可信性管理

GB/T 19000.4
ISO 9000-4

实施指南

咸奎桐 编

中国标准出版社

内 容 提 要

本书作为 GB/T 19000.4—ISO 9000-4《质量管理和质量保证标准 第4部分：可信性大纲管理指南》国家标准的实施教材，对该标准及其相关内容作了说明，但并不局限在对标准的解释上，而是比较系统地阐述了可信性管理体系的构成及其重要内容；对可信性管理、可信性分析方法、软件可信性管理、寿命周期成本等可信性领域的重要课题及标准化状况作了程度不同的说明，在对可信性领域给出总体描述的基础上，提供了应用示例。

本书可供质量管理、标准化工作者，以及与可信性相关的人员和高等院校有关专业的师生使用和参考；对欲采用 GB/T 19000 系列标准的企业，尤其是对已经通过或准备通过质量认证的企业的领导和管理人员、工程技术人员更具有指导作用。

可信性管理

GB/T 19000.4
ISO 9000-4 实施指南

咸奎桐 编著

责任编辑 吴碧英

*

中国标准出版社出版

北京复兴门外三里河北街16号

邮政编码：100045

电 话：68522112

中国标准出版社秦皇岛印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

开本 850×1168 1/32 印张 5⅜ 字数 152 千字

1997年12月第一版 1997年12月第一次印刷

*

ISBN 7-5066-1454-5/Z·254

印数 1—2 500 定价 15.00 元

*

标 目 320—01

前　言

在社会生活中，人们对产品关注的焦点问题是：

性能：

产品的性能（包括可信性）能否满足用户的期望和需要；

费用：

费用不仅仅指开发和生产产品的费用，还包括使用、维护和最终处理的费用，亦即是产品寿命周期费用；

更新周期：

产品何时投放市场，更新的时间多长合适？

这些因素在产品寿命周期的各个阶段中受到控制和协调，用户对产品是否满意，取决于产品的信誉、生产者对这些因素控制的程度。

术语可信性包括可靠性、维修性、可用性和维修保障。其中可靠性、维修性和可用性是产品自身的特性，并经常作为关键的产品要求被予以规定，而维护保障则是指对所需维修的项目具有提供所需资源的能力。可信性是产品最重要的性能特性之一，其表现在对产品满足用户要求的全部能力中，可信性特性起到主要作用，有时这种作用优于其它质量特性起着主导作用。

产品的可信性对成本的影响主要是指其使用和维护费用，但通过可接收的寿命周期成本实现对总费用的影响。

通常情况下，用户购买产品考虑的主要因素是其初始价格，但这只是买来了产品的所有权，更重要的是还应考虑它的使用和维护费用，最初的购买费用只是产品总费用的一部分，这一点常常被人们忽略。我们可以通过简单的计算来说明，假如产品的寿命周期总费用一定，如果产品设计得可靠和便于维护，即更可信，那么使用和维护的费用可以大大降低。通常产品在改进和研制方面要追加费用，而这部分费用的追加是通过牺牲使用和维护费用来实现的。因此，我们的着眼点应放在综合和

权衡产品的设计、开发、使用和维护的费用，这也成为可信性领域中关于寿命周期费用的理论依据，也可以说是现代工业经济理论的一种思路。

关于产品的更新换代周期，也就是产品寿命问题，传统的观念是产品的寿命越长越好，现在人们的观念已经改变，产品以怎样合适的周期进行更新成为人们日益关注的一个问题，也成为可信性研究的一个重要课题。

以上论及的产品的性能、费用和更新周期都与产品的可信性密切相关，也就是说产品可信性对上述因素有着重大的影响，因此产品的可信性问题越来越受到了人们的重视。

随着质量工作的深入，人们越来越深切地感到可信性工作的重要性，因此国家技术监督局专门发布了《关于加强产品可靠性工作的若干意见》的通知，明确指出"可靠性是产品的重要质量特性，它既是用户、消费者最关心的问题，也成为一些出口机电产品和重大装备在国内和国际招标中竞争的焦点。在改革开放的新形势下，如何适应社会主义市场经济发展的需要，大幅度地提高我国产品质量与可靠性，促进企业参与国内外市场的竞争，是工业部门要抓紧抓好的一项重要工作，……"。该通知从七个方面论述了如何加强产品可靠性工作。这是我国政府部门在充分认识到可靠性工作重要性的基础上，准备加大可靠性管理的力度，以提高我国产品的整体质量与可靠性水平，增强国际市场的竞争力。

