QJ

中华人民共和国航天行业标准

FL 0111

QJ 2172A—2005
代替 QJ 2172—91

卫星可靠性设计指南

Guide to satellite reliability design

2005－04－11 发布　　2005－07－01 实施

国防科学技术工业委员会　发 布

目　次

前言 V
1 范围 1
2 规范性引用文件 1
3 术语定义和缩略语 2
4 一般要求 2
4.1 可靠性设计的基本要求 2
4.2 卫星可靠性设计应遵循的准则 3
4.3 权衡分析 4
5 可靠性指标论证 4
5.1 概述 4
5.2 卫星可靠性参数的选择 5
5.3 可靠性指标的确定 8
5.4 可靠性参数选择和指标确定的工作内容、方法和程序 9
5.5 卫星论证阶段可靠性指标论证的工作内容 10
5.6 方案阶段 11
5.7 注意事项 11
6 可靠性模型的建立 12
6.1 概述 12
6.2 目的 12
6.3 任务可靠性模型 12
6.4 步骤 13
6.5 卫星系统常用可靠性模型 13
6.6 复杂网络可靠性模型 16
6.7 具有多功能单元的系统可靠性模型 17
6.8 注意事项 18
7 可靠性分配 18
7.1 概述 18
7.2 目的 18
7.3 原则 18
7.4 步骤 18
7.5 方法 19
7.6 注意事项 22
8 可靠性预计 23
8.1 概述 23

8.2 目的 23
8.3 原则 23
8.4 步骤 23
8.5 方法 25
8.6 注意事项 26
9 故障模式、影响及危害性分析 27
9.1 概述 27
9.2 目的 27
9.3 原则 27
9.4 步骤 27
9.5 方法 27
9.6 CA 的基本方法 31
9.7 FMECA 的输出 34
9.8 示例 35
9.9 注意事项 35
10 故障树分析 36
10.1 概述 36
10.2 目的 36
10.3 原则 36
10.4 步骤和方法 37
10.5 示例 38
10.6 注意事项 38
11 元器件选用与控制 38
11.1 概述 38
11.2 元器件选用控制的目的 39
11.3 元器件选择控制的原则 39
11.4 元器件选择控制要求 39
12 材料、机械零件和工艺选用控制 40
12.1 概述 40
12.2 目的 40
12.3 材料、机械零件和工艺选用控制原则 41
12.4 步骤与方法 41
13 可靠电路设计 43
13.1 概述 43
13.2 电路优化、简化设计 44
13.3 瞬态和过应力保护 46
13.4 CMOS 电路防锁定设计 48
13.5 单粒子事件防护设计 54

14 元器件降额设计 60
14.1 概述 60
14.2 元器件的降额参数和量值 61
14.3 几点说明 67
15 热设计 67
15.1 概述 67
15.2 目的 67
15.3 热设计原则 67
15.4 热设计步骤 69
16 冗余设计 69
16.1 概述 69
16.2 目的 70
16.3 原则 70
16.4 步骤 71
16.5 方法 71
16.6 注意事项 73
17 电路容差分析 73
17.1 概述 73
17.2 目的 74
17.3 原则 74
17.4 步骤 74
17.5 方法 76
17.6 示例 78
17.7 注意事项 79
18 电磁兼容性设计 79
18.1 概述 79
18.2 卫星总体的电磁兼容性（EMC）设计 79
18.3 设备/分系统 EMC 设计 83
19 潜在电路分析 85
19.1 概述 85
19.2 目的和适用范围 86
19.3 方法 87
19.4 步骤 87
19.5 应用说明 88
20 环境及其防护设计 89
20.1 概述 89
20.2 卫星环境及影响 89
20.3 抗辐射设计 90

20.4 防卫星静电放电（ESD）设计 92
20.5 防振设计 93
20.6 防潮设计 94
21 机械产品可靠性设计 94
21.1 卫星结构可靠性设计 94
21.2 卫星机构可靠性设计 102
22 软件可靠性 104
22.1 概述 104
22.2 一般要求 105
22.3 方法 106
22.4 步骤 107

前　言

本标准代替QJ 2172—1991。

本标准与QJ 2172—1991相比主要有以下变化：

a） 本标准主要按 QJ 1408A 第 200 工作系列进行编写。原标准安全性设计、维修性设计、人机工程设计、可靠性试验、可靠性设计评审、可靠性评估等内容不作为本标准的内容，增加了 CMOS 防锁定设计、单粒子事件防护设计、卫星机构可靠性设计、最坏情况分析、机械零件及工艺选用控制等。

b） 各章按基本统一的条目编写（可适当合并或剪裁）：概述、目的、一般原则、步骤、方法、示例、在卫星应用中注意事项等。

c） 卫星可靠性工作项目表按 QJ 1408A 的要求选用。

d） 卫星可靠性指标参数选用表按 GJB 1909.1、GJB 1909.4 的要求进行。

e） 可靠性建模中去掉一些不常用的模型、公式。

f） 可靠性预计强调可靠性模型和 GJB/Z 299B 以及 MIL—HDBK—217F。

g） 可靠性分配增加最小工作量法，适应市场经济发展规律及要求。

h） 在一般要求中增加可靠性设计准则。

i） 自原标准颁布实施十多年来，卫星元器件、材料、工艺选用、潜在电路分析、FMEA、FTA、软件可靠性设计等技术已有很多新的成果与经验，已反映在标准中。

j） 容差分析技术增加了最坏情况电路分析技术（WCCA）。

k） 本标准提出了卫星应用中应注意的问题。

l） 本标准有的内容强调了一些概念及管理，如可靠性指标、软件可靠性等，目的在于更好地应用本标准。

本标准由中国航天科技集团公司提出。

本标准由中国航天标准化研究所归口。

本标准起草单位：中国航天标准化研究所、中国航天科技集团公司第五研究院。

本标准主要起草人：李祚东、徐雷、肖名鑫、任立明、周海京、余振醒、郭树玲、朱德懋、程尚达、文跃普、张华、张伟、赵大鹏、白光明、刘志全、龚得荣。

本标准于1991年2月首次发布，本次为第一次修订。

卫星可靠性设计指南

1 范围

本标准规定了卫星系统、分系统及设备可靠性设计和分析的方法。

本标准适用于卫星系统、分系统及设备的可靠性设计，卫星地面设备及其它航天器可参照执行。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包含勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 2036—1994　印制电路术语

GB/T 3187—1994　可靠性、维修性术语

GB/T 17574—1998　半导体器件　集成电路　第2部分：数字集成电路

GJB 33A—1997　半导体分立器件　总规范

GJB 72—1985　电磁干扰和电磁兼容性名词术语

GJB 450A—2004　装备可靠性工作通用要求

GJB 451—1990　可靠性维修性术语

GJB 597A—1996　半导体集成电路总规范

GJB 768A—1997　故障树分析指南

GJB 813—1990　可靠性模型的建立和可靠性预计

GJB 1029—1990　卫星热设计准则

GJB 1909—1994(所有部分）　装备可靠性维修性参数选择和指标确定要求

GJB 2438—1995　混合集成电路总规范

GJB 3590—1999　航天系统电磁兼容性要求

GJB/Z 27—1992　电子设备可靠性热设计手册

GJB/Z 35—1993　元器件降额准则

GJB/Z 89—1997　电路容差分析指南

GJB/Z 102—1997　软件可靠性和安全性设计准则

GJB/Z 123—1999　宇航用电子元器件有效贮存期及超期复验指南

GJB/Z 299B—1998　电子设备可靠性预计手册

QJ 1408A—1998　航天产品可靠性保证要求

QJ 2176—1991　航天器布线设计和试验通用技术条件

QJ 2437—1993　卫星故障模式、影响及危害性分析

QJ 2668—1994　航天产品可靠性设计准则　电子产品可靠性设计准则

QJ 3027—1998　航天型号软件测试规范

QJ 3050—1998　航天产品故障模式、影响及危害性分析指南

QJ 3057—1998　航天用电气、电子和机电（EEE）元器件保证要求
QJ 3065.1—1998　元器件选用管理要求
QJ 3103—1999　印制电路板设计规范
QJ 3125—2000　航天产品材料、机械零件和工艺保证要求
QJ 3126—2000　航天软件产品保证要求
QJ 3128—2001　航天软件开发规范
QJ 3217—2005　潜在分析方法和程序
MIL—HDBK—217F—1991　电子产品可靠性预计
NASA—STD—5001　空间飞行器硬件结构设计和试验安全系数
ECSS—Q—70A—1996　空间产品保证——材料、机械零件和工艺

3　术语定义和缩略语

GB/T 3187—1994、GJB 451—1990确立的术语和定义适用于本标准。
下列缩略语适用于本标准。
EDAC——error detected and corrected，故障检测与纠正；
EVA——extreme value analysis，极值分析；
RSS——root square sum，和平方根分析；
SCA——sneak circuit analysis，潜在电路分析；
SEE——single event effect，单粒子效应；
SEU——single event upset，单粒子翻转；
SGS——structure grounding system，结构接地系统；
SPG——single point ground，单点接地点；
TID——total ionizing dose，总电离剂量；
WCCA——worst case circuit analysis，最坏情况电路分析。

4　一般要求

4.1　可靠性设计的基本要求

可靠性设计的基本要求包括：

a）　产品承制单位应依据 QJ 1408A—1998 制定可靠性保证计划；

b）　产品可靠性保证计划应包括涉及整个研制过程中相互有联系、协调的可靠性管理、可靠性工程等工作项目，应纳入产品研制计划，以保证规定的可靠性工作项目圆满完成，并与其它研制工作密切结合、协调一致，以防止重复工作，提高投资效益；

c）　产品可靠性保证计划应按照产品本身的特点及合同（或任务书）要求，确定可靠性工作项目及工作内容、范围；

d）　卫星可靠性保证计划应在型号两总主持下，由可靠性设计师制定，经评审及批准后实施，计划修改应履行同样的程序；分系统、设备等也应制定相应的可靠性保证计划，履行类似的审批程序；

e）　通过功能和可靠性分析来鉴别系统、分系统、设备的全部薄弱环节；

f）　通过可靠性指标论证、可靠性建模、分配和预计来估计产品（系统、分系统或设备）可靠性定量要求；

g） 系统设计中应尽量避免单点失效；

h） 通过合理冗余提高系统（设备）的任务可靠性；

i） 通过加大设计裕量（如降额应用）和采用光、机、电、软件可靠性设计技术，使故障率减至最小。

表1列出卫星可靠性保证计划在各研制阶段的可靠性工作项目，可靠性设计与分析是其中重要组成部分。

表1 卫星可靠性工作项目表

工作项目	工作类别	技术指标论证阶段	方案阶段	工程研制阶段		
				初样阶段	试样或正样阶段	生产阶段
可靠性工作计划	管理	Δ	√	√	√	√
对转承制单位和供货方的监控	管理	Δ	Δ	Δ	√	√
可靠性评审	管理	Δ	√	√	√	√
故障报告、分析和纠正措施系统	工程	×	Δ	√	√	√
故障审查	管理	×	Δ	√	√	√
可靠性模型的建立	工程	Δ	√	√	○	×
可靠性分配	计算	Δ	√	√	○	○
可靠性预计	计算	Δ	√	√	√	○
故障模式、影响和危害度分析	工程	Δ	Δ	√	○	○
故障树分析	工程	Δ	√	√	○	○
潜在电路分析	工程	×	Δ	√	√	○
电子元器件和电路容差分析	工程	×	×	√	○	×
电路最坏情况分析	工程	×	×	√	○	×
元器件、材料和工艺控制	工程	Δ	Δ	√	√	√
可靠性关键项目	管理	×	Δ	√	√	√
确定功能试验、包装、贮存、装卸、运输及维修影响	工程	×	Δ	√	√	○
环境应力筛选	工程	×	×	√	√	√
可靠性研制与增长试验	工程	×	Δ	√	√	×
可靠性验证试验	工程	×	×	Δ	√	Δ
注：√表示适用；Δ表示选用；○表示设计更改时应用；×表示不适用。						

4.2 卫星可靠性设计应遵循的准则

卫星可靠性设计应遵循的准则有：

a） 在确定卫星总体、系统、分系统及设备方案时，应对性能、可靠性、经济性、安全性等指标充分运用最佳设计方法和综合权衡优化设计技术；

b） 优先选用在实际任务环境中经过考验、验证、技术成熟的技术方案、硬件和软件，充分考虑产品设计的继承性，支持对提高产品可靠性有利的技术进步；

c） 简化设计：尽量简化系统配置，减少硬件和软件的数量和规模；

d） “三化”（通用化、系列化、组合化）设计：多采用标准部件、组件、元器件、组装件和接口，减少元器件型号、规格及生产厂家；

e） 冗余设计：采用合理的硬件、软件的冗余设计，尽量消除单点失效；

f） 环境防护设计：充分进行环境影响分析，实施硬件和软件的环境防护设计（热设计、电磁兼容设计、抗辐射设计、防静电放电设计、防振防潮设计等）；

g） 降额设计：对电子、电气和机电产品或元件采用降额设计、电路容差设计及最坏情况设计、防瞬态设计；

h） 裕度设计：对非电产品开展裕度设计；

i） 卫星电子产品可靠性设计准则参照 QJ 2668—1994 执行；

j） 新技术、新器材必须经过充分论证、试验和鉴定，方能引入新产品设计。重要零、部（组）件必须经检测、试验、鉴定合格后，方能装机进行整机试验。

4.3 权衡分析

权衡分析是在一系列约束下的系统最优化问题，是设计过程的一个基本组成部分，从系统级的参数开始向设备设计的具体参数依次进行权衡分析。

方案设计阶段，权衡分析在大范围的系统参数中进行，例如权衡性能、费用、进度及风险等参数，以获得最优的方案，随着设计的深入，要求进一步确定指标，权衡分析在更低一级的系统参数中进行。如可靠性、维修性、可用性、安全性、保障性及寿命周期费用。当参数值（指标）确定后，在每个参数内进行权衡。例如在可靠性权衡分析中，人们可选用下述备选方案以获得一个满足设备可靠性要求的设计：更可靠的元器件；设计简化；元器件降额；冗余。即使在每一个参数中也还需进行进一步权衡分析，如冷备还是热备；分系统、设备冗余还是元器件、组件冗余。

权衡分析的基本步骤是：

a） 确定权衡的问题，建立权衡准则及约束条件；

b） 综合备选的设计方案；

c） 分析备选设计方案；

d） 根据权衡准则评定分析结果，以消除超出限制边界的那些分析结果；

e） 选择满足权衡准则及限制边界的备选方案，或重定备选方案，重复步骤 b）到 e），以取得新的解答。

5 可靠性指标论证

5.1 概述

卫星可靠性设计面临的首要问题是明确它的可靠性目标要求（通常这些要求是定性与定量相结合的），通过卫星设计、研制、生产和试验过程的努力，把可靠性作为一个重要方面“引入”系统或产品之中并最终实现这些目标。

卫星可靠性定量要求的工作就是可靠性参数的选择和指标确定的工作，它直接关系到卫星执行任务能力的提高和全寿命周期费用的节省，是影响卫星可靠性的关键因素之一。卫星可靠性定量要求的工作主要应明确下述几点：

a） 可靠性参数选择；

b） 可靠性指标确定；

c） 可靠性定量要求与型号论证、研制工作的关系。

可靠性工程发展的一个重要标志是产品可靠性定量要求（即参数的选择和指标的确定工作）的出现。它是在总结长期工程实践经验，并伴随着近代数理统计学和系统论发展的基础上的产物。它对推动装备

研制目标的实现是一个大的进步。可靠性定量要求可以对产品的设计和实物取得比较确切的、可予验证的科学度量，减少单纯定性要求（例如“可靠性尽量高”等）的不确定性、模糊性。

卫星可靠性定量要求工作的实施主要应依据国家军用标准GJB 1909—1994。这个系列标准包括总则、导弹和运载火箭、核战斗部、卫星、军用飞机、舰船、装甲车辆和军用汽车、火炮和弹药共九项标准。系列标准根据不同装备的共性和自身特点对定量要求中的可靠性、维修性参数的选择原则与方法，指标量值确定的原则与方法，以及这项工作在研制过程中的实施办法作出了比较明确的规定。其中GJB 1909.4—1994“卫星”是GJB 1909—1994标准的一项，卫星的可靠性参数选择和指标确定工作的开展应同时遵循GJB 1909.1—1994“总则”和GJB 1909.4—1994“卫星”这两个标准的要求。

就一般的系统或产品而言，表述系统可靠性和维修性的参数是直接与战备完好、任务成功、维修人力及保障资源有关的。这里提出了一个重要的概念，即系统或产品完整的可靠性维修性的规定和度量通常并不是单一的表述。为了满足对装备可靠性维修性不同的要求，应当从四个独立的方面，采用直接与下述四方面有关的参数加以度量：

a） 战备完好的可靠性维修性参数：规定或实现可靠性、维修性对系统或设备的战备完好应有的作用，它们涉及到不能投入使用的故障出现的概率和排除此类故障使系统得以恢复所需的努力。例如可靠性参数的平均不能工作事件间隔时间，维修性参数的平均恢复时间。

b） 任务成功的可靠性维修性参数：与系统任务期间偶然（随机）故障出现的概率有关的参数。例如可靠性参数的可靠度 $R(t)$、故障率 $\lambda(t)$、故障前平均工作时间（MTTF）等， 维修性参数的平均维修时间、平均修复时间等。

c） 维修人力费用的可靠性维修性参数：由可靠性和维修性决定的系统维修人力费用部分。例如可靠性参数的平均维修间隔时间，维修性参数的维修工时率。

d） 综合保障费用可靠性维修性参数：实现系统可靠性和维修性所需消耗的保障器材、物资、人力的度量。

通常，系统或产品的可靠性维修性应有两类参数——使用参数和合同参数，并且这两类参数之间通常存在一定的转换关系。使用参数是直接反映对系统或产品的使用需求的可靠性维修性参数；合同参数是在合同和研制任务书中表述使用部门对系统或产品可靠性和维修性要求，并是研制单位在研制生产过程中能够控制的参数。但卫星的这两类参数之间没有差别，因此也不存在转换的问题。卫星飞行产品的数量极少，要求一次成功，并通过地面充分试验验证与改进设计过程加以保证。卫星不同于有些装备（如飞机、导弹与运载火箭），经过一个试生产、试用阶段，进一步在现场环境下暴露设计与工艺等问题，经过改进，使产品实现可靠性增长，进入成熟期，达到目标值（或规定值）。因此从很大程度上讲，必须要求卫星一上天就投入实际使用，就达到目标。由于这种首颗星存在较大技术风险的客观事实，研制单位与用户间往往在文件中采用门限值（或最低可接受值）。

可靠性维修性指标就是对应参数的量值。就指标而言，存在使用参数的门限值、目标值和合同参数的最低可接受值、规定值。其中门限值或最低可接受值是系统或产品必须达到的，而目标值或规定值是系统或产品被要求达到的。目标值是规定值确定的依据，而门限值则是最低可接受值确定的依据。

5.2 卫星可靠性参数的选择

5.2.1 参数选择的原则和方法

卫星可靠性参数选择应考虑：系统或产品的类型和复杂程度；系统或产品的使用要求；以及考核或验证方法。

一般情况下卫星对战备完好性没有苛刻的要求，在这些方面通常不提出严格的定量要求值，它们对战备完好率要求也不作专门强调。

复杂的系统或产品由许多分系统组成，为了全面描述反映系统或产品特征的可靠性要求，需要采用较多的参数去描述。如卫星的一般电子系统可以用MTTF表示，但姿态与轨道控制的推力器则用工作总次数和总时间表示，电源系统镉镍蓄电池用对应一定的放电深度下的充放电次数表示，帆板展开机构（一次性）和星箭包带火工品则用成功率表示。

现阶段我国的卫星在轨道运行期间是不可修复的，即卫星在任务期间不能维修，因此不宜选用与任务成功有关的维修性参数，也不宜选用与维修保障费用有关的参数。

可靠性参数与指标的提出应当与产品的验证方法相对应，使初始提出的要求参数和量值能通过适当的验证加以确认。没有适当科学的验证方法作基础的参数和指标实际上是不可实施和操作的，因此也是没有实际意义的。

不同的系统或产品，其生产数量可以有很大的差别，下属的分系统、设备在研制鉴定中生产的数量也有很大差别。生产数量较多的产品可以通过统计试验的方法去验证，而生产数量极少的产品多是利用元器件经验数据通过分析预计方法加以验证。卫星基本上属于后者。卫星只有一至两颗，卫星的电子设备如星载计算机、姿态与轨道控制测量与执行部件、测控发射机和接收机（或应答机），电源控制电路等工程鉴定设备一般只有两台左右。这些产品只能通过分析的方法对指标加以验证；但卫星上所用的火工品爆炸螺栓，机构的轴承有可能生产几十个，甚至几百个，因此对它们的可靠性指标可以进行必要的实物试验验证。

卫星可靠性参数应根据型号特点，按表2选择。表2列举了卫星任务可靠度、在轨工作可靠度、在轨工作寿命、平均任务持续时间、单点失效概率、在轨测试交付可靠性和返回式卫星返回可靠度等七个与任务成功有关的可靠性参数，三个与卫星贮存有关的可靠性参数。表2分别说明了这些参数的类型、不同等级产品（系统、分系统、设备）适用范围，明确了这些参数的使用频繁和重要程度（优选、适用和不适用），但要强调两点：

a） 应以保证卫星在轨任务成功性为重点，卫星在轨工作寿命及轨道工作可靠度一般是必选参数；

b） 卫星在轨运行不能维修，因此没有维修性指标要求，但应提出星载设备在研制试验和发射场测试中便于维修更换的要求，以及卫星在轨故障对策要求。

表 2　卫星可靠性参数选用表

序号	参数名称	类型		使用范围										反映目标	
		使用参数	合同参数	卫星	有效载荷如通信、导航等	卫星服务系统 结构	电源	热控	测控	控制	推进	返回	设备级	任务成功性	保障费用
1	任务可靠度	√	—	★	★	★	★	★	★	★	★	★	★	√	—
2	在轨测试交付可靠度	√	—	Δ	Δ	—	Δ	—	Δ	Δ	Δ	—	—	√	—
3	在轨工作可靠度	√	√	★	★	★	★	★	★	★	★	—	★	√	—
4	在轨工作寿命	√	√	★	★	★	★	★	★	★	★	—	★	√	—
5	返回可靠度	√	√	★	Δ	—	—	—	—	—	—	Δ	—	√	—
6	平均任务持续时间	√	—	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	—	√	—
7	单点失效概率	√	—	—	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	√	—
8	贮存寿命	√	—	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	—	√
9	贮存期测试周期	√	—	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	—	√
10	贮存可靠性	√	—	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	—	√
注：★表示优选参数；Δ表示适用参数；√表示适用的参数类型和反映目标。															

表2的七个与任务成功有关的可靠性参数中除在轨工作寿命和单点失效概率外，其余五个均属可靠度。主要的区别是寿命期的时间区域和相应环境剖面、任务剖面的不同。

表 2 中参数说明：

a） “ 任务可靠度 ” 的时间从发射到在轨工作终期，包括发射，转移轨道（仅适用于地球同步轨道卫星），轨道运行，以及返回与着陆（仅适用于返回式卫星）。

b） “ 在轨测试交付可靠度 ” 是卫星进入工作轨道，建立了正常的工作模式之后，在交付用户之前，由研制单位为主对卫星系统和有效载荷、服务系统的功能、性能进行全面测试评定阶段的可靠度。根据卫星任务要求，卫星在轨测试设置种种工作模式主要通过卫星遥测和有效载荷数据（如遥感器、通信转发器等输出信息）分析作出判断。测试交付持续时间因不同卫星而异，资源卫星约持续两个月。

c） “ 在轨工作寿命 ”：卫星进入工作轨道，开始任务运行至工作结束的时间。

d） “ 在轨工作可靠度 ” 是卫星在轨工作寿命期的可靠度。它包括卫星工作寿命期内的各种预定工作模式的实施。如通信广播卫星的转发器工作、轨道保持；遥感成象卫星的成象、记录、传输、相机的定标、侧摆、调焦等。

e） “ 返回可靠度 ”：是返回式卫星所特有的反映任务成功一部分的可靠性参数。其时间从卫星第一个执行返回有关的遥控指令始，至返回舱着陆止。涉及的分系统包括姿轨控、推进减速发动机、测控（含星上数据管理），结构（返回舱、舱间分离火工品）、热控(再入大气层防热）、减速降落伞和信标机等分系统和返回设备。

f） “ 平均任务持续时间 ”(MMD）是综合反映卫星在轨工作可靠性和在轨工作寿命的一个任务成功的可靠性参数。这一参数可用于卫星系统分析中，以寿命单位评价卫星的任务成功可靠性。

g） “ 单点失效概率 ” 是卫星单点失效环节在轨工作寿命终期的失效概率。

表 2 中的三个与贮存有关的可靠性参数是贮存寿命、贮存可靠性和贮存期测试周期。目前对卫星贮存可靠性的定量要求的验证方法尚待作进一步研究，主要是贮存期元器件的失效率数据尚欠缺。因此这一参数可作备选参数，在条件成熟时使用。

5.2.2 参数选择说明

5.2.2.1 卫星可靠性参数的多样性

卫星的可靠性参数原则上应当反映工作准备完好性（即战备完好性）、任务成功和维修、保障费用四个方面。但是如前所述，我国现阶段的卫星尚不能达到在轨维修的程度，本质上它是一个不可修复的系统。随之而来的是维修保障费用的有关参数是不适用的。因此这四个方面的参数，在现阶段实际只有两个方面可供我们选用，即战备完好性和任务成功方面的参数。

5.2.2.2 卫星可靠性参数以任务可靠度为主

卫星没有单独就战备完好性提出相应的参数。客观上卫星战备完好性是存在的，对卫星应当有这样的要求，即一旦火箭发射命令下达时，卫星应当处于完好的状态。但是卫星发射前的测试允许持续的时间一般是比较充裕的，卫星发射窗口（即每天允许的发射时间区间）一般也没有十分苛刻的要求。此外，卫星大部分入轨后工作的设备将通过遥控或程控适时开机工作。这种情况有别于某些突发性工作的系统。因此保证卫星任务完好性本质上与保证卫星任务可靠性的要求没有差别。如果我们把握了任务成功可靠度这个参数，应当说卫星战备完好性也就把住了。

卫星强调以保证卫星在轨任务成功为重点，卫星在轨工作寿命及在轨工作可靠度通常是必选的参数。这是根据卫星的特点，并借鉴国外卫星型号工程的经验提出的。即在任务成功这个重点方面，任务可靠性中的在轨工作可靠度是表述卫星可靠性的主要参数。尽管卫星各分系统的构成和寿命分布有所不同，但大部分设备均可采用指数分布的寿命模型（即失效率λ为常数），可以比较方便地取得相应的分析数据和可靠度结果。对卫星上使用的火工品这样的较低层次产品，它们服从二项分布，同样可以用可靠度进行度量。

5.2.2.3 选择任务可靠度的原因

卫星相对比较单一的可靠性参数选择除了上述不可修复和对战备完好无苛刻要求外，还有四个原因：

a） 任务成功的可靠度可以比较全面地表述卫星系统和分系统设备的可靠性特性；

b） 这种可靠度度量方法有比较成熟的分析技术，便于在工程上推广应用；

c）卫星的极小子样特性排除了系统通过试验验证其可靠性的可能性，只能通过分析验证的方法实现；迄今为止，分析验证能取得较多相对可靠、可用于分析的基础数据也正是指数分布的元器件和非电元部件的失效率；

d）“卫星任务可靠度”中包含的发射时间（一般中低轨道几分钟至十几分钟，地球同步轨道卫星转移轨道持续时间数天）与在轨工作时间相比是很短的，即使考虑发射段环境带来的不利影响，对于长寿命卫星而言，它们对系统全寿命期中的可靠性定量评价的贡献甚小。

5.3 可靠性指标的确定

5.3.1 可靠性指标确定的依据

卫星及其各级产品可靠性指标的确定是一个过程，它们是卫星的使用需求与实际可能权衡研究的结果，是对过去、现在和将来技术能力、水平及资源利用等诸多因素的综合分析的产物。

卫星可靠性指标确定应依据的基本因素是需要和可能，具体而言是使用需求、相似产品的可靠性水平和预期采用的技术使卫星可能达到的可靠性水平。

通常一个新系统或产品可靠性指标的确定是在系统方案设计后期。此时可供分析决策用的信息是十分有限的。采用相似产品的比对分析，可以获得相对可信的可靠性现状数据。它是指标确定中，对新系统或产品的潜在能力进行分析的一个重要信息源。

预期采用的技术（如确定用大规模集成电路取代大量分立半导体器件）将可能对新系统或产品的可靠性带来重大影响，这是新系统或产品指标确定中潜在能力分析的又一重要的信息源。

5.3.2 指标表述的完整性

5.3.2.1 概述

在提出卫星可靠性定量要求的同时，应当明确其：

a） 寿命与任务剖面；

b） 故障判别准则；

c） 指标的验证方法；

d） 约束和假设条件。

对采用试验或现场使用验证的应包括置信水平，接收/拒收判据。由于指标的阶段性还应当明确达到指标的时间（或阶段）。这些内容明确的要求都是使指标具有确切含义所必不可少的。

5.3.2.2 关于寿命剖面和任务剖面

寿命和任务剖面首先应当包括卫星的使用条件和环境，包括温度、振动、冲击、压力、粒子辐照等。使用环境的不同，可靠性不同。同一辆卡车在城市公路上行驶和在高低不平的山路上行驶，其可靠性显然是不同的；电子设备在野外环境使用和在实验室环境的应用可靠性也是不同的。

任务剖面还应包括卫星经历的事件，任务阶段工作模式和持续的时间。同样一颗卫星，其在轨工作寿命不同，可靠性也不同；工作模式的变化直接关系到星上不同设备的不同组合和工作时间的差异（如遥感光学成象卫星相机照相，数据传输系统开关的频繁程度和持续时间），这些都将影响到相关产品的可靠性。

因此只有寿命剖面和任务剖面的确定，可靠性指标才是有意义的。

5.3.2.3 关于故障判别准则

不同的卫星型号，其任务成功或失败的判别依据，可以有很大的差异。有时我们考虑其技术的成熟性或在完成卫星主要任务的同时有一些“ 搭载 ”项目。这些项目或定为试验项目或将它们列入非关键项目，即它们的成败并不影响主任务的完成。我们在卫星成功/失败准则中应当对之明确地加以规定，即卫星的成败与这些项目无关。这样对应的卫星任务成败的可靠性模型就不包括这些单元。其确定的系统可靠性定量要求与假如把这些项目都考虑进去（即假设它们直接与卫星成败有关）的结果是不同的。

另一种情况是构成卫星主要系统中的若干单元的失效可能会在一定程度上影响到系统的次要功能或某些非本质的性能指标的降低。例如某中低轨道卫星，滚动与俯仰各有一台红外地球敏感器。在正常时，它们各自独立完成自己的测量功能：测量地球弦宽以确定这两个轴的卫星姿态。如果系统设计考虑了一旦任意一个红外地球敏感器失效后，两轴姿态测量基本功能将由一个正常工作的敏感器通过测弦宽和弦中独立完成。虽然测姿精度有所下降，但可能在系统性能允许的偏差范围内。同样两个红外地球敏感器构成的单元，系统设计有无单机可独立完成两轴姿态测量功能的考虑，二者可靠性是并联与串联的关系，可靠性定量指标是不同的。

因此故障判别准则，即任务成功判别准则，是可靠性指标确定的另一个不可缺少的工作内容。

5.3.2.4 关于验证方法的确定

确定的可靠性指标目标是否真正实现了，应当有适当的方法去验证。没有验证的要求是无法检查的要求，实际上是空洞的要求。因此验证是指标实现的检查和确认。

不同的系统或产品可靠性指标的验证方法是不同的。如前所述，卫星的定量验证只能通过分析的方法，即利用元器件等的经验数据和概率统计分析进行可靠性预计的方法来实现。它不同于某些其他系统或产品强调试验与使用验证，强调现场使用实际指标的获取。

5.3.2.5 关于其他假设和约束条件

卫星定量要求实际包括的产品范围是有一定限制的：电子、电气和机电，以及部分有失效率数据的非电设备和部件。卫星可靠性定量要求原则上不包括星体主结构、设备的非活动机械结构部分（如机壳、光学玻璃、天线本体）等，因为这些项目没有可供分析验证使用的基础定量数据。

假设和约束条件还包括失效分布假设（一般设备：指数分布，火工品：二项分布等）、元器件失效率数据、分析预计采用的方法等。

这些假设和约束条件都是为了更确切地定义和验证指标的。

完整准确的指标表述是为了给指标以单一的、含义清晰的解释或理解，使用户和研制单位有明确和统一的认识，因此它也是真正实现预期目标所必需的。

5.4 可靠性参数选择和指标确定的工作内容、方法和程序

可靠性是产品的诸多属性的一种，必须不失时机地设计到产品中去。只有处理好、衔接好与系统或产品论证设计过程中的其他各项工作的关系，才能既不超前，也不延迟做好相应的工作，顺利地达到预定的目标。

卫星在论证和工程研制阶段的可靠性参数选择和指标确定的程序、工作内容、工作职责和注意点概括起来有以下几个要点：

a） 可靠性参数选择和指标确定从论证阶段开始，到方案阶段确定。它是一个由粗到细，逐步深化的过程。工程研制主要的任务是跟踪管理，保证这些指标的实现。

b） 可靠性参数选择和指标确定是用户和研制单位共同的责任。整个工作是不断沟通和协调的过程，在阶段上又有所侧重。总的程序是由用户到研制单位，根据卫星论证与研制过程可获取的相应信息的多少，以及与项目工程管理的程序相吻合的原则提出。

在早期指标论证阶段，以用户为主完成，包括：

1） 对相似型号的可靠性状态进行分析；

2） 使用和寿命剖面及使用保障条件的确定；

3） 可靠性参数和指标建议的提出；

4） 纳入战术技术要求文件。

在方案阶段，应由研制单位为主完成，包括：

1） 进行可靠性设计、分析；

2） 确定合同指标；

3） 进行指标分配；

4） 纳入相应的合同文件。

在工程研制阶段主要应由承制方通过一系列工程设计研制和有效的管理及严格控制实现目标的要求。

c） 卫星在战技指标和可行性论证的同时应选择可靠性参数，开展任务需求分析，进行初步预测。

d） 卫星在方案阶段应确定寿命和任务剖面，开展故障对策分析，建立故障判据，开展权衡分析，通过可靠性建模、预计确定和分配指标，并纳入相应的文件。

5.5 卫星论证阶段可靠性指标论证的工作内容

GJB 1909.4—1994附录中的示例反映了卫星研制工作的现状，说明了研制单位可靠性指标论证的工作内容。在卫星论证阶段主要有两项工作。

5.5.1 使用需求论证

由使用部门与研制单位结合，初步提出卫星的任务和使用要求，开展需求和任务分析，提出卫星系统方案设想。

在此阶段可靠性方面尚不能提出定量的要求，但可以根据过去型号的经验确定拟选的可靠性参数。

5.5.2 可行性论证

研制单位根据初步使用要求，开展总体和分系统的可行性方案论证，进行多方案的分析比较，在此基础上初步确定卫星总体的主要功能、构成和技术指标（包括可靠性），初步确定卫星与运载火箭、地面测控与应用系统等的接口，初步明确卫星的任务阶段、时间、主要工作模式、环境条件、设备工作时间或循环次数，提出卫星成功或失败判据。

此阶段可靠性方面应搜集相应或相同设备的可靠性数据和元器件的失效率数据，根据已初步明确的卫星技术状态进行初步可靠性建模，预计分析。对卫星可靠性水平或潜在能力有一个初步的预测，在此阶段，特别是对冗余技术的应用和元器件质量等级的确定，要在分析基础上提出明确的意见。并且以此为基础，提出卫星定量要求的设想和向分系统进行指标分配方案设想。

总体与分系统综合各种分析，开展关键技术的设计和原理样机的攻关研制试验，包括可靠性的一些关键问题（如活动部件的可靠性关键，基础上设计试验验证），对方案的可行性作关键实物验证。

5.6 方案阶段

卫星的总体和分系统技术指标得到更深入的论证，技术状态通过设计分析和模样机的研制进一步确定，可行性实物验证的信息反馈到系统方案中。

可靠性工作方面可以确定卫星的寿命和任务剖面，搜集攻关和模样机实物的硬件组成信息（元器件品种规格和数量，冗余配置等）。在前一阶段明确卫星成败判据的基础上，借鉴相似、相同产品的可靠性数据，具备了更深入开展可靠性建模和预计的基础工作。

应当说通过两项预计所获得的可靠性指标和分系统的分配值是有相当可信程度的。

综上所述卫星的可靠性参数和指标确定的工作应当建立在必要的历史数据和分析设计的基础上，它是参与系统权衡分析的最后产物，是系统设计不断深化的产物。

通过上述过程我们不难看出，卫星可靠性参数选择相对比较简单，而指标确定的前提条件是卫星基本技术状态（功能、性能和主要接口）的确定和产品、元器件可靠性经验数据的获取。关键是建立在基本确定的技术状态基础上的可靠性模型建立和预计分析。正确的建模和预计是卫星可靠性指标确定的主要基础，也是卫星最终可靠性指标验证的主要依据。

可靠性参数指标确定工作从总体上看是与其他技术工作同步进行的，经过多次迭代的过程，使卫星系统的综合指标达到满足使用部门需求的相对优化目标。卫星可靠性参数和指标的确定工作是卫星可靠性工程的一项工作。论证工作的核心是在把握卫星的任务需求和使用需求的前提下，以适当的形式参与权衡分析，把对卫星设计和研制的可靠性要求以定量的方式明确下来，再通过工程研制阶段的设计把这些要求落实到卫星各级产品中去。

5.7 注意事项

5.7.1 完整理解卫星可靠性要求及验证

卫星的可靠性定量要求是卫星可靠性要求的重要方面。但是在强调定量要求的同时，我们必须高度重视定性要求和相应的验证方法的实施。只有这两者的结合才能真正全面把握卫星的可靠性。卫星这种特殊的装备有一次成功，高可靠性的要求，它们的研制周期一般较长，产品价格昂贵，生产数量极少。严格的设计、分析、生产研制要求和有限试验及信息的充分利用对于保证卫星最终产品的高可靠是非常必要的。在某些情况下定性的工作要求对于高可靠性实现可能更为重要和关键。

基于上述原因，在卫星可靠性设计和验证方面，强调了定性要求和分析验证的内容。应通过各级产品的可靠性预计、故障模式和影响分析、研制试验和可靠性试验、故障报告系统活动来完成可靠性验证，并通过可靠性预计完成可靠性指标的分析验证。通过故障模式和影响分析查明各种故障模式原因，并采取补偿措施以改进可靠性，重点是查明单点故障模式，消除或减少其影响，从而定性地评价卫星可靠性。明确树立定量与定性相结合的要求和验证的完整概念是十分重要的。即卫星的可靠性要求不能等同于定量要求。卫星可靠性要求验证的两个特点是：不采用统计试验验证方法；定量与定性设计分析和各种试验故障处理信息的综合评定。

5.7.2 卫星没有维修性定量要求，不等于没有维修性要求

卫星没有任务期间的维修要求，因此不存在定量维修性参数和指标。但是卫星没有定量维修性要求，不等于没有维修性要求。卫星在研制阶段存在维修性问题，这些问题必须在产品设计中加以考虑。维修性作为卫星产品保证的一个独立部分，同样有许多值得重视和必须完成的设计、分析工作。卫星维修性是指地面总装、测试和试验中对其故障可修复的一种特性。在卫星各级产品设计中应重视其维修性设计。如设备/部件的总体布局和设备/部件内部组件的布局应充分考虑修理与更换的良好可达性，努力避免拆卸时对其他部分的影响；装配方法应力求简便易行快捷；又如努力提高产品的互换性与通用程度，采用模块化设计，努力实现冗余件与备用件在状态（含接口）上的一致性；紧固件的标准化和防止安装时失落星内、难以觅寻措施；努力减少特种工具；设置设备贮存期间测试所需的外部检测点；降低对维修的技能要求等。卫星地面保障的电气和机械设备(EGSE和MGSE）的标准化、通用化和提高自动化测试记录或操作水平，设置必要的机内检测的故障自检功能等。

