兵器可靠性設計之一

工程設計手册

可靠性設計

第五机械工业部第二一〇研究所

一九八二年二月

保密文件根据说明的正当理由提供，由陆军代表的正式部门根据国防文件中心（DDC）ATTN规定进行确认，地址是DDC-TSR，Cameron Station，Alexandria，VA22314。

欢迎对手册提出批评和建议，来信請寄：

Commander

US Army Materiel Development and Readiness Command，Alexandria，VA22333

DA表格2028可以用来填写评论和建议，这种表格可通过正常的出版物提供渠道获得。

目　录

第一章 概　论

第二章 环境条件

第三章 可靠性测量

第四章 模型的建立和分析

第五章 可靠性要求的分配

第六章 人为因素

第七章 因果表

第八章 失效模式和影响分析

第九章 失效模型

第十章 参数变化分析

第十一章 设计和生产审查

附录A 詳細設計审查清单

附录B 可靠性数据源

附录C 有关人为因素的文献

第一章 概 論

1-0 符号表

A＝可利用性
MTBF＝平均故障间隔时间，时间$^{-1}$
MTTR＝平均故障修理时间，时间$^{-1}$
I，II＝下标，表示系统Ⅰ和系统Ⅱ

1-1 概述

可靠性工程是研究确保产品成功完成其功能任务的各种因素的一门学科。工程技术人员为在最短时间内以最低成本生产出具有最大使用性的设备和系统而受到很大压力和限制。这样，便产生了原始的可靠性科学，它包括以下两个方面：

（1）注意零部件

（2）处理不确切性

由于工程技术人员和管理人员变得更加善长于定量确定所生产的可信赖设备和系统，所以发展了各种定量确定可信赖设备和系统的分类方案。在这些方案中，“可靠性”这个词具有几种含义，所有的含义都与词典的含义相关，但是某些含义相当狭隘和特殊。

S可靠性（参考文献3，A版本）的传统狭隘意义是“某种产品在规定环境条件下于特定间内完成其预定功能的概率”。在可靠性的各种计算中，实际上更经常采用以下延伸定义：

S可靠性指的是产品成功地完成其任务的概率，但是产品在任务执行开始时必须处于良好状况。

本系列文献各章节中，当某个术语是以某种特殊规定的统计含义使用时，习惯在该术语之前加上“S”一字，如S-可靠性，S-正态，S-可利用性，S-置信度。

这种S-可靠性的概念主要适用于具有简单任务的各种产品项、使用设备、简单车辆、或各种系统的组件。对于大的复杂系统而言，例如防空系统（包括雷达和武器）、坦克中队，或大规模的通讯网络，则更适宜应用更加复杂的概念（例如系统有效性），来描述系统的价值。

在设备的设计、发展和现場使用过程中，可靠性工程师不能只局限于收集数据和进行保险统计服务方面的工作，还必须做其它更多方面的工作。可靠性工程师对产品发展过程中所作出的各种大量判定十分敏锐，而且他也应协助做出这些判定。可靠性工程师有责任使设备具有特定的寿命。它必须能夠根据许多其它重要参数，例如成本、重量、尺寸和时间对各种可靠性参数进行权衡和协调。重点放在失效数上，而对失效的原因可不予以考虑。可靠性数学模型必须反应出对失效原因的工程研究以及消除这些失敗原因的程度。这种数学模型必须能根据设计阶段到現場使用阶段的情況预测S-可靠性，以确保失效概率不超过允许极限。S-可靠性是一种定量概率函数，这种概率函数在设计阶段必须能夠预测，在试验中能夠测

量，在生产上能够确保，在现场能够保持。总之，在产品的整个寿命周期内，这种概率因数必须是可控制的，其它的系统特性，例如可维护性和安全性，也会影响到系统的功能以及相关分系统的功能，其中包括维修支援设备、检查和服务，修复备件提供以及实际的修复工作。这样，可靠性和其它的设计考虑一起为发展满足任务目的和要求的合格系统提供了基础。这整个项目称为系统工程。本章的目的在于提供对系统工程以及可靠性与可维护性、安全性和性能的权衡协调的一般理解。