在日益强调产品质量的今天，推广应用 ISO 9000 族质量管理和质量保证标准已经成为世界潮流，在世界范围内形成了一种"ISO 9000 现象"。可信性作为质量的重要组成部分，在国际上也颁布了一套可信性管理系列标准，称为 IEC 300 系列，并且 IEC 300 系列已被纳入到 ISO 9000 系列之中，为在应用 ISO 9000 族标准的同时开展可信性工作奠定了基础。作为 IEC 300 系列标准的牵头标准之一的 IEC 300-1《可信性大纲管理》，已被 ISO 以双编号 ISO 9000-4/IEC 300-1 的形式发布，该标准也于 1996 年已被等同采用为国家标准，编号为 GB/T 19000.4。本书作为这一标准宣贯教材的同时，也收录了 IEC 300

系列的一些相关标准。

本书共分七章，重点是第二、三、四章。第二章描述了可信性管理标准体系及计算机辅助可信性管理系统模型，第三章论述了可信性大纲及其要素和工作项目，第四章介绍可信性分析方法的特点和应用。

本书的素材主要来源于作者的两份科研报告："可信性管理的研究"和"可信性分析方法应用研究"。这两份科研报告在国家技术监督局组织的专家评审中获得了一致的好评，在评审结论中要求以此为基础完成宣贯教材的编写，为宣贯《可信性大纲管理指南》提供教材。

本书的第六章由中国标准化与信息分类编码所金江同志提供素材，在此表示衷心地感谢。

由于作者水平有限，书中难免有错误或不妥之处，敬请广大读者批评指正。

编　者

1997 年 3 月

目　　录

第一章 概 述

第一节 可信性工程概述

一、可信性的发展历程

可靠性作为一门技术学科的提出，始于二战之后。起因是二战期间，美军运往远东的设备、装置在运输和保管过程中，有半数以上因不能使用而报废。因此，1943 年美国组成了由军界、学术界、生产厂组成的联合小组进行可靠性研究，从而奠定了可靠性工程学基础。1957 年美国国防部电子元器件可靠性咨询小组(AGREE)的报告，给可靠性(Reliability)下了定义，并确定了可靠性工程研究的方向。

到了 60 年代，随着电子技术的飞速发展，可靠性工程的理论和应用也得到了相应的发展，并形成了自己的体系、方法和技术，统计方法在可靠性工程中得到广泛的应用。美国在此期间颁布了一系列军用标准，并保证了阿波罗登月计划的实现。到了 70～80 年代，可靠性技术得到了进一步发展，出现了许多新技术，如 FMEA(故障模式、影响及效果分析)、FTA(故障树分析)、马尔可夫技术和 Monte Carol 模拟等。另一方面，在应用领域，不仅在军用和航天设备上应用可靠性技术，在大量民用产品上，也提出了可靠性要求、进行可靠性试验、给出可靠性指标。因此，可靠性已经和人们的生活息息相关。

1990 年国际电工委员会第 56 委员会(IEC/TC 56)在它的第 315 号文件中借用了 IEC 50(IEV 191)的术语“可信性”(dependability)，代替了传统的“可靠性”，从此可信性这一术语在国际上被广泛使用，并成为“广义可靠性”的代名词。此后 IEC/TC 56 也由原来的“可靠性、维修性技术委员会”改为“可信性技术委员会”。

在 IEC 50(IEV 191)中对可信性的定义是：“描述可用性及其影响因素：可靠性、维修性和维修保障性能的一个集合术语。

其内容可用图 1-1 表示。

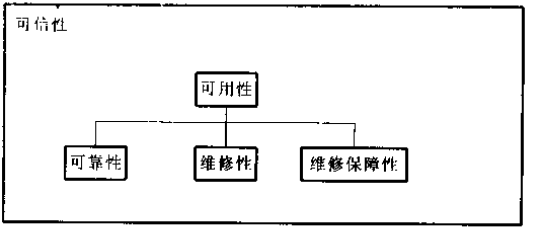


图 1-1　可信性与可用性及其影响因素关系

IEC/TC 56 用可信性作为它的名称之后，作了许多卓有成效的工作，其中最突出的一项工作就是修订 IEC 300 号标准，并以此为基础推出了一个“工具箱”式的可信性管理标准结构，目前，基本形成了 IEC 300系列的可信性管理标准，进而形成了一套可信性管理标准体系，因此，为可信性管理工作的广泛深入地开展奠定了基础。

