系统可靠性的数学理论

曹晋华　程侃

中国科学院应用数学研究所
1981·6

前　言

随着科学技术的发展，技术装备愈来愈复杂。可信性，维修性系统可与性的问题愈来愈受到重视，已成为技术装备在今研制、生产和使用过程的一个极重要的方面。其原因可以从不可信所造成的后果看出。系统失效常常带来的不仅是经济上的损失，或者广商声誉的损失，有时还会有生命上的损失。因此，提高和改善系统可信性就成了一个紧迫的任务。当然可以采取多种途径来实现，如从技术方面，或从经营管理方面来着手。在其中的每一方面都已经积累了许多知识。

近二〇多年来，可信性理论本身也已迅速发展。系统可信性的数学理论已成了可信性工程的一个重要的基础理论。

本讲义介绍了系统可信性的基本理论和常用的数学方法。内容包括：评定系统可信性的定量指标，常见失效分布，修复的不可修系统，网络系统，失效树分析，关联系统，分析可修系统的几个重要方法，最后还介绍了模拟方法。

从讲义的选材上看，有其局限性。我们没有去讨论可信性试验的统计处理方法，以及其统计方法的应用。因为国内在这方面已做了不少工作。此外，本讲义没有涉及系统可信性的各种最优化问题（最优更换策略，最优维修策略，贝叶斯的最优化等），这是一个重要的缺陷。这次由于时间仓促难以弥补。在适当的机会，我们将要补上有关的章节。

阅读本讲义需要微积分与概率论的基本知识。所要用的其它数学知识，在附录中作了简介。本讲义可供理工院校的学生或研究生选修可信性数学理论和数学参考书。材料可根据学生的数学基础而增减。本讲义也可供有关的工程技术人员和数学

本作者参考。

对于讲义中所用"失效"一词应作广义的理解，因为在有修理时，失效仅仅意味着"暂时的故障"，也可以通过修理使其功能得到恢复。文中为叙述简便，一律采用"失效"一词。

本讲义第一、二、四、五、六、十章和附录由程侃同志执笔，第三、七、八、九章由曹晋华同志执笔。由于水平所限和时间仓促，错误在所难免，望不吝指正。

编者 1980·7·

中国科学院应用数学研究所

重印说明

这次重印此讲义之前，来不及对讲义进行全面的修改和补充。这次只是对个别的地方作了必要的修正和补充，就整个讲义来说没有多大变化。

编者 1981·6

中国科学院应用数学研究所

目　录

第一章 系统可信性中的基本概念

本章简单介绍系统可信性研究中的一些基本概念，其中包括评定一个系统的可信性性能的数量指标，以及常见的系统和改善系统可信性的考虑。这些典型系统细致的可信性分析将在后面的章节中讨论。

§1 评定系统可信性的数量指标

粗糙地讲，由一些基本下件（也可以包括人）组成的完成某种特定功能的整体，可以称为一个系统。例如一个核电站可以看成一个系统，而其中的安全保护装置可以看成是它的分系统。但是如果我们单独地对安全保护装置的性能进行研究，则可以把它看成一个系统。因此，系统的概念是相对的。而在可修系统中，系统不仅是指物，而且还包括人——修理工。我们的目标是对系统的性能进行可信性分析，以求对系统（或人—机系统）有一定量的了解，从中找出薄弱环节进行改善。

由于系统的复杂性，可以从不同方面来评定系统完成其功能的能力大小。自然也应有不同的数量指标来刻划其性能。例如，对于一个一旦失效就会引起灾难性后果的系统——如核电站安全保护系统，系统首次失效时间分布将是一个重要的指标。而对于一个失效后可以修复，且失效并不引起灾难性损失的系统，则相邻失效间隔的分布，在$(0,t)$时间中失效次数的分布，在任一时刻t系统正常工作的概率等指标亦反映了系统性能的重要方面。本节将给出评价系统可信性时常用数量指标的定义。

假定系统从时刻$t=0$开始正常运行，则系统有寿命，

它是一个非负随机变量（Y，$\bar{Y}$）系统随时间的进程如图1.所示。在失效后无修理的情形，系统一旦失效便永远停留在失效阶段；在失效可作有修理时，系统总是正常与失效交替出现，若系统正常，称它处于开工阶段；若系统失效，称它处于停工阶段，显然，开工阶段或停工阶段都可以由非负r.v.来描述，用（X_i，Y_i）表示开工、停工的第i个周期。对于不可修系统，系统首次失效时间X及其分布是一个重要的可信性指标；对可修系统，系统首次失效时间X_1，与其后停工时间Y_1的联合分布更能刻划系统的全面性能。