1-2 系统工程

近年来，系统这个字开始包括：

(1) 主要任务设备 (The prime mission equipment)

(2) 工作和维修要求的设备装置 (The facilities required for operation and maintenance)

(3) 人员的选择和培训 (The selection and training of personnel)

(4) 工作和维修程序 (Operational and maintenance procedures)

(5) 试验鉴定仪器和数据处理 (Instrumentation and data reduction for test and evaluation)

(6) 专门活动计划和验收程序 (Special activation and acceptance programs)

(7) 后勤支援程序 (Logistic support programs)。

特别是，把一个系统定义为（参考文献，版本A）："工作和支援设备、人员、设施以及软件的任一复杂性程度的综合体；以上各种因素作为一个整体使用，而且能够完成和支援某项功能作用"。

系统工程（参考文献2）就是科学、工程和管理研究在下列各方面的应用：

(1) 应用定义，综合、分析、设计、试验和鉴定的迭代过程，把某种工作要求转变为对系统性能参数和系统结构的描述。

(2) 以使整个系统设计最优化的方式把相关技术参数综合在一起，并确保全部物理功能和程序的相互一致性。

(3) 把可靠性、可维护性、安全性、耐久性（包括电子战的各种考虑），人为因素以及其它各种因素综合为总的工程研究项目。

从系统管理角度看，系统工程仅是系统发展（从最初概念阶段、到合同确定阶段、工程发展阶段、生产阶段和工作阶段）所要求的5项重要工作之一。这5项工作是订货生产、计划控制、结构管理、系统工程以及试验和应用。图1-1概括了这些工作在系统发展每一个阶段中的一般作用及其相互间的关系。有关系统管理的更详细情况见参考文献8。

系统工程在一次作用周期中，由4步组成（见图1-2）。第一步考虑威力预测研究、理论研究、陆军的各种可能任务及所要求器材和系统的各种来源；然后再将这些研究转变为基本的功能要求或工作说明。第一步研究的一般结果是表示基本功能工作以及它们相互顺序和关系的一组方框图。即使硬件有助于实现基本的系统设计，在第一步中也不作特殊的说明。第一步只是形成作为最终答案的初步假设。

第二步中，根据各种限制，如设计、成本时间以及各种特殊任务要求，对第一步所作的

初步假设进行鉴定，以建立设计设备，规定系统间相互关系、规定设施装置以及确定对人员、培训、培训设备方法要求的准则。

第三部包括系统设计研究，此项工作与第二步和第四步工作同时进行，以便：

（1）确定各种后选功能和功能顺序；

（2）确立各种功能对设计、人员、培训和程序数据的要求；

（3）找出能够满足任务要求的最佳途径；

（4）选择最佳设计方法，以把全部任务要求综合在硬实硬件和有关支援活动中。

通常情况下，第二步中的研究涉及到各种权衡协调工作，其中数据的表达形式是方块图、轮廓图、系统内部与外部相互关系要求、比较矩阵以及辅助选择每种方法的数据。第三步的系统设计研究中所采用的某些科学方法是：概率论、统计推断、模拟、计算机分析、信息论、排队论、伺服机理理论、控制论、数学、化学和物理学。

第四步工作是应用第三步所选择的设计方法把第二步规定的全部设计要求综合到合同制成品（CEI）中。第四步的工作结果是，根据规定的工程资料和有关会签，提出合同制成品详细设计、发展和试验的准则。第四步得出的成果用于：

（1）确定系统间的相互关系；

（2）以公式表示从选用装置或技术得出的额外要求和功能；

（3）提供用以改进和论证第一步所得系统要求和功能流程图的反馈数据。

在系统工程过程的第一次过程完成之后，已经确定的各种改进方案、后选方案，各种限制，各种附加要求以及各种技术问题应再根据最初假设（初始设计）进行系统工程研究，以使设计更加实际可靠。这种系统工程的循环研究过程一直进行到产生令人满意的设计方案为止，或一直进行到可以利用的条件（时间、金钱等）用完，而且现有的设计可以接受时为止；或一直进行到一些条件和要求不再能够达到时为止。