在轨运行中，卫星姿态失稳，建立应急模式或系统重构，或主份失效切到备份等，或软件的重新注入等，虽然为卫星故障的修复，但更多地应将它们理解为可靠性的问题：通过可靠性硬件冗余、容错或系统重构，纠正故障或采取相应的补偿措施。

6 可靠性模型的建立

6.1 概述

系统是由相互作用和相互依赖的若干组成部分结合成的具有特定功能的有机整体。可靠性模型是指系统可靠性逻辑框图及其数学模型。

可靠性模型包括系统、分系统或功能组件的可靠性框图及数学模型。可靠性框图应与功能框图和技术状态相一致。可靠性框图内使用的产品名称、代号应与功能框图、产品规范中所使用的名称相一致。

可靠性数学模型是用概率统计等数学理论对可靠性框图的数学描述，其输入和输出应适合所分析对象的输入、输出要求。对所有环境来说，系统可靠性模型都一样，但系统中不同设备的失效率会随环境的不同而不同。

当系统要经历几个工作阶段时应该针对每一个工作阶段建立单独的可靠性模型，然后再建一个系统模型。可靠性模型应随着研制工作的进展、随着任务剖面的改变而不断地加以修改、充实和完善。

卫星可靠性建模工作应从方案阶段开始，在方案阶段就应有整星和分系统的可靠性模型。

GJB 813—1990关于可靠性模型建立的步骤与方法适用于本标准。

6.2 目的

建立系统可靠性模型的目的如下：

a） 进行可靠性指标分配、可靠性预计以便进行设计调整，选择最佳设计方案；

b） 评定卫星产品的可靠性；

c） 故障模式、影响及危害性分析等。

6.3 任务可靠性模型

卫星系统的任务可靠性系指卫星系统、分系统或功能组件在某一特定的任务剖面内完成其规定功能的能力。是与任务成功直接相关的一项重要参数。任务可靠性模型应能描述在完成任务中产品各单元的预定用途。预定用于冗余或替换工作模式的产品单元应该在模型中表示为并联结构，或适用于任务阶段及任务范围的类似结构。

任务可靠性模型包括一个任务可靠性框图和一个相应的任务可靠性数学模型。

6.4 步骤

6.4.1 产品定义

明确卫星系统构成及任务、功能要求；明确任务阶段、工作环境，发射与空间飞行阶段经历的主要事件及经历的时间；明确分析的层次及有关分系统、设备的功能、构成及任务；明确卫星系统、分系统任务成功判据及有关分析假设等。

产品定义的主要内容有：

a） 产品的目的、用途及任务；

b） 产品及分系统的性能参数和容许极限；

c） 产品的结构极限参数及功能接口；

d） 产品故障判据；

e） 产品的寿命剖面和任务剖面；

f） 规定分析层次，系统下属有分系统、设备等层次，应确定建立模型的最低层次。

6.4.2 建立可靠性框图

根据产品功能绘制可靠性框图；明确完成产品功能所需的单元并根据产品各单元绘制产品的可靠性框图。在可靠性框图中，明确系统各分系统、设备及单元的可靠性关系（串联、并联或表决等），标明各相关系统、分系统、设备及单元名称或代号。对框图可附加说明有关假设条件。

6.4.3 建立可靠性数学模型

选用合适的数学方法（如概率法、布尔真值法、蒙特卡罗法等），建立可靠性数学模型。对有关假设应进行说明。

6.5 卫星系统常用可靠性模型

6.5.1 串联结构

串联结构是可靠性数学模型中最简单、最常见的一种结构。串联结构中系统是否能正常工作取决于系统所有各部件是否正常地执行其功能。某一部件发生故障导致整个系统发生故障。串联系统可靠性框图见图1。串联结构中假设任何一个部件的故障在统计上与任何其它部件的故障或成功无关。在多数实际用途中这是最常见的情况。如果假设条件不成立，则必须采用条件概率计算。

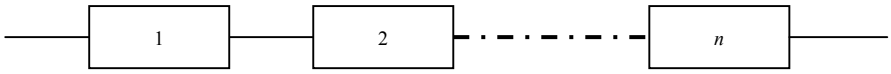


图 1　串联系统可靠性框图

在各单元的失效统计独立的条件下，系统可靠性R_S按式（1）计算：

$$R_S = \prod_{i=1}^{n} R_i \quad \cdots\cdots (1)$$

式中：

n——串联单元数；

R_i——第i单元的可靠性。

在所有单元都为指数寿命情况下，系统可靠性R_S按式（2）计算：

$$R_s = e^{-\sum_{i=1}^{n}\lambda_i t} \quad \cdots\cdots (2)$$

式中：

λ_i——第i单元的失效率。

在单元不是指数寿命情况下，系统可靠性R_s按式（3）计算：

$$R_s = e^{-\int_o^t \sum_{i=1}^{n}\lambda_i(t)dt} \quad \cdots\cdots (3)$$

6.5.2 并联结构

在可靠性数学模型中最常见的另一结构是并联结构。并联结构中，当所有部件都发生故障时，系统才发生故障。并联系统可靠性框图见图2。

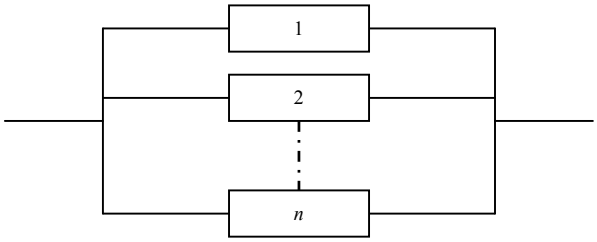


图 2　并联系统可靠性框图

并联系统可靠性按式（4）计算：

$$R_s = 1 - \prod_{i=1}^{n}(1 - R_i) \quad \cdots\cdots (4)$$

当单元为指数寿命时，并联系统可靠性按式（5）计算：

$$R_s = 1 - \prod_{i=1}^{n}(1 - e^{-\lambda_i t}) \quad \cdots\cdots (5)$$

6.5.3 贮备冗余系统

贮备冗余系统一般有冷贮备（无载贮备）、热贮备（满载贮备）和温贮备（轻载贮备）。贮备系统通常用n+1个单元和一个高可靠转换开关组成，一个单元工作，n个单元作贮备。当工作单元失效时，转换开关把一个贮备单元接入，系统继续工作。这样直到所有单元都失效时，系统才失效。

贮备冗余系统可靠性框图见图 3。

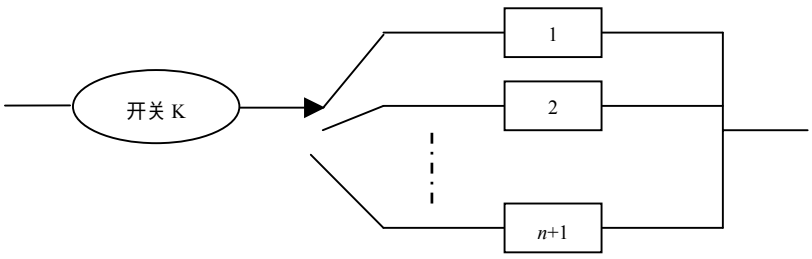


图 3　贮备系统可靠性框图

6.5.3.1 冷贮备

对于冷贮备，设转换开关完全可靠，单元为指数分布，则系统可靠性按式（6）计算：

$$R_{\mathrm{s}} = \sum_{i=1}^{n+1}\left[\prod_{\substack{j=1\\ j\neq i}}^{n+1}\frac{\lambda_{\mathrm{j}}}{\lambda_{\mathrm{j}}-\lambda_{\mathrm{i}}}\right]e^{-\lambda_{\mathrm{i}}t} \quad \cdots\cdots (6)$$

各单元失效率相同为 λ 时，系统可靠性按式（7）计算：

$$R_{\mathrm{s}} = \sum_{i=0}^{n-1}\frac{(\lambda t)^{\mathrm{i}}}{i!}e^{-\lambda \mathrm{t}} \quad \cdots\cdots (7)$$

转换开关不完全可靠，其可靠性为常数R_{k}时，

n个相同指数单元，系统可靠性按式（8）计算：

$$R_{\mathrm{s}}(t) = \sum_{i=0}^{n-1}e^{-\lambda t}\frac{(\lambda R_k t)^{\mathrm{i}}}{i!} \quad \cdots\cdots (8)$$

n个不同指数单元且n=2，系统可靠性按式（9）计算：

$$R_{\mathrm{s}}(t) = e^{-\lambda_1 t} + R_{\mathrm{k}}\frac{\lambda_1}{\lambda_1-\lambda_2}(e^{-\lambda_2 t}-e^{-\lambda_1 t}) \quad \cdots\cdots (9)$$

开关服从失效率为λ_{k}的指数分布，两个不同指数单元时，系统可靠性按式（10）计算：

$$R_{\mathrm{s}}(t) = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1+\lambda_{\mathrm{k}}-\lambda_2}(e^{-\lambda_2 t}-e^{-(\lambda_1+\lambda_{\mathrm{k}})t}) \quad \cdots\cdots (10)$$

6.5.3.2 热贮备

对热贮备可按并联结构考虑。

6.5.3.3 温贮备

对温贮备，设系统各单元为指数分布、失效率相同，工作时单元失效为λ，贮备时单元失效率为μ，任意n，系统可靠性按式（11）计算：

$$R_{\mathrm{s}}(t) = \sum_{i=1}^{n}\left[\prod_{j=1,\,j\neq i}^{n}\frac{\lambda+(n-j)\mu}{(i-j)\mu}\right]e^{-[\lambda+(n-i)\mu]t} \quad \cdots\cdots (11)$$

n=2时，系统可靠性按式（12）计算：

$$R_{\mathrm{s}}(t) = e^{-\lambda t} + \frac{\lambda}{\mu}e^{-\lambda t}(1-e^{-\mu t}) \quad \cdots\cdots (12)$$

n=3时，系统可靠性按式（13）计算：

$$R_{\mathrm{s}}(t) = e^{-\lambda t} + \frac{\lambda}{\mu}e^{-\lambda t}(1-e^{-\mu t}) + \frac{1}{2}\left(\frac{\lambda}{\mu}+\frac{\lambda^2}{\mu^2}\right)e^{-\lambda t}(1-e^{-\mu t})^2 \quad \cdots\cdots (13)$$

2个不相同指数单元，开关指数失效率为 λ_{k} 时，系统可靠性按式（14）计算：

$$R_s(t) = e^{-\lambda_1 t} + \frac{\lambda_1 e^{-\lambda_2 t}}{\lambda_1 - \lambda_2 + \mu_2 + \lambda_k} - \frac{\lambda_1 e^{-(\lambda_1+\mu_2+\lambda_k)t})}{\lambda_1 - \lambda_2 + \mu_2 + \lambda_k} \quad \cdots\cdots\cdots\cdots (14)$$

6.5.4 表决系统（K-out-of-n:G）

表决系统也是一种冗余方式。系统由n个单元组成，而系统成功地完成任务只需要其中的k个单元工作，即是表决系统，即k/n结构。其中k小于n。

表决系统可靠性方框图见图4。

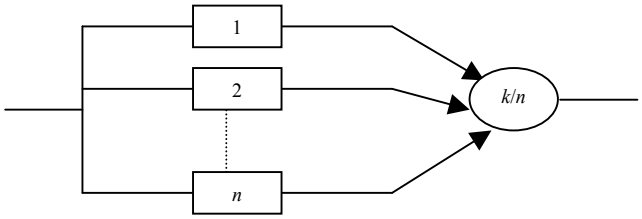


图 4 $k/n(G)$ 系统可靠性框图

在各单元可靠性相同的情况下，均为R_0，设表决器可靠性为R_m，则系统可靠性按式（15）计算：

$$R_s = R_m \sum_{i=k}^{n} \binom{n}{i} R_0^i (1 - R_0^i)^{n-i} \quad \cdots\cdots\cdots\cdots (15)$$

6.6 复杂网络可靠性模型

系统可靠性模型除上述串联、并联、贮备冗余和表决系统等典型结构外，还有复杂网络模型。对于这类复杂网络，一般可以用如下两种方法进行建模。

6.6.1 状态枚举法

该方法适用于n较小的场合。设系统由n个单元组成，每个单元的状态有正常（1）、失效（0）两种状态。系统的状态要么为1（正常），要么为0（失效），则系统共有2^n个状态。若系统正常的状态有m个，则系统的可靠性为m个状态的概率之和。

$$R_s = \sum_{i=1}^{m} p(s_i = 1) \quad \cdots\cdots\cdots\cdots (16)$$

一般采用表格进行计算(见表3)：

表 3 状态枚举法工作表

状态号	单元 1 状态	单元 2 状态	……	单元 *n* 状态	系统状态	概率
1						
2						
…						
n						
注：系统可靠性=所有系统状态为1的各项概率之和。						

6.6.2 全概率分解法

在系统s中选一单元x，令x的可靠性为$R(x)$，则根据全概率公式，系统的可靠性为：

$$R(s) = R(x)P(s|x) + (1 - R(x))P(s|\bar{x})$$

事件$s|x$及$s|\bar{x}$把系统s分成了两部分，简化了系统。如果事件$s|x$及$s|\bar{x}$还较复杂，则可在事件$s|x$及$s|\bar{x}$中再选定一个单元y，按全概率法继续分解为：$s|xy$、$s|x\bar{y}$或$s|\bar{x}y$、$s|\bar{x}\bar{y}$，直至方便计算为止。

如图5所示的复杂网络：

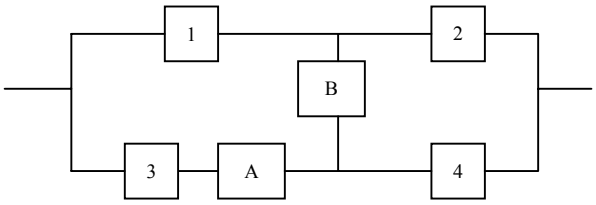
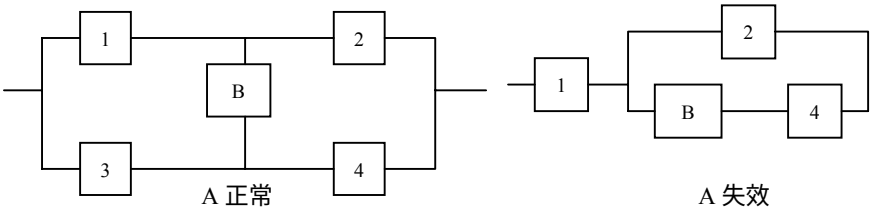


图 5　复杂网络系统可靠性框图示例

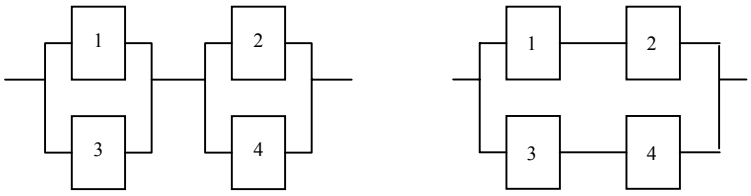
首先，以A为分解单元，将图5简化为以下两图(图6a)、图6b））：



a）　　b）

图 6　复杂网络系统分解可靠性框图

其次，以B为分解单元，再将A正常时系统的框图（（图6a））进行简化（图7a)、图7b）：



a）　　b）

图 7　复杂网络系统再分解可靠性框图

6.7　具有多功能单元的系统可靠性模型

在系统中的某一单元可能具有多种功能，且在系统中重复出现。在这种系统中，单元之间不独立。对于具有多功能单元的系统，可靠性建模的一般方法是：

a）　按前述的可靠性建模方法建模；

b）　按$R^n=R$简化模型。

考虑如下可靠性框图（见图8）：

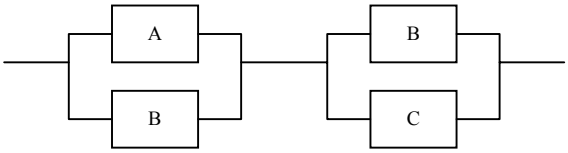


图 8　多功能系统可靠性框图

则系统的可靠性模型为：$R_s=（R_a+R_b-R_aR_b）（R_b+R_c-R_bR_c）=R_b+（1-R_b）R_aR_c$

在模型简化中，用到了$R_b^2=R_b$。

6.8　注意事项

可靠性建模应注意：

a）　对不同的任务（工作模式）应分别建模；

b）　应根据产品工作原理、对任务可靠性的影响及逻辑关系建立模型，特别是对有冗余的情况，应判别清楚是哪一种冗余；

c）　应约定所分析对象的产品层次，将模型建到所约定层次；

d）　约定层次越低，模型越复杂，但对冗余设计考虑得越充分，故建模中应尽量往下延伸；

e）　卫星总体单位应注意各分系统之间的交叉冗余情况。

7　可靠性分配

7.1　概述

卫星系统可靠性指标分配是指系统可靠性指标按照一定的原则和方法分配到规定的层次（分系统、设备/部件等）。可靠性分配与可靠性预计相互迭代，不断完善。预计结果可作为进行可靠性分配的参考。

7.2　目的

可靠性指标分配的目的是将可靠性的定量要求分配到规定的较低产品层次，以保证系统可靠性要求的实现。具体表现为：

a）　落实系统可靠性指标；

b）　确定分系统／设备的可靠性指标。

7.3　原则

可靠性分配的一般原则如下：

a）　复杂度高的产品，分配较低的可靠性指标；

b）　技术上成熟、继承性好的产品，分配较高的可靠性；

c）　处于较恶劣环境的产品，分配较低的可靠性；

d）　重要度高产品，分配较高的可靠性；

e）　考虑其它指标，优化设计、综合权衡；

f）　可靠性分配后，必须确保留有一定余量。

7.4　步骤

可靠性分配的步骤如下：

a）　设计（更改）信息：产品设计或设计更改情况；

b）　确定被分配的指标值：需要分配的系统可靠性指标量值；

c） 建立（修正）系统可靠性模型：根据分配的需要建立系统可靠性模型（见第 6 章），或根据设计更改修正可靠性模型；

d） 选用合适的分配方法，逐级将指标分配到各分系统、设备等：将系统可靠性指标分配到所要求的产品层次；

e） 各级可靠性指标：得到不同层次产品的可靠性分配结果；

f） 是否满足使用要求：将可靠性分配值与使用要求进行分析对比，若满足要求，则分配工作结束，否则，进行再分配，直至满足要求。

可靠性分配的步骤流程图见图9。

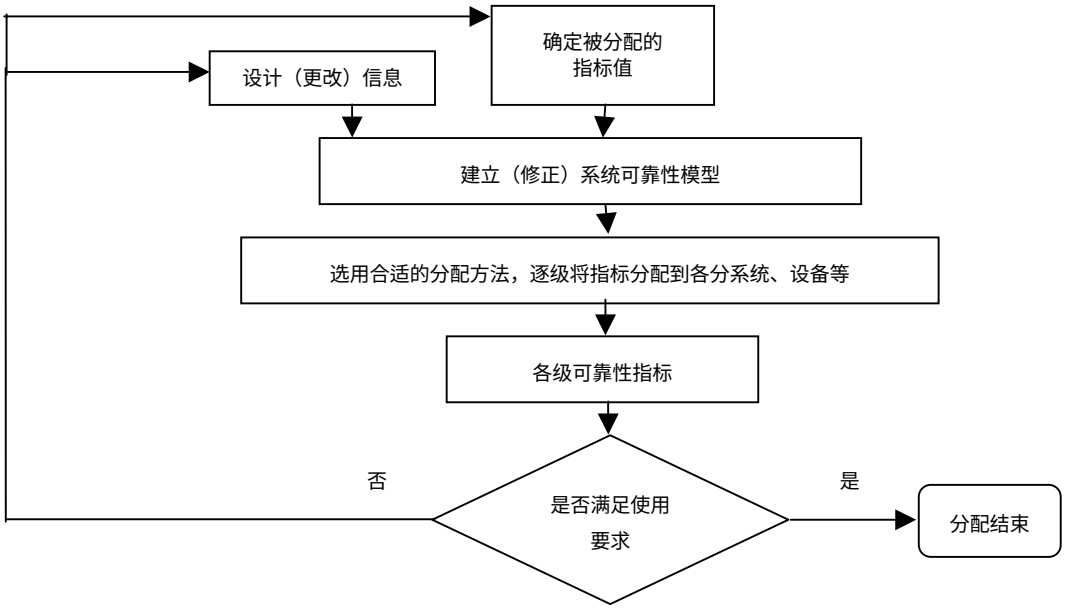


图 9　可靠性分配的步骤

7.5　方法

7.5.1　等分配法

串联系统按式（17）进行分配：

$$R_i = R_0^{1/n} \quad \cdots\cdots (17)$$

式中：

n——分系统或设备串联个数

R_i——配给分系统的可靠性指标；

R_0——系统可靠性指标。

并联系统按式（18）进行分配：

$$R_i = 1 - (1 - R_0)^{1/n} \quad \cdots\cdots (18)$$

7.5.2　比例分配方法

这个方法适用于各分系统的任务时间与系统任务时间相同的串联系统。这种分析方法要求用失效率表示可靠性指标，且认为串联系统任务失效率正比于单元任务失效率。

a） 约束条件为式（19）：

$$\sum_{i=1}^{n} \lambda_i^* \leq \lambda_s \quad \cdots\cdots (19)$$

式中：

λ_i^* ——分配给第i个分系统的失效率；

λ_s ——系统要求的失效率。

b） 求出各系统的预计失效率 λ_i。

c） 求出加权因子 W_i 见式（20）：

$$W_i = \lambda_i / \sum_{i=1}^{n} \lambda_i \quad \cdots\cdots (20)$$

d） 求出分配给分系统 i 的失效率见式（21）：

$$\lambda_i^* = W_i \lambda_s \quad \cdots\cdots (21)$$

7.5.3 加权分配法（AGREE 法）

这种方法既考虑每个分系统的复杂性，也考虑其重要性。它适用于服从指数分布的电子设备，系统由k个分系统串联而成。第i个分系统的最低故障前平均工作时间见式（22）：

$$\theta_i = \frac{NW_i t_i}{n_i[-\ln R_0]} \quad \cdots\cdots (22)$$

相应的第i个分系统的可靠性见式（23）：

$$R_i(t_i) = \exp(-t_i / \theta_i) \quad \cdots\cdots (23)$$

式中：

t_i ——第i个分系统的任务时间；

W_i ——第i个分系统的加权因子，表示第i个分系统发生失效将导致系统失效发生的概率；

n_i ——第i个分系统中的组件数目；

N——系统中的组件总数；

R_0 ——系统可靠性指标要求；

$R_i(t_i)$ ——分配给第i个分系统的可靠性；

θ_i ——分配给第i个分系统的故障前平均工作时间。

7.5.4 比例组合法

如果一个新设计的系统与老的系统非常相似，也就是组成系统的各分系统类型相同，只是根据新的情况，对新系统提出了新的可靠性要求，那么我们就可以根据比例组合法由老系统中各分系统的失效率，按新系统可靠性的要求，给新系统的各分系统分配失效率，见式（24）。

$$\lambda_i' = \lambda_i \lambda_s' / \lambda_s \quad \cdots\cdots (24)$$

式中：

λ_i' ——分配给新系统中第i个分系统的失效率；

λ_s' ——新系统要求的失效率指标；

λ_i ——老系统中第i个分系统的失效率；

λ_s ——老系统的失效率。

7.5.5 评分分配法

这种方法是根据人们的经验，按照几种因素进行评分。由评分的情况给每个分系统分配可靠性指标。主要考虑四种因素（每种因素的分数在1～10之间）：

a） 复杂度。它是根据组成分系统的元部件数量以及它们组装的难易程度来评定。最简单的评 1 分，最复杂的评 10 分。

b） 成熟性。根据分系统目前的技术水平和成熟程度来评定。水平最低的评 10 分，水平最高的评 1 分。

c） 工作时间。根据分系统的工作时间来评定。分系统一直工作的评 10 分，工作时间最短的评 1 分。

d） 环境条件。根据分系统所处的环境来评定。分系统工作过程中会经受极其恶劣而严酷的环境条件的评 10 分，环境条件最好的评 1 分。

这样分配给每个分系统的失效率 λ_i 见式（25）：

$$\lambda_i = C_i \lambda_0 \quad \cdots\cdots (25)$$

式中：

C_i ——第i个分系统的评分系数，见式（26）；

λ_0 ——系统要求的失效率指标。

$$C_i = \omega_i / \omega \quad \cdots\cdots (26)$$

式中：

ω_i ——第i个分系统的评分数，见式（27）；

ω ——系统的评分数，且 $\omega = \sum_{i=1}^{n} \omega_i$ 。

$$\omega_i = \prod_{j=1}^{4} Y_{ij} \quad \cdots\cdots (27)$$

式中：

Y_{ij} ——第i个分系统第j个因素的评分数；

j=1代表复杂度；

j=2代表成熟性；

j=3代表工作时间；

j=4代表环境条件。

i=1,2，…，n为系统总数。

各分系统的评分数是根据设计工程师或可靠性工程师的实践知识和经验给出，可以由专家打分给出，也可以由工程组用某种表决方式给出。

7.5.6 修正评分分配法

按式（28）分配各分系统的可靠性：

$$R_{\mathrm{i}} = \frac{[1-(1-R_0)C_{\mathrm{i}}]}{(R_0 / \prod_{i=1}^{k}[1-(1-R_0)C_{\mathrm{i}}])^{1/\mathrm{k}}} \quad \cdots\cdots (28)$$

式中：

R_{i}——第i个分系统的可靠性；

R_0——系统可靠性指标要求；

C_{i}——第i个分系统的评分系数（见7.5.5）；

k——系统由k个分系统串联组成。

7.5.7 最小工作量法

该方法假定系统由n个分系统串联组成。该方法对可靠性较低的分系统要求可靠性有大的提高。假定已得到n个分系统的可靠性预计值且按非减顺序排列 $R_{\mathrm{i}}(i = 1,..., n)$，即 $R_1 < ... < R_{\mathrm{n}}$，则系统的可靠性为 $R_{\mathrm{s}} = \prod_{i=1}^{n} R_{\mathrm{i}}$。记系统可靠性指标为 R_{s}^*，则当 $R_{\mathrm{s}} < R_{\mathrm{s}}^*$ 时，说明系统可靠性还达不到指标要求，至少需要有一个 R_{i} 必须提高其可靠性至 R_{i}^* 以使 $R_{\mathrm{s}} \geq R_{\mathrm{s}}^*$。从而需要一定的工作量或费用，包括人、财、物等费用。假定每个分系统具有相同的工作量或费用函数 $F(R_{\mathrm{i}}, R_{\mathrm{i}}^*)$，此函数表示第$i$个分系统的可靠性从 R_{i} 提高到 R_{i}^* 所需要的工作量或费用，则需要的总工作量或费用为 $\sum_{i=1}^{n} F(R_{\mathrm{i}}, R_{\mathrm{i}}^*)$。最小工作量法即在 $\prod_{i=1}^{n} R_{\mathrm{i}}^* \geq R_{\mathrm{s}}$ 的条件下，使 $\sum_{i=1}^{n} F(R_{\mathrm{i}}, R_{\mathrm{i}}^*)$ =min(最小）。则该优化问题具有唯一解式（29）：

$$R_{\mathrm{i}}^* = \begin{cases} R_0, \text{若} i \leq k \\ R_{\mathrm{i}}, \text{若} i > k \end{cases} \quad \cdots\cdots (29)$$

即使前k个分系统的可靠性由 R_{i} 提高到 R_{i}^*（即 R_0），其它分系统可靠性保持不变。说明提高系统可靠性薄弱环节的可靠性，可在满足系统可靠性指标的前提下使工作量或费用最小。式中k为满足式（30）的最大的j：

$$R_{\mathrm{j}} < (R_{\mathrm{s}}^* / \prod_{i=j+1}^{n+1} R_{\mathrm{i}})^{1/\mathrm{j}}, \ j=1,2,\ldots, n \quad \cdots\cdots (30)$$

其中 $R_{\mathrm{n}+1} = 1$。R_0 为式（31）：

$$R_0 = (R_{\mathrm{s}}^* / \prod_{i=k+1}^{n+1} R_{\mathrm{i}})^{1/\mathrm{k}} \quad \cdots\cdots (31)$$

此时系统可靠性满足指标要求，即 $R_{\mathrm{s}} = \prod_{i=1}^{n} R_{\mathrm{i}}^* = R_{\mathrm{s}}^*$。

7.6 注意事项

可靠性分配应注意：

a） 可靠性分配应从研制阶段早期开始进行；

b） 可靠性分配应与可靠性建模、可靠性预计结合进行，随着设计修改，可以对可靠性分配值进行必要的调整，但应经过审批；

c） 可靠性分配的方法较多，应结合卫星工程实际及产品特点、可靠性模型、使用要求、技术发展水平、研制经验等进行选择；

d） 应将系统的可靠性定量要求分配到分系统、设备（部件）或更低的产品层次，作为各级产品设计和评价的依据；

e） 可靠性分配应考虑产品的复杂性、成熟性和重要性等因素；

f） 可靠性分配应留一定余量。

8 可靠性预计

8.1 概述

可靠性预计是定量地估算设备或系统设计是否满足规定的可靠性要求的过程。预计结果可给出影响可靠性的因素，为设计决策提供产品可靠性的相对度量，作为决策依据之一。在研制阶段的早期进行可靠性预计是最有用、最经济的。可靠性预计是产品设计的部分。

GJB 813—1990中规定的可靠性预计的程序与方法适用于本标准。

8.2 目的

可靠性预计的主要目的是对系统、分系统与设备的可靠性进行预测，以确定设计是否能满足规定的可靠性要求，或是否需要对设计进行适当的修改。

可靠性预计是从可靠性角度出发，对不同的设计方案进行比较，为设计决策提供依据；发现设计中的薄弱环节，为设计改进或生产过程控制提供依据；为可靠性试验方案设计提供依据；为可靠性分配、维护使用提供信息。

8.3 原则

可靠性预计一般原则如下：

a）对电子产品的可靠性预计，国产元器件可采用 GJB/Z 299B—1998，进口元器件可采用 MIL—HDBK—217F—1991；

b） 对自制电子元器件，可根据收集的信息进行预计，也可根据对自制电子元器件所采取的质量控制措施，在 GJB/Z 299B—1998 中选用相当的元器件进行可靠性预计；

c） 对非电产品，可根据该非电产品试验信息及可靠性评估数据、相似产品信息、国外非电产品数据等进行可靠性预计；

d） 应根据产品所处的研制阶段、数据等情况选用合适的可靠性预计方法；

e） 在产品的方案阶段、初样阶段，可采用元件计数法、相似产品法等进行初步可靠性预计；

f） 在产品的初样阶段后期、正样阶段，应采用元器件应力分析法等进行详细的可靠性预计；

g） 应建立产品的任务可靠性模型并对整星、分系统、设备各级在任务剖面内的任务可靠性进行预计；

h） 预计的最低功能级一般应与 FMEA 的最低功能级相一致；在任何功能级的可靠性预计结果，应做为高一级预计的输入；

i） 可靠性预计应从方案阶段开始，以确定分配到各功能级的可靠性指标的可行性；

j） 在研制过程中，设计一旦变更，就要重新进行预计；早期的预计着重于方案的可行性和可靠性的研究，随着设计工作的深入，采用不同的预计方法；

k） 在不同状态与环境下工作的功能级，应给出不同状态与环境条件下预计的结果；

l） 当设备中非电子零部件失效率不可忽视、软件程序的成败严重影响设备工作时，应对预计的结果加以修正，使之尽量接近工程实际。

8.4 步骤

可靠性预计步骤流程图见图10。

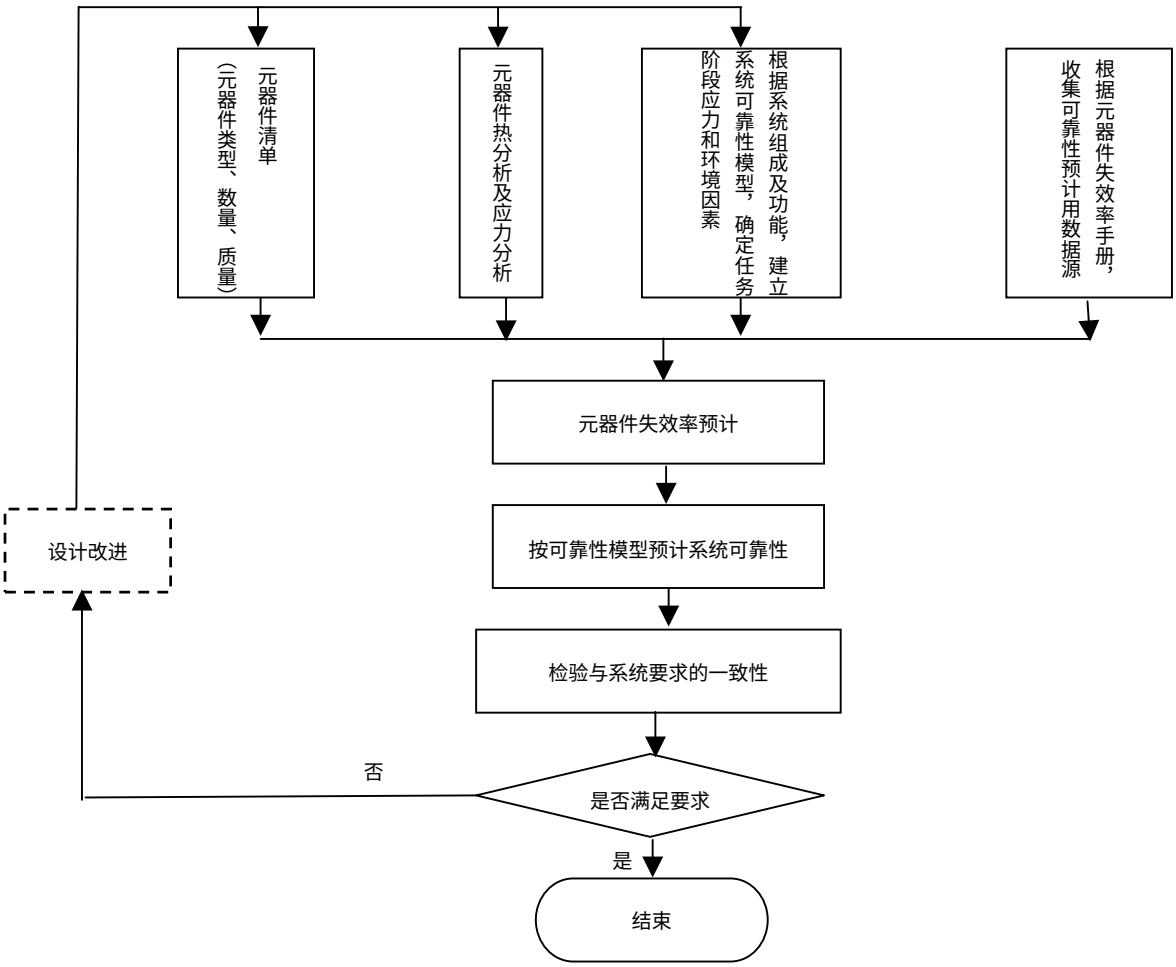


图 10　可靠性预计的步骤

可靠性预计步骤如下：

a） 根据系统组成及功能，建立系统可靠性模型，确定任务阶段应力和环境因素：可靠性建模见第 6 章，以确定产品各组成单元之间的可靠性关系；

b） 元器件清单：系统各设备、功能模块所包含的元器件类型、数量、质量等；

c） 元器件热分析及应力分析：得到可靠性预计元器件应力分析法所需要的温度、电应力等信息；

d） 根据元器件失效率手册收集可靠性预计用数据源：根据 GJB/Z 299B—1998、MIL—HDBK—217F—1991 收集元器件失效率预计有关的数据；

e） 元器件失效率预计：根据 GJB/Z 299B—1998、MIL—HDBK—217F—1991 进行预计，或根据实际经验和试验数据确定（卫星产品进行可靠性预计要求统一采用卫星可靠性保证计划规定的卫星电子元器件在轨应用失效率数据或其它元器件失效率数据源）；

f） 按可靠性模型预计系统可靠性：根据任务时间、环境因子等逐级进行预计，直至系统；

g） 检验与系统要求的一致性：预计结果满足要求，则预计结束；否则，指出可靠性薄弱环节，提出设计改进建议，待设计改进完成后再重新进行可靠性预计，直至满足要求。

8.5 方法

8.5.1 相似设备法

将研制的设备和已知可靠性的相似设备进行比较，从而估计设备可能达到的可靠性水平。

相似设备法适用于方案论证阶段。

8.5.2 功能预计法

对新设计的产品进行可靠性预计时，用以前经过验证的产品功能和可靠性，来估计新设计的同类产品功能的可靠性。

功能预计法适用于方案论证阶段。

8.5.3 元器件计数法

元器件计数法对国产元器件引用GJB/Z 299B—1998，对进口元器件引用MIL—HDBK—217F—1991。这种方法把设备内所包含的所有元器件的失效率相加而得到整个产品的失效率。预计是自下而上直至系统进行的。这种预计方法适用初样设计早期阶段。

8.5.3.1 所需要的信息

元器件计数法所需要的信息包括：

a） 所采用的元器件的种类与数量；

b） 元器件的质量等级；

c） 设备环境。

8.5.3.2 计算公式

元器件计数法的设备总失效率按式（32）计算：

$$\lambda_s = \sum_{i=1}^{n} N_i \lambda_{Gi} \pi_{Gi} \quad \cdots\cdots (32)$$

式中：

λ_s——设备总失效率，（10^{-6}/h）；

λ_{Gi}——第i种元器件的通用失效率，（10^{-6}/h）；

π_{Gi}——第i种元器件的通用质量系数；

N_i——第i种元器件的数量；

n——设备所用元器件的种类。

该公式适用于在同一类别的环境。如果设备中的单元或元器件在不同的环境中工作，则应分别在不同的环境中考虑，然后对失效率相加，得到设备的总失效率。

8.5.4 元器件应力分析法

元器件应力分析法详见GJB/Z 299B—1998。应力分析法在初样设计后期应用。

应力分析法预计是在考虑元器件类型和工作应力等级及每个元器件的降额特性的情况下，把设备失效率做为所有单个元器件失效率的函数来确定。

元器件应力分析法的基本步骤：

a） 列出所预计设备的所有元器件类型直至可用 GJB/Z 299B—1998、MIL—HDBK—217F—1991 所规定的元器件分类的最低层，以便准确使用失效率模型或有关图、表；

b） 统计各类型元器件的数量并指出在电路中的作用（如二极管的开关、电压调整等）；

c） 给出元器件的工作环境及温度 T，给出环境系数；

d） 给出元器件的质量等级及质量系数；

e） 给出元器件的电应力比 S；

f） 给出预计工作所需的各种 π 系数、模型参数；

g） 查表或按照基本失效率模型，给（计算）出元器件在规定工作环境条件下的基本失效率 λ_b；

h） 按元器件应力分析法公式计算各元器件的工作失效率 λ_P（元器件工作失效率为质量、环境、温度、电应力、封装等的函数；除微电路外，大多数元器件的工作失效率 λ_p 模型都为基本失效率 λ_b 与环境系数 π_E、质量系数 π_Q 及一系列其它有关的 π 系数的乘积）；

i） 将所预计模块/单元中各元器件的工作失效率相加，得到模块/单元的总失效率；

j） 按可靠性数学模型及任务时间计算系统、设备的可靠性。

8.5.5 非指数故障密度函数的修正

可靠性预计的方法基于一个重要的假定，即元器件失效服从指数分布。当系统包含有其失效密度函数在所关心的时间间隔内不能以指数分布近似表示的元器件时，或者对系统的不可靠性起决定性影响的零件的失效的密度函数不服从指数分布时，必须加以修正。机械零件一般属于这种零件。

在这种情况下，不能把所有的零件的失效率相加，因为其中有些零件的失效率随时间的变化很大。在这种情况下应对每一设备中含有恒定失效率的零件的部分和含有变化失效率的零件的部分分别考虑。