二、可靠性工程的发展

可靠性技术一开始就是与工程实践密切结合起来的，也可以说是一门实践性很强的技术，因而可靠性工程也应运而生了。

在可靠性工程中，以可靠性设计、试验、分析、管理四方面内容为主。而在设计、试验和分析活动中，可靠性管理贯穿始终。可靠性管理水平决定于可靠性分析、试验、设计水平。

可靠性设计是保证产品可靠性的第一步，因而可靠性设计技术的应用和发展状况对保证和提高产品的可靠性至关重要。由于一些高、精、尖产品有较高的可靠性要求，而传统的可靠性设计无法满足要求，因而一些新的针对不同的环境和对象的可靠性设计技术应运而生，如：“热设计”，是为了防止由于设备在工作过程中升温太高而出现的不可靠；“容余技术和容错设计”不仅在硬件设计中得到应用，而且已经被应用到软件上；“电磁兼容性(EMC)设计”则是为了保证系统在电磁环境中，性能不降低，仍能正常、有效地工作，即抗电磁干扰。

可靠性建模是可靠性设计的主要内容之一，基于不同的分析方法可以建立不同的模型。建模首先是物理模型，然后才是数学模型。所采

用的可靠性分析方法是建立物理模型的基础。因而可靠性分析是可靠性设计的关键。可靠性分析方法很多，比较成熟的分析方法有FMECA（故障模式、效应和危害度分析）、FTA（故障树分析）、RBD（可靠性框图分析）、Markov（马尔可夫分析）、Parts Count 元件计数分析）、C/C（因果分析）、Event Simulation（事件模拟分析）、System redution（系统衰减分析）、Event tree（事件树分析）、Truth table（真值表）等。为了便于这些分析方法的应用，需要针对每一种方法制定出一项标准。在上述的分析方法中，前三种方法 IEC 已经制定了标准，其编号分别为 IEC 812、IEC 1025、IEC 1078，这些方法如何选择，在 IEC 300-3-1 中为我们提供了指导。

可靠性预计和分配也是可靠性设计的另一主要内容。可靠性预计和分配在缺乏数据的情况下是困难的，而数据的获得离不开可靠性试验。因而获得必要的可靠性数据成了可靠性试验的主要目的。有关可靠性试验的方法和类型很多，在许多的著作和标准中都有论述，这里不再赘述。可靠性设计的管理主要通过设计评审来体现。IEC 颁布了设计评审的国际标准，其编号为 IEC 1160。

三、可信性与质量的关系

可信性包括了传统的可靠性及维修保障等内容。历史上，可靠性与质量的关系问题一直争论较大。一种观点认为，质量包括可靠性，可靠性是深化了的质量；另一种观点则认为，两者在管理对象上侧重点不同。质量管理是随着大批量生产发展起来的，着重于生产质量；而可靠性技术是随着复杂系统（电子产品）和大系统（首先是航天系统）发展起来的，着重于设计、试制质量。这些观点各反映了问题的一个侧面，但对它们的本质并未作说明。下面试从两者的定义进一步说明其区别。

ISO 8402 中给质量下的定义是："反映实体满足明确或隐含需要的能力的特性总和"。

这个定义还给出了四个注解，其中注 3 是："一般根据特定的准则将需要转化为特性。需要可包括性能、合用性、可信性（可用性、可靠性、维修性）、安全性、环境、经济性和美学。"

IEC 50（IEV 191）给可信性下的定义为：描述可用性和它的影响因

素：可靠性、维修性及维修保障等性能的一个集合性术语。

从上面的定义中可以看出，可信性所包含的一些要素（如：可用性、可靠性、维修性）用于定义产品的需要，可信性是产品质量特性之一。而质量则用以表示产品满足的那些需要，而不是特性本身，因此两者并不是互相包容的关系。但质量与可信性拥有一些共同的特性，两者互相补充。

因此，两者的研究领域都包括了管理和保证、方法、技术和工具等内容。基于此，可信性管理已与质量管理结合起来，可信性管理系列标准（IEC 300 系列）已同质量管理和质量保证系列标准（ISO 9000 系列）结合起来，两者共同促进产品整体质量与可信性水平的提高。