其它各种因素（例如可靠性、可维护性、安全性和人为因素）作为系统工程过程的一个部分是各自独立存在的，但是它们对工程原理有影响，而且这些因素互相之间以及对整个系统计划提供了各种特定输入。有关这点可能存在的固有问题是："怎样才能知道到什么时候设计才是算合格的？"或"怎样测量系统的有效性？"解答这些问题便能得出有关系统有效性的概念。

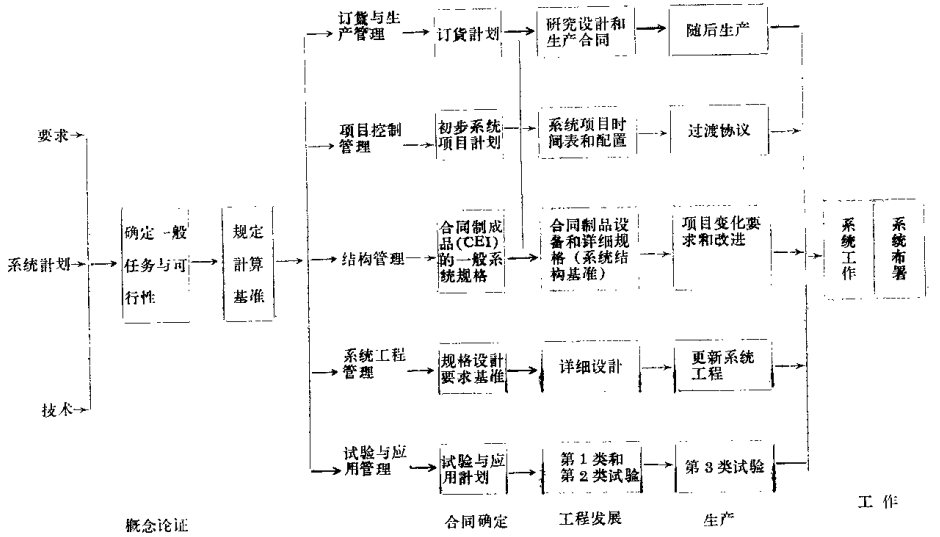
要求
系统计划
技术
确定一般任务与可行性
规定计算基准
订货与生产管理
项目控制管理
结构管理
系统工程管理
试验与应用管理
订货计划
初步系统项目计划
合同制成品(CEI)的一般系统规格
规格设计要求基准
试验与应用计划
研究设计和生产合同
系统项目时间表和配置
合同制品设备和详细规格(系统结构基准)
详细设计
第1类和第2类试验
随后生产
过渡协议
项目变化要求和改进
更新系统工程
第3类试验
系统工作
系统布署
概念论证
合同确定
工程发展
生产
工作

图1-1 系统管理工作

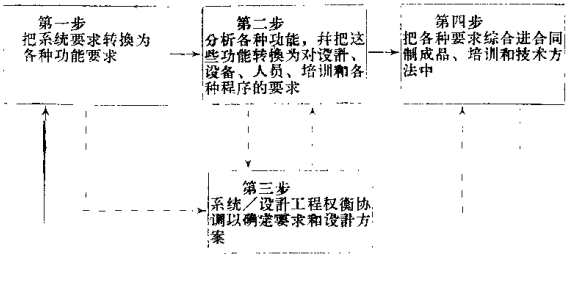

图1-2 基本的系统工程过程

1-3 系统有效性

系统有效性的定义是（参考文献，版本B）：能够期望某种产品达到一组特定任务要求程度的测量值，这种测量值也可表达为可利用性、可依赖性和能力的函数关系。在评定系统或其部件的优点时，时间和成本是非常关键的因素，因此在作出有关购买、使用、维修或报废任何一种设备的行政决定时，必须要考虑这两个因素。