如含有恒定失效率的零件有x个，则这部分可靠性由式（33）计算：

$$R_1(t) = \exp[-(\sum_{i=1}^{x} \lambda_i)t] \quad \cdots\cdots (33)$$

对于含有变化失效率的部分如果含有B个零件，则可靠性由式（34）计算：：

$$R_2(t) = \prod_{i=1}^{B} R_i(t) \quad \cdots\cdots (34)$$

当两部分失效相独立时，则设备可靠性是：R（t）=R_1（t）R_2（t）

这类修正适于具有失效时间服从正态分布、威布尔分布、对数正态分布或极值分布的零件。

8.5.6 非工作失效率的修正

在预计时所给出的元器件失效率都以工作时间为基础。有些设备的非工作时间占据了使用寿命的很大一部分。故其失效率应当修正成包括非工作期间的失效率。通常最简单的模型见式（35）：

$$\lambda_T = \lambda_{op} d + (1 - d)\lambda_{nop} \quad \cdots\cdots (35)$$

式中：

λ_T ——总失效率；

λ_{op} ——工作失效率；

λ_{nop} ——非工作失效率；

d ——占空因子，即工作时间与总时间之比。

8.6 注意事项

可靠性预计应注意：

a） 应按 GJB 813—1990 规定的要求进行可靠性建模与预计；

b） 可靠性预计应考虑并区分不同的任务和工作模式；

c） 可靠性预计应随着研制工作的进展逐步细化；

d） 电子产品可靠性预计一般采用 GJB/Z 299B—1998，但卫星用元器件不少是自制或按“协议”制造的，对这些元器件，若已有试验、评估数据，则应首先采用，但应经过确认和批准；

e） 元器件应力分析法是一种详细可靠性预计方法，在进行预计时，需要许多详细的信息，故应根据方法对数据的要求，对每项数据进行细致的准备；

f） 卫星系统分不同的产品层次，下层次的预计结果可作为上层次产品的输入，但在低层次产品可靠性预计时，一般应将可靠性模型建立到元器件级（特别是对于有大量元器件冗余的情况）。

9 故障模式、影响及危害性分析

9.1 概述

故障模式、影响及危害性分析（failure mode，effects and criticality analysis，缩写为FMECA）是在工程实践中总结出来的，以故障模式为基础，以故障影响或后果为中心，根据分析层次，并通过因果关系推理、归纳进行的分析活动。

FMECA是GJB 450A—2004和QJ 1408A—1998中规定的可靠性工作项目。

卫星型号实施FMECA工作应符合QJ 3050—1998、QJ 2437—1993的要求。

9.2 目的

FMECA通过逐一分析卫星各组成部分的故障对系统整体工作的影响，可以得到产品的I、II类故障清单，单点失效清单以及可靠性关键项目清单，从而识别出设计中的薄弱环节和关键项目，并为评价卫星及其各组成部分设计的可靠性提供参考和依据。同时，适时地、有效地应用FMECA技术，还能够为预防和控制故障、改进产品设计和生产工艺、降低研制风险提供有价值的信息。

9.3 原则

为保证卫星FMECA结果的有效性，除应执行有关标准和型号技术文件要求外，在实施时还应遵循以下一般原则：

a） 卫星及其各级产品的 FMECA 应由设计主管人员完成，型号可靠性人员负责提供必要的技术支持和指导；

b） 应在型号可靠性大纲中明确实施卫星 FMECA 的计划安排和基本要求，包括分析层次、基本假设、严酷度分类、数据来源、分析表格及分析报告格式等，并实施监督、检查和评审，以强化同一卫星型号内 FMECA 分析的计划性、一致性；

c） FMECA 分析结果应影响设计，对于所识别的设计薄弱环节和关键项目应在设计、生产等方面制定并采取有效措施加以改进和控制，并实施必要的跟踪和验证；

d） 应随设计的进展不断更新 FMECA 的内容，当设计发生更改时，应对更改部分进行分析，以确保更改不会引入新的问题而降低系统的可靠性。

9.4 步骤

实施 FMECA 的步骤如图 11 所示。

应当强调，FMECA是一个反复循环迭代的过程，其原理应作为设计人员的基本思维方式，贯穿整个设计过程。FMECA的结果应随研制工作的进展加以更新。FMECA还特别强调“事前预防”，即尽可能在产品设计确定之前实施分析和改进，以最大限度地降低故障的危害。

9.5 方法

9.5.1 方法概述

FMECA包括故障模式及影响分析（FMEA）和危害性分析（CA）两部分内容。以下分别说明其基本方法。

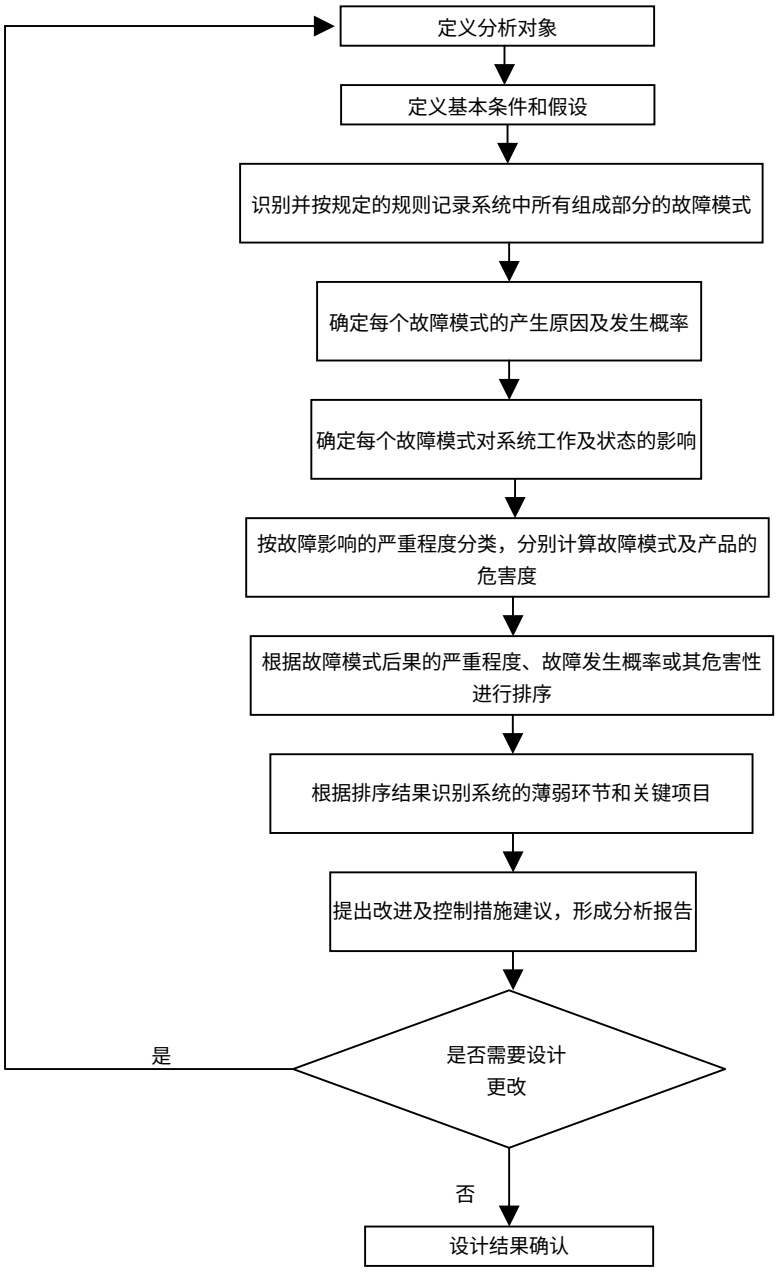


图 11　FMECA 的步骤

9.5.2 FMEA 的方法

FMEA的基本分析方法包括硬件分析法和功能分析法，两者的主要区别在于硬件分析法以每个分析对象的硬件故障为分析的出发点，而功能分析法则侧重考虑分析对象的功能故障模式。通常，功能法在设计早期硬件不能确定的情况下使用，当可以获得硬件的相关信息和数据时，则应使用硬件法进行分析。功能

分析法得到的分析结果相对比较概括，而硬件分析法的分析结果比较具体。硬件分析法是目前卫星研制中实施FMEA的主要分析方法。以下对这两种FMEA方法分别予以说明。

9.5.2.1 硬件分析法

该方法列出每个独立的硬件产品，分析每个硬件可能的故障模式及其影响。该方法通常适用于硬件产品设计的图纸及有关的设计信息已基本确定的情况。

硬件法一般是以自下而上的方式进行，分析从最低层次产品开始，逐级向上，通过迭代的方式向系统更高级别的产品进行。

9.5.2.2 功能分析法

该方法重点考虑每个组成部分产品的功能及其故障。分析时，首先应确定各组成部分的功能以及对应的功能故障模式的描述，然后进行分析。

功能法在硬件产品不能唯一确定时采用。当设计工作已完成系统功能框图，但没有确定所使用的硬件时，通常采用功能法进行分析。该方法一般在设计的早期使用，并应随着设计进展或设计更改而更新。对于较高产品层次，通常也采用功能分析法。

在具体工作中，分析人员可根据卫星产品的复杂程度、研制状态及有效数据的情况，决定所采用的分析方法。硬件分析法和功能分析法可独立进行，也可根据需要结合使用。

对于复杂的卫星系统，FMEA通常采用硬件法和功能法相结合的方法，以自下而上的方式进行。

根据各级卫星产品的不同特点及不同的研制阶段，FMEA的分析方法可以进行适当的调整。图12给出了上述两种分析方法在工程各研制阶段具体应用的示例。

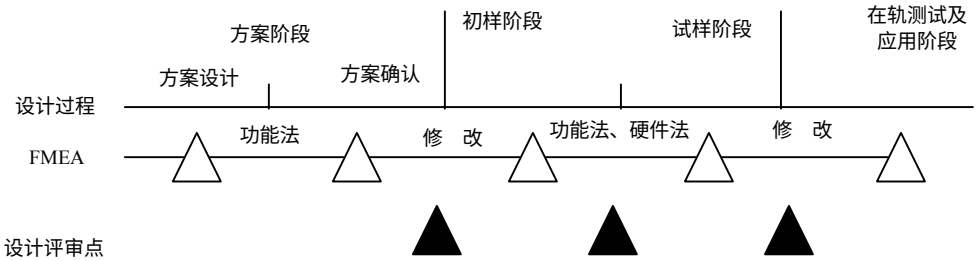


图 12 FMECA 在各研制阶段的应用示例

FMEA工作表格可采用表4所示的形式，填写说明如下。

表 4 卫星故障模式影响分析表

型号名称（代号）： 研制阶段：

分系统：		设备或部件：			功能模块：		任务阶段：			工作模式：	
序号	产品或功能标志	功能	故障模式	故障原因	故障影响		严酷度类别	是否单点失效	故障检测方法	补偿措施	建议与说明
					本级产品	上级产品					

填表人： 审核： 日期：

研制阶段：填写卫星型号所处的研制阶段，如论证、方案、初样研制和正样研制等阶段。

型号名称（代号）、分系统、设备或部件、功能模块：分别填写卫星、分系统、设备或部件和下一级产品（如印刷电路板、接口电路等）的名称或代号。

任务阶段：填写分析所对应的卫星任务阶段，如发射准备、发射、轨道运行等。

工作模式：填写卫星、分系统、设备或部件分析对应的工作模式，如卫星的初始姿态捕获、初始轨道捕获、在轨测试、正常轨道运行、轨道调整、返回、安全应急等工作模式，设备的正常工作、不工作、备份单元自主与地面控制切换等工作模式。

序号：序号编排应本着方便查找的原则，可按硬件层次分级编号，也可采用其他方法。

产品或功能标志：填写被分析产品（或产品功能）的名称和标志，应注意：

——当采用功能分析法时，应逐一列出各输出功能的标志；

——当采用硬件分析法时，该产品原理图的符号、产品型号、设计图纸的编号等均可作为产品的标志。

功能：填写产品或其组成部分（硬件、功能块或功能单元）的功能的具体内容。应根据事先进行的产品定义，在该栏中具体填写被分析产品所具有的功能，该功能应与产品的设计要求及有关的功能分解的结果相一致。

要特别注意的是，填写内容应包括与接口部分的关系。接口部分的支持作用、辅助作用是被分析产品在正常完成任务时所必需的，如供电、冷却、加热部分或产品的输入、输出信号部分等。

故障模式：填写通过分析或经验信息得到的硬件或功能输出可能的故障模式。

在功能分析法的 FMEA 中，通常应考虑下述五种情况对应的故障模式：

——功能丧失；

——功能降级，输出能力减弱或性能变差；

——不能准时启动（即提前或滞后动作）；

——间歇性工作异常；

——不能准时停止工作。

硬件 FMEA 应考虑星上各类产品，包括电子、电气、机电、机械、热、光学、推进、压力、气动、火工等方面产品可能的故障模式。

在故障模式分析中，应强调识别和说明被分析对象在所有任务阶段和所有工作模式情况下的全部故障模式。

应重视卫星备份硬件的切换、故障检测与隔离环节的故障模式分析，确保备份的作用不被上述接口的故障影响所抵消。凡无法独立检测备份单元故障的环节均应视作潜在的单点失效。备份单元检测与切换环节中故障模式分析应考虑的主要方面有：

——自主切换单元的故障诊断、逻辑控制和切换；

——备份单元的状态检测能力；

——主份单元故障检测能力；

——相关故障或从属故障的可能；

——切换环节误动作和不能准时通、断；

——主、备份间反复切换等。

应重视分系统间和设备间各种接口（机、电、热等）以及卫星与运载火箭、地面测控、发射场和应用系统间的接口故障模式识别和分析。

在 FMEA 中，一般只假定单一的硬件故障，即不考虑两个不相关故障同时出现的情况。但在硬件单一故障分析中，应注意可能出现的连锁影响，即二次故障。有时这两种故障的组合可能对系统产生严重的后果。

故障原因：填写故障模式出现的最可能的物理和化学机理。这种原因应包括本身和外部因素（如试验、测试设备与方法，操作，运行程序，软件，环境等）。

在一个故障模式存在二个以上的故障原因时，所有可能的独立故障原因均应予以确认和填写。

故障影响：填写每一故障模式对产品功能、运行和状态所产生的可能后果。应分别填写故障模式对本级产品（含相邻产品）的影响和对上级产品（直至分系统和卫星）的影响。

严酷度类别：按故障对卫星、分系统影响的程度，对每一故障模式的严酷度均应确定其等级。严酷度类别可分为四级，分级准则规定如下：

I 级——灾难性的：故障将导致分系统功能丧失或基本丧失，进而使卫星任务失败或出现不可接受的任务降级，工作寿命严重减少（如设计寿命减少 1／2 以上），或人员伤亡、财产重大损失。

其中卫星或分系统级的单点失效环节应在 FMEA 工作表格中加以标识。

II 级——关键性的：故障将导致分系统主要功能明显下降，对卫星任务完成有重要的影响，或财产损失，或卫星工作寿命有较多的减少（如设计寿命减少 1／2～1／4）。

III 级——非主要的：导致分系统功能一定的下降，但对卫星任务的完成没有大的影响，或备份功能丧失，或卫星工作寿命有所减少（如设计寿命减少 1／4 以下）。

IV 级——可忽略的：对分系统功能和卫星任务的完成几乎没有影响。

在实施 FMEA 中，可参照上述分级的原则，制定具体产品的严酷度类别划分准则。

故障检测方法：填写卫星在任务阶段（轨道运行和发射）中．某故障模式出现后，对其如何诊断或检测，可包括直接遥测、间接工程判断、无法检测等。

补偿措施：填写在产品设计中为避免或减少故障造成的影响，已经采取的补救措施，包括对故障的隔离和控制、备份或替换方式的采用、地面遥控干预等。

建议与说明：填写各种建议和对表格填写的补充说明，可包括下述内容：

——设计拟采取纠正措施的建议；

——为减少 I、II 级故障模式出现，建议或已经采取的其他措施，加工艺修改，生产加工的质量控制，地面试验，环境防护要求，贮存、运输、操作和维修的限制，检测要求等；

——有别于常规设计的特点说明，如新材料、特殊工艺，引进元器件等；

——其他。

填表人、审核、日期：填写FMEA工作表格的填表人、审核签署及审核日期。

9.6 CA 的基本方法

9.6.1 概述

卫星CA是FMEA的扩展和继续，因此，它要求在FMEA结果的基础上进行。FMEA中的信息如产品功能、故障模式和原因、任务阶段及严酷度分类等，可直接作为CA的相应信息加以记录。

CA的内容是根据每一个故障模式所造成后果的严酷度类别及故障模式的发生可能性，对其进行综合度量并排序。

CA根据分析方法的不同划分为定性分析法和定量分析法。分析人员应根据分析的产品层次及可获得的故障率数据决定使用的分析方法。以下对这两种CA方法分别予以说明。

9.6.2 定量分析法

该方法是使用产品具体数据定量计算危害性（度）数值的分析方法。用定量分析法进行CA需要被分析产品相应层次的故障率数据。

定量分析时，每个故障模式的危害度值定义为：

$$C_m=\alpha\beta\lambda_p t \cdots\cdots (36)$$

式中：

C_m——故障模式的危害度；

λ_p——该产品在其任务阶段内的失效率；

α ——故障模式的频数比；

β ——故障影响概率；

t ——任务阶段的工作时间。

9.6.3 定性分析法

当不能获得准确的产品故障率数据时，故障模式发生的可能性可使用预先定义的级别来定性描述，即进行定性分析。定性分析法也不使用故障模式频数比α和故障影响概率β。在进行定性CA时，每个故障发生的可能性被分成离散的级别，分析人员基于工程经验对故障模式发生频率进行判断，确定相应的故障概率等级，填入CA记录中，并完成整个分析工作。

CA工作表格可采用表5所示的形式，填写说明如下。

表 5 卫星危害性分析表

型号名称（代号）： 研制阶段：

分系统：			设备或部件：			功能模块：		任务阶段：			工作模式：		
序号	产品或功能标志	功能	故障模式	故障原因	严酷度类别	故障概率或故障概率数据源	故障影响概率 β_j	故障模式频数比 α_j	失效率 λ_P	工作时间 t	故障模式危害度 C_{mj}	产品危害度 $C_r=\Sigma C_{mj}$	说明

填表人： 审核： 日期：

型号名称（代号）、研制阶段、分系统、设备或部件、功能模块、任务阶段、序号、产品或功能标志、功能、故障模式、故障原因、严酷度类别各栏填写与 FMEA 表格相同，填写时可直接采用 FMEA 表格的内容。

故障概率或故障率数据源：该栏应填写被分析对象的故障模式发生概率或相应故障概率数据来源。

当某元器件、零（部）件缺乏故障率数据而只能进行定性 CA 分析时，即只能用故障模式发生概率等级来评价时，应确定相应的故障模式发生概率等级，并填入该栏。故障模式发生概率的等级一般分为五级，包括：

A 级（经常发生的）：在产品工作期间内，某一故障模式的发生概率大于或等于产品在该期间内总故障概率的 20%。

B 级（有时发生的）：在产品工作期间内，某一故障模式的发生概率大于或等于产品在该期间内总故

障概率的 10%，但小于 20%。

C 级（偶然发生的）：在产品工作期间内，某一故障模式的发生概率大于或等于产品在该期间内总故障概率的 1%，但小于 10%。

D 级（很少发生的）：在产品工作期间内，某一故障模式的发生概率大于或等于产品在该期间内总故障概率的 0.1%，但小于 1%。

E 级（极少发生的）：在产品工作期间内，某一故障模式的发生概率小于产品在该期间内总故障概率的 0.1%。

进行定性分析时，不填写本表格后续各栏的内容，仅根据此栏中的概率等级和故障影响的严酷度类别绘制危害性矩阵，以便对故障模式危害性的大小进行比较。

当进行定量 CA 时，应在此栏填写计算所使用的失效率数据的来源，如 GJB/Z 299B—1998 或 MIL—HDBK—217F—1991 等。

故障影响概率β_j：故障影响概率β_j表示假定产品第 j 个故障模式已发生时，其故障影响导致初始约定层次出现某严酷度类别后果的条件概率。它表示分析人员对特定故障模式导致特定故障影响的可能性的判断。该值是凭经验主观判定的。它从故障模式导致故障影响的可能性大小的角度进行度量，一般分为“必然”、“很可能”、“有可能”、“不可能”四种情况，每种情况可给出一个β 数值。可参考的故障影响概率（β）估计值见表 6。

表 6　供参考的故障影响概率（β）估计值

β（条件概率值）	说　明
$\beta=1$	必然导致出现某一严酷度类别的后果
$0.1<\beta\leq1$	很可能导致出现某一严酷度类别的后果
$0<\beta\leq0.1$	有可能导致出现某一严酷度类别的后果
$\beta=0$	不可能导致出现某一严酷度类别的后果

工程中，当无法估计某一故障模式的故障影响概率β 时，通常按 1 计算，对于特定严酷度类别的故障影响，此时的危害度的计算结果是偏保守的。

故障模式频数比α_j：故障模式频数比α_j是产品第 j 个故障模式的发生概率与该产品全部故障发生概率之比，它以小数或百分数形式，表示某个部件或产品发生故障时，表现为确定的故障模式的概率。常用器件的故障模式频数比数据可从有关文献资料中查到。非电产品的频数比数据目前比较缺乏，工程中可根据经验以类比方式进行推断。

失效率λ_p：填写被分析产品在任务阶段中，在工作状态下的失效率。可根据可靠性预计的结果确定该值。

工作时间 t：该栏记录任务阶段内的产品工作时间。注意，如果多个产品工作时间一样，在进行 CA 时，工作时间也可以不参加危害度计算。此时危害度实际上就会是一个λ_p被α、β 修正后的失效率。

故障模式危害度 C_{mj}：故障模式危害度 C_{mj} 指在给定严酷度类别下，被分析对象某个故障模式的危害度，危害度 C_{mj} 定义为：

$$C_{mj}=\alpha_j\beta_j\lambda_p t \quad \cdots\cdots (37)$$

假设被分析产品的故障率为$\lambda_p=0.01\times10^{-6}$/小时，所分析的当前故障模式的频数比$\alpha_j=0.5$，工作时间 t

＝20h，产生 I 类严酷度后果的故障影响概率β_j=0.1，则该故障模式产生 I 类严酷度故障后果的危害度值计算如下：

$C_{mj}=\alpha_j\beta_j\lambda_p t = 0.5\times0.1\times(0.01\times10^{-6}) \times20 =1\times10^{-8}$

产品的危害度 C_r 是由 C_{mj} 组成的。当产品有 n 个故障模式，且属于同一个严酷度类别时，则故障模式的总危害度为：

$$C_r=\Sigma C_{mj}\ (j=1，2，\cdots\cdots n) \cdots\cdots (38)$$

式中：

C_r——产品在某类严酷度下的危害度值；

j——产品在某类严酷度下的故障模式数；

C_{mj}——第j个故障模式的危害度值。

这样，对于一个产品，若有I、II、III、IV类严酷度的故障模式危害度，则每一类都有一个总危害度。所以，该产品的危害度必然是由属于不同严酷度类别的四个总危害度来描述的。

定性或定量分析时，均可绘制危害性矩阵。典型的危害性矩阵的形式如图13所示。

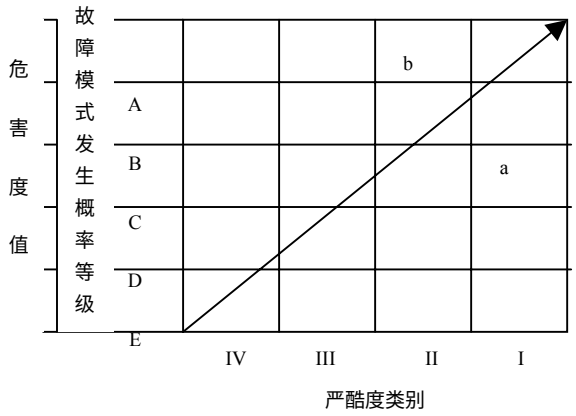


图 13　典型危害性矩阵形式

危害性矩阵是通过在矩阵中填入产品代码或故障模式识别号构成的，描绘了每个产品故障模式的严酷度类别以及发生的概率等级或危害度值。

危害性矩阵是确定纠正措施优先顺序的有效工具。一般情况下，矩阵中右上角显示的项目，是应立即采取措施的项目。这些故障模式有高的发生概率，并会对系统产生灾难性影响。沿对角线向矩阵的左下角移动，故障的危害性逐步减小。

9.7　FMECA 的输出

分析人员按规定要求将FMECA过程记录下来，并经过整理即可形成FMECA报告。FMECA报告应进行签署，并在研制的各个阶段作为设计文件的一部分提交设计评审。

FMCEA报告一般包括：

a）　概述：包括对设计的评价，以及对关键设计特性、项目不进行 FMECA 的理由说明等；

b）　系统定义，包括分析对象和分析范围、任务描述、剖面、成功和故障判据、数据来源等；

c）　基本规则与假设，包括分析方法、约定层次划分、严酷度分类等；

d）　功能框图和可靠性框图；

e） 分析结果数据及要求填写的工作记录，可包括：FMEA 表格、CA 表格、危害性矩阵、关键项目清单（应包括严酷度为 I 类和 II 类的故障模式清单、单点故障清单、危害度值较大的故障模式清单等）；

f） 结论与建议。

9.8 示例

功能FMEA和定性CA示例见QJ 3050—1998附录A1。

硬件FMEA和定量CA示例见QJ 3050—1998附录A2。

9.9 注意事项

FMECA应注意：

a） 考虑卫星工作环境条件与任务要求的关系，在实施卫星 FMECA 时，应结合具体的任务要求，对卫星在各种特殊空间运行环境中可能产生的故障模式及其后果进行全面的研究和分析；

b） 由于卫星具有在轨运行难于维护的特点，在其工作过程中对故障的检测是通过遥测手段实施的，因此要求在实施卫星 FMECA 时对于星上较为关键的产品、功能和故障等，应确定其检测方法是否恰当和充分；

c） 卫星 FMECA 中对维修性内容的分析主要针对地面试验和地面测试情况，对卫星运行阶段的 FMECA 则较少考虑维修性的有关内容；

d） 为提高型号的工作寿命和可靠性，卫星系统中采用了较多的冗余设计，在实施卫星 FMECA 时应加强对这些冗余设计的分析，并特别注意共模（共因）故障的影响，以确保卫星设计的可靠性；

e） 卫星型号较高产品层次实施分析时，应利用 FMECA 的层次迭代关系，将较低层次 FMECA 结果综合到高一层次产品，分析结果的层次迭代关系可简述为：低层次产品某故障模式对高一层次的影响就是高一层次产品的一个故障模式，而低一层次产品导致该故障影响的故障模式，就是高一层次产品该故障模式的故障原因；

f） FMECA 作为产品设计分析的重要手段，必须与产品设计同步进行，便于及早发现产品中的潜在薄弱环节，在设计评审和可靠性专题评审时，FMECA 结果应作为重要内容予以评审；

g） FMECA 以卫星各级产品的故障模式及相关故障数据为分析基础，能否准确获得这些信息是决定 FMECA 工作有效性的关键，因此，各级卫星产品的研制和生产单位应在实际工作中注意收集、整理有关的产品故障信息，并通过规范有效的方法逐步建立和完善相应的故障信息数据库；

h） 在实施 FMECA 过程中应明确以下几个关键的概念：

——故障检测方法：故障检测方法是指在卫星运行过程中，当某一故障模式发生时，操作人员用来检测和识别故障的方法和手段，如某个遥测信号的变化等，研制试验（包括可靠性试验）和生产检验不是卫星运行过程中的活动，因此不能作为故障的检测方法；

——单点失效：所谓单点失效是指能引起系统故障的、且没有冗余或替代的工作方式作为补救的局部故障，单点失效通常需要设计予以特别的关注；

——补偿措施：补偿措施指在产品设计中为避免或减少故障造成的影响，已经采取的补救措施，一旦故障发生，这些措施将发挥作用，将故障的后果控制在可接受的水平，工程中采用的设计补偿措施一般可包括故障时能保持继续工作的冗余设备、安全或保险装置、可替换的工作方式等；

——纠正措施：纠正措施是指在实施分析后，针对故障产生的原因、条件等采取的设计改进措施，其目的是防止故障发生或降低故障发生的可能性，它不同于假定故障发生而采取的设计补偿措施；

——共因故障和共模故障：在分析冗余系统时，应特别注意那些由共同原因导致的同时故障，或由共同模式导致的同时故障，前者称共因故障，后者称共模故障，共因故障和共模故障是一种不独立的相依故障事件，它们可能同时发生从而导致冗余系统的失效。

10 故障树分析

10.1 概述

故障树分析（fault tree analysis，缩写为FTA）是一种将系统故障形成的原因由上至下，按产品层次以倒立树枝状逐级细化的分析方法，是对复杂系统的设计、试验或使用中出现的故障进行分析的常用工具。

在故障树分析中，把最初定义的不希望发生的事件（故障）称为顶事件，最底层得到的毋需再进一步分析的事件称为底事件，介于顶事件与底事件之间的结果事件（指由其他事件或事件组合所导致的事件）称为中间事件，它们各自由相应的符号表示。顶事件、中间事件和底事件通过各种逻辑门进行连接，不同的逻辑门代表不同的意义并使用不同的符号。逻辑门描述了事件间的因果关系，逻辑门的下端是输入事件，代表原因；逻辑门的上端是输出事件代表结果。有关故障树的基本概念，如事件及其符号、逻辑门及其符号、割集、结构函数、重要度等，请参考GJB 768A—1997第3章。

在逻辑门中，与（and）门、或（or）门和非（not）门是三种基本门：与门表示仅当所有输入事件发生时，输出事件才发生；或门表示至少一个输入事件发生时，输出事件就发生；非门表示输出事件是输入事件的逆事件。其他的逻辑门为特殊门，可通过特定的规则用基本门的组合来表示。

概括地讲，FTA具有分析方法直观、应用范围广泛等特点，但由于其逻辑性强、分析难度大、定量计算复杂等特点限制了其应用。因此，在卫星产品设计过程中，应根据需要有选择地实施分析。

卫星型号实施FTA工作应符合GJB 768A—1997及型号有关技术文件的要求。

10.2 目的

FTA是系统可靠性分析的重要工具之一，在产品设计阶段，FTA可帮助判明产品潜在的故障模式，发现可靠性薄弱环节，便于改进设计。通过FTA，可得到最小割集等定性分析结果和顶事件发生概率和底事件重要度等定量分析结果。通过这些结果可确定产品中的可靠性薄弱环节和关键件，从而为改进设计提供依据。

10.3 原则

在FTA过程中，建立故障树是一个关键步骤，也是实施故障树定性、定量分析的最基本前提条件。建树是否完善将直接影响定性分析和定量计算结果的准确性。故障树应当是实际系统故障组合和传递的逻辑关系的正确描述。建树工作要求建树者对于系统及其各个组成部分有透彻的了解。所以，应由系统设计人员亲自建树，并与其它方面专家密切合作，这样建成的故障树才是一棵符合实际、能解决实际问题的故障树。

建树是一个多次反复、逐步深入、不断完善的过程。通过建树可透彻了解系统的故障逻辑关系，找出导致顶事件的所有基本故障原因事件或基本故障原因事件组合，从而辨识出系统在安全性或可靠性设计上的薄弱环节，以便改进设计，这比简单地算出一个可靠度数值更具有工程实用价值。

人工建树是工程中较为常用的方法，作为对建树活动的基本保证，GJB 768A—1997的5.1.3给出了以下的人工演绎法建树基本规则：

a） 明确建树边界条件，确定简化系统图；

b） 故障事件应严格定义；

c） 首先寻找的是直接原因事件；

d） 应从上向下逐级建树；

e） 建树时不允许逻辑门—逻辑门直接相连；

f） 妥善处理共因事件。

10.4 步骤和方法

10.4.1 分析准备

10.4.1.1 产品定义和描述

应在产品的设计资料的基础上，详细定义被分析的产品对象及其边界，并明确描述产品的任务及功能要求、可靠性框图以及有关的故障信息（如FMECA结果）等。

10.4.1.2 确定分析假设

根据产品的设计特征和分析的要求进行必要的假设，例如确定分析不予考虑或不做进一步分析的事件。分析人员应明确这些分析假设并在有关文件中予以说明。

在分析准备阶段确定的有关信息，通常是初步的，因此，上述内容应在分析过程中不断地补充、细化和更新，以确保分析结果符合实际情况。

此外为确保分析结果正确并真实反映产品设计的实际情况，分析人员还应随时征求其他设计、使用和维修人员的意见，以确保达到预期的分析目的。

10.4.2 实施分析

10.4.2.1 分析步骤

分析步骤如图14所示。

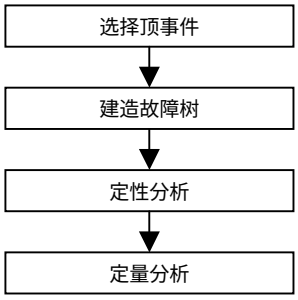


图 14 FTA 分析步骤

10.4.2.2 选择顶事件

根据卫星特性和实施FTA的要求，选择最为关注的不希望事件作为分析的出发点，即顶事件。应结合有关工程信息，如FMECA的结果（如I类故障、单点失效）、试验信息、类似型号研制经验，针对关键产品（功能）或关键故障（失效）事件确定顶事件。

对于顶事件，应给出严格、明确、详细的定义。此外，该步骤还应进一步明确被分析产品的范围、层次、边界定义等内容。

10.4.2.3 建造故障树

在卫星设计过程中，采用演绎法人工建树。

对于初步完成的故障树中各种特殊事件与特殊门，还应进行转换或删减，变成仅含有底事件、结果事件以及“与”、“或”、“非”三种逻辑门的故障树，这种故障树称为规范化故障树。

将建好的故障树规范化以便于分析，同时尽可能对故障树进行简化和模块分解以节省分析工作量。

建树步骤的详细说明见GJB 768A—1997的5.1和5.2。

10.4.2.4 定性分析

用下行法或上行法求出单调故障树所有最小割集，即所有导致顶事件发生的系统故障模式。在没有基础数据因而无法进一步定量分析的情形下，可以仅作定性比较。

关于单调故障树定性分析的详细说明见GJB 768A—1997的5.3。

10.4.2.5 定量分析

在获得底事件相关信息的条件下，求出单调故障树顶事件发生概率和一些重要度指标。

关于单调故障树定量分析的详细说明见GJB 768A—1997的5.4。

10.5 示例

人工演绎建造故障树方法示例见GJB 768A—1997的5.1.4。

单调故障树定性分析示例见GJB 768A—1997的5.3.6。

顶事件发生概率计算示例见GJB 768A—1997的5.4.3.3。

重要度计算示例见GJB 768A—1997的5.4.4.5。

10.6 注意事项

10.6.1 基本概念和分析假设

FTA是逻辑性很强的故障分析方法，为避免分析错误，在分析之前，应确保分析人员正确理解故障树基本概念，并给出一致的分析假设。

10.6.2 一阶最小割集的控制

FTA 分析得到的一阶最小割集代表了产品的单点失效，应在设计和研制工作中予以特别关注。

10.6.3 多状态故障树的处理

如果故障树的底事件描述一种状态，而其逆事件也只描述一种状态，则称为两状态故障树；如果故障树的底事件描述一种状态，而其逆事件包含两种及以上互不相容的状态，并且在故障树中出现上述的两种或两种以上状态的底事件，则称为多状态故障树。对于多状态故障树，应进行必要的预先处理，将其转化为两状态故障树，再进行分析。有关多状态故障的处理请参考GJB 768A—1997的5.5及附录B的内容。

10.6.4 应用计算机辅助工具进行故障树的分析

对于较复杂的卫星产品故障树，依靠人工进行定性分析的工作量很大，而要进行定量分析则几乎是不可能的，因此，故障树的分析工作通常需要借助计算机辅助分析工具完成。在使用计算机辅助分析工具时，应确保软件所提供的分析方法与标准及型号技术文件的规定相一致。

11 元器件选用与控制

11.1 概述

电气、电子和机电元器件(以下简称元器件)的可靠性是卫星可靠性的基础，元器件的选用控制也就成为卫星可靠性设计最重要的基础工作之一。

元器件选用包括元器件的选择和使用，在卫星的可靠性设计阶段主要考虑元器件的选择。在元器件选择过程也要考虑元器件的降额使用以及最坏情况分析等有关问题，这些问题将在本标准的其它章条中叙述，本章将主要说明元器件选择控制的有关要求。

卫星元器件的选用控制除了在设计阶段必须对元器件的选择进行严格的控制外，还应对元器件的使用全过程进行必要的控制。有关元器件选用控制的其它要求应按QJ 3057—1998的规定。

11.2 元器件选用控制的目的

元器件选用控制的目的是：通过正确选择和使用元器件，确保卫星在性能、可靠性、进度和成本等各方面在卫星全寿命周期内满足卫星的总体要求。

为达到上述目的，卫星型号的质量和可靠性管理部门应按有关文件、标准编写元器件保证大纲，作为实施和检查元器件选用控制的依据。

11.3 元器件选择控制的原则

卫星元器件选择控制的原则如下：

a） 选择满足卫星性能、使用寿命、环境、安全性、可靠性要求的元器件；

b） 优先选择列入军用元器件合格产品目录(QPL）或合格生产厂目录(QML）的元器件；

c） 采取以下措施，以保证卫星的研制进度并节省经费：

——选择元器件时应有备用方案，以保证卫星的研制进度；

——根据不同卫星及其使用部位，选择元器件的不同质量等级；

——采用已有的并经实践证明行之有效的元器件规范或专用技术条件；

——选择用于关键部位的高质量等级元器件应提出：监制、验收以及其它必要的要求。

d） 尽可能压缩元器件品种和供货单位；

e） 在质量满足要求的前提下，优先采用国产元器件。

11.4 元器件选择控制要求

11.4.1 元器件选用目录或优选目录

元器件质量管理部门应按11.3的有关原则制定元器件选用目录或按型号制定元器件优选目录，作为元器件选择的依据。当必须选择目录外元器件时，应按QJ 3065.1—1998的规定履行审批手续。

11.4.2 限用元器件

除非特别批准，限制选择下列元器件：

a） 含有放射性材料的元器件；

b） 能够产生有害人身健康气体的元器件；

c） 空心电阻器；

d） 未经充分试验或未经空间运行的塑料封装的半导体分立器件；

e） 需要熔断器座的熔断器。

11.4.3 元器件极限参数及使用环境的选择

电子线路设计人员必须了解所选元器件的特性，特别是元器件的极限参数或最大额定值及元器件允许使用的环境。应根据不同的应用场合，按本标准第14章及GJB/Z 35—1993合理降额使用。

必须重视改善元器件的使用环境，尤其当采用了大功耗元器件时，电子线路及有关结构应参照GJB/Z 27—1992进行可靠性热设计。

11.4.4 元器件控制规范及质量等级的选择

必须根据卫星对元器件的可靠性要求及质量管理部门规定的质量等级选用范围选择元器件的控制规范和质量等级。

若质量管理部门未规定元器件质量等级的选用范围，则国产元器件的质量等级应按GJB/Z 299B—1998选取；进口元器件应按MIL—HDBK—217F—1991选取。

11.4.5 元器件辐射强度保证(RHA)等级或静电放电敏感度等级(ESDS)的选择

对辐射敏感的元器件或静电敏感的元器件，应根据元器件在卫星上所处的部位以及在空间运行的时间，参照GJB 33A—1997、GJB 597A—1996、GJB 2438—1995选择适用的RHA等级或ESDS等级。

当无适用的RHA等级或ESDS等级的元器件可供选择时，应采取防护措施。

11.4.6 新品元器件选择

必须选择新品元器件时，应按规定申请新品研制，报请有关部门审批。新品元器件应通过集团公司或型号院进行设计定型或生产定型鉴定后，方可用于卫星等的正样产品上。

11.4.7 超过有效贮存期元器件的选择

当选择的元器件超过了GJB/Z 123—1999规定的有效贮存期，应按该标准进行超期复验，复验合格的元器件方可用于卫星的正样产品上。

11.4.8 元器件选择明细表

设计人员根据卫星型号的研制阶段选择元器件后，应参照表7的格式编制元器件选择明细表，由主管设计师或工程组长核准，由物资管理部门按型号汇总。汇总的元器件选择明细表须经评审组评审，通过评审的元器件选择明细表，可作为采购部门编制元器件采购文件的依据。

