法已经成为质量保证、安全性保证、产品责任预防等不可缺少的依据和手段，因此受到各方面的广泛关注。

日本科技连过去所进行的卓有成效的可靠性教育和普及活动，不仅有研究班和专题讨论会，还有关于可靠性的出版活动等。但遗憾的是，有些活动不完全是有组织地进行的，为了扩大活动的领域，在最近的可信性活动的高潮中，日本科技连出版社决定出版《日本科技连可靠性技术丛书全15卷》，虽然不免稍有动手已晚之感。

与所谓的可靠性技术专著相比，这套丛书的特点是具有更广泛的基础知识，尽可能简明易懂，讲述比较详尽，以适应从初学者到干部技术人员，乃至科处长等各类人员使用的要求。此外，为了使从事计划、设计、生产、质量管理、维修等各项业务，以及电子、电机、机械、精密仪器等各主要行业的人员喜欢阅读本书，执笔者邀请了各方面经验丰富的专家参与筹划。

这套丛书的另一个特点是，为了便于用作现场常备的参考书，并且携带方便，故采用32开本。读者可以分册阅读，

容易安排时间，并掌握其最基础的知识。

希望这套丛书能成为与可靠性有关的工作人员的案头书，
在今后发展可靠性活动中起到引路的作用。

《日本科技连可靠性技术丛书》

主编

市田 嵩

川崎义人

盐见 弘

前 言

可靠性工程中最普及的方法是威布尔概率纸法, FMEA (故障模式和影响分析) 及 FTA (故障树分析), 这种说法在日本大概是没有异议的。

那么, 为什么 FMEA、FTA 如此 闻名呢? 首要的原因是日本科技连可靠性机械分会(理事长: 铃木顺二郎) 将它们调查研究的成果和日本科技连例行研讨会的内容结合起来, 归纳总结成《FMEA·FTA 实施法》一书(日本科技连出版社出版, 获1982年度日经质量管理文献奖)。

FMEA 及 FTA 于50年代末至60年代初就已奠定了基础, 最初应用于美国的军事和宇宙开发等领域中, 当时认为它并不是什么新的方法。但是, 后来作为一种预测评价方法用于评价安全性, 特别是评价原子能发电站的安全性, 以及用于 PLP (产品责任预防) 等有关问题后, 人们对它们才有了新的认识。

FMEA 是人所共知的定性评价方法, 它和过去的以可靠性框图为基础, 使用故障率数据进行可靠性定量预测的 FTA 法, 是相互对应的。

FMEA 的优点是: 即使没有定量的可靠性数据, 也能找出有问题的地方, 这是它首要的特点。在日本, FMEA 不仅用于设计阶段, 而且在工艺分析阶段, 也可见到很多应用实例。此外, 在 QC (质量管理) 方面, 也在研究利用 FMEA, 以提高产品质量, 扩大产品功能。

另一方面，FTA 着眼于部分与整体的可靠性在功能方面的联系，并且重视“与”及“或”逻辑关系的分析，它也是一种分析故障机理的重要方法。从思想方法上讲，它并不就是QC领域中过去使用的因果图的扩充，更适用于以推理的方式找出故障产生的原因。

总之，两者都是可靠性方法中便于使用并行之有效的办法，而且和威布尔分析法一样，都十分易于普及。当然，如果忽视根据实际试验或现场数据所作的统计性的，并且是实质性的故障分析，恐怕也只能是纸上谈兵。希望读者也能掌握本丛书其它各册所叙述的基本方法，以便获得综合的效果。

本书的内容如下：第一章 概论；第二章 系统可靠性分析基础（包括FMEA、FTA在内的可靠性分析方法概要，以及FMEA、FTA的基础知识）；第三章 FMEA、FTA的一般方法；第四章 FMEA的分析、使用方法和实例（为本书的核心内容，叙述了概念、方法和较多的实例）；第五章 FTA的实例（为本书的核心内容，叙述了概念、方法和应用实例）；第六章 系统可靠性分析的其它方法，补充了FMEA和FTA所未包含的部分，叙述了其它方法——ETA（事件树分析）、CCFA（共同原因故障分析）、ESA（事件序列分析）及CCA（原因—后果分析）等。