图 1-2 描述了质量范畴中的可信性概念。从中可以看出可信性与质量是不可分割的一个整体。

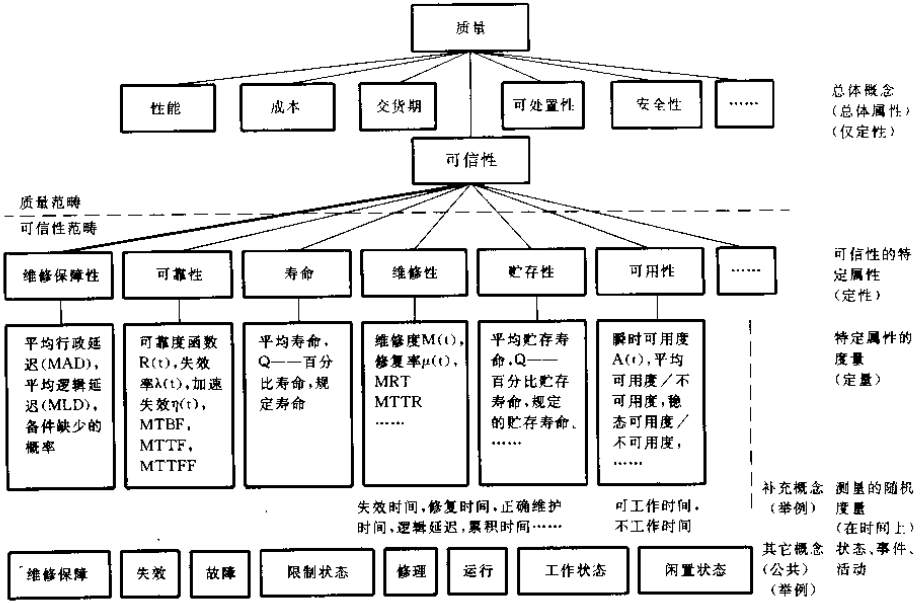


图 1-2　在质量范畴中的可信性概念

第二节　基本概念

在可信性领域内涉及的概念较多，有关的国家标准有 GB 3187—91《可靠性、维修性术语及定义》、GB 4888—85《故障树名词术语和符号》以及 GB/T 6583—ISO 8402《质量管理和质量保证　术语》。这些标准对可信性领域的术语给出了明确的定义，本节就其中常用的、重要的术语作出说明。

一、可信性　Dependability

1. 定义

可信性这一术语来自 IEC 50(191)《国际电工术语(IEV)——第 191 章：可信性和服务质量》，在国家标准 GB/T 6583—ISO 8402 中对其作出了如下定义：

"描述可用性及其影响因素：可靠性、维修性和维修保障等性能的一个集合术语。

注 1. 可信性通常仅用于非定量描述的场合。

2. 可信性是质量中与时间有关的一个方面。

3. 以上所给出的可信性的定义和注 1 均出自 IEC 50(191)，在 IEC 50(191)中也包括了有关的术语和定义。"

2. 说明

从可信性的定义中可以看出，这一术语是作为一个集合名词出现的，它包括了可靠性、维修性、可用性和维修保障性等广义可靠性范畴(可靠性、维修性和可用性)和维修保障性。既然是一个集合名词，那么它本身是很难量化的，因此它在非量化描述的场合使用，当需要量化描述时，则应当使用可靠性、维修性、可用性和维修保障性及其特征量。可信性这一术语在 1990 年由 IEC 给出后被广泛使用，首先国际上 IEC/TC 56 在 1990 年将原名"可靠性和维修性(Reliability and Maintainability)技术委员会，"改为"可信性(Dependability)技术委员会"，其后 IEC/TC56 对其制定的可靠性领域的标准进行了全面的改革，引入了体系化的概念，提出一个可信性管理标准框架，形成了三个层次的可信

性管理标准结构，目前这一体系已成为 IEC TC 56 制修订标准计划的依据。并且第一层标准已经颁布。随着这一体系的改善必将对可信性标准化工作产生积极的促进作用。

二、可靠性 Reliability

1. 定义

GB 3187—1994《可靠性、维修性术语及定义》中对"可靠性"一词作出广义和狭义的两种解释。广义可靠性是指产品在其整个寿命周期内完成规定功能的能力。它包括狭义可靠性和维修性；狭义可靠性则指产品在某个规定时间内发生失效的难易程度。本书中出现的可靠性是指狭义的可靠性，在国标中的定义如下：

"产品在规定条件下和规定的时间内，完成规定功能的能力"