表 7 元器件选择明细表

工程型号： 系统代号： 分系统或单机代号： 研制阶段：

序号	元器件名称	型号规格	采用标准	质量等级	单机用量	生产单位	备注
编制人： (签名) 日期： 年 月 日		审核： (签名) 日期： 年 月 日		评审组长： (签名) 日期： 年 月 日		批准： (签名) 日期： 年 月 日	

11.4.9 元器件选择评审

若无其它规定，元器件的选择评审应在厂(所）及院(基地）两级进行。评审的具体要求按QJ 3065.1—1998的规定。

12 材料、机械零件和工艺选用控制

12.1 概述

卫星机械产品故障已占卫星总故障的相当比例。造成机械产品故障的原因主要是设计选用材料及工艺不合理，外购零件或借用件不合格等。卫星质量与可靠性与材料、机械零件和工艺的选用有直接关系。设计师、总指挥应控制对星上材料、机械零件和工艺的选用，QJ 3125—2000、ECSS—Q—70A—1996规范了材料、机械零件和工艺选用控制要求与程序。设计师应与材料和工艺部门密切配合，以选用好的材料、机械零件和工艺。

材料、机械零件和工艺选用控制包括技术和管理两方面要求，除了设计人员必须遵循本标准的有关规定外，还应指定相应的管理机构负责选用控制的管理工作。

12.2 目的

材料、机械零件和工艺的可靠性是卫星等航天器可靠性的基础，材料、机械零件和工艺的选用控制是

保证卫星等航天器可靠性最重要的基础工作之一。

材料、机械零件和工艺控制总的目的是：确保用于卫星上的材料、机械零件和工艺使卫星在功能、可靠性、进度和成本等各方面在卫星的全寿命周期内满足卫星的总体要求。

为达到上述目的，应按卫星的有关文件、标准分别编写材料、机械零件和工艺的保证大纲作为实施和检查材料、机械零件和工艺选用控制的依据。

12.3 材料、机械零件和工艺选用控制原则

12.3.1 材料及机械零件选用原则

卫星材料及机械零件选择准则如下：

a） 材料及机械零件选择必须满足卫星等航天器技术指标要求，适应卫星等航天器运行工作环境的物理、化学特性条件，保证其质量和可靠性要求；

b） 卫星等航天器上应尽可能选择经过发射和轨道运行考验的材料及机械零件；

c） 优先从产品大纲规定的材料及机械零件选用目录中选择；应尽可能压缩材料及机械零件的牌号、品种、规格和供应单位；

d） 尽可能选择按国家标准、国家军用标准、航天行业标准、航天企业标准进行质量控制的材料及机械零件；

e） 选用新研制的或没有标准的材料及机械零件的数量必须控制在最低限度，应进行充分的论证和试验，对试验结果进行鉴定，并严格审批手续；

f） 选择材料及零件时，应充分考虑其供应的持久性和工艺稳定性。

12.3.2 工艺选用原则

工艺选用原则如下：

a） 无论工艺已被确认或有待确认，工艺选择均应考虑工艺的下列要素：

1） 可检验性；

2） 可操作性；

3） 稳定性；

4） 经济性。

b） 应优先采用已被确认的工艺，优先顺序如下：

1） 在航天行业标准中规定的工艺；

2） 通过应用试验，获得满意结果并已确认的工艺；

3） 同一生产厂已成功使用的工艺。

c） 尽可能选用已在卫星等航天器上成功应用过的成熟工艺。

d） 工艺选用必须从卫星等航天器的整体、工艺全过程考虑其选择工艺的合理性。当需用多种工艺制造卫星时，必须考虑各种工艺的协调性。

12.4 步骤与方法

12.4.1 材料选用

12.4.1.1 编制材料清单

材料应按优选目录选用，对新材料应进行确认与验证。

材料清单应包括下列主要内容：

a） 卫星代号；

b） 材料名称及牌号；

c） 生产厂、采购文件(规范或标准）；

d） 材料的主要物理、化学特性和类型；

e） 工艺参数(表面粗糙度、热处理、混合比例、固化温度等）；

f） 用途和使用部位；

g） 环境要求；

h） 批准状态(根据批准机构、试验报告和类似的应用情况等确定）。

12.4.1.2 材料评价

对未知特性的关键材料在确认之前，应逐件进行评价。进行评价时应制定材料评价大纲。

至少应考虑下列内容：

a） 材料使用范围的限制；

b） 材料的物理、化学和/或功能特性及其数值和允许偏差等；

c） 环境参数对特性的影响；

d） 验收准则。

12.4.1.3 材料确认

材料确认的内容包括：

a） 卫星承制方应编制关键材料评价大纲，备齐所需的评审文件；

b） 对材料关键特性应进行评价，在评价之前，卫星承制方应提供采购文件、验收方法及相关文件；

c） 对每种关键材料，卫星承制方应制定确认大纲，再进行检查或确定材料以合适的安全系数满足飞行要求，已获得确认状态；

d） 确认状态取决于确认报告和相应技术文件的评审。

12.4.2 机械零件选用

12.4.2.1 编制机械零件清单

机械零件清单应包括下列主要内容：

a） 卫星代号；

b） 机械零件名称及牌号；

c） 机械零件的种类；

d） 生产厂、采购文件(规范或标准）；

e） 功能和特性摘要；

f） 用途和使用部位；

g） 使用环境要求；

h） 批准状态(根据批准机构、试验报告和类似的应用情况等确定）。

12.4.2.2 零件评价

对所有关键机器零件应进行评价和鉴定或仅进行鉴定。

关键机械零件的评价应考虑下列内容：

a） 编制关键机械零件评价大纲，备齐所需的评审文件；

b） 机械零件的物理、化学、功能特性及其尺寸和公差；

c） 环境参数对特性的影响；

d） 验收准则。

12.4.2.3 零件鉴定

零件鉴定的内容包括：

a） 对关键零件卫星承制方均应进行鉴定；

b） 对关键零件，卫星承制方应制定鉴定大纲，再进行检查或确定零件是否以合适的安全系数满足设计要求；

c） 在开始鉴定前，鉴定文件要齐全；

d） 鉴定状态取决于鉴定报告和相应文件的评审。

12.4.3 工艺选用

12.4.3.1 确定关键工艺与编制工艺清单

工艺清单应包括下列内容：

a） 工艺(项目）代号：在工艺清单中作为该工艺的标志，在卫星等航天器各研制阶段应相同；

b） 工艺名称；

c） 工艺规范；

d） 工艺说明(加工方法简述）；

e） 用途和使用部位；

f） 工艺提供方(工艺实施单位）；

g） 批准状态(根据批准机构、试验报告和类似的应用情况等确定）。

在对卫星等航天器上所用工艺进行关键性分析和风险分析的基础上，确定关键工艺项目并进行标识。同时将其清楚地分类。

12.4.3.2 工艺评价

对所有关键工艺应进行评价和确认或仅进行确认。

工艺评价应考虑以下几个方面：

a） 卫星承制方应根据工艺关键性分析对需评价的关键工艺进行评价；

b） 卫星承制方应编制关键工艺的评价大纲和报告；

c） 关键工艺评价至少应考虑其使用范围限制、执行参数及允许偏差，确定安全系数和验收准则。

12.4.3.3 工艺确认

工艺确认的内容包括：

a） 卫星承制方应根据工艺关键性分析对所有关键工艺进行确认；

b） 卫星承制方应编制并执行确认大纲；

c） 确认状态取决于相应文件的评审和批准报告。

13 可靠电路设计

13.1 概述

电路是电子产品最基本的组成部分，它们的可靠性对卫星的寿命及可靠度有着至关重要的影响。

电路设计与产品设计应同步进行，在产品电性能设计的同时，应尽可能同步进行电磁兼容性（EMC）设计、热设计、机械结构设计、可靠性设计和防辐射设计，在它们之间建立起并行设计的概念，即一体化设计的新思路、新观念。

可靠电路设计应将传统的电路设计经验、设计方法与机、电、热一体化设计的新观念相结合，同时还

要与现代电路设计手段相结合，例如进行EDA（电子设计自动化）软件仿真设计。对于复杂的逻辑电路，建议采用VHDL软件配合EDA软件进行设计，主要根据VHDL的语法规则，对系统目标的逻辑行为进行描述，然后通过综合工具进行电路结构的综合、编译、优化，通过仿真工具进行逻辑功能的仿真和系统时延的仿真。当然即使采用VHDL软件进行设计，最终生成的目标电路，其复杂度也与电路的描述方法和设计规划水平有关。

电路优化设计是建立在最优化方法的基础上，为解决电路设计而开拓出的新的设计理论和方法，卫星可靠电路设计应遵循之，同时应与可靠电路设计相结合。

卫星系统的可靠电路设计包括的内容很多，主要有电路简化、优化设计；瞬态干扰和过应力保护；电磁兼容性设计、印制板设计、CMOS电路防锁定设计、单粒子事件防护、电路容差设计与分析、潜在电路分析、降额设计等。本章主要规定电路简化、优化设计；瞬态干扰和过应力保护；CMOS电路防锁定设计；单粒子事件防护等。

13.2 电路优化、简化设计

13.2.1 电路优化、简化设计原则

电路优化、简化设计应遵循以下原则：

a） 方案简单。在满足合同规定的或总体要求的性能指标的条件下，线路越简单就越可靠。所以卫星用电路的设计决不要追求超过任务要求的高技术指标，决不要为了性能上的少许改进而增加大量的元器件。

b） 具有飞行经验与继承性。设计中要尽可能采用经过飞行试验考验的、可靠性高的、最好是标准化的线路和元器件。

c） 具有技术成熟性。若采用未经飞行试验考验的新元件、新线路、新技术、新材料或新工艺，在上天以前必须经过预先研究和充分的地面试验鉴定，完成质量评价后才能用于飞行件。对新技术既要严格把关，又要积极采用。例如对卫星上某些专用电路二次集成技术，模块化高频化二次电源技术等，应当积极而慎重地研究和应用。用厚膜混合工艺组装的高可靠模块电源是卫星二次电源的发展方向。要求将滤波模块与电源模块组合在一个模块内，同时具有输入端、输出端共模差模抑制电路和输入端浪涌电流抑制电路，输出端还具有隔离二极管等。

d） 按元器件优选目录规定选用元器件，尽可能压缩元器件的品种、数量、规格和厂家。

e） 选用集成度高的元器件。集成度的提高，可减少元器件之间的连接、接点以及封状数目。

f） 正确使用元器件。应充分掌握元器件的参数、功能、性能等技术指标与要求以及其使用规范。

g） 电路设计要兼顾性能和可靠性，不能顾此失彼。

h） 合理简化。为了提高可靠性所必需的冗余电路不能省略；为了提高稳定性和可测试性所加的元器件一定不可少；不要因为简化一个元器件而使其它元器件承受过高的电应力；用一个元器件来完成几种功能时必须十分慎重，不能用未经验证的元器件来代替经过验证的可靠元器件，应注意有一些“兼用”是不稳定的、不可靠或不正确，例如用 CMOS 集成电路的转换电平“兼作”比较电压基准就是如此。

i） 注意综合利用电路的软件功能和硬件功能，充分发挥软件功能而使电路硬件得到简化。

j） 数字逻辑电路设计要采用布尔代数简化技术来消除多余元件，用最少的逻辑门和输入端来实现同样的逻辑功能。对于复杂的逻辑电路，采用 VHDL 软件配合 EDA 软件进行设计，先进行虚拟设计，最终确定目标电路。

k） 尽可能采用数字电路取代模拟电路。数字电路标准化程度高、稳定性好、通用性强、噪声容限大、接口参数易匹配、比模拟电路可靠，所以用数字电路代替模拟电路是简化设计提高可靠性的一个途径。

l） 尽可能采用集成电路取代分立器件，因为集成电路本身就是标准电路，焊点和连线少，密封性好，同一芯片上的半导体器件等温性好，集成电路失效率比用相同功能的分立器件组成的电路低。当集成度增加时，集成电路失效率增加不多，所以应采用中大规模集成电路来代替许多小规模集成电路。

m） 电路设计具体要求：

1） 可靠电路设计应弄清电路特性要求，然后选择与之匹配的电路类型和元器件。电路类型很多，如模拟电路和数字电路，有源电路与无源电路，集总参数电路与分布参数电路，小功率电路与大功率电路，谐振腔式电路与微带结构电路，窄带电路与宽带、超宽带电路等。要求电路类型与电路特性吻合，且与元器件选用匹配。

2） 可靠电路设计应满足电路匹配特性要求。匹配特性是所有电路设计共同关心的问题，这是电路设计的关键。如牢牢把握电路输入与输出匹配，最佳噪声匹配，功率匹配和阻抗匹配。

3） 可靠电路设计还应满足稳定性要求。首先要求电路本身稳定，即实现无条件稳定；同时要求在规定的环境条件下，由于电路参数变化引起电路性能变化，要控制在任务要求的范围内。

4） 可靠电路设计还应注意寄生响应要求，控制杂散信号影响，注意静电放电特性要求和微放电要求。由于卫星的长寿命、高可靠等特殊要求，这些要求在电路设计时也应加以足够重视，使设计的电路能适应空间各种环境条件，特别对于射频（微波）电路更显得重要；同时能适应卫星、各分系统间、各设备间相互干扰和影响，使大家能兼容工作。

5） 采用 CMOS 电路时，还应注意抗锁定设计，要求满足 Vss≤Vin≤Vcc (Vdd)和 Vss≤Vout≤Vcc (Vdd）等抗锁定条件。

6） 可靠电路设计还应满足空间抗辐射加固要求。

7） 可靠电路设计、元器件选用应与装联工艺密切结合。

n） 采用微组装技术（MPT）。

13.2.2 微组装技术

随着表面贴装技术（SMT）工艺日趋成熟和片式元器件（SMD）可靠性的日益提高，MPT是星、船可靠电路设计的首选方向。混合集成电路（HIC）主要指薄膜混合集成电路和厚膜混合集成电路，是用薄膜技术和厚膜技术的成膜方法制造，然后贴半导体芯片或其他元器件构成的集成电路，具有高密度、高可靠、高的电气和物理性能，也是星、船可靠电路设计的发展方向。

近几十年来，集成电路进入高速发展时代，大规模（LSI）、甚大规模（VLSI）、超大规模（ULSI）集成电路的不断发展，一片集成电路取代几十片、几百片乃至上千片中小规模集成电路已不鲜见，电路设计与组装技术结合，导致组装技术向微组装方向发展。微组装技术是在混合集成技术基础上发展起来的一门更高级、更精密、更复杂的综合性技术。其典型产品就是多芯片组件模块（MCM）。MPT在要求小型轻量的军事领域，在要求高速度的计算机领域和要求高性能、高密度的高新技术领域和航天技术领域有着广阔的应用市场。

从组装结构上可以把微组装技术分为三个组装层次：芯片互连技术、一级组装技术和二级组装技术。

芯片互连技术是指将IC芯片的焊区和载体与单芯片组件或多芯片组件基板焊区直接连接起来的技术。

芯片互连主要有三种方式：倒装片焊（又叫焊料凸点焊）、丝焊、载带自动键合（TAB）和凸点载带自动键合（BTAB）。近来又发展了微凸点连接(MBB）技术。倒装片焊就是将带有凸点电极的电路芯片面朝下，使凸点作为芯片电极与基板布线层的焊点焊接，从而实现芯片级微组装。

一级组装技术包括芯片载体，单芯片组件和多芯片组件的制造技术，重点是MCM的制造技术。MCM的关键技术是高密度多层互连基板制造。一级组装技术实现模块级微组装。

二级组装技术是指一级组装技术所产生的产品组装到大型多层互连插板、插卡或母板上形成电子系统或子系统，实现产品级微组装。

微组装的组装层次如图15所示。

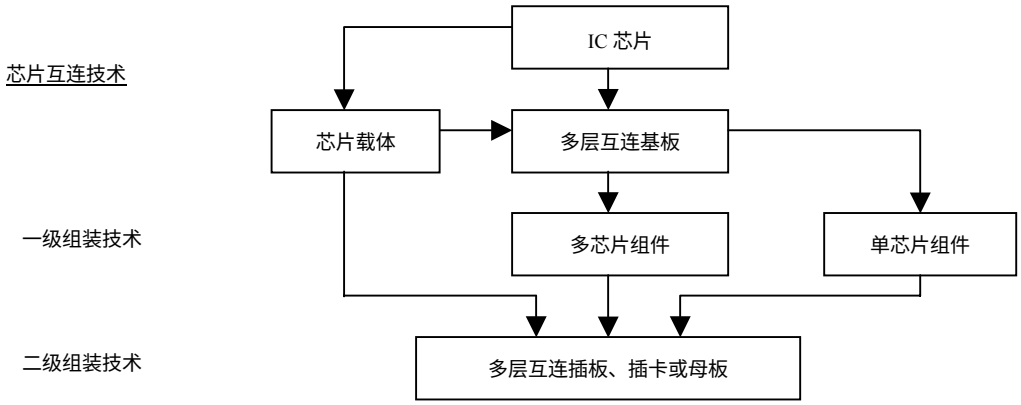


图 15　微组装技术的三个层次

13.3　瞬态和过应力保护

13.3.1　概述

卫星一次电源或二次电源、电源滤波器、印制板电子组装件上的去耦电容等，它们都会使负载呈现容性。容性负载的特性是在通电的瞬间流过一个很大的充电电流，也就是浪涌电流。极短时间的浪涌电流会损坏继电器触点，也可能使熔断器误熔断，所以要进行瞬态过应力保护。为此，有时需要实测浪涌电流，测试传感器要能响应微秒级的电流变化。一般要求设备的浪涌电流特性应小于熔断器瞬态过载特性。

对于高速系统的设计必须面对互连延迟引起的时序问题以及串扰，传输线效应等信号质量问题。元器件和 PCB 板的参数，元器件在 PCB 板上布局，高速信号布线等因素，都会引起信号质量问题。像误触发、阻尼振荡、过冲、欠冲等信号质量问题都会造成时钟间歇振荡和数据出错，所以 IC 电路稳定状态的持续时间，即一般称为建立时间和保持时间对于电路设计特别重要，为达到这个目的，器件的正确端接技术和布局的约束机制是保证信号质量的行之有效的办法。

电子线路中采用负反馈可以大大降低元器件参数变化的影响，使线路性能指标得到稳定。因此，凡是能用负反馈的地方都应采用负反馈。但应注意，由于分布电容和寄生电感的存在，往往使放大器在某些频域出现不应有的振荡（负反馈变成正反馈），或者使振荡器出现停振或间歇振荡。因此，应用自动控制原理对具有闭环反馈的电子线路进行稳定性分析，采取补偿措施，保证一定的稳定裕度是必要的。

电子线路在断→通、负载转换及状态变化的瞬态过程中，节点参数如电压、电流的相位和幅值波形等对元件性能的影响也应加以分析。许多数字脉冲和时序电路往往利用波形特性来进行操作，如脉冲前沿或后沿触发等。因此波形的准确性，上升、下降时间及延时准确性往往成为电路正常工作的关键。错误触发、复位不良、负阻效应、可控硅效应等问题都是必须避免的，因此，必须进行过渡过程分析和时序分析。要注意逻辑电路实际时延和用仿真软件进行仿真时理想时延的差异。

电子器件常常被电压瞬变所损坏。小型半导体器件因为引线接头的热惯性很小，特别容易受到损坏。MOS器件、由肖特基热垒法生产的高频元器件、许多微电路（如采用小的有效结面积、薄的介电材料、喷镀金属的截面和N^+保护环结构的ROM、RAM及PROM）、精密薄膜电阻等元件很容易被静电放电所损坏。因此应当采取防静电和防瞬态影响的措施。瞬态影响有二种表现，一是使元器件永久损坏；另一种是造成瞬态干扰，即所谓单次翻转事件（SEU），如双稳态触发器或施密特触发器被偶然触发，计数器可能改变计数，存贮器可能由于激励电流或直接的磁场效应而改变，开关可能改变状态，瞬变可能被当作控制信号而放大和译码等。

13.3.2 设计原则

13.3.2.1 一般原则

瞬态和过应力保护设计的一般原则为：

a） 对于不同类型的元器件，应根据其过应力失效模式的种类采取不同的保护措施；

b） 凡是能用负反馈的地方都应采用负反馈；

c） 应用自动控制原理对具有闭环反馈的电子线路进行稳定性分析，采取补偿措施；

d） 电子线路在断→通、负载转换及状态变化的瞬态过程中，节点参数如电压、电流的相位和幅值波形等对元件性能的影响应加以分析；

e） 许多数字脉冲和时序电路必须进行过渡过程分析和时序分析，注意逻辑电路实际时延和用仿真软件进行仿真时理想时延的差异；

f） 应当采取防静电和防瞬态影响的措施。

13.3.2.2 与一次电源间接口过流保护设计原则

与一次电源间接口过流保护设计原则为：

a） 采用的短路保护措施应尽量分散到设备、部件、模块单元级，优选分散到模块单元级；

b） 同一功能的主份单元与备份单元不能共用一个过流保护，应分别设置；

c） 采用双独立母线供电的卫星，主份单元与备份单元的过流保护要分别挂一根母线，应分别设置。

13.3.2.3 二次电源与负载间电接口过流保护设计原则

二次电源与负载间电接口过流保护设计原则为：

a） 采用的短路保护措施应尽量分散到模块单元或单元线路，可采用分级设置模式，且主份负载与备份负载应分别设置；

b） 一旦某个负载出现短路故障后，应考虑故障能切换，能重新组合成新的工作模式；

c） 二次电源本身的输出容量，在热效应允许情况下，应尽可能大一些。

13.3.2.4 二次电源自身保护过流保护设计原则

二次电源自身保护过流保护设计原则为：

a） 采用的短路保护措施应为限流—自动恢复保护，禁止采用截流型保护；

b） 采样点可设置在原边回路和副边回路，优选设置在原边回路；

c） 最大阀值的设置应与热设计结合，即应考虑在空间环境压力$<1.3\times10^{-3}$Pa 下，二次电源仍能维持正常工作，绝对杜绝二次电源因热失控而出现故障。

13.3.3 方法

13.3.3.1 瞬态电压保护常用方法

进行瞬态电压保护的常用方法是：

a） 在应受保护的电压线和吸收高频的地线之间加装电容器；

b） 采用二极管或稳压管保护以防止电压超过固定值（错位值）；

c） 采用串联电阻以限制电流值。

13.3.3.2 不同类型的元器件过应力保护方法

对于不同类型的元器件，应根据其过应力失效模式的种类采取不同的保护措施，其方法是：

a） 对二极管，过应力失效模式有两种：反向击穿和浪涌电流过大而烧毁。采取的措施是给二极管串联一电阻，限制浪涌电流；并联一电容，抑制瞬变电压。

b） 对三极管，过应力保护方法为：

1） 电源对地加电容以抑制由电源来的瞬态干扰；

2） 基极加输入电阻减小基极浪涌电流；

3） 基极对地加反向二极管或电容或稳压管以防止基极—发射极反向击穿；

4） 集电极—基极间加稳压管以防止反向击穿；

5） 集电极对地加稳压管以防止反向击穿。

c） 对晶闸管，过应力失效模式主要是控制端电流过大和电压过高。可用 LR 积分器来限制初始浪涌电流，或用电阻限制电流；用稳压管限制电压瞬变。

d） 对 TTL 器件：

1） 电源对地加电容以抑制由电源来的瞬态干扰；

2） 输入对电源、输入对地各加反向二极管以防止输入信号高于电源或低于地电压；

3） 输出对地加反向二极管，以防止输出电压负于地电压。

e） 对 CMOS 器件，主要是防止锁定失效和防静电（为静电敏感器件）。

13.3.3.3 与一次电源间接口设计方法

一旦发生对主母线短路故障，过流保护常用切断与主母线电连接的方法。这些方法有三种形式或将其组合应用：

a） 熔断器保护设计；

b） 过流自动保护设计；

c） 遥控切换保护设计。

13.3.3.4 二次电源与负载间电接口设计方法

一旦发生二次电源输出短路故障，过流保护可采用两种方法：

a） 切断与二次电源输出的电连接，包括熔断器保护和遥控切换保护；

b） 限流保护，包括采用限流电阻和新型稳压限流器件。

13.3.3.5 二次电源自身保护方法

二次电源自身保护方法为：

a） 电流互感器采样方法，其采样点有设置在功率变压器原边回路和功率变压器副边回路两种方法；

b） 电阻器采样方法。

13.4 CMOS 电路防锁定设计

13.4.1 概述

13.4.1.1 锁定现象

CMOS电路采用NMOS、PMOS互补对称结构，具有抗干扰能力强和静态功耗低等优点而得到广泛应

用，但由于存在寄生可控硅结构，容易引起锁定失效。锁定是一种状态，该状态下由于输入、输出或电源的过应力，触发了内部寄生可控硅结构，形成一条低阻抗通路，并在消除或终止触发条件后仍保持。上述过应力可以是过电压或电流浪涌、过快的电压或电流变化率、或任何其它能引起寄生可控硅结构形成正反馈的非正常状态，例如辐射单粒子效应。

13.4.1.2 CMOS 电路触发锁定分类

不考虑单粒子效应，CMOS电路触发锁定分两类：

a） 电源端过压触发：电源电压上升，超过最大额定电压 V_{CCmax}（V_{DDmax}）而触发 CMOS 电路产生锁定，称为电源过压触发；

b） 输入或输出端电流触发：外界高电压造成输入端或输出端流入或流出足够的电流而触发 CMOS 电路产生锁定，称为电流触发。

CMOS电路触发锁定并保持其锁定态，必须满足寄生可控硅结构被外界的过电应力触发，且建立了正反馈；工作电源能提供CMOS电路保持锁定态所需的电压和电流。

13.4.1.3 锁定特性

GB/T 17574—1998规定如下锁定特性（详细阐述，参见标准）：

a） 锁定电压 *Vlatch*；

b） 锁定电流 *Ilatch*；

c） 锁定电源电压 $V_{CC}(latch)$（$V_{DD}(latch)$）；

d） 锁定电源电流 $I_{CC}(latch)$（$V_{DD}(latch)$）；

e） 锁定态（电源）电压 $V_{CC}(L)$（$V_{DD}(L)$）；

f） 锁定态（电源）电流 $I_{CC}(L)$（$I_{DD}(L)$）；

g） 锁定态保持电流 $I_{CC}(H)$（$I_{DD}(H)$）。

13.4.1.4 不发生锁定触发的理想条件

不发生锁定触发的理想条件为：

a） $V_{CC}(V_{DD}) \leq V_{CC}\max(V_{DD}\max)$；

b） $V_{CC}(V_{DD})+0.5V \geq V_{IN} \geq V_{SS}-0.5V$；

c） V_{CC}（V_{DD}）$+0.5V \geq V_{OUT} \geq V_{SS}-0.5V$。

在具体的线路中，由于种种原因上述条件往往遭受破坏而得不到满足，抗锁定设计就是要在这种情况下使CMOS电路不发生锁定。

13.4.1.5 不同工艺中小规模 CMOS 电路系列的锁定特性

不同工艺的中小规模CMOS电路，锁定特性有明显差异，如表8所示。

表 8 不同工艺的中小规模 CMOS 电路锁定特性

项目	4000 系列	HC/HCT 系列	AC/ACT 系列	FCT 系列	HCS、HCTS、ACS、ACTS
生产工艺	金属栅	硅栅	硅栅、外延	微量掺杂、外延	兰宝石
锁定电源电压	>20V	>7V	>6V	>6V	无锁定
输入端 锁定电流	>±10mA	>±20mA	>±20mA	>±20mA	
输出端 锁定电流	>±10mA	>±20mA	>±50mA	>±50mA	

13.4.2 CMOS 电路工作电源及供电回路抗锁定设计

13.4.2.1 电源电压

就抗锁定设计言，CMOS电路工作时，任何情况下（包括电源接通和关断）连同纹波、噪声等等，电源端电压的峰值不得超过允许的最大值V_{ccmax}（V_{DDmax}），超出了允许的最大值称为过电压。过电压，特别是在过压脉冲激励下，容易使CMOS电路诱发锁定。

13.4.2.2 电源负载调整率

简单的低频数字电路，配置的电源可以很简单，整流、滤波加一个稳压二极管就行。随着系统频率和复杂程度的提高，对电源的要求也相应改变。在一些情况下，还要求具有良好的动态负载调整率，否则负载快速变化时，会出现过大的电压上冲和跌落，影响系统的速度、功耗和噪声容限。特别是由于噪声容限得不到保证而影响正常工作，甚至造成锁定。

计算功耗是为了估算负载对电源电压的影响，也是为了进行降额设计。CMOS电路功耗由静态和动态两部分组成：

a） 静态功耗由最大静态电流乘以电源电压；

b） 动态功耗可分为三份：

——由外部负载电容充放电电流造成；

——由内部节点电容充放电电流造成；

——由 P 沟和 N 沟晶体管瞬间穿透导通电流造成。

13.4.2.3 供电回路滤波去耦

要规范和精心设计印制板上由电源回路和接地回路构成的供电回路。供电回路阻抗增加，会恶化电源的工作性能，降低CMOS电路的噪声容限，造成负载之间耦合，引起功能的混乱。一点接地、辐射状布线、缩短长度、加大宽度等原则，对减小供电回路阻抗都很重要。

当供电回路出现电压浪涌，或CMOS电路负载变化时，都会使电路电源电压上冲或跌落，去耦电容可以减少上冲或跌落的幅度。

13.4.2.4 电源限流

13.4.2.4.1 稳压电源限流

如果系统采用分散供电，可以做到电源和相应负载独立限流。如果系统集中供电，一个电源供应多个负载，电源的限流特性是根据总负载确定的，要实现各负载独立限流，只能将负载分组，各组采取限流。

13.4.2.4.2 电源入口电阻器限流

在印制板组装件的电源入口处串以电阻器，是最简单的一种限流方法。它的负面影响是：电源电压随负载变化而变化，影响系统的驱动能力、工作速度、噪声容限，以及造成各负载之间耦合。可以依靠去耦电容来降低耦合程度，但不能全部去耦，因此在供电回路中以减小串接电阻器的阻值，或不串接电阻器为好。

13.4.2.4.3 采用并联稳压二极管的电阻器限流

电阻器限流并联稳压二极管，在相当大的程度上可以削弱电阻器限流带来的负面影响，同时还可以吸收供电回路出现的浪涌电压，减少过压触发锁定的可能。

13.4.2.4.4 采用限流型低压差线性稳压电源

低压差线性稳压电源具有低功耗稳压，限流等特性。采用它，既能弥补一般二次电源限流特性的不足，又能取代电阻器限流，消除其负面影响，是CMOS电路实现局部稳压限流的理想器件。

13.4.2.5 电源操作注意事项

13.4.2.5.1 电源的开启和关闭

不应通过电源的开启和关闭，直接向电子线路供电或断电，特别是一些线性稳压电源在开启时伴有过压脉冲，造成CMOS电路过电压触发锁定。必须另外设置一个供/断电开关。先接通电源开关，电源正常工作后，再利用供/断电开关，向电子部件供电或断电。只有在供/断电开关关断的情况，电源方能启动或停止。

13.4.2.5.2 多电源系统电源电压动态过程的匹配

多电源系统电源操作顺序应做到：CMOS电路的工作电压建立在先，输入信号建立在后；反之，要先切断输入信号，然后断开工作电压。复杂的系统，有时可能做不到，应尽可能采用单电源供电，不得已时，各个电源的电压建立过程力求相互匹配。

即使是单电源供电系统，由于各个CMOS电路的局部滤波电容值不同，负载变化也各异，特别是个别CMOS电路单独采用电阻器限流，这些原因使得各个CMOS电路电源端电压建立过程不一致。应使这种电压差异减小到最低限度。

13.4.3 CMOS 电路输入回路抗锁定设计

13.4.3.1 CMOS 电路输入端抗锁定条件

输入回路抗锁定设计的关键在于使输入回路不向输入端提供电流，或提供的电流小于规定的锁定电流值。

任何情况下，若能满足：$V_{SS} \leq V_{IN} \leq V_{CC}(V_{DD})$，CMOS电路输入端电流很小，可以忽略，就不可能产生输入端锁定电流。

若不能满足上述条件，则应满足条件：$I_{IN} \leq Ilatch$。

13.4.3.2 单电源系统输入回路存在的触发锁定因素

单电源系统一般都能实现CMOS电路的直接互连，但要注意以下情况：

a） 个别 CMOS 电路电源端回路的阻抗较大，电源端电压的建立过程慢于输入信号的建立。或负载电流瞬时增大，电源电压出现跌落。参看图 16，上述两种情况都会造成 $V_{IN} > V_{CC}(V_{DD})$。同样，接地端到地线回路的阻抗较大，负载电流瞬时加大时，接地端电位抬高，造成 $V_{IN} < V_{SS}$。

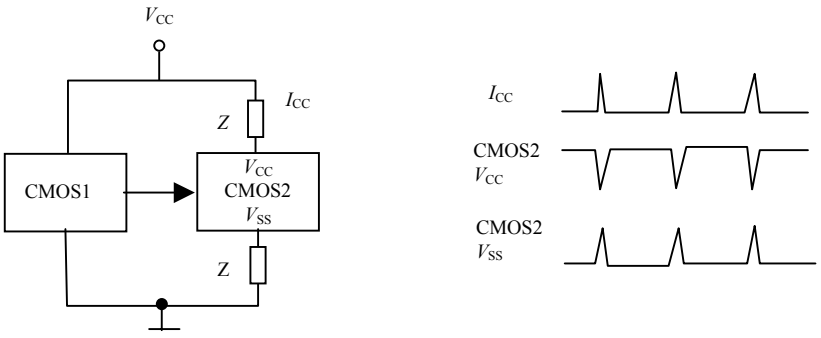


图 16 个别 CMOS 电路的输出

b） 信号经长线与输入端相连，如图 17 所示，当开关闭合时，由于长线分布参数 L 和输入电容 C 的作用，A 点会出现负向振荡，幅值大小与输入线长度有关。强干扰还会通过耦合进入未加屏蔽的长线。

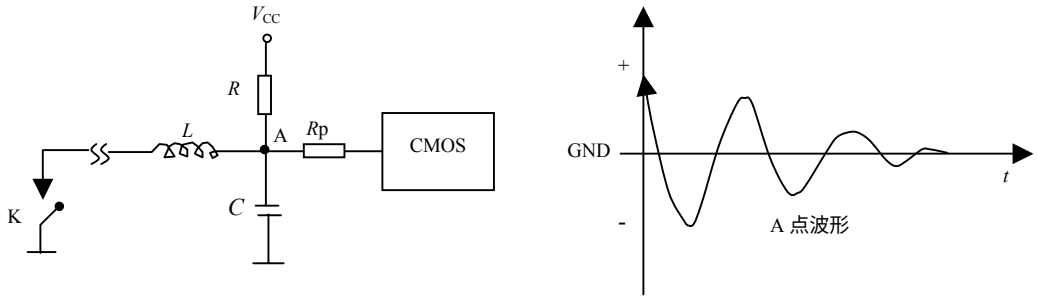


图 17　信号经长线与输入端相连时的振荡

c）　由于某些线路固有的特点，有可能在 CMOS 电路输入端产生电流。例如 RC 微分线路，R 接 V_{CC} 时，会产生大于电源电压的正向微分脉冲；R 接地时，会产生低于 V_{SS} 的负向微分脉冲。见图 18。

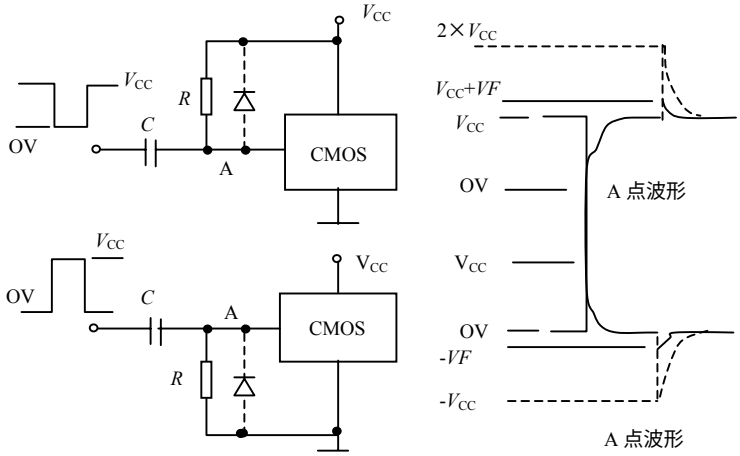


图 18　RC 微分电路的微分脉冲

再如由反向器构成的多谐振荡器（见图19），注意A点波形，每一个振荡周期，会出现一个高于V_{CC}，一个低于V_{SS}的两个尖峰电压。

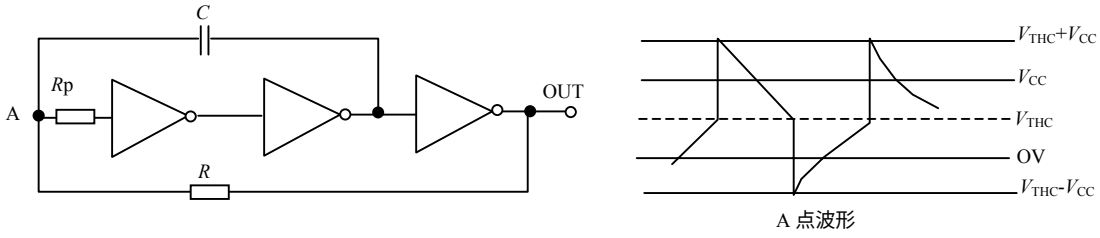


图 19　多谐振荡器的尖峰电压

13.4.3.3　多电源系统输入回路存在的触发锁定因素

13.4.3.3.1　等电压多电源系统

参看图20，电源1理应先于电源2建立。反之，电源1后于电源2关断，实际上，往往难于控制这种先后

顺序。

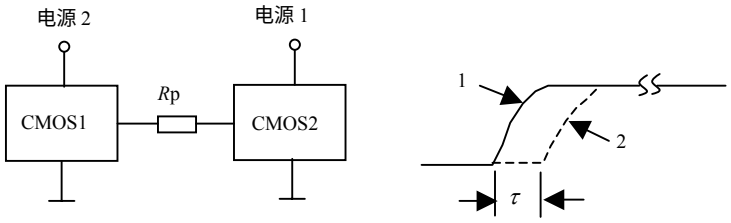


图 20　两电源系统输入回路

13.4.3.3.2　不等电压多电源系统

不等电压多电源系统往往有以下两个特点：

a）　信号源的工作电源不但有正电源，还可能有负电源，例如双电源运算放大器。若不采取措施，输出信号就有正负极性。

b）　作为信号源正电源的电压值，一般高于 CMOS 电路的电源电压值。同时 CMOS 电路电源电压还经常迟后于信号源电压建立。例如 CMOS 电路电源是由信号源电源降压稳定而成。