希望本书能为广大读者在使用FMEA、FTA时提供参考，并得到广泛的实际应用。

盐见 弘
1983年8月

缩 写 词 表

AQL	可接受质量水平
CA	致命度分析
CCA	原因—后果分析
CCFA	共同原因故障分析
CMFA	共同模式故障分析
DR	设计评审
ELD	事件逻辑图
ESA	事件序列分析
ETA	事件树分析
F/EMECA	故障/误操作模式、影响和致命度分析
FHA	故障危险分析
FM	故障模式
FMEA	故障模式和影响分析
FMECA	故障模式、影响和致命度分析
FT	故障树
FTA	故障树分析
MTBF	平均无故障工作时间
PA&A	预测、分配和评价
PDCA	计划、实施、检查和处理
PDPC	过程决策程序图
PHA	初步危险分析
PLP	产品责任预防
PM	预防维修
QA	质量保证

QC	质量管理
RPN	危险优先数
SEEA	软件错误和影响分析
SFP	单一故障点
SPF	单一故障点

目 录

译者序	III
《可靠性技术丛书》出版序言	V
前言	VII
缩写词表	IX
第一章 概 论	1
1.1 可靠性技术的定量及定性方法	1
1.2 发展历史	3
1.3 FMEA、FTA的应用范围	4
第二章 系统可靠性分析基础	6
2.1 故障机理	6
2.1.1 对象	6
2.1.2 功能	7
2.1.3 条件	9
2.1.4 时间	9
2.1.5 概率	10
2.2 FMEA与FTA的概念和使用方法	10
2.3 可靠性框图与FTA	15
2.3.1 串联、并联模型与AND、OR逻辑	15
2.3.2 可靠性框图	20
2.3.3 真值表	22
2.4 最小路集与最小割集	24
2.4.1 最小集合	24
2.4.2 共同原因故障	26
2.4.3 故障树与可靠性框图的简化, 求最小集	

合的方法	27
2.4.4 由最小路集、最小割集求可靠度、不可靠度的方法	29
2.5 布尔代数和故障树的简化	32
2.6 故障树的重要度	35
2.6.1 结构重要度	35
2.6.2 概率重要度	39
第三章 FMEA、FTA的一般方法	41
3.1 序言	41
3.2 故障模式和影响分析 (FMEA)	44
3.2.1 FMEA概述	44
3.2.2 FMEA的准备工作	46
3.2.3 FMEA的格式	48
3.2.4 FMEA小结	65
3.3 故障树分析 (FTA)	68
3.3.1 FTA概述	68
3.3.2 FTA的准备工作	70
3.3.3 熟悉分析对象	71
3.3.4 选定顶事件	72
3.3.5 FT的建立与简化	73
3.3.6 定性分析——求最小集合的方法	88
3.3.7 定量分析——概率计算与重要度	91
3.3.8 FTA小结	98
第四章 FMEA的分析、使用方法和应用实例	100
4.1 序言	100
4.1.1 FMEA的观点	100
4.1.2 分析层次、生产过程和FMEA的关系	100

4.2 FMEA的使用方法	102
4.2.1 FMEA的种类和使用意义	102
4.2.2 其它方法（在预防维修、设计检查、工艺 监督方面的使用）	102
4.2.3 应用FMEA的体系	108
4.2.4 FMEA实施结果的跟踪调查	108
4.3 FMEA的分析和评价	116
4.3.1 实施FMEA的准备工作	116
4.3.2 按照FMEA格式进行分析与评价	118
4.4 FMEA的实例及注意事项	133
4.4.1 应用于新产品设计至工艺设计阶段的 FMEA的实例	133
4.4.2 因故障模式未确认而失败的实例	147
4.4.3 在金属铸模设计上应用FMEA的 实例	149
4.4.4 在质量指标分析方面应用FMEA及设 计评审（设计审查，DR）的实例	152
4.4.5 应用FMEA的效果	160
4.4.6 实施FMEA应注意的问题	162
第五章 FTA应用实例	167
5.1 序言	167
5.2 FTA在可靠性设计与分析方面的应用	167
5.2.1 海洋探测系统的FTA	167
5.2.2 炼油厂供水设备的FTA	170
5.2.3 列车运行管理系统的FTA	174
5.2.4 邮件处理设施的FTA	175
5.3 FTA在安全方面的应用	180