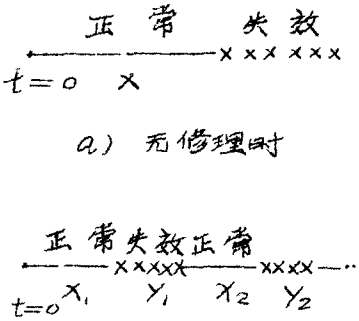


图1、系统随时间的进程示意图

1° 系统首次失效时间X及可信度

显然，系统首次失效时间即其寿命，相应的分布函数(df)记作$P(X\le t)=F(t)$。系统平均首次失效时间为$EX=\int_0^\infty x\,dF(x)$.（$E$表示数学期望）

对任意$t>0$，系统在时刻t的可信度$R(t)$定义为：在一定的工作条件下，在$(0,t]$中系统完成其预定功能的概率。沿用上面的记号，即

$$(1)\qquad R(t)=P(X>t)=1-F(t)\overset{记}{=}\bar{F}(t)$$

从可信度$R(t)$的定义知，$R(t)$是在$(0,t]$中系统不允许有失效的概率。

2° 首次开工、停工时间 (X_1, Y_1) 的联合分布

当系统复杂时，开工停工时间 X_1，Y_1 不一定独立，因此需要研究其联合分布函数

$$(2) \qquad F(x,y) = P(X_1 \leq x, Y_1 \leq y), \quad x, y \geq 0.$$

由 (2) 容易得边缘分布：系统首次失效时间 X_1 的分布，停工时间 X_1 的分布，停工时间 Y_1 的分布，以及它们的均值。

3° 利用率 (Availability)。

假定我们所研究的系统在任一时刻只有正常工作或失效两种可能性。因此我们可以引进一个 0-1 值函数来描述系统的性能。对 $t > 0$ 记

$$(3) \qquad S(t) = \begin{cases} 1 & \text{若在时刻 } t \text{ 系统正常} \\ 0 & \text{若在时刻 } t \text{ 系统失效} \end{cases}.$$

系统在时刻 t 的利用率 $U(t)$ 定义为

$$(4) \qquad U(t) = P\{S(t) = 1\}$$

即系统在时刻 t 正常的概率。利用率 $U(t)$ 有时也叫做点利用率，因为它只与一个点 t 有关。

注意，在 $U(t)$ 的定义中，我们不关心时刻 t 以前系统是否发生过失效或修理，而只关心时刻 t 系统正常与否的概率。

称

$$(5) \qquad \tilde{U}(t) = \frac{1}{t}\int_0^t U(x)\,dx$$

为 $[0, t]$ 上的系统平均利用率。而若极限

$$(6) \qquad \tilde{U} = \lim_{t \to \infty} \tilde{U}(t)$$

存在，则称 $\tilde{U}$ 为极限平均利用率。而若极限

$$U = \lim_{t\to\infty} U(t) \tag{7}$$

存在，则称 U 为平稳状态下的利用率。

利用率是系统可信性的主要指标之一，工程应用中特别感兴趣的是平稳状态下的利用率 U，它告诉我们大约有 U 的时间比例，系统处于正常阶段。

4° $(0,t]$ 中系统失效数 $N(t)$ 的分布

在失效下件有修理的情形，系统随时间的进程是一串正常、失效相交替的序列，因此，对 $t>0$，$(0,t]$ 中系统失效数 $N(t)$ 是一个取非负整数值的 r.v.。我们感兴趣的是 $N(t)$ 的分布