13.4.3.4　CMOS 电路输入回路抗锁定措施

13.4.3.4.1　措施之一——电阻限流

输入端加限流电阻，如图19中的R_p，对防止电流触发锁定，效果显著是抗锁定设计的重要措施，但要注意它对工作速度所产生的影响。

13.4.3.4.2　措施之二——二极管箝位

二极管箝位所起的是分流作用，如果二极管为锗二极管或肖特基二极管，正向导通压降小，使得流入或流出CMOS电路的电流接近零，达到抑制电流触发锁定的目的。

13.4.4　CMOS 电路输出回路抗锁定设计

13.4.4.1　CMOS 电路输出端抗锁定条件

正常情况下，输出高电平时，向外供给电流；低电平时，从外吸取电流。要从CMOS电路的输出端触发锁定，情况得反过来，输出高电平时，外界向它供给（正向触发电流）；低电平时，外界从它吸取（负向触发电流）。输出回路抗锁定设计的关键也是要使输出回路不向输出端提供不正常的触发电流，或提供的电流小于规定的锁定电流值。和输入端一样，应满足下列两个条件中的一个：

a）　任何情况下，若能满足 $V_{SS} \leq V\text{out} \leq V_{CC}(V_{DD})$，就不可能产生输出端锁定电流；

b）　若不能满足条件 a），则应满足 $I_{out} \leq I_{latch}$。

13.4.4.2　输出回路存在的触发锁定因素

13.4.4.2.1　输出端接大电容性负载

CMOS电路输出端的电容负载，在充电之后，若发生以下情况，电容上的电荷通过输出端释放成为锁定触发电流：

a）　CMOS 电路电源端掉电，电压下降；

b）　CMOS 电路电源端电压瞬时跌落，当供电回路阻抗高、动态负载大、滤波不好时，尤为明显。

13.4.4.2.2　输出端连接长线或接监测设备

输出端连接长线或接监测设备的触发锁定因素：

a）　CMOS 电路输出经长线与负载相连，易受外界干扰，引入浪涌电压，造成 $V_{ouT} > V_{CC}(V_{DD})$或 $V_{ouT} < V_{SS}$；

b） CMOS 电路输出端若与测试设备相连，当设备接地不良时，也会引入种种干扰电流。

13.4.4.3 CMOS 电路输出回路抗锁定措施

防止输出端电流触发锁定的主要措施也是采用电阻器限流或二极管分流。图21是一个实例，生产厂建议：当C_x大于0.5 μF时，应串联限流电阻R_p，或在R_x上并联一个二极管。

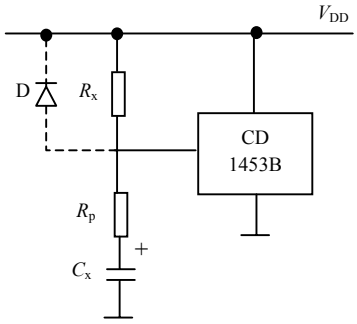


图21 采用电阻器、二极管防锁定

13.5 单粒子事件防护设计

13.5.1 概述

随着半导体技术的发展和空间应用的广泛， SEE效应的随机性和多样性给航天器可靠性设计带来严重挑战。解决SEE问题的难点在于：系统中不可能全部采用SEE“免疫”硬件，系统工程师必须在可选用的器件、系统性能、SEE风险、价格等各种因素之间做出权衡；SEE问题涉及辐射环境、半导体物理、辐射效应产生机理等多种因素，不能直接照搬可靠性预示方法和工具；需要工程设计人员同辐射效应分析人员的密切配合。

空间辐射对星载电子设备的破坏作用可分为两大类：总剂量电离效应TID和单粒子事件效应SEE。总剂量电离效应是长期暴露在电离辐射环境导致的器件性能损伤，通常称为辐射剂量累积效应。单粒子事件效应是单个入射电离粒子在一个器件中沉积足够能量所引发的效应，属于随机发生的效应。

SEE失效模式取决于入射粒子和器件类型。通常将失效模式分为软错和硬错两大类。定义软错为器件发生非破坏性效应，表现为存储单元的位翻转，电路输入/输出端口或电路逻辑发生的瞬态变化，也包括器件运行中断、功能异常、发生HALT等现象。硬错是造成器件功能永久性破坏的效应，它有可能，但不一定，导致器件物理损坏。无论是硬错还是软错，对于一种给定的应用有可能容许其发生，也有可能不容许其发生。对TID影响的分析是从发射时刻开始累计，直到失效时间或者失效剂量才评估。SEE属于随机事件，首先要通过地面辐射试验获得器件在辐射环境中的特性；还要通过计算预示给定飞行轨道的辐射环境。空间辐射环境预示与器件试验结果一起用来计算该器件在特定飞行任务中发生SEE的概率。对SEE危害程度的评估涉及到辐射物理、器件工程、固态物理、电子工程、可靠性分析、系统工程等很多技术领域。

13.5.2 目的

通过分析和评估SEE风险，帮助型号研制人员用最低的价格和较为简便的方法将SEE风险降低到可以承受的水平，保证卫星在辐射环境中的成功运行，是空间飞行器产品电路单粒子防护设计的目的。

13.5.3 原则

单粒子事件防护设计原则如下：

a） 尽量选用具有抗灾难性 SEE 能力的器件；

b） 关键部位尽量选用 SEE 加固器件；

c） 采用非抗 SEE 加固器件的电路必须采取电路级加固措施；

e） 电路加固设计必须确保电路不存在发生灾难性 SEE 的隐患；

f） 电路加固设计要保证非灾难性 SEE 发生不影响电路的正常功能。

13.5.4 步骤

单粒子事件防护设计步骤如下：

a） 结合卫星任务进行星载电子设备所面临的空间辐射环境预示，以确定引发电路 SEE 的辐射源和 SEE 发生频度；

b） 进行器件 SEE 效应在电路中的传播分析，以 SEE 效应对电路影响的危害度分析作为电路抗 SEE 加固设计基础；

c） 确定器件选用原则，关键部位尽量选用 SEE 加固器件；尽量选用具有抗灾难性 SEE 能力的器件；

d） 对非 SEE 加固的关键器件进行单粒子效应敏感度评估；

e） 基于可获取到的器件进行电路加固设计，必须防止电路中存在发生致命性 SEE 的隐患，可允许非致命性 SEE 发生，但其发生不得影响电路正常功能；

f） 进行电路抗单粒子效应加固效果评估，确保加固后的电路不会因 SEE 导致功能异常、更不会导致电路失效。

13.5.5 方法

13.5.5.1 单粒子效应的分析与评估

单粒子效应的分析与评估方法：

a） 器件单粒子效应敏感度试验：通过重离子试验、高能质子试验或锎源试验获得 LET 阈值（L_{th}）、饱和错误截面（σ_{sat}）、质子能量阈值等器件单粒子效应敏感度参数。

b） 单粒子翻转率预计：器件的单粒子翻转率是器件临界电荷 QC、器件敏感区域的几何尺寸（与设计有关）和航天器轨道环境的函数，普遍采用 CRÈME、Space Radiation 等软件计算单粒子翻转率。软件可以根据特定星际和磁层的气象条件、航天器轨道、电子元器件周围的屏蔽层及所用器件的特性，计算入射到任何地球轨道上任何航天器内部电子元器件的宇宙射线的微分/积分通量和 LET 能谱；利用试验获取的器件单粒子效应敏感度特性，可计算出 SEU 率。

对于翻转阈值比较低（30MeVcm2/mg以下）的器件，在工程上，可采用Petersen近似公式估算器件在Adams 10%最坏环境下的单粒子翻转率。

13.5.5.2 系统抗单粒子效应的要求和分析

13.5.5.2.1 系统抗单粒子效应的要求

在对系统提出抗单粒子效应要求之前，必须完成航天器在寿命期内的轨道辐射环境预示。如根据轨道高度、倾角给出宇宙射线环境的LET谱、质子最坏情况的注量和能量以及太阳耀斑的影响。

在提出系统抗单粒子效应要求时，考虑的是在轨道粒子辐射环境中系统的性能指标要求。这些要求应考虑单粒子效应发生时对任务性能影响的各种可能性，主要有两个主要方面：系统可用性及信息（数据）质量。

13.5.5.2.1.1 系统可用性

系统可用性要求设计师考虑严重事件可能导致的任务损失，以及若干需要地面干预或自主恢复的事件。一般而言，系统的可用性用“ 不因单粒子效应导致任务损失 ”表示，这一要求表明，对单粒子效应的

要求相当于单点失效应不造成任务损失的可靠性要求。其它的可用性要求可以根据系统可接受的单粒子效应引起的干扰程度、干扰频度、干扰最大持续时间来确定。在提出抗单粒子效应要求时，往往需要在任务目标和成本之间折衷。

13.5.5.2.1.2 信息的完整性

当对系统或分系统分别提出要求时，应考虑有效载荷功能要求提出信息（数据）完整性的要求。因为在许多情况下，单粒子造成的软错误只影响数据，而不改变系统的功能。

13.5.5.2.2 SEE 传播分析

研究SEE如何在航天器内部传播及其所造成的影响。在很多方面，SEU传播分析类似于传统的电路模拟和故障模式及影响分析（FMEA）。

13.5.5.2.2.1 器件分析

在确定敏感区域以及对器件工作影响后，将进一步研究SEE对器件性能的影响。例如，针对SEU效应的分析包括：

a） 器件工作异常；

b） 器件输出错误；

c） 存贮器结构中错误的存取；

d） 传输线上的噪声毛刺；

e） 器件模式改变（如由工作状态转为待机状态）；

f） 器件定时错误。

可以用利用传统的电路模型，用带有SEU引发错误的数字测试向量确定对器件性能的影响，也可以在SPICE中注入一瞬态信号，来模拟对器件性能的影响。

器件SEU传播分析方法流程见图22。

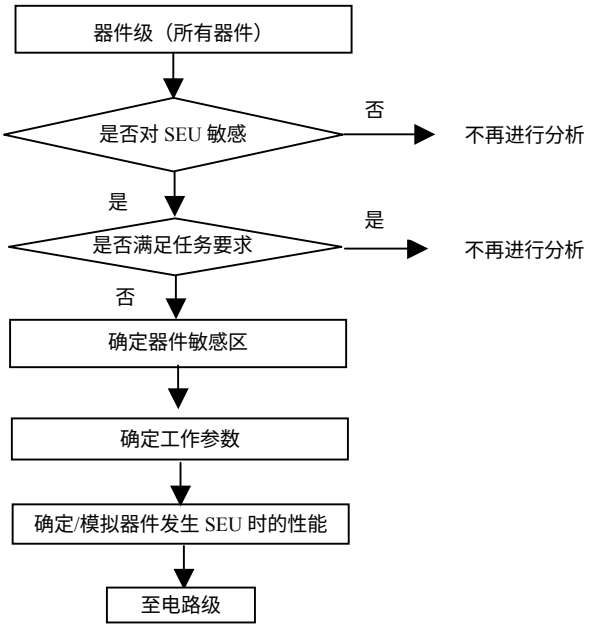


图22 器件SEU传播分析方法

13.5.5.2.2.2 电路级分析

电路级分析步骤遵循13.5.5.2.2.1 c）~13.5.5.2.2.1 e），但分析的重点是器件的性能对电路的工作和性能的影响。如已知在静态存储器SRAM中发生位翻转，但电路级的效应取决于SRAM的应用：

a） 用于数据贮存的 SRAM 中发生 SEU，将导致错误数据点；

b） 用于存贮软件程序的 SRAM 中发生 SEU，将导致处理器非法操作；

c） 用于两个集成电路（如处理器和直接存贮器寻址控制器）共享缓存的 SRAM 中发生 SEU，将导致严重的错误隐患（如程序流程、错误数据点等）。

分析可使用模拟或数字工具进行模拟，分析结束就会给出在电路中潜在的SEU及其对电路工作的影响。

13.5.5.2.2.3 系统级分析

在分系统级、系统级分析中可采用同样的方法，在每一级的分析中均将前一级作为黑箱，不关心其内部细节，只分析其对更高一级的影响。

13.5.6 单粒子效应防护设计技术

13.5.6.1 概述

单粒子辐射效应发生在星载设备半导体器件中。对单粒子效应的防护可以从器件选用、电路设计、整机设计等多层次采取措施。采用具有抗单粒子效应能力的器件是最稳妥的解决途径，但受各种因素限制这一技术途径很难实现。例如：没有或缺少抗单粒子效应的加固器件、无法得到这类器件或者是经费不足以支持全部采用这类器件。因此，必须从电路、整机层次采取防护措施，防止器件中发生的单粒子效应对电路、设备和系统的功能、性能造成影响、损伤和故障。

13.5.6.2 列入辐射加固保证计划

单粒子效应防护是辐射加固保证的重要组成，辐射加固保证影响项目的所有方面：设计、生产、产品保证的采购。因此应贯穿于从可行性研究开始的整个项目寿命的始终。

基本步骤：

a） 辐射环境分析；

b） 通过试验和分析确定系统、部件、元器件的响应；

c） 确定对策；

d） 对策的实施与验证；

e） 在任务期间监视“加固对策”的有效性；

f） 加固经验的传递。

加固保证要反映在“辐射效应控制计划”中，包括定义外部环境、部件所在内辐射环境、要求的辐射设计裕度。定义分系统工程师需要采取的必要措施。

13.5.6.3 器件选用原则

器件选择的动态过程见图23。

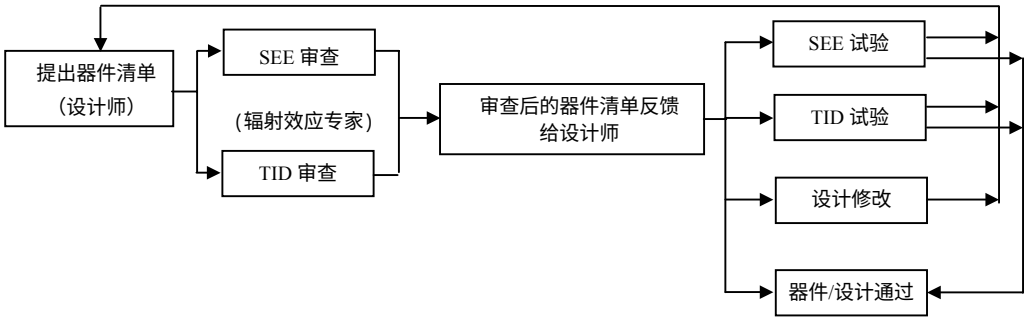


图 23 器件选择的动态过程

13.5.6.3.1 选用器件时应对其单粒子效应敏感度进行评估

单粒子翻转敏感度主要取决于器件敏感单元的几何尺寸、版图结构和工艺，因此对器件单粒子翻转敏感度的评估可以利用已有的同一版图结构和同一工艺的器件的试验数据或分析结果，试验数据可查选国际上有关辐射效应数据库或公开发表的试验数据。

13.5.6.3.2 器件单粒子效应敏感度排序

对于单粒子引起的翻转，敏感度由低到高的顺序可以排列为：CMOS/SOI、CMOS/SOS、体硅CMOS、NMOS、I^2L、TTL。

为避免单粒子引起的闩锁，推荐采用不存在闩锁问题的CMOS/SOI、CMOS/SOS或外延CMOS工艺器件。外延CMOS器件具体应用时，应对其闩锁阈值进行评估。

13.5.6.4 电路和设备级单粒子事件防护设计准则和方法

13.5.6.4.1 单粒子翻转的防护设计

13.5.6.4.1.1 单粒子翻转的防护设计措施

可采用硬件、软件和容错技术从系统级进行单粒子翻转防护设计。

13.5.6.4.1.2 对于存储器类器件

存储器类器件防护设计包括：

a） 存储器抗 SEU 配置策略：

——操作系统的内核及预期不再更改的程序放在 ROM 区；

——与航天器安全、有效载荷安全、航天员安全以及飞行成败有关的程序和数据放在 ROM 区；

——可编程器件的初始化程序及系统的中断向量需要驻留在 ROM 区。

b） 采用 EDAC 技术对重要数据存储器（SRAM、EEPROM）进行 SEU 防护。

EDAC是防止单粒子翻转的有效技术。可用纯软件方式实现，也可用电路、ASIC芯片实现，目前采用ASIC方式实现EDAC编码已成为主流趋势。一些新型辐射加固的CPU已将EDAC算法集成在芯片中。

单粒子对存储器器引发SEU的后果是在数据应用中体现，因此消除其影响的思想是基于容错，即允许SEU发生、而不允许SEU引发的错误扩展。采取的措施是在应用数据时给予检错、纠错。也即，在CPU从存储器读取数据时进行检错纠错。常用的检错纠错方法有：

——奇偶校验码；该方法只能检测错误，而不能校正错误；

——海明码：可校正一位错误并检测两位错误；

——R-S 码：能够检测和校正数据结构中的多位和连续错误。

c） 采用三重冗余存储及表决系统。

将重要数据存放在存储器内三个不同的物理位置，应用时从三处取出，按照三取二比对/刷新原则处理也可以消除SEU造成的瞬时错误。

13.5.6.4.1.3 与控制有关的器件

a） 硬件系统设计；

——采用多机冗余和容错系统；

——采用定时监视器（WDT）。

b） 软件设计。

软件是SEU防护的重要途径，已被广泛应用，并取得有效成果。在软件设计中可以采用：自诊断

程序、多重编码、指令复执、程序卷回、分支流程作两次以上有效性判别、程序模块间的隔离、建立健康和安全模式、软件定时监视器WDT、地面遥控注入等方法。还可以借助初始化消除瞬态干扰影响。对多余内存单元要进行处理，确保将程序引回到正常入口。

13.5.6.4.1.4 比较器应用中的 SEU 防护措施

输入端电压差（V_{IN+}-V_{IN-}）尽可能大。

13.5.6.4.2 单粒子闩锁的防护设计

所有CMOS设计者都在输入、输出端口采用边界保护和钳位电路来防止常规电路应用中出现的锁定。然而，在辐射环境中瞬态信号不再局限于I/O端口，重离子或质子电流脉触发的锁定可能发生在I/O端口、也可能发生在CMOS器件的内部。一旦发生锁定，体硅CMOS中的寄生可控硅结构将被置为导通状态、并保持状态直到电源关闭或者被锁定区域的电压降到很低。发生锁定期间电流可能很高，在某些电路中几百毫安以上的电流流过锁定发生部位，使其局部迅速升温，不仅造成局部材料损伤，还会使锁定蔓延到其它部位。

因其潜在的灾难性破坏作用，对于空间系统锁定成为非常严重的问题。最保守的方法是不采用任何锁定易发器件。也提出了一些在系统级或分系统级通过敏感锁定引起的过电流、然后关断电源，破坏锁定状态维持的条件来克服锁定的方法。然而，必须在锁定发生后几个毫秒之内关闭电源才能避免灾难性故障发生。很难保证锁定检测电路完全有效，因为在复杂电路中存在很多具有不通电流特征的不同锁定通路。

a） 推荐采用 CMOS/SOS 或 CMOS/SOI 器件。

由于CMOS/SOS和CMOS/SOI工艺器件不存在寄生可控硅结构，因而不存在发生单粒子锁定效应的问题。

b） 电源端限流。

由于单粒子引起器件锁定的路径和电流特性比较复杂，设计师应综合考虑器件的SEL响应、电路设计和防护方法。目前多采用在器件电源端增加限流电阻的方法。为了减少印制板设计困难，也经常采用划分电路模块，按模块添加限流电阻的方式。其缺点是造成电路板上各器件所用电源不等，容易带来CMOS器件可控硅效应的副作用。通常也采用在电路板电源入口处统一限流的方法。

c） 采用定时监视器 WDT 可解决单粒子引起的微锁定问题。

d） 多机容错结构中要采取各单机单独供电工作模式，防止锁定对整机的影响。

13.5.7 某型号卫星控制处理机的设计示例

某型号卫星姿态控制分系统（ACS）在整个任务寿命期间（设计寿命15年）为卫星提供精确、可靠和高度自主的控制。姿态控制系统有为任务各阶段控制卫星姿态所需要的各种敏感器、控制执行机构和电子处理设备。系统运行高度自主，包括自检、故障模式检测以及必要时采取纠正措施。

卫星控制处理机（SCP）是ACS的主要部件，它以微处理器为核心，使用固件（软件存在PROM中）实行所要求的数据处理和控制算法。SCP是对总剂量辐射、单粒子翻转（SEU）及静电放电（ESD）加固的，以满足严格的运行和自主控制要求。

SCP采用美军标的MAS281微处理器，该CPU为CMOS/SOS工艺，提供600kbps的数据处理能力，并能高效地执行高级软件语言Ada。支持CPU的还有专门设计的CMOS/SOS大规模集成电路和进行I/O处理的专用混合集成电路。

SCP 的线路和组装设计是按 HS-601 卫星 17 年任务要求设计的，对半导体器件的总剂量辐射防护提

供了至少 2：1 的裕量。由于 SCP 采用了 CMOS/SOS 工艺，因此对 SEU 基本不敏感，出错率为 2×10^{-9} 位/天，此值相当于 SCP 每 700 年出错一次。因此，卫星不会因为 SCP 中的 SEU 而丢失姿态。

SCP软件都存贮在PROM中作为固件，成为不会丢失信息的存贮器。在RAM中存贮了任务表、状态变量、系数、ACS数据、再编程数据和遥测数据。数据RAM有EDAC保护，EDAC对存贮的数据能纠正一个位的错误和检出双位错误。SCP采用处理器和单元两级看门狗定时器电路进行故障检测。

除完成正常控制功能以外，还有内容广泛的自主故障监测和响应（AFDR）逻辑。设计AFDR的目的是对卫星关键部件的健康状况进行连续监测，并在出现异常时，执行自主纠正程序，以维持卫星的通信服务。此外，AFDR的状态还通过遥测传到地面，以帮助地面人员对异常进行分析研究。

14 元器件降额设计

14.1 概述

元器件降额使用是一项十分重要的元器件应用原则。元器件应用必须全面贯彻GJB/Z 35－1993。

元器件降额就是使元器件使用所承受的应力低于其额定值，以达到延缓其退化，提高使用可靠性的目的。通常用应力比（工作应力与额定应力之比，又称降额因子）和环境温度来表示。

降额准则就是规定电子、电气和机电元器件在不同应用情况下应降额的参数和量值。降额准则还包括与降额有关的元器件应用指南。

通常元器件有一个最佳的降额范围。在这个范围内，元器件的工作应力的降低对其失效率的降低有显著的改善，设备的设计容易实现，且不必在设备的重量、体积、成本方面付出大的代价，见图24。

元器件降额定为三级。选哪一级是根据设备的可靠性要求、设计成熟性、维修费用和难易程度，以及对安全性要求、设备的重量、尺寸的限制等因素来确定的。

a） Ⅰ级降额：

最大的降额，元器件使用可靠性的改善最大，比之更大的降额对可靠性的改善有限，而且要付出更大的代价。

适用于对安全性要求高、可靠性要求高且采用新技术、新工艺的，失效后不宜维修，重量、尺寸有苛刻限制的设备。卫星使用的元器件均实施Ⅰ级降额。

b） Ⅱ级降额：

中等降额，对元器件使用可靠性的改善明显，设计上较Ⅰ级降额易于实现。

适用于失效将引起装备或保障设施损坏，有高可靠性要求且采用专门设计，需要支付较高的维修费用的设备。

c） Ⅲ级降额：

最小的降额，对元器件使用可靠性改善的相对效益最大，但绝对效益不如Ⅰ级和Ⅱ级降额，在设计上最容易实现。

适用于无安全性要求，采用成熟技术，故障后可以迅速、经济地修复，对尺寸和重量无大的限制的设备。

降额可以有效地提高元器件的使用可靠性，但降额是有限度的。如上所述，过度的降额所取得的实际效益与付出的代价比会降低，不值得。此外，有些元器件过度降额会使其正常特性发生变化，如晶体管的工作点，放大系数下降，甚至有可能找不到满足设备或电路要求的元器件。过度的降额还可能引入元器件新的失效机理。如电阻器、电容器受潮变质，金属化纸介电容器漏电“自愈效应”的明显下降，小型云母

电容器的低电平失效。过度降额还可能导致元器件数量的不必要增加，结果反而使设备的可靠性下降。某晶体管失效率与应力比的关系见图24。

实际使用中允许降额量值的某些变动，但不允许改变降额等级。凡达不到降额要求的元器件均应列入可靠性关键项目。更不能用降额来补偿解决劣质元器件的使用问题。

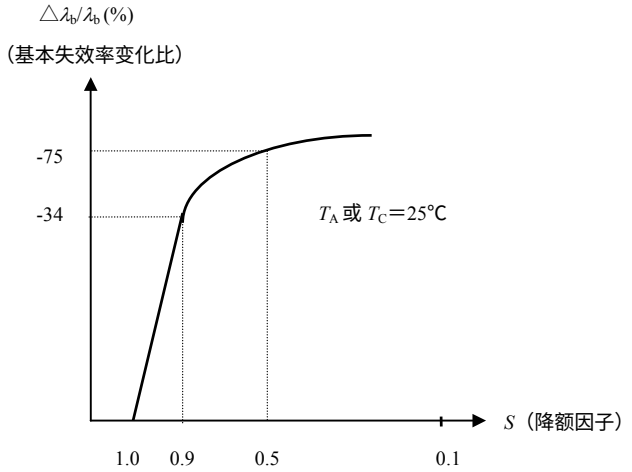


图 24　某晶体管失效率与应力比的关系

14.2　元器件的降额参数和量值

各种元器件的降额参数和量值见GJB/Z 35—1993, 该标准提出了12类72种元器件的降额要求，元器件降额概况见表9。大部分元器件绘有降额曲线。半导体器件的降额曲线如图25，电容器降额曲线如图26，电阻器的降额曲线形式与半导体器件相似，功率管降额曲线如图27。

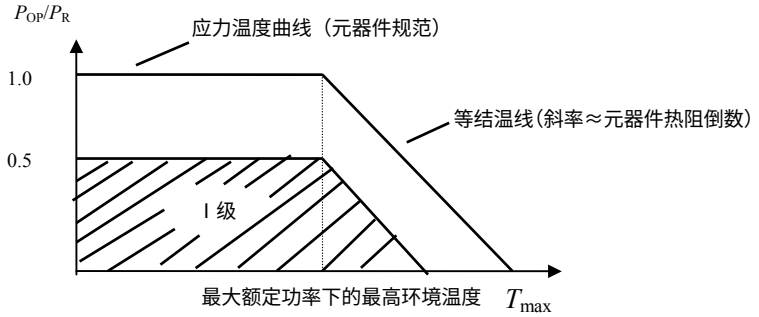


图 25　晶体管降额曲线

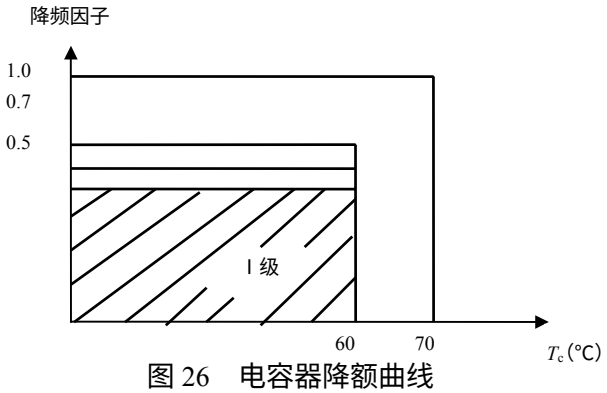


图 26　电容器降额曲线

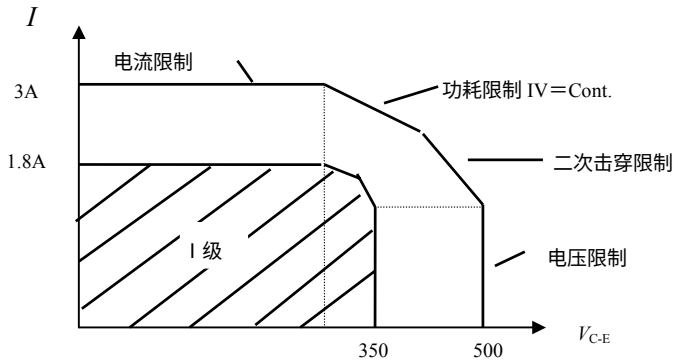


图 27　功率管降额曲线

表 9　元器件降额准则一览表

元　器　件　种　类			降　额　参　数	降　额　等　级		
				Ⅰ	Ⅱ	Ⅲ
集成电路	模拟电路	放大器	电源电压	0.70	0.80	0.80
			输入电压	0.60	0.70	0.70
			输出电流	0.70	0.80	0.80
			功　　率	0.70	0.75	0.80
			最高结温　℃	80	95	105
		比较器	电源电压	0.70	0.80	0.80
			输入电压	0.70	0.80	0.80
			输出电流	0.70	0.80	0.80
			功　　率	0.70	0.75	0.80
			最高结温　℃	80	95	105
		电压调整器	电源电压	0.70	0.80	0.80
			输入电压	0.70	0.80	0.80
			输入输出电压差	0.70	0.80	0.85
			输出电流	0.70	0.75	0.80
			功　率	0.70	0.75	0.80
			最高结温　℃	80	95	105
		模拟开关	电源电压	0.70	0.80	0.85
			输入电压	0.80	0.85	0.90
			输出电流	0.75	0.80	0.85
			功　　率	0.70	0.75	0.80
			最高结温　℃	80	95	105
	数字电路	双极型电路	频　　率	0.80	0.90	0.90
			输出电流	0.80	0.90	0.90
			最高结温　℃	85	100	115
		MOS 型电路	电源电压	0.70	0.80	0.80
			输出电流	0.80	0.90	0.90
			频　　率	0.80	0.80	0.90
			最高结温　℃	85	100	115
	混合集成电路		厚膜功率密度　W/cm^2	7.5		
			薄膜功率密度　W/cm^2	6.0		
			最高结温　℃	85	100	115
	大规模集成电路		最高结温　℃	改进散热方式以降低结温		

表 9（续）

元器件种类		降额参数		降额等级		
				I	II	III
分立半导体器件	晶体管	反向电压	一般晶体管	0.60	0.70	0.80
			功率 MOSFET 的栅源电压	0.50	0.60	0.70
		电流		0.60	0.70	0.80
		功率		0.50	0.65	0.75
		功率管安全工作区	集电极—发射极电压	0.70	0.80	0.90
			集电极最大允许电流	0.60	0.70	0.80
		最高结温（T_{jm}）℃	200	115	140	160
			175	100	125	145
			≤150	T_{jm}-65	T_{jm}-40	T_{jm}-20
	微波晶体管	最高结温		同晶体管		
	二极管（基准管除外）	电压（不适用于稳压管）		0.60	0.70	0.80
		电流		0.50	0.65	0.80
		功率		0.50	0.65	0.80
		最高结温（T_{jm}）℃	200	115	140	160
			175	100	125	145
			≤150	T_{jm}-60	T_{jm}-40	T_{jm}-20
	微波二极管 基准二极管	最高结温		同二级管		
	可控硅	电压		0.60	0.70	0.80
		电流		0.50	0.65	0.80
		最高结温（T_{jm}）℃	200	115	140	160
			175	100	125	145
			≤150	T_{jm}-60	T_{jm}-40	T_{jm}-20
	半导体光电器件	电压		0.60	0.70	0.80
		电流		0.50	0.65	0.80
		最高结温（T_{jm}）℃	200	115	140	160
			175	100	125	145
			≤150	T_{jm}-60	T_{jm}-40	T_{jm}-20
固定电阻器	合成型电阻器	电压		0.75	0.75	0.75
		功率		0.50	0.60	0.70
		环境温度		按元件负荷特性曲线降额		
	薄膜型电阻器	电压		0.75	0.75	0.75
		功率		0.50	0.60	0.70
		环境温度		按元件负荷特性曲线降额		
	电阻网络	电压		0.75	0.75	0.75
		功率		0.50	0.60	0.70
		环境温度		按元件负荷特性曲线降额		
	线绕电阻	电压		0.75	0.75	0.75
		功率	精密型	0.25	0.45	0.60
			功率型	0.50	0.60	0.70
		环境温度		按元件负荷特性曲线降额		

表 9（续）

元器件种类		降额参数		降额等级		
				I	II	III
电位器	非线绕电位器	电压		0.75	0.75	0.75
		功率	合成、薄膜微调	0.30	0.45	0.60
			精密塑料型	不采用	0.50	0.50
		环境温度		按元件负荷特性曲线降额		
	线绕电位器	电压		0.75	0.75	0.75
		功率	普通型	0.30	0.45	0.50
			非密封功率型	—	—	0.70
			微调线绕型	0.30	0.45	0.50
		环境温度		按负荷特性曲线降额		
热敏电阻器		功率		0.50	0.50	0.50
		最高环境温度 ℃		T_{AM}-15	T_{AM}-15	T_{AM}-15
电容器	固定玻璃釉型	直流工作电压		0.50	0.60	0.70
		最高额定环境温度 T_{AM} ℃		T_{AM}-10	T_{AM}-10	T_{AM}-10
	固定云母型	直流工作电压		0.50	0.60	0.70
		最高额定环境温度 T_{AM} ℃		T_{AM}-10	T_{AM}-10	T_{AM}-10
	固定陶瓷型	直流工作电压		0.50	0.60	0.70
		最高额定环境温度 T_{AM} ℃		T_{AM}-10	T_{AM}-10	T_{AM}-10
	固定纸/塑料薄膜	直流工作电压		0.50	0.60	0.70
		最高额定环境温度 T_{AM} ℃		T_{AM}-10	T_{AM}-10	T_{AM}-10
	电解电容器 铝电解	直流工作电压		—	—	0.75
		最高额定环境温度 T_{AM} ℃		—	—	T_{AM}-20
	电解电容器 钽电解	直流工作电压		0.50	0.60	0.70
		最高额定环境温度 T_{AM} ℃		T_{AM}-20	T_{AM}-20	T_{AM}-20
	微调电容器	直流工作电压		0.30～0.40	0.50	0.50
		最高额定环境温度 T_{AM} ℃		T_{AM}-10	T_{AM}-10	T_{AM}-10
电感元件		热点温度（T_{HS}） ℃		T_{HS}-（40～25）	T_{HS}-（25～10）	T_{HS}-（15～0）
		工作电流		0.6～0.7	0.6～0.7	0.6～0.7
		瞬态电压/电流		0.90	0.90	0.90
		介质耐压		0.5～0.6	0.5～0.6	0.5～0.6
		扼流圈工作电压		0.70	0.70	0.70

表 9（续）

元 器 件 种 类	降 额 参 数			降 额 等 级		
				Ⅰ	Ⅱ	Ⅲ
继电器	连续触点电流	小功率负荷（＜100 mW＝		不降额		
		电阻负载		0.50	0.75	0.90
		电容负载（最大浪涌电流）		0.50	0.75	0.90
		电感负载	电感额定电流	0.50	0.75	0.90
			电阻额定电流	0.35	0.40	0.75
		电机负载	电机额定电流	0.50	0.75	0.90
			电阻额定电流	0.15	0.20	0.75
		灯丝负载	灯泡额定电流	0.50	0.75	0.90
			电阻额定电流	0.07～0.08	0.10	0.30
	触点功率（用于舌簧水银式）			0.40	0.50	0.70
	线圈吸合电压		最小维持电压	0.90	0.90	0.90
			最小线圈电压	1.10	1.10	1.10
	线圈释放电压		最大允许值	1.10	1.10	1.10
			最小允许值	0.90	0.90	0.90
	最高额定环境温度（T_{AM}） ℃			T_{AM}-20	T_{AM}-20	T_{AM}-20
	振动限值			0.60	0.60	0.60
	工作寿命(循环次数)			0.50	—	—
开 关	连续触点电流	小功率负荷（＜100 mW＝		不降额		
		电阻负载		0.50	0.75	0.90
		电容负载（电阻额定电流）		0.50	0.75	0.90
		电感负载	电感额定电流	0.50	0.75	0.90
			电阻额定电流	0.35	0.40	0.50
		电机负载	电机额定电流	0.50	0.75	0.90
			电阻额定电流	0.15	0.20	0.35
		灯泡负载	灯泡额定电流	0.50	0.75	0.90
			电阻额定电流	0.07～0.08	0.10	0.15
	触点电压			0.40	0.50	0.70
	触点功率			0.40	0.50	0.70
连接器	工作电压			0.50	0.70	0.80
	工作电流			0.50	0.70	0.85
	最高接触对额定温度 T_M ℃			T_M-50	T_M-25	T_M-20
电 机	最高工作温度 ℃			T-40	T-20	T-15
	低温极限 ℃			0	0	0
	轴承载荷额定值			0.75	0.90	0.90

表 9（续）

元器件种类		降额参数		降额等级		
				Ⅰ	Ⅱ	Ⅲ
灯泡	白炽灯	工作电压（如可行）		0.94	0.94	0.94
	氖/氙灯	工作电压（如可行）		0.94	0.94	0.94
电路断路器		电流	阻性负载	0.75	0.75	0.90
			容性负载	0.75	0.75	0.90
			感性负载	0.40	0.40	0.50
			电机负载	0.20	0.20	0.35
			灯丝负载	0.10	0.10	0.15
		最高额定环境温度 T_{AM} ℃		T_{AM}-20		
保险丝		电流额定值	＞0.5A	0.45～0.5	0.45～0.5	0.45～0.5
			≤0.5A	0.2～0.4	0.2～0.4	0.2～0.4
		T＞25℃时，增加降额 1/℃		0.005	0.005	0.005
晶体		最低温度 ℃		T_L+10	T_L+10	T_L+10
		最高温度 ℃		T_U-10	T_U-10	T_U-10
微波管		最高额定环境温度 ℃		T_{AM}-20	T_{AM}-20	T_{AM}-20
		输出功率		0.80	0.80	0.80
		反射功率		0.50	0.50	0.50
		占空比		0.75	0.75	0.75
声表面波器件		输入功率(f ＞100 MHz)		降低+10dBm		
		输入功率(f ＞100 MHz)		降低+20dBm		
纤维光学器件	光纤光源	峰值光输出功率		0.50(适用于 ILD)		
		电流		0.50(适用于 LED)		
		结温		设法降低		
	光纤探测器	PIN 反向压降		0.60		
		结温		设法降低		
	光纤与光缆	温度 ℃		上限额定值-20;下限额定值+20		
		张力	光纤	耐拉试验的 0.20		
			光缆	拉伸额定值的 0.50		
		弯曲半径		最小允许值的 2.0		
		核辐射		按产品详细规范降额或加固		
导线与电缆		最大应用电压		最大绝缘电压规定值的 0.50		
		最大应用电流 A	线规(A_{VG})	30，28，26，24，22，20，18，16		
			单根导线电流(I_{SV})	1.3, 1.8, 2.5, 3.3, 4.5, 6.5, 9.2, 13.0		
			线规(A_{VG})	14 12 10 8 6 4		
			单根导线电流(I_{SV})	17.0, 23.0, 33.0, 44.0, 60.0, 81.0		

14.3 几点说明

降额设计的几点说明如下：

a） 降额的本质对绝大部分元器件而言是降低半导体器件的结温和元件的热点温度，通过电功率的降低和环境温度的降低来实现。

b） 大规模集成电路不能降低电应力，但可通过降低环境温度来实现降额。半导体器件在高温情况下电化学反应和金属迁移会加快，导致器件老化和失效。大规模集成电路体积很小，厚度不到微米级，器件的功耗虽然不大，但在很小的空间内热向器件底部扩散，再向外部传出。工作期间有源结点会产生很高的温度和温度梯度，结点的时间常数只有几个微秒。因此必须考虑器件的散热问题。

c） 功率晶体管的二次击穿是主要的失效模式，因此在安全工作区必须降额，见图 27 示。此外功率晶体管在多次热循环中会出现热疲劳，因此要规定热循环的额定值，温度变化越大，允许的热循环次数就越少。

d） 转动部件的电机除考虑轴承负载的降额外，其工作温度必须同时考虑轴承和绕组的不同要求。温度过低对轴承不利，反之，温度过高对绕组的绝缘保护不利。

15 热设计

15.1 概述

热设计的任务是使卫星及其电子设备或部件的热参数，如温度、温度差、湿度等，保持在要求的范围内。为满足设计要求而采用的方法通常有：控制外界进出卫星及电子设备的热流；用高性能的导热和隔热部件控制传热路径；用电加热器控制温度水平或温度差；储存热能并加以利用；用气体强迫对流强化传热；用制冷机创造低温环境；湿度控制等。

15.2 目的

卫星热设计的目的是使卫星及其电子设备的热参数满足设计要求，为电子设备提供合适的热环境，进而提高卫星及其电子设备的可靠性。

电子设备热设计的目的是确保元器件工作在允许的温度范围内，确保元器件的关键部位不超过设计允许的最高温度。如高精度晶体震荡器需要恒温控制，半导体器件，尤其是大功率晶体管、集成电路的结温不能超过降额后允许的最高结温（或壳温）。以提高电子设备及元器件的可靠性。