2. 说明

说到可靠性一定离不开产品，这里所说的产品包括元器件、设备、系统及软件等。产品的可靠性是产品质量的重要特性之一，产品的可靠性的形成与产品的整个寿命周期有关。著名的科学家钱学森同志曾说过"产品的可靠性是设计出来的、生产出来的、管理出来的。"可见可靠性与产品的设计、生产和使用关系密切，设备运行时的可靠性称为工作可靠性 R_O(Operational Reliability)，产品在生产过程中已经确立的可靠性称为固有可靠性 R_I(Inherent Reliabity)产品在使用过程中的可靠性称为使用可靠性 R_U (Use Reliability)R_I 和 R_U 是从产品的应用角度出发，R_I 是产品在企业的规划阶段就已确定的指标，它和材料、零部件的选择、设计、制造、直到产品完成的每个阶段都有密切关系。R_I 是产品的内在可靠性，是产品予以保证的、并进行检测的可靠性。R_U 是指企业生产出来的具有可靠性的产品在转给用户的过程中，要经过包装、运输和保管。同时在使用中要受到环境、操作状况、维修等人为因素的影响。此外从设计的角度出发，把可靠性分为基本可靠性和任务可靠性。基本可靠性是指产品在规定条件下，无故障的持续时间或概率。它包括对维修和供应的要求，用于度量产品无需保障的时间。任务可靠性是用于描述产品完成任务的能力。它仅考虑造成任务失败的故障影响。

3. 可靠性特征量

为了定量地描述产品的可靠性，需要引入可靠性特征量，常用的可靠性特征量有可靠度(R)、平均失效间隔时间(MTBF)和失效率。

(1) 可靠度(R)

可靠度是可靠性的最直接的量化指标，它定义为，产品在规定的条件下，规定的时间内，完成规定功能的概率。通俗地说，产品的可靠度表示在规定的时间内及规定条件下正常工作的产品占产品总数的百分比。

产品不能正常工作，通常称为失效或故障(可修理)。产品的可靠度是指产品能正常工作的概率，因此，可靠度遵循一定的概率分布。根据特定产品的失效规律的不同，其可靠度的概率分布亦会不同，经常出现的可靠度的概率分布有：指数分布、正态分布、威布尔分布、伽玛分布等。

① 指数分布是指产品的失效在时间上是随机的，其可靠度函数可用下式表示：

$$R(t)=e^{-\lambda t}$$

其中，λ 为失效率，服从指数分布的产品的失效率假设是恒定的。

② 正态分布

在实际工作中，许多产品的失效是呈正态分布的，当正态分布作为产品的寿命分布时，其可靠度函数可用下式表示：

$$R(t)=\Phi\left(\frac{t-u}{\sigma}\right)$$

标准正态分布的分布函数值 $\Phi(x)$ 可查 GB 4086.1《统计分布数值表　正态分布》。

③ 威布尔分布是一种三参数模型，它概括了许多特殊的分布，如指数分布、正态分布等，其可靠度函数可表示为：

$$R(t)=e^{-\left(\frac{t-r}{\eta}\right)^{\beta}} \qquad (t\geqslant r)$$

威布尔分布已成为可靠性中最广泛使用的分布族，很多产品的失效分布服从威布尔分布，因此有人绘制了威布尔概率纸以利于其应用。

(2) 平均失效间隔时间(MTBF)

平均失效间隔时间又称为平均无故障工作时间，它定义为："在规

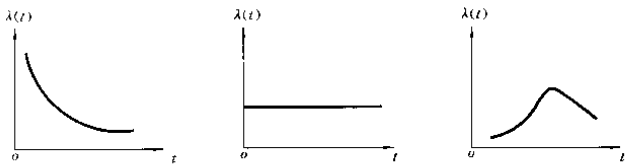
定条件下和规定时间内，产品的寿命单位总数除以在该时间间隔内失效总数之商。"在可修复的设备或系统中，MTBF 可被解释为相邻故障间隔的系统持续工作时间，MTBF 对于不可修复系统来说，又称为平均寿命。

MTBF 作为可靠性的重要指标，主要用于描述产品的基本可靠性。目前 MTBF 是用于衡量产品可靠性时使用最多的一项指标。平常所说的产品（尤其是电子元器件）寿命的大小，主要是指这项指标。提高产品的 MTBF 是产品设计、制造和使用追求的目标。

(3) 失效率(λ)

