ISO9000新系列质量管理标准中,可信性管理及可信性要素标准的宣贯资料

可信性概述

何国伟 编著

R . M . S . T

北京工业大学出版社

内 容 提 要

可信性表示可用性及其影响因素：可靠性（R）、维修性（M）、保障性（S）、测试性（T）。这些因素已成为产品质量的决定性组成部分，并极大地影响产品质量中的安全性及经济性。新的 ISO9000 系列标准已发布了可信性管理及可信性要素两个标准。本书是宣贯这两个 ISO9000 系列标准的可信性入门参考书。ISO9000 系列已列入软件质量管理，本书亦扼要介绍了软件可信性。

可信性概述

何国伟　编著

*

北京工业大学出版社出版发行

各地新华书店经销

徐水宏远印刷厂印刷

*

1997 年 4 月第 1 版　1997 年 4 月第 1 次印刷

787×1092 毫米 32 开本　8.125 印张　181 千字

印数：1～5000 册

ISBN　7—5639—0593—6/N・1

定价：9.90 元

序

旧的质量观是以性能为中心的质量观。美国吸取了越南战争的教训，自60年代起，把旧质量观转变为以效能与全寿命费用（LCC）为核心的新质量观，并以总统命令颁布。美军以20多年时间实现了这个转变。海湾战争证明了这个转变的正确性。萨达姆的53万大军在100小时的地面战斗中全军覆没，而多国部队的死伤人数却是史无前例地少。武装部队如果不实行这个转变，就必然要重蹈萨达姆的覆辙。这个规律也适用于民品。民品如果不实行这个转变，在开放的竞争市场中也会全军覆没。

1994年新版的ISO9000积极地反映了这个转变。质量要满足明确的和隐含的需要，而需要包括：性能、合用性、可信性、安全性、环境、经济性与美学。可信性表示可用性及其影响因素：可靠性（R）、维修性（M）、保障性（S）[在维修性中还分出了测试性（T）]，因此可信性可以算是R.M.S.T.的一个集合名词。此外，它还极大地影响经济性及安全性。

ISO9000系列已经把可信性作为质量的一个重要内容，ISO与IEC联合发布了可信性管理及可信性要素的标准。但可信性的基本概念还不为多数领导干部，质量体系人员及设计、工艺技术人员所掌握。本书作为ISO9000系列中可信性管理及可信性要素两个标准的宣传贯彻资料，宣讲可信性的基本概念及方法。

“产品”本来包括软件，但软件的质量管理，特别是软件的可信性，是我国软件工业的薄弱环节。最近欧洲空间局

(ESA) 的阿丽亚娜V由于软件故障导致发射失败，损失以十亿美元计，这引起了各国及我国领导部门的重视。在我国，软件可信性已开始提到日程上来了。本书也扼要介绍了软件可信性的内容。

本书的读者对象是领导及领导机关干部，质量体系人员，设计、工艺技术人员。本书可作为根本转变质量观念、学习及掌握可信性的入门参考书，也可作为大学2、3个学分的可信性教材。

本书素材主要取自可信性(R. M. S. T.)的ISO国际标准，引用了国军标、美军标及IEC标准的很多材料，在此不一一列举。

国防科工委可靠性工程技术中心
专家组组长 何国伟 1996年11月

本书符号表

A，B，…	事件
$\overline{A}$	事件 A 的余事件，事件 A 不发生
$\mathrm{E}(X)$	随机变量 X 的期望(均值)，即 μ_X
$f(x)$	随机变量 X 的概率密度函数
$F(x)$	随机变量 X 的分布函数
$N(\mu,\sigma)$	均值为 μ、方差为 σ^2 的正态分布
$N(0,1)$	标准正态分布
n	样本量
$P(A)$	事件 A 发生的概率
s^2	样本方差
$\mathrm{V}(X)$	随机变量 X 的方差，即 σ_X^2
T，X，Y，…	随机变量
$\overline{X}$	样本均值
u_p	标准正态分布的 p 分位数，$\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u_p} e^{-\frac{t^2}{2}}dt = p$
α	显著水平，生产方风险
β	使用方风险
γ	置信水平
μ_X	随机变量 X 的均值
σ_{X^2}	随机变量 X 的方差
$\Phi(u)$	标准正态分布的分布函数，$\Phi(u) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-\frac{t^2}{2}}dt$
ν	自由度
$\chi^2(\nu)$	自由度为 ν 的 χ^2 分布
$\chi_\alpha^2(\nu)$	自由度为 ν 的 χ^2 分布的 α 分位点，$P(\chi^2(\nu)<\chi_\alpha^2(\nu))=\alpha$