15.3 热设计原则

15.3.1 热设计的一般原则

热设计的一般原则如下：

a） 在满足热设计要求的前提下，应力求简化设计，减少选用的热控产品的种类和数量。

b） 优先选用结构简单、无运动部件、不耗电或少耗电的被动热控技术和产品，如热控制涂层、固定热导热管、隔热组件、扩热板、导热填料等，必要时也可选用主动热控技术和产品，如恒温电子线路控制的加热回路等。

c） 优先选用经过飞行验证的成熟技术和热控产品。选用的新产品，应通过规定的环境试验，并经过鉴定。

d） 应对全寿命周期中规定的环境条件和应力进行全面分析，设计时留有足够的余量。设计余量参见 GJB 1029—1990 第 7 章。

e） 权衡可靠性要求与其他技术指标，如加工温度范围、重量、能耗、费用及研制周期等，以获得优化方案。

15.3.2 卫星热设计原则

卫星热设计的原则如下：

a） 应考虑各阶段的环境影响，应满足卫星轨道、姿态、工作模式等可能出现的极端热工况和极端冷工况的要求；

b） 应建立卫星内电子设备热量排放的通道，选择外热流小或外热流变化小的卫星表面作为散热面；

c） 应在卫星外表面设置适当的热控涂层和多层隔热组件，降低太阳周期性照射引起的卫星及其电子设备的温度波动；

d） 应对工作温度范围、温度差、湿度要求严格的电子设备或环境进行主动控制；

e） 应对热环境更恶劣的舱外电子设备采取必要的措施，确保它们的温度满足要求；

f） 应为有效载荷提供满足要求的热接口；

g） 机械类热控产品应降额使用；电子类热控产品的元器件降额系数应符合 GJB/Z 35—1993 第 5 章的规定；

h） 必要时电加热器及其控制电路可分别或同时采用备份；起重要作用的固定热导热管应采用贮备工作方式；

i） 设计应考虑太阳紫外辐射、质子和电子辐照、原子氧侵蚀对热控产品的影响，如卫星外表面热控涂层的退化等；

j） 热控产品应安装牢固，防止活动部件在振动与冲击载荷下因变形、位移而卡死；

k） 对污染特别敏感的热控产品，如低太阳吸收比热控涂层和低发射率热控涂层，应采取措施防止和消除其在组装、试验过程中受到的环境污染；选用的热控产品的真空放气率应满足技术要求，并采取适当措施防止热控产品放气对卫星光学表面的污染；

l） 卫星外表面热控涂层和多层隔热组件均应与卫星地电导通，防止静电放电对卫星造成破坏；

m） 建造卫星热数学模型，计算卫星及电子设备的温度，检验设计的合理性。

15.3.3 电子设备热设计原则

卫星电子设备热设计原则如下：

a） 应选择稳定性好、耐温范围宽、功耗低的元器件和导热性能好的印制板。热耗散大的元器件表面应有较高的发射率，如采取黑色阳极氧化处理或喷涂黑漆、铝粉涂层。应按 GJB/Z 35—1993 第 5 章对元器件进行电压降额，电流降额，功率降额，工作结温降额，壳温降额。

b） 元器件布局应力求热耗散分布均衡，防止因热耗散过于集中而形成局部热点，安装应有利于热量的排散，热耗散大的元器件，如大功率器件，应直接安装在电子设备底板（安装面）或机壳上，也可加装散热器；对温度变化敏感的元器件要远离热耗散大、温度变化激烈的元器件或采取热屏蔽措施。

c） 增大元器件与印制板（或机壳）的安装接触面积，降低接触表面的粗糙度，增大接触压力，在接触界面间填充导热填料，如硅橡胶垫，石墨垫，导热脂等，是减小安装面接触热阻的有效途径。选用厚度大的印制线，以利于印制线的导热。减小元器件引线的安装长度，可以降低元器件和印制板之间的导热热阻。

d） 选择散热路径，包括导热散热路径和辐射散热路径等，使元器件的热量沿着这些路径传到电子设

备的底板（安装板）或机壳上。元器件的散热路径一般应以导热散热路径为主。应尽可能使元器件到热沉的导热距离最短。

e） 电子设备机壳应有足够大的安装接触面积，安装面粗糙度和平面度应符合相关规范要求，机壳表面（包括内外表面）应有较高的发射率，如采取黑色氧化处理或喷涂黑漆。

f） 元器件的恒温控制依靠电加热升温和导热、辐射散热降温，一般不设置特别的用于降温的冷却装置，如制冷器等，降低设计的复杂程度。

g） 应选用没有机械运动、不耗电或少耗电的热控部件，如金属导热条、导热板、小型热管等散热器，将热耗散大的元器件的热量传到热沉上。

h） 建立电子设备的热数学模型，根据卫星提供的边界条件，计算电子设备及其元器件的温度，检查元器件的结温（或壳温）是否低于降额后允许的最高值。

15.4 热设计步骤

15.4.1 卫星热设计步骤

卫星热设计的基本步骤如下：

a） 根据卫星构形、设备布局、轨道、姿态、工作模式、工作环境等设计输入条件，分析卫星的极端热工况和极端冷工况；

b） 根据需要排散热量的大小和分布，选择热控涂层、热管、多层隔热组件和电加热器等热控部件，控制散热路径，选择散热面的位置及尺寸；

c） 建立卫星的热数学模型，计算出极端热工况和极端冷工况的温度，与设计要求进行比较，适当调整未满足要求的设计；

d） 进行卫星的热平衡试验，验证热设计的正确性，并根据热平衡试验数据，修改设计和热数学模型。

15.4.2 电子设备热设计步骤

电子设备热设计的主要步骤如下：

a） 热设计应与电性能、机械性能、电磁兼容性能、可靠性和安全性等设计同步进行；

b） 根据工作温度范围和 GJB 1029—1990 第 4 章规定的环境设计余量确定电子设备应能承受的最高温度和最低温度；

c） 按照电性能和 15.3.3 a）的要求选择元器件；

d） 按照电原理图和 15.3.3 b）、c）、d）和 g）的原则进行元器件布局和安装工艺设计；

e） 建造印制电路板级的热数学模型，以电子设备壳体应能承受的最高温度和最低温度为等温边界条件，进行印制电路板级的热分析，检验元器件结温（或壳温）是否满足降额要求；

f） 按照机械性能要求和 15.3.3 b）和 e）的原则，设计机壳；

g） 按照印制电路板与机壳实际的连接状况，建造整机的热数学模型，以电子设备壳体应能承受的最高温度和最低温度为等温边界条件，计算元器件、印制板的温度，检验元器件工作温度范围是否满足要求，检验元器件结温（或壳温）是否满足降额要求；

h） 修改设计，直到满足全部设计要求或寻找到最佳方案；

i） 按照环境试验规范的要求进行电子设备的热真空试验，检验设计的合理性。

16 冗余设计

16.1 概述

为完成系统功能而附加一个或一套以上的元件、部件或设备，达到即使其中之一发生故障但整个系统不发生故障的结果，这样的系统称为冗余系统。卫星产品研制要经历方案论证、方案设计、初样研制和正样研制等阶段。为确保卫星的可靠性，在确定卫星可靠性指标之后，即应结合卫星可靠性建模和初步的可靠性分析结果，对可靠性薄弱环节采取必要的冗余措施。

16.2 目的

冗余设计的目的在于提高系统的任务可靠性。卫星飞行任务中最大的威胁就是单点失效，通过冗余设计可以减少单点失效，从而提高系统的可靠性。

16.3 原则

冗余设计的一般原则如下：

a） 冗余设计一般是在如下情况下采用的设计技术：

1） 在降额设计、简化设计、采用可靠性更高的部件等基本设计技术不能很好解决可靠性问题时；

2） 改进产品设计所需要的费用、时间比进行冗余配置更多时；

3） 系统中存在可靠性低的关键器件（关键器件，是指其发生一次故障就会使系统失效或者使系统丧失一个主要功能）时；

4） 不得已选用了可靠性不满足要求的元件时；

5） 系统中必须消除一定的单点失效时；

6） 要求系统必须连续、不间断工作时；

7） 通过地面测试仍存在难以检查的单元时。

b） 冗余设计有效实施的时机：

1） 冗余设计应在产品研制阶段的初期进行，冗余设计实施越晚，采用冗余系统的自由度就越小；

2） 冗余设计是在有关系统可靠性分析和取得一定的试验数据之后对可靠性薄弱环节采取的设计措施，具体采取何种冗余设计方式要视具体情况而定。

c） 硬件的冗余设计一般在较低层次（设备、部件）使用，功能冗余设计一般在较高层次进行（分系统、系统）。

d） 冗余设计的冗余单元可以是相同的，也可以是不同的。

e） 冗余设计应考虑不同故障模式下冗余系统工作模式的不同：

1） 电路中两只串联的二极管，对短路故障，它们相当于并联；对开路故障，它们为串联；

2） 由于故障模式的不同，阀门和开关的连接方式（串联、并联）随故障模式的不同，冗余方式有时会变换。

f） 冗余设计中应重视冗余转换的设计：

1） 保证可靠性增长不要被由于构成冗余布局所需要的转换器件、检测器件和其它外部器件所增加的故障概率抵消；

2） 在进行切换冗余设计时，必须考虑切换系统的故障概率对系统的影响，尽量选择高可靠的转换器件。

g） 冗余单元的工作状态应该是可检测的：

1） 冗余单元如果不能被测试，冗余设计所带来的好处会被冗余单元功能的不确定所抵消；

2） 在系统进行冗余设计时，设计师必须考虑冗余设计的可检测性，采用冗余是否能达到提高可靠性的目的，可检测性至关重要。

h） 冗余设计应考虑对冗余器件的有效隔离：

1）冗余设计中对冗余元件的有效隔离可以防止故障效应对冗余网络中的其它元器件产生有害的影响；

2） 冗余设计对故障传播的敏感性可以应用 FMECA 的方法加以确定；

3） 可以用保险丝、断路器、过载继电器等隔离和保护冗余设计结构，这些元件可以保护冗余设计结构免受元件失效的二次影响。

i） 冗余设计应考虑对共模/共因故障所带来的影响：

1） 采用同样部件进行冗余可以降低随机故障，但有可能同一个故障原因造成两者（主份、备份）都出故障；

2） 采用同样软件进行冗余可能会出现因同一错误,而造成（主份、备份）都出故障；

3） 若冗余配置在同一区域，该区域遭到破坏，两者都可能受损。

j） 应正确使用冗余设计：

1） 冗余设计会使系统的重量、体积、功耗、复杂度、费用和设计时间增加；

2）复杂度的提高会导致非计划的维修增多；

3）冗余采用的部件数量的增加，出现故障的概率也会增加；

4）冗余设计提高了系统任务可靠性，但降低了基本可靠性，为缓和这种矛盾，应当尽可能在较低层次而不是在较高层次采用硬件冗余。

因此，必须充分地进行分析权衡，从实际出发，使实施的冗余设计有效。

冗余设计的结果要反映到各种可靠性分析（可靠性预计、FMEA、FTA等）中，并能验证其稳定性。

16.4 步骤

冗余设计的步骤如下：

a） 明确卫星可靠性指标要求；

b） 实施其它可靠性技术，确认实施冗余设计的必要性，如通过可靠性预计发现可靠性不能满足可靠性指标要求、通过 FMEA、FTA 等发现了单点故障等）；

c） 根据系统体积、重量和费用，确认冗余的可能性；

d） 根据有关可靠性分析结果（包括可靠性预计、FMEA、FTA 等）明确可靠性薄弱环节，确认实施冗余设计的主要对象；

e） 选用合适的冗余措施；

f） 验证。

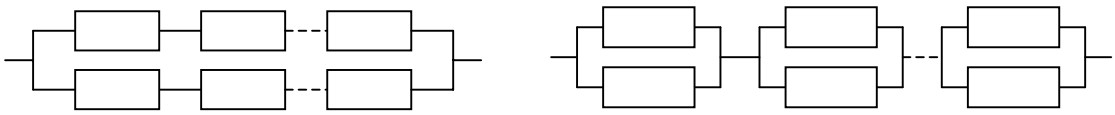
16.5 方法

冗余设计的方法根据所考虑对象、功能等的不同而不同：资源耗费最少的冗余设计；系统可靠性最大的冗余设计。

冗余方式通常有两大类，即工作冗余：当出现故障时不需要外部的元件、部件和设备来完成检测、判断和转换；非工作冗余需要检测及转换设备，当故障发生时切换至正常部件、设备以代替故障部件、设备。

采用冗余是否能达到提高可靠性的目的，检测及转换设备的可靠性至关重要，同时，还取决于对故障单元的有效隔离，防止故障效应对冗余网络中其它单元的有害影响。

冗余方式有整体冗余和单元冗余之分：把一个整体作为冗余对象称为整体冗余；把一个单元作为冗余对象为单元冗余。见图28。



整体冗余　　单元冗余

图 28　整体冗余和单元冗余

可靠性并联系统是最简单的冗余系统。并联单元越增多，则并联系统可靠性的相对改善也越少。

应注意，失效率为常数的单元并联后，并联系统的失效率不是常数，它不服从指数分布。

表10中给出了三种基本类型冗余技术的可靠性特性、可靠性函数等。

表 10　三类型基本冗余技术的可靠性特性、可靠性函数

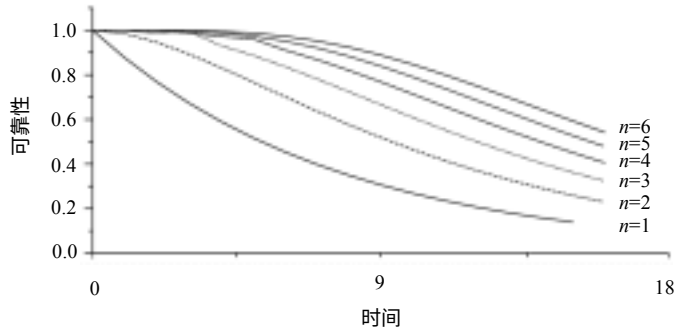
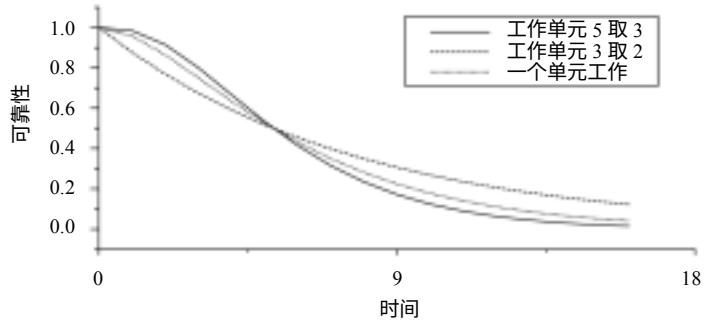
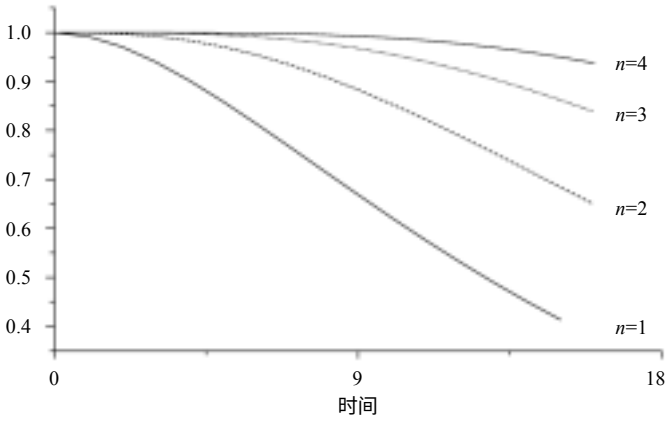
类型	事项	内容
并联冗余	说明	a）　该冗余方式是最常用的冗余方式，也称热冗余（热备份）； b）　其工作方式是：*n*个单元通常都处于工作状态，即使其中一个单元出现故障，系统也不会出现任何问题而连续工作，直至所有单元均出现故障。
	特性	a）　具有切换冗余的优点； b）　与切换冗余不同的是不需要转换就能克服硬件故障； c）　随着并联单元的增加，所获得的可靠度的增长逐渐下降； d）　失效率为常数的单元并联后，并联系统的失效率不是常数，它不服从指数分布。
	可靠性函数	
表决冗余	说明	a）　表决系统也称为*n*中取*k*系统 b）　其工作方式是：组成系统的*n*个单元中，通过表决系统判断正常工作单元不少于*k*个，就判定系统不会失效。
	特性	a）　表决系统是计算机和电子数字线路经常采用的有效的冗余设计； b）　降低虚警数量（降低了间歇故障）； c）　缺点是由于表决使判断时间放慢。
	可靠性函数	

表 10（续）

类型	事项	内容
贮备冗余	说明	a） 该冗余方式是备用冗余的基本模型，也称切换冗余（温/冷备份）； b） 其工作方式是：系统一个单元在工作，*n*个单元处于备份状态，当工作单元出现故障时，由切换开关切换到其它单元继续工作，从而保证系统正常工作。
	特性	a） 可用于模拟和数字电路； b） 对存在间歇故障模式的系统有效； c） 缺点是转换延时和转换失效； d） 数学模型根据转换器件可靠与否、备份单元失效率的不同而不同。
	可靠性函数	

16.6 注意事项

冗余设计应注意：

a） 冗余单元可以相同，也可以不同；

b） 冗余虽提高了任务可靠性，但降低了基本可靠性；

c） 随着冗余数量的增加，提高可靠性的幅度却相对下降；

d） 冗余必须全面考虑系统多重工作模式的需要（某一模式为并联，但另一模式可能为串联）；比如推进系统的电爆阀，对于阀门打开是并联，但对于泄漏是串联；如两只串联的二极管，对短路故障，它们相当于并联；对开路故障，它们为串联；

e） 每个冗余单元都应该是可检测的。

17 电路容差分析

17.1 概述

GJB/Z 89—1997给出了详细的电路容差分析方法。最坏情况电路分析（WCCA）是容差分析的内容之一，在GJB/Z 89—1997基础上，已有新的成果与经验。本章在简要介绍容差分析的同时，侧重给出WCCA的分析指南。

电路容差分析是GJB 450A—2004的一个工作项目。容差分析技术是一种预测电路性能参数稳定性的方法，主要研究电路组成部分参数偏差，在规定的使用条件范围内，对电路性能容差的影响。

WCCA已成为容差分析中的一项重要内容，也是QJ 1408A—1998规定的工作内容。WCCA是在电路各元器件参数在最坏情况组合下对电路性能、元器件应力进行的分析。导致元器件参数变化的原因包括元器件的质量水平、元器件老化引起的漂移、施加于电路中每个元器件上的应力（如温度、湿度、辐射

等）以及外部电输入。WCCA的内容包括：评价电路性能在最坏情况下的容差及其漂移、元器件在最坏情况下是否过应力。

WCCA需要得到设计、材料、元器件等方面的详细信息，因此，WCCA不适合在产品的方案阶段使用。其最佳使用时机应在初步设计完成之后。

在产品设计、研制过程中，设计上有任何的改动都应重新进行WCCA。通常在产品研制越往后，产品设计越难改动，且改动代价越高。因此，在电路设计完成后，应尽早进行WCCA。

17.2 目的

由于卫星的热、辐射、真空等环境，电子元器件的参数可能发生漂移或元器件过载，导致电路或电子产品的性能下降或失效。

容差分析的目的是通过摸清元器件参数变化对电路性能影响的大小，评估在规定环境及极端环境条件下电路的工作情况以及性能对元器件参数变化的灵敏度，回答是否满足设计或工作要求，提出改进措施建议。

17.3 原则

原则如下：

a） 简单功能电路都应进行分析；

b） 一般产品应根据复杂程度及元器件数量规模，结合有关可靠性分析结果选定关键电路进行分析；

c） 容差分析有多种分析方法，应根据各方法的特点有针对性地试验并收集有关数据，或根据特定的数据选用特定的方法。

17.4 步骤

17.4.1 容差分析

电路容差分析的分析程序见图29。

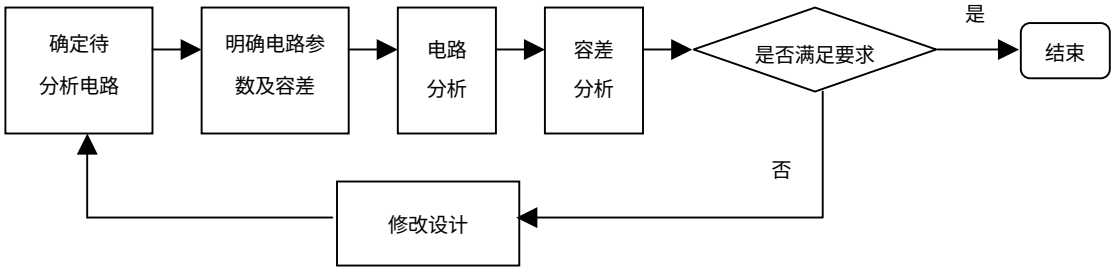


图29 电路容差分析程序

GJB/Z 89—1997给出了电路容差分析程序的具体要求及容差分析的方法。

电路容差设计是容差分析的结果之一。任何元器件都有公差，公差的存在将导致电路参数误差。当误差超过一定的限度（设计容限）时，就产生故障。

容差设计有三条途径：

a） 更改电路设计，使电路允许元器件有较大的公差；

b） 全部采用低公差高稳定性的元器件；

c） 只对电路参数影响大、敏感的元器件采用低公差、高稳定性的元器件。

第一条属于电路优化设计，需用电路计算机辅助设计工具；第二条成本高、研制周期长；第三条强调抓关键环节，应用广泛。

电路容差分析结果是进行电路容差设计的重要依据。电路容差分析与电路容差设计的关系见图30。

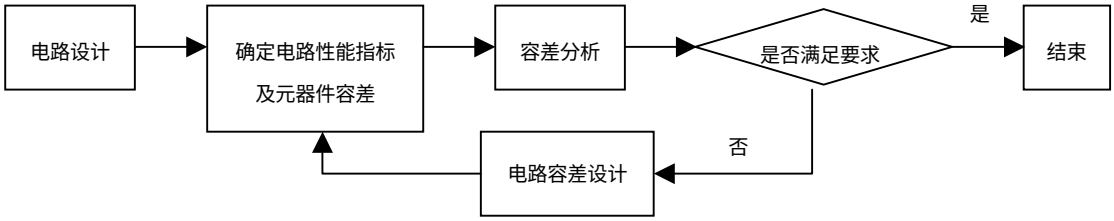


图30　电路容差分析与电路容差设计的关系

17.4.2　最坏情况电路分析

17.4.2.1　明确待分析电路

WCCA程序见图31。明确待分析电路的内容包括：

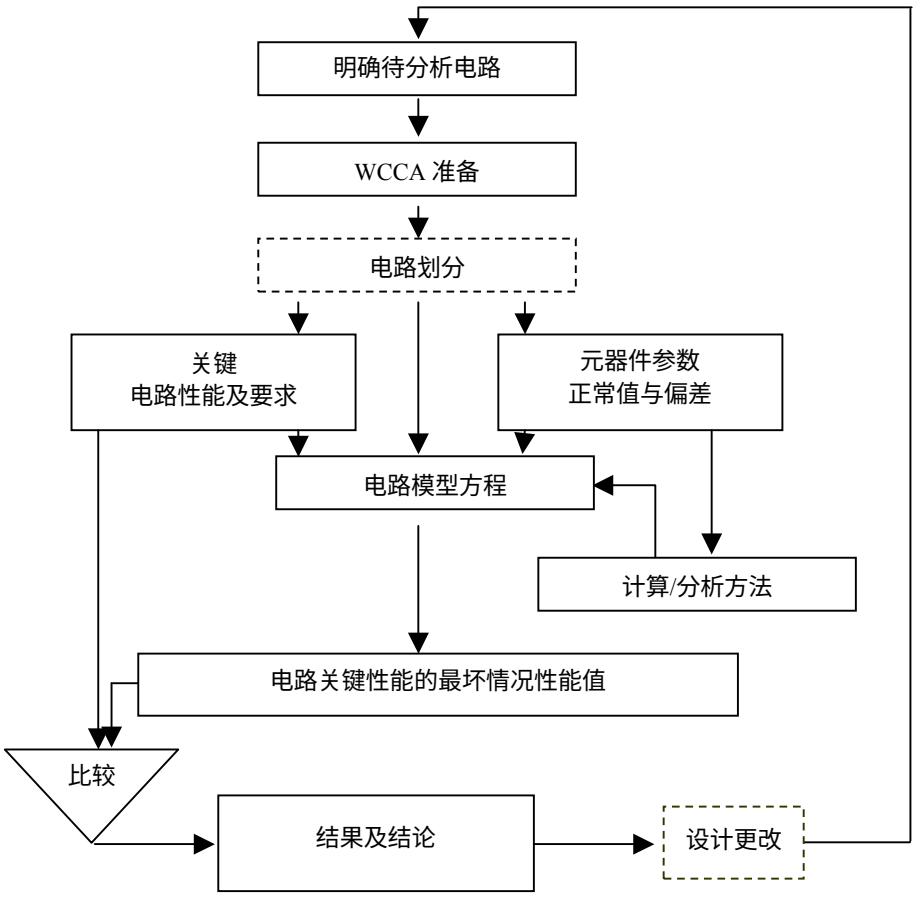


图31　WCCA程序

a） 确定关键电路，由于时间、费用等的限制，首先应对关键电路进行 WCCA，因此，要明确哪些电路或电路类型需要进行最坏情况分析，如影响长寿命卫星长期工作的关键电路；

b） 工作原理和功能分类，介绍工作原理应作为最坏情况分析报告的一部分，以提供一些电路的背景资料，功能分类描述电路执行的各项主要功能及其子功能，便于对电路有更好的了解，便于对大规模电路进行合理的分割；

c） 电路性能规范分析，在开始分析前，分析人员应对系统的要求和规定有全面、正确的理解。

17.4.2.2 WCCA 准备

WCCA准备就是准备进行WCCA所需要的各种初始信息，包括系统/产品/电路的性能技术要求、原理图、方块图、工作原理、元器件清单、元器件降额要求等数据。

17.4.2.3 电路划分

对简单电路，本节的工作不一定需要进行。对复杂电路，在有限的分析手段条件下，为方便进行WCCA，可将电路分解成易于进行WCCA的子电路。

17.4.2.4 关键电路性能及要求

电路的性能可能有多个，在有限的时间、经费条件下，一般可选择关键性能进行WCCA。电路关键性能的选择，应根据产品的任务要求确定。

17.4.2.5 元器件参数正常值与偏差

WCCA为定量分析，需要输入必需的参数，包括元器件参数极值、额定值、偏差、指标要求、分布类型等。

17.4.2.6 计算/分析方法

选用合适的WCCA方法。方法见17.5。

17.4.2.7 电路模型方程

在用具有WCCA分析功能的软件进行分析时，模型已在软件中，不必给出；人工分析时需给出，但对较复杂的电路是很困难的。

17.4.2.8 电路关键性能的最坏情况性能值

经分析，得到分析结果。

17.4.2.9 比较

将最坏情况分析结果指标要求进行对比，包括最坏情况性能结果与性能指标、元器件最坏情况应力与降额要求的比较，以判断是否满足要求。

17.4.2.10 分析及结论

根据WCCA方法进行分析，总结提出可能的设计改进建议。

17.4.2.11 设计更改

根据分析结论及建议，将有关信息反馈给设计，特别是在WCCA结果不满足要求的情况下，供设计更改参考。在设计更改完成后，再进行WCCA，直至满足要求。

17.5 方法

17.5.1 电路容差分析方法

电路容差分析方法包括最坏情况试验法、最坏情况分析法、蒙特卡落法、伴随网络法、阶矩法等。电路容差分析方法详见GJB/Z 89—1997。

17.5.2 WCCA 方法

WCCA方法分为最坏情况元器件应力分析和最坏情况电路性能分析。最坏情况电路性能分析有EVA、RSS和蒙特卡落等方法。

最坏情况元器件应力分析和最坏情况电路性能分析可分别独立进行。

灵敏度分析是最坏情况电路性能分析过程中的一个环节。在实施EVA、RSS和蒙特卡落之前，必须进行灵敏度分析。

WCCA的深度和广度受分析进度、费用、分析软件等的约束。

17.5.3 最坏情况元器件应力分析方法

最坏情况元器件应力分析的目的是检测最坏情况条件下电路元器件工作参数值是否超过额定值。如果超过额定值，元器件将被认为是过应力使用。过应力条件包括稳定条件和瞬态条件。如果有降额规定，最坏情况应力分析要验证在最坏情况条件下元器件是否符合降额规定。

最坏情况元器件应力分析是将不同的最坏情况组合施加到被评估的元器件上，以保证该元器件所受到的应力是其可能遇到的最坏情况应力。

进行最坏情况应力分析一般应先制定一个工作表。在该工作表中，列出所分析的电路中所有元器件及其参数、元器件参数的额定值、降额因子、降额后的值，再按元器件类别或按电路节点分别进行最坏情况应力分析计算。最后，将计算结果填入工作单中，并与额定值或降额后的额定值进行比较，判断元器件是否过应力使用。

在有脉冲功率或电流情况下，要特别注意瞬时电流峰值与瞬时温度的上升在应力分析时要用均方根值而不能用平均值。

17.5.4 EVA 方法

17.5.4.1 直接代入法

该方法适用于电路性能函数在工作点可微且变化较大、设计参数变化范围较大、最坏情况分析精度要求不高的场合。

该方法的基本步骤如下：

a） 给出每个元器件参数的最坏情况极大值；

b） 给出每个元器件参数的最坏情况极小值；

c） 给出电路性能方程；

d） 给出最坏情况参数组合：正灵敏度参数的上偏差、负灵敏度参数的下偏差形成最坏情况最大值组合；正灵敏度参数的下偏差、负灵敏度参数的上偏差形成最坏情况最小值组合；

e） 根据电路性能方程计算最坏情况性能值（最大和最小值）；

f） 与性能指标要求进行比较。

若最坏情况最大和最小值均在规定的电路性能容差范围内，则表明电路通过极值分析（EVA），工作结束。否则，提出相应的有关的改进措施及建议。

17.5.4.2 线性展开法

该方法适用于电路性能函数在工作点可微且变化较小、设计参数范围较小、最坏情况分析精度要求不高的场合。

设电路性能方程为$y=f$（x_1，x_2，…，x_n），将函数在额定值处Taylor展开，略去一阶以上高次项，则得到y的变化量Δy与元器件参数变化量Δx_i之间的线性关系为式（39）：

$$\Delta y = \sum_{i=1}^{n} \frac{\partial y}{\partial x_i} \Delta x_i \quad \cdots\cdots (39)$$

式中：

$\partial y / \partial x_i$ ——y对x_i的偏导数，或为灵敏度s_i，在各参数额定值处取值；

Δx_i——参数x_i的偏差，当有补偿和负反馈时，Δx_i为参数原偏差、补偿偏差和负反馈偏差等的绝对值之和。

偏差Δy、Δx_i可为正，也可为负，正与负的绝对值也可不等。

17.5.5 RSS 方法

RSS为统计方法。该方法的一个基本假设是电路性能服从正态分布。要求的输入是所有参数的概率分布的均值和标准偏差，且各参数相互独立。分析的结果是平均值和电路性能的概率分布（假设为正态分布）的标准偏差，从而得到给定概率下电路性能参数的最坏情况范围。该方法的结果与EVA相比偏差范围更小。

参数的典型概率分布有：正态分布、均匀分布、三角形分布，但常用的是正态分布。

对任意性能函数$y=f(x_1, x_2, \ldots, x_n)$，将函数在$x_i$额定值处Taylor展开，略去一阶以上高次项，则$\Delta y$按（39）式计算。

若Δx_i或x_i的标准偏差为σ_i，则在x_i相互独立的情况下，Δy或y的标准偏差、均值为式（40）、（41）：

$$\sigma_y = \left(\sum_{i=1}^{n} \left(\frac{\partial y}{\partial x_i} \sigma_i\right)^2\right)^{\frac{1}{2}} \quad \cdots\cdots (40)$$

$$\mu_y = f(x_1, x_2, \ldots, x_n) \quad \cdots\cdots (41)$$

式中各x_i在额定值处取值，从而据此可得到电路性能出现最坏情况值的概率。

RSS为近似方法，泰勒展开略去二次项及以上各次项，带来了误差；当参数不都服从正态分布时，若电路性能按正态分布则带来了误差。当参数个数较多时，按中心极限定理，性能参数近似服从正态分布。

17.5.6 蒙特卡落方法

见GJB/Z 89—1997第5.2.3。

蒙特卡落法是当电路中元器件参数服从某种分布时，对参数进行抽样从而分析电路性能偏差的一种统计分析方法。

实施方法是：若电路性能函数包含m个参数，记为$X=(X_1, X_2, \ldots, X_m)$，则根据每个参数的分布函数对每个参数进行第一次随机抽样X_1，其抽样值记为$X_1=(X_{11}, \ldots, X_{1m})$，将其代入电路性函数表达式，得到第一个电路性能的随机抽样值$y_1=f(X_{11}, \ldots, X_{1m})$，再进行第二次抽样，其抽样值记为$X_2=(X_{21}, \ldots, X_{2m})$，得到第二个电路性能的随机抽样值$y_2=f(X_{21}, \ldots, X_{2m})$，如此反复，得到$n$个随机值。从而对$y$进行统计分析，画出直方图，求出电路性能参数$y$出现在不同偏差范围内的概率。

蒙特卡落法适用于可靠性较高的电路。蒙特卡落法的抽样次数应满足统计分析的精度要求。

17.6 示例

一个放大器电路（见图32），若电阻值的偏差为±10%，则用EVA方法，有：

最大增益$=R_{2max}/R_{1min}=\dfrac{10000+10000\times10\%}{1000-1000\times10\%}=\dfrac{11000}{900}=12.22$

最小增益=$R_{2\min}/R_{1\max}=\dfrac{10000-10000\times10\%}{1000+1000\times10\%}=\dfrac{9000}{1000}=8.18$

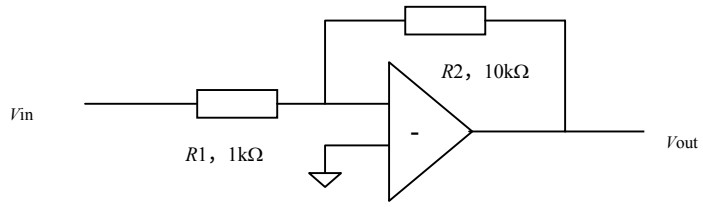


图32　简单放大电路

如果指标要求增益不小于9.0，则上述结果不满足要求。此时，可以重新设计以选择电阻值（增加*R*2或减小*R*1），或选择精度更高的元器件。如增加精度，由10%提高到达5%，则最大、最小增益分别为11.05、9.05，满足指标要求。

17.7　注意事项

进行容差分析时应注意：

a）　电路中元器件数量较大时，一般需要有关辅助分析软件方可完成；

b）　考虑元器件数量规模对仿真软件运行效率的影响，一般需要将电路进行分割；

c）　应根据有关可靠性分析（如FMEA、FTA）结果选取关键电路进行。

18　电磁兼容性设计

18.1　概述

电磁兼容性（EMC）定义为：设备（分系统、系统）在共同的电磁环境中能一起执行各自功能的共存状态，即该设备不会由于受到处于同一电磁环境中其它设备的电磁辐射导致或遭受不允许的降级；它也不会使同一电磁环境中其它设备（分系统、系统）因受其电磁辐射而导致或遭受不允许的降级。

卫星载有多种电子设备，它们在不同频率区间和不同功率条件下工作，有些强信号、大功率设备易发射干扰，而有些弱信号、高灵敏度设备易受到干扰，又因卫星内部设备和元器件安装密度高、电缆网很复杂，卫星在发射场进行测试和发射后在空间飞行中，又可能遇到人为干扰（如导航台、雷达站等）及自然干扰（如雷电、静电及宇宙电磁干扰等），引出了系统内（卫星内设备和电缆网等）和系统间（卫星与运载、卫星与靶场、卫星与测控系统和卫星与空间环境等）的电磁兼容性问题。

卫星EMC设计指卫星在研制过程中需要采取的控制干扰和提高抗干扰能力的技术措施，以保证卫星系统内部和外部电磁兼容性指标的实现，确保卫星在特定的电磁环境中完成飞行任务。

卫星EMC有关术语见GJB 72—1985，有关要求见GJB 3590—1999。

18.2　卫星总体的电磁兼容性（EMC）设计

18.2.1　接地与隔离

卫星金属结构主体电容量较大，可为各电系统提供参考零电位，因此是卫星结构接地系统（SGS）的主要组成部分。应当靠近一次电源地线端，在星体主结构上选择一个易于外部操作的卫星单点接地点（SPG）。该点在地面测试时引出地线单点接大地。

一般电子设备有浮地、单点和多点接地三种方式。卫星一般选用混合接地方式，即1MHz以下低频设备单点接地，10MHz以上高频设备多点接地，1MHz～10MHz时酌情选用。

必须良好接地，接地不良有时比不接地还坏（产生更大干扰）。同样，不应连接的地方必须电隔离。设备机壳、底板及星体结构均不能作为直流电源或低频信号的回流通路。

一次电源系统的太阳电池阵、蓄电池组及地面硅光电池模拟器应单点接地。当一次电源母线不通过SPG与SGS相连时，一次电源母线应与星体结构隔离，直流隔离电阻不应小于1MΩ。一次电源地线端应以最短距离和最低阻抗搭接到星体参考点。

一、二次电源间应有变压器等隔离，其直流电阻应大于1MΩ。二次电源应单点接地。二次电源所有用户馈电线、回流线均应与机壳隔离，其直流电阻大于1MΩ。二次电源接地板应就近与星体参考点良好搭接。

其它低频电路采用单点接地，射频电路采用多点接地。设备间信号接口尽量采取信号与回线双绞连接方式，且确保回线与机壳隔离。在实现有困难时可设信号回线的单点接地板最后搭接到接地参考点。信号地应分模拟地和数字地。为了消除地线闭环引入的干扰，接口处应采用隔离变压器、中和变压器、继电器、差动放大共模输入和光电耦合器等隔离措施，后者因线性差仅适用于数字电路。

除射频设备与特殊情况外，线路应与机壳隔离。

所有接地线应尽可能短，甚高频电路地线一般长度小于25mm，并镀银。

18.2.2 搭接

搭接是在两个金属表面间建立低阻抗通路，是接地的一种措施。其作用为：实现低频电路和机壳屏蔽接地，提供电源的故障电流回路，减少设备间电位差，防止静电积累，为射频电路及天线提供均匀结构面，实现对电冲击的保护，为故障电流及闪电防护提供通路。

星体结构的零部件应尽量通过直接搭接连成整体。对邻近点，结构上相邻两点间直流电阻不大于50mΩ；对结构上两端点间直流电阻不大于50mΩ。

星载设备与星体结构应直接搭接或通过搭接条间接搭接。对于电源、易产生干扰或敏感设备、火工品及易受雷击部件，直流搭接电阻不应大于2.5mΩ。

几种有关搭接的规定：

a） A 类（天线搭接）：天线应与星体结构良好搭接，以获得所要求的天线方向图并满足天线性能要求。

b） C 类（电流回路搭接）：对使用星体结构作为电流回路的系统，应对作为电流回路的搭接通路进行规定，以确保电源和负载间的电压在电源品质要求的范围内。特别注意易爆燃料区的设备，为防止电源故障引起点火爆炸，直流搭接电阻应尽量小。

c） R 类（射频搭接）：包括射频设备及对射频敏感设备的机壳与星体结构直流搭接电阻应小于 2.5mΩ，且搭接条长宽比要小于 5，以减小感抗。

d） S 类（静电搭接）：星内或星外部易产生静电积累的部件（线尺寸大于 75mm 的绝缘体、天线除外），应与星体结构可靠搭接，直流电阻小于 1Ω。

e） H 类搭接：适用于故障状态电压冲击防护，搭接电阻一般不应超过 0.1Ω。

f） L 类搭接：适用于雷电防护，避免雷电效应直接或间接影响系统的工作性能，搭接电阻一般不超过 2.5mΩ。

如果某一搭接适用于多种类型的搭接目的（如A、R、S等），设计时应选用最严格的搭接要求。

搭接的工艺要求：

a） 一般设备和结构应首选直接搭接，活动部件的连接可以使用有一定宽度的金属搭接条，一般长宽比小于 5，以保证低的电感/电容（L/C）比值；

b） 应采用电化学序列同组材料，在不同组金属搭接时应插入垫片，搭接处宜加保护层；

c） 金属表面应紧密接触，被搭接表面应光滑、清洁、没有高阻特性和阳极化膜，应有足够压力保持接触良好；

d） 搭接设计要考虑振动、冲击和温度等环境条件的影响，不应仅考虑焊料增加机械强度；

e） 搭接处应采取防潮、防腐蚀措施；

f） 要保证搭接处或跨接处能承受预料的电流。

各材料最小腐蚀搭接见表11。

表11 最小腐蚀搭接

阳极金属	铝、铜或镀锡的铜跨接片的连接	
表中越靠上的金属阳极越强，也就比它们下面的金属更易受腐蚀	需要在跨接片与搭接体之间使用的垫圈	其它部分
Ⅰ镁	铝合金，在任何安装螺母或螺丝头的地方都适用	螺丝和螺母镀镉或镀锌
Ⅱ铝 铝为主的合金 锌－镉	不用垫圈	
Ⅲ碳钢 （不锈钢除外） 铁 铅 锡 锡－铅焊料		
Ⅳ镍 铬 不锈钢	所有铝跨接片都要用镀锡或镀镉垫圈 镀锡的铜或铜跨接片可不用垫圈	最好用不锈钢的螺丝和螺母（也可用镀锌或镍）
Ⅴ铜 银 金 铂 钴 石墨 上述金属为主的合金 钛		只能用铜跨接片搭接，并彻底消除接触表面的全部锡层