失效率是可靠性工程应用广泛的特征量，在 GB 3187—1994 中的定义为："工作到某时刻尚未失效的产品，在该时刻后单位时间内发生失效的概率"。在产品的寿命服从指数分布的情况下，产品的失效率假设为恒定的，此时它与 MTBF 成倒数关系，即 $\lambda=1/\text{MTBF}$。

通常产品的失效可分为早期失效、偶然失效和耗损失效三种形式，图 1-3(a)(b)(c)分别描述了这三种类型的失效率与时间的关系。



(a)　　(b)　　(c)

图 1-3　失效率与时间的关系

对于复杂产品上述的三种类型的失效都可能发生，因此，常用浴盆曲线来描述失效率与时间的关系

三、维修性　Maintainability

1. 定义

GB 3187—1994 的定义：

"在规定条件下，按规定的程序和手段实施维修时，产品在规定的使用条件下保持或恢复能执行规定功能状态的能力。"

2. 说明

维修性和可靠性是产品的两个重要特性，两者都是影响产品可用性的重要因素，也是可信性的重要内容。维修性是一种设计和安装特性，它同可靠性一样是产品的一种固有特性。这种固有特性是由产品设计赋予的。如果要求维修简便、迅速和经济，就必须拆装容易、换件迅速，不需要专用工具。因此就要求在设计时，合理地设计零部件外形、尺寸及其配置与连接，满足互换性要求等。

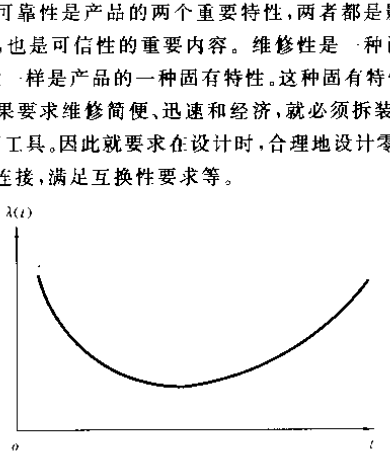


图 1-4 浴盆曲线

维修性与维修是两个不同的概念，维修性是一种设计要求，它是以总停机为基础，其中包括有效的修理时间、后勤时间和行政时间，这些要求是可以规定、测量和验证的；而维修则是对设计结果的具体实施，它仅限于有效的修理时间。维修又分为预防性维修和修复性维修。对于某个具体的产品而言，其设计完成后，维修性水平就确定了，通过维修活动只能保持其维修性水平，而不能提高其水平。

在描述维修性时，常会出现下列概念：

——可达性：是指维修产品时，能否迅速方便地达到维修部位的特性。通俗地说就是维修部件能否"看得见、摸得着"。很显然，可达性好的产品，维修就迅速、简便，而且差错、事故也会减少，所需的费用也会减少。

——互换性：有故障的或不能正常工作的部件，能否更换，或是否能方便地用同样的部件予以替换而无需校准。

——可测性：能否检测出系统的故障，并把有故障的产品隔离、存放到能够进行维修的地方。

复杂性：系统中有多少子系统、采用了多少零部件，这些零部件是标准件还是专用件。

这些概念对于掌握维修性的概念，开展维修性设计是必不可少的。

3. 维修性特征量

描述维修性的主要特征量有平均修复时间(MTTR)、最大修复时间和维修率等。

(1) 平均修复时间(MTTR)

MTTR 是在规定时间内，修复性维修所造成的累积不工作时间除以同一期间内所完成的修复性维修活动总数之商。它是排除一次故障所需修复时间的平均值。MTTR 仅考虑有效的修复性维修时间，用于其它方面消耗的时间则没有考虑。

(2) 最大修复时间

最大修复时间是完成全部规定的修复性活动的 90%或 95%所消耗的最大修复性维修的系统不工作时间。只有在系统有允许不工作时间时，最大修复时间的要求才是有用的。最大修复时间是按所有修复性维修活动的 95%规定的，因此超过最大修复时间的维修活动，不能多于总维修时间的 5%。

(3) 维修率(MR)

MR 是在给定时间内累积维修次数除以在同样时间内为完成维修所消耗的累积工作小时数所得的结果。维修率可用来表示每一维修级别或所有维修级别的情况，修复性维修和预防性维修均包括在内。维修率是涉及系统相对维修负担的一种度量，它提供了一种对比各种系统的方法。

四、可用性 Availability

1. 定义

可用性这一术语在 GB 3187－82 中称为有效性，在这一标准的修