λ	故障率
$\lambda(t)$	故障率函数
η	信号噪音比
θ	平均故障间隔时间
$\in$	属于
$\overline{\in}$	不属于
$\wedge$	估计值符号，如 θ 的估计值为 $\hat{\theta}$

本书缩略语表

A	可用性 availability，年金
AQL	可接收质量水平 acceptable quality level
BIT	机内测试 built-in test
CDR	关键设计评审 critical design review
D	可信性 dependability
E	效能 effectiveness
ESS	环境应力筛选 environmental stress screening
FAR	虚警率 false alarm rate
FDR	故障检测率 fault detection rate
FIR	故障隔离率 fault isolation rate
FRACAS	故障报告、分析及纠正措施系统 failure reporting，analysis and corrective action system
FRSP	失效率抽样方案 failure rate sampling plan
IEC	国际电工委员会
ISO	国际标准组织
LCC	寿命周期费用 life cycle cost
LRV	现场可更换单元 line replaceable unit
LTPD	批容许不合格品率（即极限不合格品率） lot tolerance percent defective
M	维修性 maintainability
MDT	平均延误时间 mean delay time
MMMH	平均维修工时 mean maintenance man hours
MTBCF	致命性故障任务时间 mission time between critical failure
MTBD	平均需求间隔时间 mean time between demands

MTBF	平均故障间隔时间　mean time between failures
MTBM	平均维修间隔时间　mean time between maintenance
MTBR	平均拆卸间隔时间　mean time between removals
MTTF	平均故障前时间　mean time to failure
MTTRS	平均系统恢复时间　mean time to restore system
PDR	初步设计评审　preliminary design review
PRR	生产准备评审　production readiness review
PRST	概率比序贯试验　probabilistic ratio sequential test
QDDM	质量及可信性数据管理　quality and dependability data management
RGT	可靠性增长试验　reliability growth rest
R.M.S.T.	可靠性、维修性、保障性、测试性　reliability，maintainability，supportability，testability
S	保障性　supportability
SEI	软件工程研究所（美军）　software engineering institute
SRGT	软件可靠性增长试验　software reliability growth test
SRR	系统要求评审　system requirements review
SRU	车间可更换单元　shop replaceable unit
T	测试性　testability
TAAF	试验—分析—改进　test-analyse and fix test
TRR	试验准备评审　test readiness review
VRP	减小变差计划　variability reduction program

目　录

第一章　可信性的基本概念

§1.1　可用性(A)、可靠性(R)、维修性(M)、保障性(S)、测试性(T)的概念

根据GB/T6583—ISO8402的定义，“产品的质量(quality)反映产品满足明确和隐含需要的能力的特性总和。”在过去的有些资料中，把质量定义成“适用性”、“符合目的性”、“使用方满意”或“符合要求”，那些只反映了质量的某些方面，都不够全面。

上述的“需要”，按定义，可包括：性能，合用性，可信性（可用性、可靠性、维修性、保障性），安全性，环境，经济性和美学。

这里的“性能”是需要的一个方面，也就是旧质量观中心考虑的问题。如一架飞机飞多高，速度为多少，载几吨货……是考虑飞机质量的旧质量观的主要内容，是以性能为中心的。

“产品在给定的内在条件下，满足给定的定量特性要求的自身特性叫产品的‘固有能力’(capability)”，简写为C，反映产品的性能。

“可信性（dependability）是一个集合性术语，它用来表示可用性及其影响因素：可靠性、维修性、保障性”，“它仅用于非定量条款中的一般性描述。”这个概念是随着科学技术的发展，首先是军事技术的发展，而发展起来的。