18.2.3 屏蔽

屏蔽可防干扰外泄或外界干扰进入。

铜和铝是各种频率下的良好电屏蔽材料，对电磁波有较大的反射损耗。屏蔽体厚度仅维持足够的结构强度即可。

铁及高导磁率合金是较好的磁屏蔽材料。

设备屏蔽盒应注意屏蔽的连续性。金属板间的接缝要采用焊接或卷接，接缝配合面应清洗，并清除非导电物质。面板与盒体接缝应填充导电衬垫并用螺钉密布紧固。屏蔽盒应尽量少开槽开孔，有孔时应用导电衬垫、导电玻璃、金属网等来保持屏蔽效果。

高频同轴电缆为实体屏蔽，效果较好。低频电缆多用金属编织网，其覆盖面积应大于百分之九十。电缆屏蔽应接地。

18.2.4 滤波

无论是抑制干扰源和消除干扰耦合，还是增强接收电路的抗干扰能力都可采用滤波技术。

抑制干扰的主要方法按次序为：接地、布线、屏蔽、滤波。接地良好可降低屏蔽和滤波要求，而屏蔽良好可以降低滤波要求。故滤波器只在必要时使用。能使用简单的防干扰电容器就不必采用复杂滤波器。

设计和使用滤波器应注意：

a） 能承受所考虑的电压、电流、高低温、真空和力学环境；

b） 正确选用电容器的类型和质量，防电容器击穿造成短路，射频去耦不能用极化电容或钽电容器；

c） L 型滤波器对应高阻抗噪声源用电容器，对应低阻抗电源使用电感器；

d） 为了抑制外部传导干扰，印制板应采取去耦措施；

e） 滤波器输入与输出线应隔离，必要时加屏蔽，滤波器尽量靠近被滤波线路，用短线或屏蔽线连接；

f） 不因插入滤波器而改变对信号源的阻抗。

18.2.5 电缆网

电缆网设计是实现整星电磁兼容的重要环节。

按QJ 2176—1991电缆束分为五类：

Ⅰ类：适用于电源和控制电路；

Ⅱ类：适用于高电平信号电路；

Ⅲ类：适用于低电平信号电路；

Ⅳ类：适用于所有电爆装置电路；

Ⅴ类：适用于高频信号电路。

布线布缆原则：基本上每一类导线不与另一类导线安排在一束电缆内；不同类型的线束在空间上分开，尽量减少干扰耦合，利用有限布线空间分配最佳间距，一般大于2cm～10cm；敏感线束与干扰线束分开布缆时二者最好垂直走向，至少夹一定角度；电缆束尽量贴近结构铺设，以减小电容性耦合和耦合回路面积。每隔一定距离要加以固定。

线型的选择与屏蔽的端接按QJ 2176—1991的4.2屏蔽要求、4.3屏蔽端接和屏蔽接地执行：

a） 直流电源采用双绞合线，必要时加屏蔽；

b） 低阻抗小于 1kΩ、低电平小于 1V，音频信号采用屏蔽双绞合线，屏蔽层在信号接收端单点接地；双层屏蔽的内层单点接地，外层多点接地；

c） 高阻抗低电平音频信号在传输距离大于 1m 时采用阻抗变换装置，不能变换时屏蔽应两端接地；

d） 高电平音频信号用双绞线或屏蔽对线，屏蔽层在信号源端单点接地；

e） 基准电压或电流的种类应尽量少，按音频信号处理；

f） 前后沿小于 5μs、频率 100kHz 的控制信号采用双绞线，屏蔽层多点接地；

g） 射频信号线使用同轴电缆、平衡屏蔽电缆、特性阻抗小于 100Ω的平衡电缆，或使用波导；

h） 含电爆装置的电路，应采用屏蔽的双绞线，必要时采用双层屏蔽；在接插件处屏蔽层 360 度端接到导电的接插件壳内部；

i） 对低电平低频信号为保证屏蔽层单点接地的可靠性，屏蔽层应加绝缘护套以防意外接地。

如连接器的外壳与结构间有良好的低阻抗通路，可把屏蔽层端接在外壳上；也可通过连接器的插针将两根导线的屏蔽层连接以保证屏蔽的连续性；射频电缆的屏蔽层应延伸到连接器外壳内，并端接到导电良好的连接器上。导线屏蔽层端接到连接器上时，插针背面的无屏蔽的绝缘导线长度对小型插头不应大于2cm，对芯点较多的插头也应尽量短。

18.3 设备/分系统 EMC 设计

18.3.1 设计要求

卫星设备/分系统EMC设计的要求如下：

a） 应控制自身干扰，如减小频谱宽度，控制工作频率、脉冲幅度和上升时间，控制高次谐波、边带和寄生分量以压缩干扰，选择不易产生和传播干扰或抗干扰能力强的元器件；设备采用良好的工艺，合理布线和布局等。

b） 良好接地。除前面叙述外，对于出现较大瞬变电流的电路或低电平电路要用单独的地线、直流馈线与回线应绞合并远离控制线，必须交叉时应互相垂直。出现地线环路问题时可采用浮地隔离技术（如变压器、光电隔离等）。

c） 设备/分系统内干扰部件和敏感部件分别供电以减少低频高电平传导干扰；暂不用的干扰部件或敏感部件应临时断电；在能完成任务的前提下，避免使用灵敏度过高的元器件。

d） 每个设备或印制板的电源端、输入输出端加滤波。

e） 对有强电磁辐射的或对电磁场敏感的器件应加大间距，采用良好的电磁屏蔽，尤应注意屏蔽有关电缆敷设的路径。

f） 电源变压器和音频输入变压器应用接地的静电屏蔽。

g） 多芯插座或多芯电缆中接有高、低电平信号或带有噪声的信号时，应将它们分开，并尽量在中间安排地线或隔离线。

h） 对电抗电路的转换开关应采用非线性电阻或其它措施来控制其高峰值瞬变干扰。大电流电路一般不应接入电感线圈，并应使用屏蔽电缆，对于切断大电流的开关，必要时彻底屏蔽并加滤波。

i） 继电器、电磁阀线圈应跨接二极管或电阻器，继电器触点应有消弧措施，必要时将继电器及其附属电路屏蔽起来。

18.3.2 接收机

接收机EMC设计应考虑的措施如下：

a） 接收机接收有用信号的带宽应压缩至最低限度，接收机的灵敏度和动态范围要合理选用，防止灵敏度过高易受干扰，可在传输电路中考虑采用限幅和消隐电路以防大幅度脉冲干扰，应使用滤波器来减少接收基波以外的杂波或谐波干扰；

b） 天线引入线尽量短且必须屏蔽，信号输入电路应有足够的动态范围，输入端元件、电路、电缆应有足够绝缘强度且工艺精良；

c） 机内射频部分与输出部分应分开屏蔽，高频放大、混频、中频放大级应互相隔开，进出机壳的线应尽量少；

d） 本振应屏蔽并具有良好的屏蔽连续性，必要时使用双层屏蔽，屏蔽罩良好接地，振荡器单点接地；

e） 机内尽量不安放产生干扰的器件如继电器、开关等，必须使用时，继电器应屏蔽，线包应单独供电，线包及触点采取降低干扰措施；

f） 外电源供电输入端应滤波，所有控制电缆应屏蔽，各输出端应有抑制寄生干扰的旁路电容器或滤波器；

g） 接收机应与星体良好搭接。

18.3.3 发射机

发射机EMC设计应考虑的措施如下：

a） 应采取措施抑制从天线发射的谐波和寄生信号，发射机到天线的连接应保证良好匹配和电接触；

b） 机箱内高低电平线路尽量分开，功率级应良好屏蔽和滤波；

c） 低电平输入线应屏蔽，进出设备的控制线路应屏蔽和滤波；

d） 电源输入电路应抑制发射信号产生的传导干扰；

e） 高压电路、元件、电缆应使用足够绝缘强度的材料和工艺；

f） 发射机应良好接地并远离对射频敏感的设备。

18.3.4 数字电路

数字电路是一种最常见的宽频干扰源，有的也是易受干扰的敏感设备，设计时应注意：

a） 采用对称型开关的 A/D 和 D/A 变换器，较之非对称型所发射的干扰要小，抗干扰也好；

b） 尽量采用高电平、低采样速率的方式；

c） 设备进出口采取抑制干扰措施；

d） IC 引出线要短且应接负载，否则会起天线作用，即发射干扰；

e） 合理走线以免不必要的耦合，线路及机壳均应以正确方式接地；

f） 电源线应去耦以抑制负载感生的瞬变。

18.3.5 电爆装置

电爆装置EMC设计应考虑的措施如下：

a） 星上电爆装置的敏感度安全余量不低于 20dB（一般设备不低于 6dB）；

b） 引爆电源用一次镉镍电池或单用一组电源，并单独接地；

c） 电缆采用带绝缘护套的双绞屏蔽线或双层屏蔽电缆，屏蔽层单点端接，并远离其他电缆敷设；

d） 电爆装置壳体应良好搭接到星体结构，其屏蔽电缆及连接器应保持屏蔽连续性；

e） 电爆管两端平时应短路；

f） 电路中不允许有暂时的浮线，应接入电阻，同时电路中应接有安全跨接线和安全继电器或开关；

g） 点火电路中装上熔性保护电阻，防止点火后造成电源短路。

18.3.6 电源分系统

电源分系统EMC设计应考虑的措施如下：

a） 一次和二次电源必须良好接地；

b） 对二次电源本身产生的干扰进行抑制，二次电源用开关稳压器应采用适当的屏蔽来减小电源机壳中产生的电磁干扰辐射，但是输入引线的作用象天线一样辐射噪声，为减小噪声要求在所有输入引线到地之间加电容器旁路，或选用合适的滤波电路；

c） 对负载引起的干扰进行抑制，降低共用电源内阻，对使用共用电源的负载进行隔离，以降低母线上感生的噪声，驱动电磁继电器的电源线上存在着继电器噪声，不宜再给其它电子线路供电，但仍可给其它电磁开关、阀门、电机等供电，工作时间错开；

d） 尽可能采用分散体制二次电源，如果暂时做不到，可对负载进行分类，采取分散与集中相结合的方式，负载分类原则按大小电流、噪声干扰源、火工品线路、高灵敏线路等，也可由负载位置来分，特别是大电流、弱信号负载的供电线应尽量短。

18.3.7 印制电路板

印制电路术语和定义见GB 2036—1994。印制电路板EMC设计应考虑的措施如下：

a） 设计布线按 QJ 3103—1999 的 5.6.2.2.4 执行；

b） 应按电路类型对元件、逻辑组件进行分组，相对集中，按线路排列，减小耦合，相互独立的功能块四周用地线圈起，如一个逻辑模块中两部分用于不同的电路，则两电路应当工作在同一频率或时钟速率，逻辑模块不工作时应不供电（因为它们是乱真信号的电压源），最好能接地，以减少意外的检波和再辐射；

c） 时钟、振荡器等高电平电路应与低电平、高敏感电路隔离，容易发射干扰的和敏感的元器件应采用屏蔽罩，设计振荡器时，信号电平只要能保证可靠工作即可，避免过高信号电平，高速器件要安排在靠近插头的地方；

d） 每块印制板的直流电源输入端要去耦，板上电源线每隔 12cm 时接地总线进行旁路去耦。印制板上地线最好网状分布，并尽可能使网格面积接近，电源线与地线尽量粗且平行走线，最好是在印制板两面上下平行。

19 潜在电路分析

19.1 概述

19.1.1 潜在电路的概念

复杂系统在运行中所出现的故障，按其原因可分为两大类。一类是由于系统中一个或多个元器件失效引起。另一类则无法归结为元器件失效，称之为“非失效相关”的系统故障。在“非失效相关”的系统故障中，除去少数由于操作、使用不当和偶然性的工艺缺陷引起的外，绝大多数可归结为设计问题，如“潜在电路”。

所谓“潜在电路”，是指电气电子电路中存在的一种状态。在特定的条件下，它能够导致系统出现“非期望的功能”或抑制“所期望的功能”。这种状态不是由故障引起的，而是被无意中设计到硬件系统或软件程序中的一种状态。

19.1.2 潜在电路的表现形式

潜在电路有四种表现形式：

a） 潜在路径：电流或信号所流经的非期望的路径。

b） 潜在时序：是指电流或信号以非期望或矛盾的时间顺序、或在非期望的时刻、或延续一个非期望的时间段发生，从而使系统出现异常状态。

c） 潜在指示：关于系统运行状况的模糊或错误的指示。潜在指示可能误导系统或操作人员做出非期望的反应。

d） 潜在标志：是指关于系统功能的错误或不确切的标志。潜在标志可能会误导操作人员。

19.1.3 潜在电路的特点

复杂系统中潜在电路的特点是：

a） 潜伏性：卫星总体工程是多学科技术的高度综合体，由很多设计人员通过分工协作进行。由于每个设计者的责任范围有限，导致对部分电路正常的功能设计对其它电路却意味着潜藏的危险状态和条件。

b） 普遍性：中外航天史上均不乏由于潜在电路引起的飞行失败、设备损毁的重大事故案例。

c） 突发性：由于潜在状态的激发条件不被设计人员所认识，因此对于潜在条件的激活和潜在状态的后果不可能有全面的事先的准备和防范“预案”，往往表现为“突然发生”、“措手不及”、“出人意料”等。

d） 测试性差：许多潜在问题的激励条件在一般测试状态下是很难具备的，所以潜在问题往往在常规测试中不表现出来。因此，如果认为经过“严格的”测试甚至飞行试验没有问题就不会有潜在电路了，这种观点是不符合实际的。美国红石火箭的发射失败案例，是在红石火箭第 62 次发射时发生的，即说明上述道理。

e） “危害严重、发现困难、解决容易”：“危害严重”是由于没有针对性的防范措施所引起。由于可能产生多余功能和抑制设计功能，往往导致严重后果；“发现困难”说明了发现潜在电路问题的难度（要求分析系统所有的期望和非期望的功能、行为）；“解决容易”是指相对发现问题的困难程度和解决问题的巨大效益而言，解决潜在问题所花费的代价、时间等要求并不苛刻。往往加、减一支二极管、一条接线或更改操作顺序，即可避免出现潜在电路或防止潜在电路的危害。

19.1.4 潜在电路分析

潜在电路分析是指用来识别系统中潜在状态的分析技术，也是解决“非失效相关”的系统故障的重要和有效的分析手段之一。

潜在电路分析（SCA）是GJB 450A—2004中规定的工作项目之一。QJ 3217—2005中给出了航天产品进行潜在电路分析的一般方法与程序。

19.2 目的和适用范围

潜在电路分析的目的，在于通过事先进行的有序的分析工作，发现潜在电路（包括上述四种类型）问题的存在，并揭示其潜在的激励条件。

潜在电路分析原则上适用于任何电气控制系统（极其简单的系统除外）。任务关键系统、安全性关键系统应作为潜在电路分析的重点。在这些系统中，一旦发生事故，损失很大，后果严重。因此，分析的效费比很高。

具体地，选定进行潜通分析的系统和分析范围，可参考以下因素：

a） 系统应用方面的因素：

1） 系统承担的功能是关键的；

2） 异常的系统功能可能会导致人员伤亡或重大的设备毁坏；

3） 在操作中难于对潜在问题进行纠正或根本不可能纠正。

b） 系统计划方面的因素：

1） 系统由多个承包商进行开发研制，系统接口复杂；

2） 系统设计经常进行更改；

3） 承制方没有进行彻底的系统分析。

c） 系统设计方面的因素：

1） 系统具有一定的复杂性，安排的试验难以发现所有的潜在问题；

2） 系统对关键功能进行直接的主动控制，如供配电系统；

3） 系统与其他系统或功能有较多的接口关系；

4） 根据试验结果或经验，系统被怀疑存在潜在问题。

19.3 方法

19.3.1 基于网络树生成和拓扑模式识别的分析方法

任何系统，无论其结构复杂程度和系统各部件相互连接的性质，总能够按照其物质流、能量流、数据流和逻辑信号流的传播模式，以网络树的形式表示系统各部件间的相互连接关系。网络树表达了系统中物质流、能量流、数据流和逻辑信号流传播的最重要的结构信息。

由于拓扑结构上相似的系统倾向于表现出相似的功能，因此可以通过对网络树进行拓扑识别，并利用事先建立的关于特定拓扑模式的线索表，识别系统所具有的功能。

基于网络树生成和拓扑模式识别的分析方法是，首先对系统进行适当的划分以及结构上的简化，生成网络树；其次识别网络树中的拓扑模式；最后，结合线索表对网络树进行分析，识别出系统中存在的潜在状态。

19.3.2 基于功能节点识别和路径追踪的分析方法

潜在电路分析也可以在对复杂系统进行划分和简化的基础上，通过关键功能节点的识别和功能节点间因果路径的追踪，结合线索表进行分析。

系统中的功能节点可划分为源和目标两类。功能路径是指为完成系统的某项特定功能，系统内物质流、能量流、数据流或逻辑信号在功能节点间的传输路径。对于功能路径的识别是针对特定的源和目标进行的。

基于功能节点识别和路径追踪的分析方法是，首先对复杂系统进行划分和简化，其次识别出系统中的功能节点，追踪出功能路径，最后结合线索表进行路径分析。

19.4 步骤

19.4.1 准备阶段

潜在电路分析的步骤分为三个阶段，即准备阶段、分析阶段、结论阶段。参见QJ 3217—2005图2。其中准备阶段的工作程序包括：

a） 资料收集：资料收集的原则是尽可能多地收集与待分析系统相关的资料，这些资料应准确、全面、有效；

b） 资料消化：资料消化的原则是全面系统地整理和消化原始资料，据此掌握系统所有期望的运行模式、状态和功能；

c） 数据预处理：数据预处理的工作一般包括：为保证系统完整性而进行的系统补充定义、虚拟器件定义、连通性数据修补、系统划分、系统简化、元器件模型表建立、确定分布参数等。

19.4.2 分析阶段

19.4.2.1 基于网络树生成和拓扑模式识别的分析程序

基于网络树生成和拓扑模式识别的分析程序包括：

a） 网络树生成：网络树生成一般需借助计算机辅助分析软件工具进行。在电路规模较小时，也可以由人工生成网络树。

b） 拓扑模式识别：从第一棵网络树开始分析；对每棵树，从系统的第一种运行模式开始分析；对每种运行模式（含不可忽视的过渡状态），首先由非断分支组成状态网络树，接着识别出网络树中所有可能的基本拓扑模式。

c） 结合线索表的网络树分析：对每棵树、每种运行模式中的各基本拓扑模式，结合开关状态表，回答线索表中的每个问题，借以发现潜在状态(基于网络树生成和拓扑模式识别的分析方法，所依据的线索一般包含三类：元器件应用线索、功能设计线索和拓扑结构线索）。

19.4.2.2 基于功能节点识别和路径追踪的分析程序

基于功能节点识别和路径追踪的分析程序包括：

a） 功能节点识别。识别系统的运行模式和开关性器件的状态表；根据对系统的功能分析，完成目标的识别；根据对系统的功能分析，完成源的识别。

b） 路径追踪。假定系统中所有开关性器件处于闭合位置，通过路径追踪，识别出在源和目标之间的所有路径。

c） 结合线索表的路径分析。对每条路径，结合系统运行模式和开关性器件的状态表，识别路径的激发条件；必要时，追踪激发路径；对每个激发条件进行分析，根据潜在电路分析线索表，识别出潜在状态(基于功能节点识别和路径追踪的分析方法，所依据的线索一般包含两类：路径线索、路径—器件线索)。

19.4.3 结论阶段

记录分析结论，按潜在路径、潜在时序、潜在指示、潜在标志对问题进行分类汇总；整理得到的结论，对发现的潜在问题进行分析，提出改正建议；将发现的问题提交设计方进行交流和确认；形成潜在电路分析报告。潜在电路分析报告的内容一般包括分析过程、分析结论、改正建议及设计方交流和确认情况等。潜在电路分析报告的主要内容，也可用潜在电路分析报告简表的形式提供，参见QJ 3217—2005附录E图E.1。

19.5 应用说明

19.5.1 潜在电路分析软件工具

对于元器件总数不超过50个的电子/电气系统的潜在电路分析，可以用人工方法进行；但超过上述规模时，应借助潜在电路分析软件工具进行。

19.5.2 潜在电路分析与其他分析技术的综合

潜在电路分析致力于预先识别由于设计疏忽或人为操作错误引起的系统失效因素，因此在很多情况下，潜在电路分析可弥补其他技术的不足。

潜在电路分析与其他技术的综合应用，可提供关于系统失效的更全面的信息和取得更好的效果。

潜在电路分析的任务确定，可以依据任务功能分析、功能故障分析、危险分析、故障模式和影响分析（FMEA）的结果。

潜在电路分析可以与其他的可靠性分析技术在一定程度上共享输入数据和分析结果。

19.5.3 潜在电路分析的分析层次

潜在电路分析可以应用于一个完整的系统，也可以应用于重点选择的分系统、关键功能或关键设备。

19.5.4 潜在电路分析的计划安排

随着系统研制阶段的推进，改正潜在电路的代价直线上升。因此为实现最佳的投资效益，潜在电路分析应在工程研制的尽可能早的阶段进行，并随着研制阶段的进展不断进行更新分析。

在方案研制阶段，潜在电路分析可利用系统框图、系统原理图进行设计方案的潜在电路分析或系统级的潜在电路分析。

在工程研制阶段的后期，如全尺寸工程研制阶段（初样、试样、正样）完成后，可以依据系统的具体物理实现，进行设备级或制造级的潜在电路分析。

19.5.5 潜在电路分析的组织

承担潜在电路分析任务的人员应由三方面的人员组成，即系统设计人员、待分析系统领域（如电气或电子领域）的专家和潜在电路分析的专家。其中设计人员主要负责提供设计数据及相关内容的咨询，分析任务则主要由后两类专家独立完成。设计人员和分析人员之间应就分析数据和结论进行及时沟通和交流，以保证分析结论的正确、有效。

19.5.6 潜在电路分析的监控和评价

应对潜在电路分析的过程进行监控，对潜在电路分析报告进行评价，以确保潜在电路分析结论的有效性，并能够及时反映到设计更改上，促进潜在电路分析的闭环管理。

20 环境及其防护设计

20.1 概述

卫星可靠性设计仅仅着眼于功能设计是不够的。只有在方案阶段开始就充分考虑环境条件并进行必要的环境防护设计，才能使卫星的可靠性及寿命得到提高。

环境防护有两种方式，即构成卫星的材料、零件在使用环境下自身的防护能力；通过特定设计获得的防护能力。

20.2 卫星环境及影响

卫星环境及影响见表12。

表12 卫星环境及影响

序号	环境		主要影响	典型失效模式
1	温度	高温	热老化 金属氧化加速 结构变化 设备过热 润滑粘度下降 材料软化 化学分解和老化	绝缘失效 接点接触电阻增大 橡胶、塑料裂纹和膨胀 元件损坏、着火、焊点脱开、低熔点锡焊开裂 丧失润滑特性 结构强度减弱，绝缘质变软失效 元件材料电性能老化
		低温	粘度、浓度增大 材料变脆 物理收缩 元件性能改变	丧失润滑特性 结构强度减弱，电缆损坏，橡胶变脆 活动部件被卡住，磨损增加；触点接触不良；密封垫弹性消失 电解电容器损坏，石英晶体不振荡，电池容量下降
		高低温循环	剧烈膨胀与冷缩	加速元器件、材料机械操作和电性能变化；橡胶件表面龟裂
2	低气压		膨胀 漏气 散热不良	容器破裂，爆裂膨胀 电气性能下降，机械强度下降、绝缘击穿 跳弧、电晕放电、电设备工作不稳定甚至故障 设备温度升高

表 12（续）

序号	环境		主要影响	典型失效模式
3	真空		有机材料分解、蜕变、放气 冷焊 蒸发	放气和蒸发污染光学玻璃，轴承、齿轮、相机快门等活动部件磨损加快 二种金属表面冷焊、“ 重损 ” 聚四氟乙烯释放氟、聚氯乙烯释放氯造成腐蚀
4	振动		机械应力疲劳、电路中产生噪声	外引线、管脚、导线折断 金属构件断裂、变形、结构失效 继电器、开关瞬断、接插件性能下降 陀螺漂移增大以致故障 加速度计精度降低 粘层、键合点脱开 电路瞬间短路、断路
5	电磁辐射		产生假信号	电气、电子设备正常工作中断
6	静电		静电荷积累	卫星表面产生大电流放电，造成电子元器件持续损伤，逻辑电路乱真切换，传感器信号中噪声增大，温控表面效能丧失和卫星姿态发生颤抖
7	失重		无对流冷却	加剧高温作用
8	核辐射	宇宙射线	电子（主要是质子、γ和α射线所致）	高能质子引起半导体器件永久位移和电离表面损伤效应
		维尔诺夫—范艾伦辐射带	主要由质子和低能电子组成	损伤航天器热控表面、光学表面、太阳能电池和电子元器件
		激光辐射	电子、质子	极轨道上的航天器热控表面、光学表面及裸露的介质材料损伤，绝缘体电阻出现瞬时变化
		太阳风	太阳喷射出的等离子体的粒子流	对暴露的光学元件和热控表面造成损伤
9	加速度		机械应力 液压增加	结构变形和破坏 漏液
10	噪声		低频影响与振动相同； 高频影响设备元件的谐振	电子管、波导管、速调管、磁控管、压电元件、管壁上的继电器、传感器 活门、开关、扁平的旋转天线等均受影响、结构可能失效

由环境应力造成失效，这是可靠性问题中的基本物理现象。环境造成设备失效可分两类：

a） 完全失效；

b） 短时性功能故障。在某种环境条件的影响下设备功能不能正常发挥，一旦外界条件消失后功能仍可恢复。

20.3 抗辐射设计

20.3.1 概述

空间辐射累积剂量高，例如同步轨道卫星八年寿命期间累积剂量达10^7Gy(Si），在卫星壳体内达10^5Gy(Si）。卫星电子部件要求抗空间积累辐射加固。

空间环境主要需考虑范艾伦带高能电子和质子（包括太阳耀斑质子）辐射所造成的电子元器件和材料损伤。空间辐射环境受地球磁场控制，受太阳活动影响，结构不稳定，随时间变化。粒子通量的不确定因子是二到五。卫星轨道高低和轨道平面位置，近地点和远地点参数，进入和离开辐射带的情况及停留时间等都要细致考虑。

20.3.2 抗辐射设计原则

空间电子设备抗辐射设计原则如下：

a） 器件辐射损伤的预测必须及时进行，它影响线路功能设计和结构设计；

b） 选用耐辐射器件可在不增加屏蔽质量和复杂性的条件下使卫星寿命延长，锗器件比硅器件耐辐射好，NPN 比 PNP 好一倍，高频管比低频管好，I_c 大的管子较好，MOS 器件应优先采用抗核加固的体硅 CMOS 或 SOS/CMOS；

c） 尽可能在芯片上或子系统引入冗余并交替工作以提高抗辐射能力，因为时间中断能够使辐射引起的电荷积累效应缓解；

d） 合理采用 LSI，是因为每克屏蔽质量可使较多的线路功能得到屏蔽，但 LSI 的耐辐射容限低于 SSI；

e） 避免逻辑工艺（CMOS、PMOS、TTL 等）的混用，因为兼容性将因辐射而降低；

f） 尽可能把辐射敏感器件深藏起来，辐射敏感器件多的单元尽量靠近，以便互相屏蔽，并把装这些单元的机盒靠近厚重的构件放置；

g） 共平面的组件阵列有特别好的侧向相互屏蔽作用；

h） 采用小的局部密集附加屏蔽可使屏蔽质量最小；

i） 若在辐射路径上吸收体很薄小于 1mm，即使外面空间有一个小的立体角，也会进入大量辐射，故不容忽视；

j） 对于分立器件，应预测并规定 β 降低和结漏电增加的界限，并设计使用负反馈稳定增益的线路；

k） 对于 TTL 尤其是 I^2L，应规定扇出和集电极电流界限；

l） 对于 MOS 电路，应按 ΔV_D 分类选购，预测寿命，在 V_{DT} 和接电时间方面作出选择，并降低速度和输出驱动要求；

m） 对于线性 IC，应规定开环增益下降、输入失调电压和电流、输出驱动和最大压摆率等项的容限；MOS 和线性 IC 都应在屏蔽和价格之间权衡。

20.3.3 步骤与方法

卫星电子元器件抗辐射设计首先要计算卫星在运行寿命期内的累积辐射剂量，其次要恰当选用电子元器件，某些类型的元器件必须进行抗辐射加固。电子线路的抗辐射功能的设计和电子部件结构的抗辐射屏蔽设计也很重要。

卫星上电子元器件周围的所有物质都可以当作屏蔽或防辐射保护层，其中大部分材料是为了星体结构上的理由而采用，称为构件屏蔽。而对辐射特别敏感的电子元器件或线路（例如CPU、存贮器芯片）专门加上的防辐射保护层则称为附加屏蔽。有效地利用构件屏蔽是头等重要的，附加屏蔽只在不得已的情况下有选择地使用。

每种电子元器件对瞬时辐射和累积辐射的耐受能力不尽相同，对中子、γ射线、电子、质子辐射的耐受能力也不一样。一般电子元器件和材料的耐累积辐射容限可归纳如表13。

各类器件耐累积辐射剂量的数量级估计如表14。

表13　材料耐累积辐射容限

耐累积辐照剂量 Gy(Si)	材料	电子元器件
10^2	聚四氟乙烯、环氧树脂	
10^3	聚氯乙烯、尼龙、丁腈橡胶	硅功率晶体管、可控硅、单结晶体管、太阳电池、砷化镓开关二极管、音频管、镓控管
10^4	天然橡胶、硅橡胶、异丁橡胶、氯丁橡胶	二极管、变容二极管、齐纳管、TTL、线绕电位器
10^5	有相硅玻璃纤维、聚对苯二甲酸二酯膜、酚醛塑料	纸、塑料、液钽电容器、微波二极管、硅开关二极管、小型光电管、IC底板、正温度系数硅热敏电阻、场效应管、压电晶体
10^6	聚乙烯、聚氨基甲酸乙酯、玻璃纤维邻苯二甲酸乙烯丙基酯	硅隧道二极管、砷化镓隧道二极管、红外控头、合成电阻器、超小型陶瓷电子管或充气管
10^7	聚苯乙烯、玻璃、炭、云母、石英、硅酮清漆	炭膜、环氧管线绕电阻器、热敏电阻、云母电容、固钽、锗隧道二极管
10^8	陶瓷、磁性材料	陶瓷、玻璃电容器
10^9	—	金属膜电阻
10^{10}	陶瓷、金属	陶瓷管线绕电阻器

表14　电子元器件耐累积辐射量级 Gy（Si）

	双极型器件	NMOS	CMOS		CMOS/SOS
	分立元件，TTL线性组件	LSI	LSI	MSI、SSI	
一般加固后	2×10^4 1.5×10^3	10^1 10^2	10^1～10^2 10^3	10^2～10^3 10^4	耐瞬时辐照好 ＞10^4

20.3.4　注意事项

卫星上各部件抗辐射设计，要根据卫星在轨运行的全寿命期内的轨道位置、空间高能电子与质子环境模型，以及太阳耀斑活动周期等数据，计算出卫星所受的累积辐射总剂量。还要根据各分系统各部件在卫星内部或星体表面安装的总体布局，在计算与每一部件上下、左右、前后相邻部件的主要构件屏蔽贡献的基础上，给出每一部件所受的累积辐射剂量水平，从而提供部件抗辐射设计的依据。如果不作这种具体分析，仅按卫星星体内、外一个剂量点给出总剂量值（不考虑任何相邻构件屏蔽作用），其结果必然过于保守，计算出附加屏蔽将大大超重。

20.4　防卫星静电放电（ESD）设计

20.4.1　概述

由于太阳活动使地球磁层（从约600km高度到45000km高度）发生畸变，这种扰动称为磁球层的亚磁暴。在亚磁暴活动增强期间，磁球层的畸变会注入高能电子，使卫星表面不同程度地带电。卫星表面受到阳光照射的部分会发射光子而放出电荷，所以表面电位只有几十伏；而卫星表面的背阳光部分会积累电荷而建立高达-15kV的负电位。由于卫星温控、能源、通信、探测等不同需要，卫星表面常用不同材料组成不同形式的结构，这也是卫星表面差分充电的原因。同步轨道或亚同步轨道卫星表面差分充电（尤其在子夜到黎明时区多发生）到那么高的电位差，就会发生静电放电，如国外卫星观测到外表温控敷层大面积放电电流达到1400A。这种电弧放电和闪电雷击相似，可能造成卫星温控表面效能丧失、逻

辑电路乱真切换、电子元器件持续性损伤、传感器信号中噪声增大、卫星姿态发生颤抖以至姿态丢失、星地通信设备增益衰减等严重问题。

近地轨道卫星由于低能离子流和电子流远远大于高能粒子流，一般不会充电到高负电位。

20.4.2 减少差分充电

卫星表面充电是入射和再发射电子不平衡的结果。这种不平衡不但和环境条件（轨道高度、电子能量、阳光照射与否）有关，也和卫星外表材料特性（体电导、表面电导、二次发射率、光发射率等）有关。

20.4.2.1 外表面材料

设计时应尽可能使用导电材料，所有表面都良好接地，避免可能会积累电荷的空腔和大的绝缘面积，这样可以使卫星表面电位大大降低。国外有的同步轨道科学卫星上，涂敷一种透明又导电的铟—锡氧化物薄层材料，取得一定效果。

对于二次表面镜（SSM），可以用导电通路把它的边角和卫星的主结构连接起来（接地）。

太阳电池阵边角用导电涂料喷涂和接地到卫星壳体，要用导电带覆盖并接地。

如果选用二次发射系数高的材料作为温控表面，可以防止卫星带电。因为二次发射系数大于1的材料，受一个电子轰击后会发射不止一个电子。除非等离子体能量为1keV至3keV以上（是二次发射电子的几倍），卫星是不可能带电的。这是无源防卫星带电技术。

20.4.2.2 卫星的金属部件

卫星的金属部件必须搭接到星体。因为金属放电有宽广的频谱（上升时间小于10ns），所以这项接地要求特别重要。并注意以下几点：

a） 太阳电池阵的蜂窝结构接地到卫星壳体，并试验检查。在任何情况下，要用金属带捆扎边角，使其电位总等于壳体电位。

b） 多层绝缘的每一层要多点接地到卫星壳体，边角要和外层捆紧，用铝保护内表面，这样边角电场强度可以减小。

c） 蜂窝结构的连接技术在于通过表面提供一个导电通路（例如用一个导电刷和适当的表面处理）。

20.4.3 降低对放电的易损性

降低对放电的易损性的措施：

a） 所有的电缆和单机，除某些敏感器外，应有效地封在法拉第罩中（通过主结构或金属箔）；

b） 导电结构件互相连结使任何构件间呈低阻抗，以形成整个卫星的电参考点；

c） 直接连结到卫星壳体的单机加金属带以保证导电率，通过适当的表面处理来保证带与蜂窝表面的电通路；

d） 装在星外的电缆（敏感器电缆）要屏蔽；

e） 尽量避免高频率和低电平线路，必要时对它加滤波或偏置，接口电路按技术要求应有共模抑制；

f） 太阳阵引线放在帆板背面。

20.5 防振设计

防振动和冲击有两类办法：或者把设备隔离起来，或者把它制造得足以耐受冲击或振动。隔离措施要同时地、有效地抑制振动和冲击。一般应对振动和冲击引起的偏移和机械应力进行分析来确定保护措施，这种分析包括设备固有频率的确定。如果所产生的机械应力小于安全工作应力，就不再专门保护。反之则应采取机械增强措施，增加支撑或设减振装置等。

针对冲击和振动进行设计时还必须考虑下述基本因素：

a） 元器件相对于支架的位置（即在支架的边角或中心）；

b） 元器件相对于冲击力或振动力方向的预期走向；

c） 安装元器件所采用的方法。

一个元器件的安装姿态、它在系统内相对于其它元器件的位置、其紧固装置发生松动的可能性都会使振动、冲击作用力发生很大的变化。

疲劳失效是振动冲击引起的主要可靠性问题，在疲劳强度设计时应当考虑。

20.6 防潮设计

卫星电子设备和光学元件等要在地面试验室和靶场经历研制试验和测试检查、运输和贮存，所以防潮问题也是必须考虑的。使用干燥剂、密封、涂防潮保护层是常用几种防潮措施。应注意不要把湿气密封在里面或使之冷凝而使湿气造成的问题更严重。还必须就涂层和密封垫排出腐蚀性挥发物或与相邻表面或依据涂层的相容性问题进行慎重的评估。

21 机械产品可靠性设计

21.1 卫星结构可靠性设计

21.1.1 概述

卫星结构设计的任务是使卫星结构满足卫星系统的构型、承载和星上仪器设备安装的要求，并尽可能减小质量，适应空间环境要求，且具有高的可靠性。同时，结构材料和加工工艺对结构产品的质量和可靠性是十分重要的影响因素，尤其对复合材料结构。目前卫星结构设计大多采用安全系数法来保证结构设计满足可靠性要求。

21.1.2 原则

卫星结构可靠性设计一般原则有：

a） 简单化。设计中应尽可能考虑采用简单结构形式，部组件之间简单的装配关系和简单的传力路线有利于进行结构应力、应变及动力响应分析；有利于简化试验工况，提高试验验证的精确性；有利于生产、装配和检验。从而有利于保证结构的质量和可靠性。

b） 继承性。优先选用经过飞行验证的成熟设计、产品和材料、工艺是降低研制风险的有效途径。

c） 采用的新设计、新产品或新材料、新工艺，应按照规定的环境条件进行验证、鉴定。

d） 通用化、系列化、组合化。尽可能按通用化、系列化、组合化(简称“三化”）原则进行设计，采用共用平台或相同的零件和组件（如承力筒等主承力结构）等，减少产品的类型和规格，简化生产工艺，特别对复合材料，减少模具，提高生产效率，便于分析和试验验证。

e） 裕度设计。应对全寿命周期中的环境条件进行全面分析，对设计中的不确定因素应留有余量。

f） 可制造性。设计中应尽可能采用成熟材料及生产工艺，生产过程的检验要求应易于实现。

g） 健壮性。应考虑设计变量的不确定性对性能的影响程度，鼓励对关键设计变量进行灵敏度分析，减少因外部条件的变化对设计的影响。

h） 应在可靠性和其他技术指标间进行权衡，以获得优化方案。

21.1.3 步骤

卫星结构可靠性设计的基本步骤为：

a） 设计任务分析。以使用要求为依据，逐项列出产品所应具有的一切功能。

b） 故障模式与影响分析。对产品功能要求进行分析研究，列出主要的结构故障模式。考虑协调性、

寿命要求、互换性、功能及安全性等各方面可能产生的问题，确定各主要故障模式的严重性级别。

c） 部件可靠性分配。给部件分配可靠性，使整个结构满足可靠性指标要求。分配指标时，必须考虑技术发展水平、工艺性、历史资料、部件复杂性或关键性等因素。

d） 应力分析。为了便于估计可靠性，用均值和方差进行应力分析。

e） 可靠性计算。根据力学模型和计算公式及结构元件参数设计计算应力分布。复杂情况可用随机有限元法计算，根据此概率分布计算可靠性。如可靠性计算结果满足可靠性指标要求，设计即完成；如不满足要求，则须修改设计，重新分析与计算，直至满足要求。