$$P_k(t) = P\{N(t)=k\}, \quad k=0,1,2,\cdots, \quad t>0 \tag{8}$$

及其均值

$$M(t) = EN(t) = \sum_{k=0}^{\infty} k P_k(t)$$

若极限

$$M = \lim_{t\to\infty} \frac{M(t)}{t} \tag{10}$$

存在，则称 M 为平稳状态下系统单位时间的平均失效数，即平稳状态下系统的平均失效率。

$M(t)$ 及 M 也是重要的可信性指标。它告诉我们在某段时间中系统的平均失效数，因此能提供需要准备多少备件更换这样一类有价值的信息。

S^*修理工在任一时刻 t 忙的概率

对于一个可修系统来讲，亦可以从修理机构的角度来考虑，对修理工来讲，在任一时刻 t 亦只有忙或闲两种可能（当系统中多于一个修理工时，可以约定修理工忙意思为至少有一修理工忙，或指其特定的含义）。我们感兴趣的是在任一时刻 $t>0$，修理工忙的概率 $B(t)$，以及在平稳状态下修理工忙的概率 B

$$B=\lim_{t\to\infty} B(t)$$

（若上述极限存在）。$B(t)$ 或 B 是反映系统中修理能力的配备是否合理的一个数量指标。若 B 小，则表明修理工经常很空。这提示我们是否可适当减小修理能力（当然要权衡考虑其它性能经济指标）。若 B 大，则表明修理工经常很忙，可以考虑增大修理能力。

对于复杂系统而言，上面的几个数量指标并不容易求到。在多数场合只能给出其相应的 Laplace（L）或 Laplace-Stieltjes（LS）变换，它们一般不易反演出来。但是有关的平均值，或者平稳状态下的结果通常比较简单。

§2 基本模型

本节介绍系统可信性中研究的一些基本模型。

1° 串联系统，并联系统。

假定系统 S 由 n 个部件组成，任一部件的失效都会引起整个系统的失效，则称 S 为 n 部件的串联系统。相仿，所有部件失效时整个系统才失效，则 S 为 n 部件的并联系统（图2）。

2° $K/n(G)$ 系统，$K/n(F)$ 系统。

若n个件组成的系统S中，有K或K个以上件正常时系统正常，则称S为K/n(G)系统。若有K或K个以上件失效时系统就失效，则称S为K/n(F)系统。

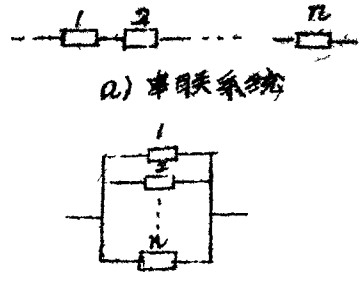


图2、串、并联系统

显然，K/n(G)系统即$(n-K+1)/n(F)$系统。而串联系统即n/n(G)系统。并联系统即1/n(G)系统。通常的表决系统亦是其特殊情形。例如，当n为奇数时，$\left(\left[\frac{n}{2}\right]+1\right)/n(G)$就是按多数个件正常与否来决定系统是否正常的一个表决系统。

实用中K/n(G)系统的例是经常能遇到的。如某种飞机的螺动机系统由3个同型号，相互独立的引擎组成，3个引擎中至少有2个好就能保证飞行的安全。因此，从可靠性的角度来研究，飞机的发动机系统就是2/3(G)系统。它可以表为图3 a)，或等价的形式图3 b)。

3° 串并联系统，并串联系统。

设系统S由n个子系统串联组成，而第i个子系统由K_i个件并行组成($i=\overline{1,n}$)，则称S为串并联系统。若系统S由n个子系统并联组成，第i个子系统由K_i个件串联组成($i=\overline{1,n}$)，则称S为并串联系统(图4)。

显然，它们推广了串联和并联系统的概念。

4° 关联系统 (coherent systems) ([1])

在上面介绍的系统中，我们发现有如下的共同点：

a) 件或系统都只有正常或失效两种可能的状态。

b) 系统正常与否，完全由系统的结构(如串联、串并联或K/n(G)等)及件的状态所决定。

因此，我们可以引进一个n元的二值函数来描述由n个部件组成的系统的性状。循次下去，就到抽象的关联系统的概念。

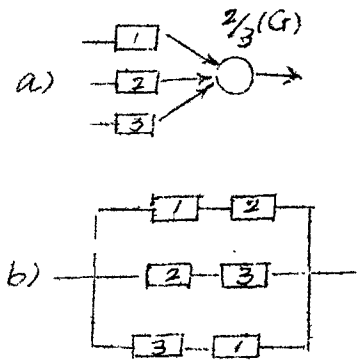
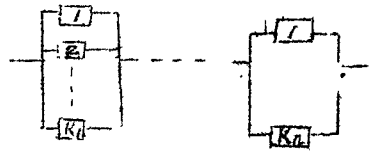