“可靠性”，即“产品在规定条件下和规定的时间内完成规定功能的能力”。

“产品或产品的一部分不能或将不能完成规定功能的事件或状态叫出故障。”朝鲜战争期间，美军的飞机有60%因故障需维修而不能使用，电子设备有50%在存放中就出故障……促使美军积极抓可靠性。这样就产生及发展成“可靠性工程（reliability engineering）”，简称R。通俗地说，产品故障出得少就是可靠性高，在规定的条件下和规定的时间内，产品的故障总数与寿命单位总数之比叫“故障率”（failure rate），通常以λ表示，这里的规定时间一般取单位时间，例如小时、天、月……如正在服役的100架飞机，一个月内出了28次故障，则每架飞机的故障率为0.28次/月。产品的可靠性高就是故障率低，故障率λ是产品可靠性的一种基本参数。故障率的倒数叫平均故障间隔时间（mean time between failures），简写为MTBF。

一般说来，产品到一定工作时间或一定时间后，故障率会愈来愈高，从而不值得再予修复。“产品从交付使用到出现不能接受的故障率（或出现不值得修复的故障）时的寿命单位数叫产品的使用寿命。”例如一台洗衣机的定时器可使用5000次。使用寿命是另一个重要的可靠性参数。

产品出故障就要维修(有些产品是经济上不值得修复的，则叫“不修复产品”)。产品在规定条件下和规定的时间内，按规定的程序和方法进行维修时，保持或恢复到规定状态的能力叫“维修性”（maintainability），简写为M。

维修级别（maintenance level）是按产品维修时所处场所划分的等级。一般设置三个基本修理级。

（1）基层级——在产品原位进行修理，通常进行换件或

维修（例如更换一个插件，更换一个模块等）或简单的、维修时间短的活动（如焊上一个脱开的焊点等等）。

（2）中继级——在中间地带的维修车间进行修理，该车间拥有修理比（1）更低层次硬件的能力。

（3）基地级——是有高度专业化的修理设施，能修理产品各层次需要修理的硬件，基地级有时是产品的原生产厂。

[注] 美空军提出了两级维修，即

（1）原位维修——在完整的产品上完成维修活动。

（2）离位维修——在拆卸下来的待修部件上完成维修。

在规定的条件下和规定的时间内，产品在某一规定的维修级别上，修复性维修的总时间与在该级别上被修复产品的故障总数之比叫“平均修复时间”（mean time to repair），简写为 MTTR。这是产品维修性的一种基本参数。

例如，产品累计 $n=100$ 次故障的总维修时间 MT 为 10 000 h，则 $\mathrm{MTTR}=\mathrm{MT}/n=\frac{10\ 000}{100}$ h/次 $=100$ h/次，显然，MTTR 短说明维修性好。这里的维修时间指的是直接维修时间。由于维修性愈来愈重要，因此，维修性工程（maintainability engineering）从可靠性工程中分立出来，成为独立学科。

产品能完成预定功能的状态叫“能工作”（operable）；否则叫不能工作。产品能工作但不需要它工作的状态叫“不工作”（not operating，dormanant）。注意：“不工作”不要与不能工作混淆。产品处于能工作的时间记为 UP（up time），产品处于不能工作的时间记为 NT（down time）。NT 是由于出了故障需要维修（也包括必要的检修）造成的，其中包括直接维修时间，也包括由于保障资源补给或管理原因例如等待维修人员、等维修设备、等备件等未能及时对产品进行维修

所延误的时间，这叫“延误时间”(delay time)。产品的设计特性和计划的保障资源能满足使用要求的能力叫产品的保障性”(supportability)，简写为S。

在规定的条件下和规定的时间内，产品在某一规定的维修级别上，维修延误的总时间与延误次数之比叫“平均延误时间”(mean delay time)，简写为MDT。它是保障性的一种基本参数。

如果累计$n=100$次维修的累计延误时间DT为3000 h，则$MDT=DT/n=\frac{3000}{100}$ h/次$=30$ h/次，显然MDT愈短愈好。由于保障性在维修性工程中的地位愈来愈重要，因此(维修)“保障性工程”(supportability engineering,)又从维修性工程中独立出来，成为独立学科。