很明显，系统的有效性受到设备设计与制造方法的影响。但是，它更受设备使用和维护方式的影响，也就是说，系统的有效性受到设计人员、生产工程人员、维修人员以及使用／操作人员的影响。系统有效性定义中所包括的可利用性、可依赖性和能力这些概念就是表示这些影响以及它们与系统有效性的相互关系的。MIL-STD-721（参考文献3，版本B）为这些概念提出了以下定义：

（1）可利用性。当某个未知（随机）时刻调用设备执行任务时，其在任务开始时所处的可工作和可使用状态程度的度量。

（2）可依赖性。在给定任务开始时产品状况的情况下，该产品在执行任务过程中在一点和数点上工作状况的变量，其中包括可靠性，可维护性和耐久性。可依赖性可以看成是如下概率，即某项产品将（a）在特定任务过程中进入或采用任何一种所要求的工作模式，以及（b）完成与这些工作模式相关的功能。

（3）能力。在任务过程中条件给定的情况下，某项产品完成任务能力的度量。

可依赖性与可靠性有关。两者所不同的是，可依赖性是一种比可靠性更加一般的概念。在意图十分明确的情况下，没有一个设计人员会对这种语义上的探讨感兴趣。

作为一个例子，研究一下利用机枪攻击飞机的情况。由于设计意图是为地面战斗支援提供增大的火力和火力覆盖区，所以这种“系统”（机枪）的有效性将十分低。机枪并不具有预定的反飞机能力。但是，这种事实和机枪可利用性或可依赖性没有太大的关系。用机枪反飞机只是使用／操作人员的不正确应用而已。另外一个例子是先前可以使用的车辆轮胎，在

车辆以90英里／小时的速度在炎热气温下（110°F）行驶时，由于接触到地面上的一个参差不齐的坑而爆裂漏气。如果大部分此类轮胎在接触负荷大及高速高温情况下能幸存，那么轮胎的爆裂(失效)是由于可靠性差而造成的，因为这种恶劣环境条件（90英里／小时，110°F，参差不齐的坑）都在这类轮胎的能力范围之内。但是，如果规定的设计要求是恶劣程度较小的环境条件（60英里／小时，80°F，没有参差不齐的坑），那么这种失效则是由于能力差而造成的。因此，如果是第一种情况，系统（轮胎）具有足够的能力，但是其可靠性较低。如果是第二种情况，可靠性可能较高，但是能力（对这种特殊使用情况而言）不够。然而，无论在哪一种情况中，对这种特殊使用情况而言，系统的有效性是低的。

在系统从概念论证到工作阶段的整个寿命周期中，系统有效性的最佳化工作是十分重要的。所谓最佳化工作就是以最后得出的有效性为依据，对可利用的各种因素（金钱、时间、人员等）进行权衡考虑，一直到获得一种在所要求资源消耗的情况下能提供最大有效性的综合方案为止。这样，最佳化的系统就必须是一种具备以下能力的系统：

（1）在最低成本下，达到或超过特定有效性等级，和／或

（2）在总成本一定的情况下，提供最大的有效性。

这种最佳化工作由图1-3的流程图表示，该图把最佳化过程表示成由以下三个步骤组成的反馈回路：

（1）设计许多能够满足工作要求和限制的系统。

（2）计算有效性和所用各类资源的最终值。

（3）对这些结果作出鉴定，并对设计和各种支援因素的恰当组合进行归纳，然后再返回到反馈回路的模型中。

最佳化还可以通过购买一辆新车的例子加以说明，或者更明确地说，把汽车选择过程中所遵循的规则或准则变为更加精确的定量项目。虽然汽车确实具有一些定量特性，如马力、成本和乘坐能力等，但是这些定量特性在大多数特定等级的汽车中都是相似的（如在廉价的Sedans级汽车和赛车中）。所以，实际上这些选择准则简化为对特殊型号和类似不可捉摸因素的某种审美要求和先验经验。同样，对武器系统的最佳设计选择在很大程度上受到各种良好工程实践经验、对类似系统了解程度以及经济因素的影响。尽管存在这种模糊概念，也必须对选择准则进行调整，以便做到：