5.3.1 医疗装置的FTA	180
5.3.2 工业机器人的FTA	183
5.3.3 汽车安全性分析的FTA	188
第六章 系统可靠性分析的各种方法.....	192
6.1 序言	192
6.2 共同原因故障分析 (CCFA)	194
6.3 时间变化因素	196
6.4 FMEA、FTA的应用	196
6.5 事件树分析 (ETA)	199
6.6 事件序列分析 (ESA)	201
6.7 原因—后果分析 (CCA)	203
6.8 运行性分析	204
6.9 结束语	205
参考文献.....	206
汉英名词对照.....	210
索引.....	214

第一章 概 论

1.1 可靠性技术的定量及定性方法

众所周知,在可靠性工程学、安全工程学以及产品责任预防 (PLP) 中,故障模式和影响分析 (FMEA) 与故障树分析 (FTA) 是一类有代表性的研究方法。从可靠性发展的历史看,很早就已开始研究这些方法,后来,主要在与安全有关的领域内受到重视,并且在与可靠性结合的过程中得到发展。

50年代是可靠性工程学巩固基础的年代,著名的美国电子设备可靠性顾问组 (AGREE) 报告是1952年至1957年间研究成果的总结,其中提出了可靠性工程学的全部基本观点。

在AGREE文献中,用串联模型表示系统或装置与其零部件 (组成部分) 的关系 (参见图2.4),明确地提出系统或装置的可靠度 $R(t)$ 可用其组成部分可靠度 R_i ($i = 1, \dots, n$) 之积表示:

$$R(t) \cong R_1(t) \times R_2(t) \times \dots \times R_n(t) \quad (1.1)$$

如用故障率 $\lambda(t)$ 表示系统与其组成部分的关系,显然,可得:

$$\lambda(t) = \lambda_1(t) + \lambda_2(t) + \dots + \lambda_n(t) \quad (1.2)$$

当然,这一关系式不是首先见于AGREE报告,例如,在第二次世界大战中,德国的卢泽 (R·Lüsser) 已将这一关系式作为古典方法的基本公式用于V2火箭的可靠度计算中,所得数值为0.75。

可以认为, 上述串联模型的概念提出后, 推动了关于装置或系统的MTBF (平均无故障工作时间) 和零部件故障率的数据积累工作, 同时也促进了定量地进行可靠性预测、分配和评价 (也称PA&A, 参见第六章)。这一工作是可靠性设计的基础, 它强调通过积累数据, 用统计方法定量地得到可靠度, 后来发展成为可靠性工程学的一个分支。上述由串联模型得到的故障率关系式(1.2), 给出了一种有代表性的基本关系。

但是, 美国在50年代后半期, 随着“民兵”导弹的研究, 对只是在数量上根据MTBF、 λ 求出可靠度, 并进行设计和管理的作法感到还不够充分。进而认识到, 尽管在数量上用统计方法定量地获得了系统可靠度, 但为了具体地改进系统, 还必须对系统在性质方面, 或者说对故障机理、定性及传统技术方面有全面的知识和深入的理解。

如果说得更极端一些, 可靠性工作的核心是将整体故障与部分故障联系起来, 分析其机理、性质, 并由此在数量上定量地掌握MTBF、 λ 值。概括起来就是:

可靠性的基 本研究	{	对故障机理、本质方面的认识, 对传
		统技术方面的、定性的研究工作;
		对故障从数量上进行统计性的、定
		量的研究工作。

而上述两方面(质和量)是互相关联的。

然而, 必须指出, 运用上述串联模型, 要想准确地从逻辑上找出整体故障和局部故障的关系是很困难的 (参见第二章)。式(1.1)仅仅是其结果的数量化表示而已。即对串联模型来说, 是以组成系统的任何一部分 (所谓OR 逻辑关系) 发生故障, 则导致系统故障, 这样一种机理为前提的 (即部分故