在维修过程中,极为重要的环节是确定产品是否出故障，及哪个部位（例如哪块电路板）出故障。“产品能及时并准确地确定其状态（可工作、不可工作或性能下降)，并隔离其内部的一种设计特性叫测试性（testability)”，简写为T。测试性工程（testability engineering)，亦有从维修性工程中分立出来的趋势。

这样，从50年代朝鲜战争结束起到现在，可靠性工程已扩展出维修性工程、故障性工程、测试性工程，简称R. M. S. T.,已成为“广义可靠性”的概念了。

产品在任一随机时刻需要和开始执行任务时，处于可工作或可使用状态的程度叫产品的“可用性”(availability)，简写为A。设产品在较长时间内，累计工作时间为UT，累计不能工作时间为NT，则定义$A_0=UT/(UT+NT)$。NT包括累计直接维修时间MT、累计延误时间DT,则$A_0=UT/(UT$

+MT+DT)，分子、分母都除以此段时间内的出故障及维修次数 n，即得

$$A_0 = MTBF/(MTBF + MTTR + MDT)$$

A_0 叫“使用可用性”(operational availability)，它与管理水平、保障设计所决定的 MDT 有很大关系。在理想情况下，MDT=0，此时

$$A_i = MTBF/(MTBF + MTTR)$$

A_i 叫“固有可用性”(inherent availability)。显然，可用性取决于可靠性参数 MTBF、维修性参数 MTTR 及维修保障性参数 MDT。

[注]产品出现伤害或损坏的风险限制在可接受水平之内的特性叫产品的“安全性”(safety)，简写为 S，也即产品不发生恶性事故的能力。不安全首先是出故障，因此，安全性与可靠性密切相关。但安全性还有一个后果防护问题，所以独立出去成为安全性工程 (safety engineering)，广义的可靠性有时也包括安全性，即 R. M. S. T. (S)(本书不介绍安全性的内容)。

§1.2 质量观念的根本转变，效能、LCC 及费效比

可靠性定义中的规定条件包括“环境条件”。产品在完成规定任务这段时间内所经历的事件和环境按时间次序描述叫“任务剖面”。产品在任务开始时可用的条件下，在规定的任务剖面中，能完成规定功能的能力叫产品的“(狭义)可信性”(dependability)，简写为 D。(其所以叫(狭义)可信性是有别于 ISO 中的(广义)可信性。)产品在规定的条件下满足给定定量特征和服务要求的能力叫产品的“效能”

(effectiveness)，简写为E。“效能是产品可用性A、可信性D及固有能力C的综合反应”。一种简单的效能定量表达式为E=ADC。产品的固有能力（capability）c，一般就是产品的性能。

例如，要从英国的空军基地起飞一批战斗轰炸机袭击非洲某国家，在下达袭击指令时，基地的20架飞机中，能起飞执行任务的只有18架，于是可用性A=18/20=90%。飞机飞往非洲的过程中，在地中海进行空中加油，有2架飞机出现故障降落在意大利基地，因此18架飞机中只有16架能到达目的地，于是（狭义）可信性D=16/18=88.89%。到达目的地的飞机发射的导弹，有80%击中目标，则固有能力C=80%，于是这次空袭的效能

$$E = ADC = 90\% \times 88.89\% \times 80\% = 64\%$$

显然，军方最终关心的是效能E。飞机性能再好，飞得再高、再快，如果飞不起来，飞不到目的地，那是没有多少用的。

产品的费用不仅仅是采购费用。产品从提出研制任务起到退出服务为止的整个寿命叫产品的“寿命周期”。在产品的寿命周期内，在产品设计、研究和研制、投资、使用、维修及产品保障中发生的或可能发生的一切直接的、间接的、派生的或非派生的与其他有关费用的总和叫“寿命周期费用”(life cycle cost)，简写为LCC。一辆汽车不能看买来的价格便宜，如果耗油量大，常出故障，其寿命周期费用可能相当高。所谓“价廉物美”的“价廉”指的是LCC少，“物美”指的是效能高。LCC是寿命周期内历年支出的总和。在计算总和时，必需考虑利率i，今年的P元，相当于n年后的将来价值$F=P(1+i)^n$，按美军、西欧、日本及我国经委规定，i以10%计算（通货膨胀率另加）。