（1）减小问题范围，以便于方法的选择；

（2）能更有把握地和有目的地对全部可能的选择方案进行研究，以适用于数学表达和分析；

（3）能更容易地把根据其他原理得到的知识和经验合并在得出的结论中；

（4）使设计方法的最后选择能以更加精确的定量项为依据，从而能够得到更加有效的鉴定和修正，并为将来的各种最佳化问题提供较好的输入数据。

最佳化模型中的参数选择也同样受系统定义的影响。比如说，汽车的购买者也许不会考虑到生产商和商人的各种服务方针。如果考虑这些服务方针，那些系统就是汽车加服务方针。如果不考虑这些方针，则系统就只包括汽车。

用于使系统有效性最佳化的实际方法不在本章探讨范围之内。例如，表1-1（参考文献4）只列出某些比较常用的技术。有关这些技术的详细情况在已经提到的参考文献中介绍，例如，参考文献26和参考文献4介绍了以下方法和例子：基本数学和统计概念、模拟、排队论、顺

序和马尔科夫过程、对策论、线性和动态编程、信息论及其他等等。这些技术对于系统有效性最佳化来说并不是独特的，也不只限于系统工程。

表1-1

部分最佳化技术

1.数学方法：
- 增滑过程
- 差分演算
- 变分法
- 梯度论
- 数值近似
- 符号逻辑
- 线性整数论
- 极大极小论

2.统計方法：
- 贝叶氏分析
- 决策论
- 试验设計
- 信息论
- 最速上升法
- 随机过程

3.编程方法：
- 动态编程
- 线性编程
- 非线性编程

4.其它方法：
- 对策论
- 蒙特卡罗法
- 排队论
- 更新论
- 寻优论
- 信号流向图
- 模拟
- 赋值论

1-4 可靠性設計的作用

可靠性研究不仅包括硬件，而且还包括各种操作、程序、软件和使用这些硬件的人员。可靠性取决于各种可靠性要求和试验，而且也取决于设备整个寿命过程中，管理工作（政府

和合同商）对可靠性规定的侧重点。通常，因为各种条件都是有限的，所以必须对某种因素（成本、时间、性能、可靠性）作出牺牲；到底对哪种因素作出牺牲，应根据管理工作决定，也就是说，管理工作是否将决定用理论可靠性“验证”来代替实际可靠性“验证”？

谈论最佳化可靠性和可靠性最佳化的分析途径要比得到一个已经最佳化的实际系统容易得多。获得较高的可靠性属于工程问题，而不是统计问题。

在对可靠性进行最佳化之前，必须了解可以改变可靠性的各种途径以及能使可靠性发生变化的各种方法的限制种类。这些分类便于讨论，而其本身并不会限制任何人的工作。在试图改进可靠性的全部变化中，并非所有变化都可在实际上起到改进可靠性的作用，特别是有关任务的数据资料不充足的情况下更是如此。