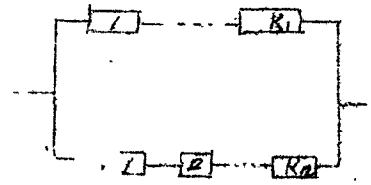
图3 2/3(G)系统

设系统S由n个部件组成，系统与部件都只有两状态：正常或失效，分别用1，0来表示。用只取0,1值的x_i表示部件i的状态，用中(X)=中$(x_1,\cdots,x_n)$表示系统的状态。称中为系统S的结构，或结构函数。

再仔细分析一下上面的具体系统，我们还会发现组成S的n个部件中的每一个，其正常与否都会影响到系统的性状。换句话说，每一部件都是系统不可少的组成部分，若从系统中除去，则会影响或改变系统的性能。其次，在别的部件的状态保持不变的条件下，一个或一些部件正常时，比起它或它们失效时，系统正常的可能性要大。这两点也与我们的经验相符。为此引出相应的定义，记



a) 串并联系统



b) 并串联系统

图4. 串并联、并串联系统

$$
\begin{aligned}
(1_i, \boldsymbol{X}) &= (x_1, \cdots, x_{i-1}, 1, x_{i+1}, \cdots, x_n), \\
(0_i, \boldsymbol{X}) &= (x_1, \cdots, x_{i-1}, 0, x_{i+1}, \cdots x_n) \qquad (1) \\
(i, \boldsymbol{X}) &= (x_1, \cdots, x_{i-1}, \cdot, x_{i+1}, \cdots, x_n).
\end{aligned}
$$

第i个部件称作与结构中无关，若其它分量保持不变，

x_i 任取确定值时，φ 的值不变，即 $\varphi(1_i, X) = \varphi(0_i, X)$，对所指 (i, X) 成立，否则，称第 i 个元件与结构 φ 相关。

称结构 φ 是单调的，若 $\varphi(0) = 0$，$\varphi(1) = 1$，以及对任意的 $X \leq Y$ 都有 $\varphi(X) \leq \varphi(Y)$ 这里 φ 的自变量 0，1，X，Y 都是 n 元向量，$0 = (0, \cdots, 0)$，$1 = (1, \cdots, 1)$，而 $X \leq Y$ 表示相应分量间 $x_i \leq y_i$，$i = \overline{1,n}$ 成立。

称结构 φ 是关联的，或系统 S 为关联系统，若满足：φ 是单调的，且每个元件都是有关的。

显然，前面讲到的系统都是关联系统。我们可以写出其结构函数。

若记 $x_1, \cdots, x_n$ 为元件 $1, \cdots, n$ 的状态。于是串联系统，并联系统，$K/n\,(G)$ 系统的结构函数分别为：

$$\varphi(X) = x_1 \cdot x_2 \cdots x_n = \prod_{i=1}^{n} x_i = \min_{i=\overline{1,n}} x_i . \tag{2}$$

$$\varphi(X) = 1 - \prod_{i=1}^{n} (1 - x_i) = \max_{i=\overline{1,n}} x_i \tag{3}$$

$$\varphi(X) = \begin{cases} 1 & \sum_{i=1}^{n} x_i \geq K \\ 0 & \text{其它} . \end{cases} \tag{4}$$

特别 $2/3\,(G)$ 系统的结构函数为：

$$\begin{aligned} \varphi(X) &= 1 - (1 - x_1 x_2)(1 - x_2 x_3)(1 - x_3 x_1) \\ &= x_1 x_2 x_3 + x_1 x_2 (1 - x_3) + x_1 (1 - x_2) x_3 + (1 - x_1) x_2 x_3 . \end{aligned} \tag{5}$$

注意，二值变量 x 的乘法中，$1 \cdot x = x$，$0 \cdot x = 0$，$x^2 = x$.