用以下改变可以提高可靠性：

（1）改变解决问题的整个方法（通讯系统的有线联系或微波联系）；

（2）改变系统的结构（飞机可以装有螺旋桨发动机或喷气发动机，机翼可以在机身上也可以在机身之下，发动机位置和数量可以调整）；

（3）改变某些模块或分系统（发动机可以电气操作，也可以液压操作，也可以通过机械横杆和齿轮进行操作）；

（4）改变某些组件（采用高可靠性的零部件或商业型零部件）；

（5）改变生产的某些细节（钢料上的孔可以用冲、钻、铰和／或烧蚀等工艺加工）；

（6）改变材质（木头、塑料、合金）；

（7）改变操作方法（要求无线电接收机的操作人员对每一个阶段分开进行调谐，或通过一个开关完成全部工作）；

（8）改变有关任务成功的定义（雷达的距离和分辨率）；

（9）改变对细节的重视程度（可根据手册表简单地选择一种合金，或对各种合金进行大量试验，以找出一种最符合使用要求的合金）。

改进可靠性的各种工作受到以下各因素的制约：

（1）设计成本

（2）零部件生产成本

（3）所需要的时间

（4）能够从事这项工作的人力

（5）外购部件和材料的可利用性

（6）成品的体积和重量

（7）操作人员的培训限制

（8）有关真实使用条件的不确切性

（9）维护保养特点和后勤供应情况

（10）各种不同用户规则的逻辑后果

（11）用户对某些结构的反对情况

（12）影响到行政上作出变化的管理优先权

（13）缺乏对材料或部件特性或零件制造途径的了解。

在任何一项特定的工作中，其它各种技术和各种限制也是同样重要的。某些变化和限制不易定量表示，而且上文所列出的那些变化和限制也不是相互排斥的。所有这些使得实质上

不可能进行完整的数学分析。

具备大部分重要失效形式是必要的，只有这样，设备的失效程度才会适度，也就是说，在出现主要失效之后，仍然可以进行某种形式性能降低的操作。例如，如果车辆的动力控制失效，假如能用手进行控制，则车辆仍可以缓行到安全地带。

必须明确说明执行任务期间的修复特点。通常可以把贮备冗余看成是一种特殊的修复情况。问题在于在出现失效情况时，怎样才能实现这种转变。在某些条件下，假如设备本身只是停止工作非常短的时间，那么从整个任务角度来看，将不算是失败。那么在什么样的情况下，系统才能避免进行修复呢？出现每一次失效后，整个系统是否会恢复到全新状况呢？只是某个分系统会恢复到全新状况，还是设备本身也许能回到其刚刚失效之前的统计现状？总之，确切的情况可能不是已知的，而且选择简单易处理的合理现实假定实际上是一项工程上的判断问题。

各种设计方法和要求由系统可靠性工程人员进行研究，包括以下几个方面：

（1）有关（a）任务，（b）成功完成和（c）良好状况（任务开始时）的定义，在进行可靠性计算时，必须十分明确。

（2）必须对可靠性与每个其他系统参数（可维护性）之间的相互关系和相互影响进行仔细的分析。

（3）必须选用一种可靠性估算方法，以便能对每种设计结果进行定量描述。

（4）必须将可靠性的各种要求与系统本身的任务进行对比和衡量。

（5）系统可靠性等级必须与整个计划的资源配置情况一致。

这些方法和要求以及其它有关这方面的情况在本手册的第三、四和五部分中介绍。

这种分析中所采用的技术包括模型的发展，这种模型考虑了以下各方面的情况：

（1）每一个任务阶段所要求的功能。

（2）每种功能的典型时间周期的确定。

（3）每种功能元件的外部和内部环境应力的确定。

（4）各种工作和维护概念。

（5）每种功能的硬件和软件系统元件。

（6）所要求的任何一种功能冗余的确定。

对于可靠性工程人员来说，各种特定的设计技术，诸如应力减小、冗余、应力／强度分析、可靠性要求的比例分配、预测、试验检验设计、参数变化分析、失效模式和效应分析以及最坏情况分析等，都是进行“研究的工具”。此外，可靠性工程人员必须做到：

（1）主动积极地参与规定可靠性理想零部件的选择工作，从而促进军用系统范围内的标准化工作。

（2）在各适当阶段参与设计的审查工作，以评定各种可靠性要求以及达到这些要求的程度。

（3）在整个计划过程中，监督各可靠性要求的达到程度。

（4）与系统工程小组的其他成员协调工作，使可靠性工作与其它工程要求结合在一起。

只有这样，可靠性工程人员才能从可靠性的角度完成系统工程工作。这些方法和技术在本手册这一部分的后几章和其它部分中予以详细讨论。其它有关这方面的内容和资料见本章结尾所列出的各参考文献；例，军用标准MIL-STD-785（参考文献1）为各种系统可靠性计