例如图 5 所示的系统不是关联系统。因

$$\varphi(x_1, x_2) = 1 - (1 - x_1)(1 - x_1 x_2) = x_1 ;$$

说明结构函数中的值与 x_2 的取值无关，这表明下件2与结构中无关，故系统不是关联的。从图上亦容易看出，把下件2除去，并不影响系统的性能。

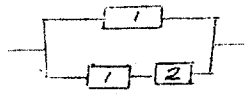


图5．非关联系统

今后假定我们研究的系统都是关联系统，关联系统由其结构函数中唯一决定。但是，当系统比较复杂时，中的表达式往往也不容易法得。例如桥形系统（图6）。它由5个下件组成。其结构函数中可表为

$$(6)\qquad \varphi(\boldsymbol{X})=\prod_{i=1}^{4}\{1-K_i(\boldsymbol{X})\}.$$

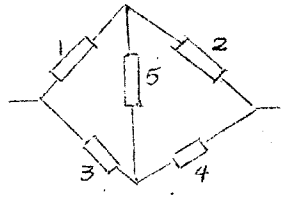


图6．桥形系统

其中

$$K_1(\boldsymbol{X})=(1-x_1)(1-x_3),\quad K_2(\boldsymbol{X})=(1-x_2)(1-x_4),$$

$$K_3(\boldsymbol{X})=(1-x_1)(1-x_4)(1-x_5),\quad K_4(\boldsymbol{X})=(1-x_2)(1-x_3)(1-x_5).$$

关于关联系统结构函数的进一步性质我们将在第六章中讨论。

§3．改善系统可信性的方法

可信性本身涉及到许多因素，它不仅与系统的设计、制造、工艺、原料等有关，而且还与其使用、维修、更换等方面相关。因此，为了提高或改善系统的可信性，我们应从各个有关方面去进行协调和平衡。

例如，从技术的角度来讲，可以通过提高元器件的可信性，或者改进系统的总设计，简化中间环节，改进工艺，采用优质原料等来达到。具体做时可从由：a）筛选来剔除早期不合格品，减少元部件的失效率。b）简化系统，改善系统的运行

条件，如提供较好的环境条件，减额使用等。(2) 改进产品的生产技术。如使元件标准化，采用先进管理控制生产过程，采用自动化生产，减少人为失误，以及提高操作者技术水平等。

另一类改善系统可信性的手段是采用备件，对元件进行合理的予防性维修或更换，或对失效元件进行维修。

在采用备件的情形，当系统中一个元件失效时，由开关转换到好备件，使整个系统仍能继续正常工作。通常可信性问题的研究中，备件可以分为冷、热两类。所谓冷备，是指在好备过程中备件性能不变，即无论好备多久，都不改变备件的工作寿命。而热备是在好备过程中备件可能会失效或性能变劣。由于好备与工作时的环境不同，所以通常假定元件在热备时有好备寿命，在工作时有工作寿命。

在采用予防性维修和更换的情形下，按照一定的原则（策略），去更换系统的元件，以便使系统的某可信性指标或某些经济指标达最优。常采用的有定期予防性维修或定期更换策略。还有失效更换或随机更换等。在元件可维修的情形，系统中配有修理工。一旦元件失效，修理工就对失效元件按一定的排队规则（如先来先修，随机次序或某种优先权等）进行修理。修复后的元件假定与新的有相同的寿命分布，并且按系统的要求重新参加运行或好备着。

由于采用了备件、予修、更换的维修，一方面使得系统可信性有显著的改善，另一方面也使得上述基本模型有了许多花样。使得对它们的研究，特别是解析方法的研究，就变得更加复杂了。后面的章节仅限于讨论备件、维修对改善系统可信性的作用。

参考文献

1. Barlow, R.E., and F. Proschan, Statistical Theory of Reliability and Life Testing, 1975.

第二章 常见的失效分布

本章讨论寿命及常见的失效分布。其中包括连续型的(负)指数分布，Gamma分布，Weibull 分布，对数正态分布，截尾正态分布；以及离散型的二项分布，几何分布，负二项分布，Poisson 分布。还讨论了二维指数分布及失效分布类[3]、[4]。

§1. 寿命分布和失效率

1° 寿命和寿命分布

在可信性研究的对象中，无论是元件或系统，在使用或储存时总有一个寿命。显然，这个寿命是与许多因素有关的，如所用的材料，制造、装配过程中的各种情形以及所在工作的环境等。所以，我们通常用一个非负随机变量 $(Y \cdot U \cdot) X$ 来描述它的寿命。X 相应的分布函数 (df) 为