算出结构元件可靠性计算值，根据各元件的可靠性计算值可以计算上一级（装配件）的可靠性，直至全系统。

21.1.4 方法

21.1.4.1 安全系数法

21.1.4.1.1 概述

机械产品可靠性设计的方法有多种，如安全裕度设计、概率设计等。目前卫星结构设计使用安全系数法（安全裕度设计）并结合验证措施来保证结构的可靠性。这种方法没有直接给出结构的可靠度，但实践证明是可以保证结构可靠性的。如果有足够的载荷和材料强度的分布数据也可采用概率设计法来进行结构可靠性设计和估算。概率设计法是以“应力—强度干涉理论”为依据，认为作用于结构、机构的载荷、承载能力是随机变量。概率设计的任务是进行分析计算以确定结构、机构的可靠性；根据可靠性指标确定构件的参数。

为保证卫星任务的完成，结构应可靠地支持星上有效载荷和其它分系统的正常工作。因此在结构的研制中必须对强度进行充分的验证，最常用的验证手段有：分析法和试验法。

首先，要明确结构的设计载荷，用分析法按照各种载荷工况进行整星结构或部件的静力和动力分析，获得结构的应力和位移。根据各类材料的强度准则，校核结构的强度。

其次，可用试验法模拟飞行中的最严酷的环境，进行静力、动力载荷的鉴定（或验收）量级的试验，通过试验技术考核和验证卫星结构的强度。

21.1.4.1.2 设计载荷的确定

应全面地考虑卫星在整个研制过程的所有载荷工况，包括：

a） 卫星结构在地面操作、发射、轨道或返回环境产生的所有载荷工况；

b） 如果卫星结构飞行中具有多种不同构型时，必须分别考虑每种构型下的载荷工况。

在每种载荷工况中，应考虑同一时刻作用在卫星结构上的可能有不同（包括热）环境引起的各种载荷的合理组合。

通常是以飞行载荷作为卫星结构设计的载荷依据来分析结构的强度。在地面操作（停放支承、起吊、翻转、运输等）环境引起的载荷可作为校核卫星结构强度的补充条件，当地面操作载荷会影响卫星结构强度时，通常用改善地面操作环境或用地面工装改善卫星结构的受载情况，以确保卫星结构的安全。

在卫星结构研制中规定了三级载荷：飞行载荷、验证载荷和设计载荷。飞行载荷或称使用载荷（limit load），是卫星正常运行时可能经受的最大载荷；验证载荷是结构作强度考核的地面试验载荷，它是飞行载荷与验证系数的乘积，它介于飞行载荷与设计载荷之间或等于设计载荷；设计载荷是飞行载荷与安全系数的乘积。

结构的设计载荷定义为：设计载荷＝飞行载荷×安全系数。

必须注意，上述的安全系数除与设计分析方法、结构构型与特性、结构材料性能、生产制造工艺等的不确定性有关外，还与结构地面试验载荷的验证系数有关。

21.1.4.1.3 验证系数和安全系数

下面列出了阿里安空间中心和美国NASA推荐的安全系数和地面试验载荷的验证系数值，可供结构设计时参考。

阿里安空间中心推荐的安全系数值（未列出载荷的试验验证系数）：

极限强设计时，最小取1.25；

屈服强度设计时，最小取1.1；

附属结构和柔性结构设计时，最小取1.5。

表15到表19，列出了NASA—STD—5001中对卫星结构各类材料的部件设计时推荐的设计安全系数和试验载荷的验证系数。对于与载荷作用时间有关疲劳和蠕变问题，应以所有使用环境下的工作寿命时间乘以4.0系数，作为疲劳和蠕变寿命的性能评估。

表15　金属结构的设计和试验的最小载荷系数

验证模型	设计安全系数		试验载荷的验证系数	
	按极限强度设计	按屈服强度设计	鉴定试验	验收或验证试验
原型	1.4	1.0[a]	1.4	不要求或1.05[b]
原型飞行件	1.4	1.25	不要求	1.2
[a] 结构在飞行、验收试验或验证试验中不会产生有害的屈服变形必须进行评估。 [b] 仅用于推进剂储箱和固体发动机壳体。				

表16　紧固件和预紧连接的设计和试验的最小载荷系数

验证模型	设计安全系数			试验载荷的验证系数	
	按极限强度设计	连接分离		鉴定	验收或验证
		安全临界值[a]	其它		
原型	1.4	1.4	1.2	1.4	不要求
原型飞行件	1.4	1.4	1.2	不要求	1.2
[a] 连接必须保持压力和/或危险材料在安全临界值内。					

表17　复合结构的设计和试验最小载荷系数

验证模型	结构几何特性	设计安全系数	试验载荷的验证系数	
		按极限强度设计	鉴定试验	验收或验证试验
原型	不连续体（材质不同）	2.0	1.4	1.05
	均质材料（材质相同）	1.4	1.4	1.05
原型飞行件	不连续体（材质不同）	2.0	不要求	1.2
	均质材料（材质相同）	1.5	不要求	1.2
注：表中系数用于有集中应力的情况。对于通常情况，这些系数能减少为原型结构用1.4和原型飞行件结构用1.5。				

表18　玻璃结构的设计和试验最小载荷系数

验证模型	加载状态	设计安全系数	试验载荷验证系数	
		按极限强度设计	鉴定试验	验收或验证试验
原型飞行件	无内压作用	3.0	不要求	1.2
	有内压作用	3.0	不要求	2.0
分析用	无内压作用	5.0	不要求	不要求

表19　结构玻璃胶结的设计和试验最小载荷系数

设计安全系数	试验载荷验证系数	
按极限强度设计	鉴定试验	验收或验证试验
2.0	1.4	1.2

21.1.4.1.4　安全裕度

安全裕度是结构设计中评估结构的强度是否满足要求的指标。

对于结构强度安全裕度定义为公式（42a）或公式（42b）：

$$\text{安全裕度}(MS) = \frac{\text{破坏应力}(\text{破坏应变})}{\text{设计应力}(\text{设计应变})} - 1 \cdots\cdots (42a)$$

或

$$\text{安全裕度}(MS) = \frac{\text{失稳临界载荷}(\text{失稳临界力})}{\text{设计载荷}(\text{设计应力})} - 1 \cdots\cdots (42b)$$

在考虑材料破坏的强度问题时，对于金属材料结构件，可参照不同的强度理论，计算其强度安全裕度。

当应用第一强度（最大拉应力）理论时，用材料的单向拉伸断裂破坏应力 σ_b 作为破坏应力，用设计载荷计算获得的最大拉应力作为设计应力；当应用第二强度（最大拉应变）理论时，用材料的单向拉伸时的最大断裂拉应变 ε_b 作为破坏应变，用设计载荷计算获得的最大拉应变作为设计应变；当应用第三强度（最大切应力）时，用材料单向拉伸时屈服的最大切应力值 τ_s 作为破坏应力，用设计载荷计算获得设计的最大切应力作为设计应力；当应用第四强度（形状改变能密度）理论时，用材料单向拉伸屈服时的形状改变能密度作为破坏应力，用设计载荷计算出各个应力分量，再获得与形状改变能密度的相当应力，由此作为设计应力。

考虑材料破坏的强度问题时，对于复合材料结构件，可参照叠层材料首层破坏的强度分析方法，确定最先破坏的单层，然后相似于上述金属材料方式，根据复合材料的不同强度理论，用公式(42a）来计算强度安全裕度。

在考虑结构件失稳破坏的强度问题时，失稳临界载荷（或失稳临界应力）可按卫星结构静力分析中解析方法或卫星结构有限元静力分析方法获得。然后用(42b）计算安全裕度。对于复合材料结构件，计算方法与金属材料结构件相同，但在计算失稳临界载荷或应力中，应考虑采用复合材料所特有的刚度计算方法。

按照强度校核规范，安全裕度必须大于或等于零，表20推荐了对不同材料、不同破坏方式下的安全裕度最小值。

表20　安全裕度最小值

金属材料结构的安全裕度		复合材料结构的安全裕度	
按材料屈服强度计算	0	按首层破坏计算	0.25
按材料极限强度计算	0.15		
按构件稳定性计算	0.25		0.3

21.1.4.2 概率设计法

21.1.4.2.1 一般方法

机械产品可靠性设计的概率设计法以“应力—强度干涉理论”为依据。记强度为S、应力为L，应力与强度均为随机变量，结构可靠度为S-L>0的概率，即式（43）：

$$R = P(S - L > 0) \cdots\cdots (43)$$

应力—强度所服从的分布常用的有正态—正态、对数正态—对数正态等模式。

对正态—正态模式，令：

$$\begin{aligned}\beta_R &= (\mu_s - \mu_L) / \sqrt{\sigma_s^2 + \sigma_L^2} \\ &= (\mu_s - \mu_L) / \sqrt{C_s^2\mu_s^2 + C_L^2\mu_L^2}\end{aligned} \cdots\cdots (44)$$

式中：

μ_s，σ_s，C_s（$=\sigma_s/\mu_s$）——分别为强度的正态分布均值、标准差、变异系数；

μ_L，σ_L，C_L（$=\sigma_L/\mu_L$）——分别为应力的正态分布均值、标准差、变异系数；

则结构可靠度为式（45）：

$$R = \Phi(\beta_R) \cdots\cdots (45)$$

式中：

$\Phi(\cdot)$——标准正态分布函数；

β_R——结构可靠指标。

对于对数正态—对数正态模式，可将其强度、应力数据均取自然对数后再按正态—正态模式计算其可靠性。结构可靠指标β_R为式（46）：

$$\begin{aligned}\beta_R &= (\mu_{lns} - \mu_{lnL}) / \sqrt{\sigma_{lns}^2 + \sigma_{lnL}^2} \\ &= \ln\left[\frac{\mu_s}{\mu_L}\left(\frac{1 + C_L^2}{1 + C_s^2}\right)^{1/2}\right] / [\ln(1 + C_s^2) + \ln(1 + C_L^2)]^{1/2}\end{aligned} \cdots\cdots (46)$$

C_s和C_L不大于0.3时，β_R可用式（47）计算：

$$\beta_R = (\ln \mu_s - \ln \mu_L) / [C_s^2 + C_L^2]^{1/2} \cdots\cdots (47)$$

对任意模式按（42a）或（42b）式计算可靠度。如果难以计算，可考虑采用近似计算，如验算点法。

在正态—正态模式下结构可靠度R与结构可靠指标β_R的值可从标准正态分布表中查得，常用的几组数据见表21。

表21 结构可靠性与结构可靠性系数的关系

结构可靠度R	0.9	0.95	0.99	0.999	0.9999
结构可靠指标β_R	1.282	1.645	2.326	3.091	3.719

根据结构试验，估计应力、强度的分布参数，即μ_s，σ_s（或C_s），μ_L，σ_L（或C_L）然后通过式（44）、(45)计算结构可靠度。

对强度、应力的函数的均值、方差计算。对一元函数$y=f(x)$，用式（48）近似求y的均值和方差：

$$E(y)=f(\mu)+f''(\mu)\sigma^2/2$$
$$D(y)=(f'(\mu))^2\sigma^2 \quad \cdots\cdots (48)$$

式中：

μ、σ——分别为强度或应力的均值、标准差。

对n元函数y（$x_1,x_2,\ldots,x_n$），若$x_1,x_2,\ldots,x_n$相互独立，则y的均值和方差用式（49）近似计算：

$$E(y)=f(\mu_1,\ldots,\mu_n)+\frac{1}{2}\sum_{i=1}^{n}(\partial^2 y/\partial x_i^2)\sigma_i^2$$
$$D(y)=\sum_{i=1}^{n}(\partial y/\partial x_i)^2\sigma_i^2 \quad \cdots\cdots (49)$$

式中：

$\mu_1,\ldots,\mu_n;\ \sigma_1,\ldots,\sigma_n$——分别为$x_1,\ldots,x_n$的均值、标准差；导数在各均值$\mu_i$处取值。

根据确定的结构可靠度指标R，根据表21及标准正态分布表查得结构可靠指标β_R，再按式（44）计算某应力或强度参数，以指导结构设计。

21.1.4.2.2 可靠系数法

可靠系数法不同于传统的安全系数法。传统的安全系数法认为强度和应力均为定值，可靠系数法认为强度和应力均为随机变量。

可靠系数分为均值安全系数、概率安全系数、随机安全系数三种。

21.1.4.2.2.1 均值安全系数为强度均值μ_s与应力均值μ_L的比值，即$\bar{k}=\mu_s/\mu_L$。在强度与应力独立情况下根据式（44），均值安全系数$\bar{k}$按式（50）计算：

$$\bar{k}=\mu_s/(\mu_s-\beta_R\sqrt{\sigma_s^2+\sigma_L^2})=\frac{1+\beta_R(C_s^2+C_L^2-\beta_R^2C_s^2C_L^2)^{1/2}}{1-\beta_R^2C_s^2} \quad \cdots\cdots (50)$$

21.1.4.2.2.2 概率安全系数k_p为概率a下的最小强度与另一概率b下出现的最大应力之比。一般a、b取0.95、0.99。在正态分布情况下，均值安全系数按式（51）计算：

$$k_p=\frac{S_{amin}}{S_{bmax}}=\frac{1-\nu_{as}C_s}{1-\nu_{bL}C_L}\times\frac{1+\beta_R(C_s^2+C_L^2-\beta_R^2C_s^2C_L^2)^{1/2}}{1-\beta_R^2C_s^2} \quad \cdots\cdots (51)$$

式中：

ν_a、ν_b——概率a、b下的正态分布分位数。

21.1.4.2.2.3 随机安全系数是将安全系数即强度与应力之比作为随机变量。在给定可靠性指标R情况下，随机安全系数的范围为式（52）：

$$1\le k\le\frac{2\bar{k}^2(C_s^2+C_L^2+1)-3\bar{k}+1}{\bar{k}-1} \quad \cdots\cdots (52)$$

式中：

$\bar{k}$——均值安全系数，按式（50）计算。

21.1.4.2.3 可靠性分项系数法

可靠性分项系数法设计表达式为式（53）：

$$\gamma_s \mu_s \geq \gamma_L \mu_L \quad \cdots\cdots (53)$$

式中：

γ_s，μ_s——分别为强度的分项系数和均值；

γ_L，μ_L——分别为应力的分项系数和均值。

当应力L和强度均服从正态分布，且$\frac{1}{3} \leq \frac{\sigma_s}{\sigma_L} < 3$时，强度和应力分项系数按式（54）计算：

$$\begin{cases} \gamma_s = 1 - 0.75 C_s \beta_R \\ \gamma_L = 1 + 0.75 C_L \beta_R \end{cases} \quad \cdots\cdots (54)$$

当应力L和强度均服从对数正态分布，且$\frac{1}{3} \leq \frac{\sigma_s}{\sigma_L} < 3$时，强度和应力分项系数按式（55）计算：

$$\begin{cases} \gamma_s = \exp(-0.75 C_s \beta_R) \\ \gamma_L = \exp(0.75 C_L \beta_R) \end{cases} \quad \cdots\cdots (55)$$

21.1.5 结构静强度、刚度可靠性设计与计算

21.1.5.1 结构静强度、刚度可靠性设计的主要内容

结构静强度、刚度可靠性设计的主要内容有：

a） 确定结构零、部件的可靠性目标值（固有可靠性）；

b） 确定所要设计的结构零、部件的故障模式；

c） 确定作用在结构上外载荷总体均值、标准差；

d） 选用材料，确定所选材料的强度均值和标准差；

e） 计算结构可靠性；

f） 若可靠性指标小于分配规定值，对简单结构单元，可根据设计表达式直接完成设计；对形状复杂结构单元，可先初步设计，然后调整材料参数或外载荷情况，修改设计，重复计算，直到满足要求。

21.1.5.2 计算与设计方法

假设零件尺寸和材料的机械性能等随机变量都是正态分布，载荷或应力也为正态分布，则结构可靠指标β_R为式（56）：

$$\beta_R = (\mu_s - \mu_L) / \sqrt{\sigma_s^2 + \sigma_L^2} \quad \cdots\cdots (56)$$

式中：

μ_s，σ_s——分别为强度的正态分布均值、标准差；

μ_L，σ_L——分别为应力的正态分布均值、标准差。

根据结构可靠指标β_R可查得可靠度R，也可根据R反求结构可靠指标β_R，从而根据使用环境及载荷选择合适的材料。

21.1.6 疲劳强度可靠性设计与计算

疲劳强度的可靠性设计与常规疲劳强度设计所不同的是，常规疲劳强度设计中的各种参数如强度、

载荷、零件尺寸等数据一般都是取其平均值，而可靠性的疲劳强度设计则要求算出零、部件上的计算应力点及其工作应力的概率分布以外，最重要的是要得到材料疲劳强度的概率分布。进行机械产品疲劳强度可靠性设计时的条件为：

a） 所用材料疲劳强度的概率分布曲线，即$P—S—N$（概率—疲劳强度—循环数）曲线；

b） 零部件上所要计算的应力点及其工作应力（该处载荷）的概率分布；

c） 疲劳强度与工作应力相结合的可靠性分析方法，与静强度可靠性设计相似。

计算疲劳强度可靠指标的方程是式（57）：

$$\beta_{\mathrm{R}} = (\mu_{\mathrm{sr}} - \mu_{\mathrm{Lr}}) / \sqrt{\sigma_{\mathrm{sr}}^2 + \sigma_{\mathrm{Lr}}^2} \quad \cdots\cdots (57)$$

疲劳强度可靠性设计的均值安全系数按式（58）计算：

$$f_0 = \frac{\mu_{\mathrm{sr}}}{\mu_{\mathrm{Lr}}} = \frac{\mu_{\mathrm{sr}}}{\mu_{\mathrm{sr}} - \beta_{\mathrm{R}}\sqrt{\sigma_{\mathrm{sr}}^2 + \sigma_{\mathrm{Lr}}^2}} \quad \cdots\cdots (58)$$

式中：

μ_{sr}，σ_{sr}——分别为疲劳强度均值、标准差；

μ_{Lr}，σ_{Lr}——分别为工作应力强度均值、标准差。

当μ_{sr}，σ_{sr}，μ_{Lr}，σ_{Lr}已给，且可靠性已定，β_{R}值可从标准正态分布表中查得。于是，可求得在给定可靠度R时的均值疲劳安全系数f_0。

则按式（59）进行结构设计：

$$\mu_{\mathrm{s}} \geq f_0\mu_{\mathrm{L}} \quad \cdots\cdots (59)$$

21.1.7 断裂强度可靠性设计与计算

断裂强度的可靠性设计就是把应力、强度、裂纹长度等作为随机变量，研究裂纹结构在应力作用下扩展断裂的可靠性大小问题。

张开型断裂是最危险的失效模式，断裂判据为式（60）：

$$K_1 \leq K_{1\mathrm{c}} \quad \cdots\cdots (60)$$

式中：

K_1——张开型断裂应力强度因子；

$K_{1\mathrm{c}}$——材料的平面应力断裂韧性。

张开型断裂纹在垂直于裂纹面的拉应力的作用下扩展而断裂。张开型的应力强度因子为式（61）：

$$K_1 = \alpha\phi\sqrt{\pi l} \quad \cdots\cdots (61)$$

式中：

α——修正系数；

ϕ——工作应力；

l——裂纹长度。

发生脆断时的临界应力ϕ_{c}为式（62）：

$$\phi_{\mathrm{c}} = \frac{K_{1\mathrm{c}}}{\alpha\sqrt{\pi l}} \quad \cdots\cdots (62)$$

发生脆断时裂纹的临界值 a_c 为式（62）：

$$l_c = \frac{K_{1c}^2}{\alpha^2 \phi^2 \pi} \quad \cdots\cdots (63)$$

此处 K_1 或 ϕ 或 l 相当于静强度中的应力。K_{1c} 或 ϕ_c 或 l_c 相当于静强度中的强度。已知它们的分布和参数后可求出均值和标准差，再按方程（44）、（45）求可靠性，或按一定的可靠性要求进行断裂强度可靠性设计。

21.1.8 卫星结构可靠性估算

卫星结构可靠性估算步骤如下：

a） 利用缩比试件的试验数据，缩比试件按相似律设计，材料和制造工艺都与结构实物一致。

b） 将子结构的强度数据作为系统结构强度数据的重要信息。

c） 对于信息特别少的极小子样情况(n=2~3)，可用综合判断比较粗糙地分析可靠性。其分析依据是：

1） 通过结构强度计算公式，可得平均值，根据该公式以往使用的准确性，判定所得试验数据平均值的准确性；

2） 分析结构生产、检验、使用过程中出现过的累积故障信息，作为结构承载能力的评价依据；

3） 只要零组件的材料、工艺制造正常，有一定继承性，则每一零组件总是具有一定可靠性水平；

4） 飞行器常常是在原结构基础上改进而来，因此，可把相近结构的统计参数作为可靠性定量分析的旁证。

d） 以计算公式求得的理论值作为基准，算出试验值与计算值之比，这样把试验数据化为无量纲参数，而后将这些无量纲参数集合成一个样本，再作统计分析。这样，可把尺寸不同而结构类型、材料、工艺制造相同的结构试验信息作为同一分析和评价的对象。

21.2 卫星机构可靠性设计

21.2.1 概述

机构由各个具有确定相对运动的构件所组成。诸如卫星与运载火箭连接与分离、太阳翼展开、天线展开、回收舱和解锁及抛盖、回收降落伞开伞和脱伞等动作均由星上机构来实现。卫星上机构若按其功能或用途分类有多种多样。常用的机构若按其动力源划分主要可分为两类，一类是以火工品点火产生的燃气作为动力源的火工机构(如：太阳翼压紧释放机构、火工切割器、星箭连接分离包带用的爆炸螺栓、舱段火工解锁机构、火工弹抛机构或火工分离推杆机构等）；另一类是非火工机构(如：太阳翼展开机构、天线展开机构、密封机构、缓冲机构等等）。

这些星上机构如果不采取可靠性设计，在真空、微重力、高低温交变、辐射、空间碎片等空间环境下，在各种力学环境下，就容易产生机构运动故障。真空低温环境可导致机构运动副冷焊；较大的高低温交变和热胀冷缩效应可导致机构卡死；辐射、真空和低温环境将影响密封机构的密封性能。而卫星机构的动作直接影响着卫星飞行的成败和预定任务的完成，所以，对卫星机构必须采取可靠性措施，才能保证机构可靠地实现其功能。

21.2.2 卫星机构可靠性设计原则

除了遵循通用机械的设计原则之外，卫星机构设计还要遵循如下原则：

a） 以在满足功能和性能要求的前提下，机构组成力求简单，减少不必要的环节；

b） 机构设计方案须经方案比较、优化筛选、故障模式影响分析后最终确定；

c） 机构设计的技术要求须充分考虑机构的贮存环境和工作环境，真空低温情况下，运动副要有防冷焊设计措施；高低温交变情况下，运动副间隙及材料间膨胀系数应匹配；

d） 原材料、紧固件、密封件、元器件选择及工艺方法选择严格执行国家、行业和企业的相关标准；

e） 严格控制机构中关键零部件的关键参数，并在技术文件中明确要求；

f） 采取合理的冗余设计措施(如火工机构的双起爆器、双药盒冗余设计）；

g） 尽量继承成熟技术或成熟产品；

h） 火工机构的起爆器宜采取钝感型起爆器，以防误爆；

i） 机构的高强度钢连接件的工艺选择须防止脆性断裂，机构零部件设计尽可能避免应力集中。

21.2.3 卫星机构可靠性设计方法

卫星机构可靠性设计与卫星结构可靠性设计有较为明显的区别。卫星结构可靠性设计主要考虑的问题是强度问题。卫星机构可靠性设计除了要求组成机构的各个零件或部件满足强度要求之外，还要保证机构可靠地实现其规定的运动。而机构运动就与运动副的装配间隙、材料匹配、表面润滑状态、环境条件、动力源提供的驱动力或驱动力矩有关，即使组成机构的各个零件或部件均满足强度要求，也不一定能保证机构可靠地工作。因此，对于机构可靠性设计，难以用几组公式来描述其设计方法，机构可靠性设计的重点是消除、减少或控制设计中的不可靠因素。可参照如下的步骤、方法进行机构可靠性设计：

a） 根据机构设计任务书及设计要求，进行任务分析，提出多种机构设计方案，进行方案论证和比较，在满足功能要求的前提下，机构组成力求简单，减少不必要的环节，优选设计方案；

b） 对初步选定的设计方案进行 FTA 和 FMEA 工作，通过分析列出单点故障清单和可靠性关键项目（关键零件或部件）；

c） 根据 FMEA 的分析结果，进一步完善设计方案，例如，对于某些重要环节增加冗余措施；

d） 进行机构的图样详细设计；

e） 复核重要零部件的结构强度，若不满足要求需修改设计；

f） 进行设计评审。

21.2.4 示例

以某型号的火工连接与分离机构(见图33)为例，简要说明卫星机构可靠性的设计思想。

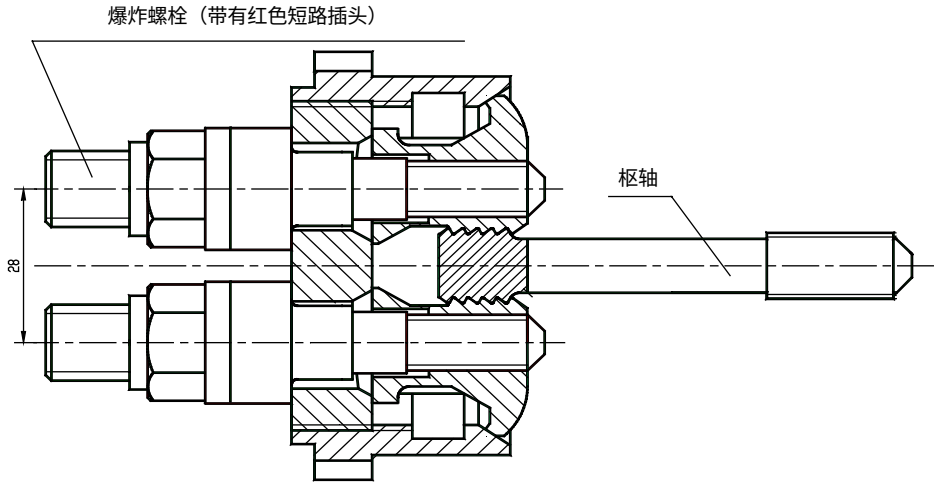


图33 某型号的火工连接与分离机构

该火工机构是某型号实现舱段连接与分离的执行机构。在爆炸螺栓点火之前，依靠枢轴方头部分的齿形和另一端的螺纹实现舱段之间的连接；当爆炸螺栓点火之后，爆炸螺栓解除了对轴套(图33中与爆炸螺栓螺纹部分连接，同时又与枢轴方头部分的齿形连接的零件)的连接，则轴套在枢轴拉力作用下向两边分开，实现了与枢轴方头部分齿形的分离，从而实现了两个舱段之间的分离。

该火工机构的可靠性设计要点如下：

a） 为了提高解锁分离的可靠性，采用双爆炸螺栓、双轴套冗余设计，两个爆炸螺栓中只要有一个点火，即使另一个失效也可保证可靠分离。

b） 由于连接载荷较大，所以要求枢轴材料的抗拉强度很高，同时又不能发生脆性断裂。为了保证连接可靠，选择了高强度、延伸率大的材料作为枢轴材料(如果采用高强度钢且淬火后的硬度很高，一味追求高强度而忽视了延伸率，则容易发生早期脆断)。

c） 为了提高连接的可靠性，防止枢轴因螺纹处应力集中而发生早期脆性断裂，在图样中技术要求中对枢轴螺纹根部圆角半径和螺纹表面粗糙度作了严格的规定。

d） 为了防止低温真空冷焊，在轴套表面采取了润滑措施。

e） 该机构的重要件在图样中有明确的标识“ 重要件 ”，重要特性有明确的标识“ Z ”。

21.2.5 注意事项

卫星机构可靠性设计应注意以下事项：

a） 在图样设计中，需充分体现 FMEA 分析结果中的“ 故障防止措施 ”；

b） 对于关键件和重要件，关键特性和重要特性均需在图样中给出明确标识；

c） 图样的技术要求中须充分考虑运动副的装配间隙、材料匹配、表面润滑状态；

d） 图样的技术要求中须充分考虑所选工艺的工艺特点，特别对于高强度钢的热处理方法、热处理后的硬度及表面处理方法的决定，必须考虑防止脆性断裂因素，图样的技术要求中杜绝采用“ 国家、行业或企业有关标准或规定中明确禁止 ”的工艺方法，慎重采用表面镀锌和镀镉工艺，需要注意其适用条件；若机构中有钛合金零部件，需在技术要求中明确提出钛合金氢脆问题的控制要求；对于有端面密封要求的机构零部件，在图样中应对其切削加工的刀痕方向作出规定，使刀痕方向与密封圈方向相同，对于有密封要求并且由焊接而形成的机构零部件，需在图样中对焊缝提出要求；

e） 火工机构(特别是有输出能量要求的火工机构，如要求火工分离推杆的速度在某个范围内）的装药量，需通过理论计算及摸底试验后才能最终落实在图样上；

f） 对于有密封要求的机构，图样的技术要求中需给出密封性能指标，动密封还需考虑密封面的润滑。

22 软件可靠性

22.1 概述

在卫星等航天器上，计算机软件已越来越重要，其可靠性水平直接关系到卫星功能的强弱和任务的成败。

软件可靠性定义有别于硬件可靠性，但比较类似，即在规定条件下，在规定时间内，不因软件而引起系统失效的概率，或在规定的时间内，在规定条件下程序执行规定功能的能力。但软件可靠性不仅与软件中存在的缺陷有关，还与系统输入和系统使用有关。

软件产品与硬件产品一样，在客观上存在缺陷，但软件不会出现硬件那样的损耗或老化，软件缺陷主要是在软件需求分析、设计、编程以及各种修改过程中人为产生的，在软件测试过程中可能被发现而

被改正。据经验统计，单个软件的失效率一般只能达到（10^{-3}~10^{-4}）/h。

软件错误与硬件出错规律不同，对软件如果用同一输入反复执行多次，则正确的总是正确的，错误的总是错误的。同一软件在不同地方使用出现的错误也不尽相同。软件的缺陷是否引起故障，主要取决于软件产品的使用方式和因输入条件变化引起程序执行的路径。

目前软件可靠性的研究主要集中于广泛收集软件错误（故障）数据和发展各种有效的分析模型两个方面。已提出相当多的软件可靠性预计模型，但目前在国内尚未实用化，仅能定性评估软件的可靠性。

与软件可靠性有关的软件属性有：

a） 安全性，安全性等级高的软件，必然要求有高的可靠性。

b） 成熟性，与软件缺陷引起错误的频率相关，成熟的软件可靠性高。

c） 容错性，软件在出现错误或软件受干扰后能维持规定性能的水平，高可靠性的软件一般都使用容错设计。

d） 可恢复性，当软件出现错误又需要重新正确工作时，软件有重建其性能水平及恢复受直接影响的数据能力。

e） 可维护性，其中又包括可分析、易修改、可测试等。

f） 软件任务书的不完整和不断补充，会导致软件的不断修改，软件的每次修改都可能会引入新的缺陷，对软件的可靠性极为不利。推荐由交办方与承制方共同成立软件任务书的特别小组，提出详细、尽可能完整的软件任务书，并审查提出必要的软件任务书的改动。该小组应维持到软件产品验收交付后。

软件可靠性设计，不仅仅局限于程序设计与实现，而是与软件整个研制过程密切相关，包括需求分析、软件设计与实现、软件测试、软件维护等。应从软件保证的角度来保证软件的可靠性。

22.2 一般要求

软件可靠性开发的一般要求如下：

a） 星用软件有高可靠性要求，必须遵循 QJ 3126—2000、QJ 3128—2001 的要求。

b） 星用软件可靠性设计应遵循 GJB/Z 102—1997 的要求，提高软件的固有可靠性。

c） 软件没有明显的生产过程，只要严格按规范进行复制和比对，一般不可能产生缺陷。软件可靠性主要靠开发过程的控制和严格、详细的测试来提高。在严格软件质量管理的基础上，贯彻软件可靠性工程。提高软件可靠性的方法主要是按软件工程的要求分阶段开发软件，要重视软件开发、测试方法和工具的研究和使用成熟的软件（正版）工具。

d） 软件开发过程中的每一个阶段都要有阶段产品——文档，对阶段产品必须进行认真评审，以尽早消除可能产生的缺陷。评审工作主要是对文档的正确性和一致性进行检查，确保软件任务书中需求完整、无遗漏，软件需求规格说明正确、全面反映了软件任务书需求，包括潜在的任务需求。软件概要设计完全实现了需求规格说明，软件详细设计完全实现了概要设计说明，编程与详细设计说明一致，算法和判别逻辑正确完整，精度满足要求，没有人为疏漏和笔误等。在软件和各类测试中要检查测试的充分性（覆盖性）和符合性。只有通过了评审，才能确认阶段工作完成，才允许进入下一阶段的工作。

e） 应严格实施软件配置管理，特别是软件状态更改的管理。提高软件可靠性的重点应是软件概要（结构）设计和详细设计，不要在编程的技巧上下太多功夫。要重视软件可靠性设计的验证（测试），不要凭“ 思维 ”去“ 优化 ”程序细节。

f） 要不断加强软件开发组织（队伍）的建设和培训，提高组织的软件成熟度等级（CMM）。

22.3 方法

22.3.1 软件可靠性需求分析方法

软件可靠性需求分析方法如下：

a） 软件可靠性需求应与硬件可靠性需求大体相当，不应随意提高软件的可靠性指标。

b） 软件需求格式说明应确保具有无歧义性、完整性、一致性、可验证性、可理解性、可追踪性和易使用性。对关键软件（或软件部件或功能）必须列出可能的不期望事件，分析导致这些不期望事件的可能原因，并提出相应的软件处理要求。

c） 对软件进行 FMEA、FTA，明确软件的关键部件、重要部件及软件的单点失效，将危害性大的部件作为软件可靠性工作的重点，一般与控制、故障检测、硬件输入输出、中断等有关的软件部件均属于关键、重要部件。

d） 高可靠性要求的软件部件设计首先应提高在不考虑冗余容错情况下单个软件的可靠性，然后再进行软件的冗余容错设计。必须考虑冗余版本或容错功能的相互独立性，同一需求下的不同版本之间不是统计独立的，因此冗余设计要有意识地实现异化，以避免类似的系统设计、结构设计、编程和测试用例的出现。同一版本软件的冗余，不仅不能应付相同的错误，而且还会增加软件结构的复杂性，而降低软件的可靠性。

22.3.2 软件可靠性设计

22.3.2.1 软件可靠性设计方法

a） 软件的体系结构、程序结构、数据结构、模块设计编程等应采用标准的、可靠的、简明的，尤其是已经过飞行试验考核的成熟技术。在此基础上可再采取加强措施，一般要求采用的新技术不要超过 1/3。

b） 软件设计应采用避错设计，要求最小复杂度、最小特权结构、设计层次清晰，要加强测试与验证等。

c） 对时间（机时）、速度、存储空间和信息等都要考虑留有 1/3 以上的余量，最终版本的实际余量可以降低。

d） 要提高软件受外部输入干扰和各种可能发生的硬件故障等影响的预防能力，一般用限（超）时处理以防止外部输入响应不及时到来的故障，用合法性判别剔除非法信号输入，用有效性判别或限幅排除超定义域的无效数据，用多途径（必要时硬件配合）和多次输入以避免因硬件永久或瞬时故障造成的错误，多次的间隔应大于最大可能干扰或不确定的持续时间，必要时还应防止错误操作（命令）的执行。

e） 必须意识到，任何提高软件可靠性的措施，均以增加系统复杂性和增加机时为代价，外部事件是小概率事件，双重或连续多次瞬时故障的概率更小，故尽管目前对软件失效率没有足够的定量数据可供参考，在提高软件可靠性的同时，必须同时考虑保持软件的简单性，简单即可靠。

f） 强实时系统中，中断或抢占式调度是有用的，但应控制中断嵌套层次，处理好中断源之间的冲突及中断响应不及时等问题。

22.3.2.2 监控定时器设计方法

监控定时器设计方法如下：

a） 必须提供监控定时器，以确保计算机不会发生机时超时或陷入死循环。

b） 监控定时器可以设置多个，但最终的、最可靠的应选用独立的时钟源、独立的硬件实现。监控定时器的定时参数应根据系统要求统筹考虑，一般对于周期性要求的，取周期的 1.3 倍~3 倍为宜，其清零时间一般为周期的 0.3~0.7 为宜，过大过小均不利对故障的及时检出和隔离。

c） 不同监控定时器应有不同的故障处理对策，即软件处理时不宜采用简单复位，要设计多个程序再启动入口，以尽可能保持系统输出状态的平稳或使系统进入安全状态。

d） 卫星的计算机软件长时间处于无法监控的自主运行状态，一般希望即使软件失效，系统也能保持某种安全状态。系统的安全状态应由系统方案决定，属于系统需求分析范畴。但软件需求一定要有安全状态，通常希望软件设计时考虑，当软件程序已无法自动恢复时，最终的监控定时器动作，能确保卫星的安全，并可进一步接受地面控制重新恢复正常工作。

e） 软件如已自主发现故障，一般不宜设计为进入死循环，等待监控定时器处理，而应立即自主转入出错处理程序入口。

22.3.2.3 冗余容错设计方法

冗余容错设计方法如下：

a） 为进一步提高软件可靠性，冗余设计是必须的，软件的冗余设计主要有多版本结构和恢复块两种方法。

b） 多版本程序设计是由多个实现相同功能的相异程序和一个管理（表决）程序组成。可采取多数表决或一票否决的对策，要考虑多版本程序的机时增加和各版本之间的相异性以避免共同故障。

c） 恢复块由一个基本块、若干个替换块（可以是降级的）和接受测试程序组成。软件需求规格说明中应对每个恢复块单独做定义和说明。运行基本块后要进行接收测试，通过则输出，否则依此调用替换块并接受测试，若全未通过接受测试，则按出错处理。

d） 信息冗余包括接受信息、保存信息（含主要数据和程序）的多个备份，一般选用双备份或三备份即可，使用前进行比对，相同或三取二表决决定。信息冗余一般还需要硬件支持。

22.3.3 软件编程方法

软件编程方法如下：

a） 程序区与数据区要分开设置，区域之间的隔离区以及内存的空白区域要用“ 陷阱 ”指令或用若干条 NOP（总长度要大于等于最长指令的长度）指令加一条跳转指令填充。将指令控制转向出错处理程序入口，不用的中断矢量区也应做类似处理。不得用随机数，也不推荐用暂停、等待等指令。

b） 重要状态信息之间应保持一定码距，以避免因一位或多位差错而引起系统错误。尤其不得使用 1 位“ 0 ”或“ 1 ”，不得用全“ 0 ”或“ 1 ”（尤其是从外部输入的信息）来判断。

c） 运行程序中不得包含不使用的可执行代码或不引用的变量。对不同阶段的多余程序（如监控程序等）应慎重处理，严防程序长期落入该程序段。

d） 应采用结构化编码方法进行代码编制。在进行软件单元编码时，必须构造下列特性：完整性、功能单一、入口/出口单一、转移有条件、防错处理完备、变量值域检查、循环需终止、标号和名字易辩识、避免全局变量和共享变量、模块规模不宜大等。

22.4 步骤

软件研制步骤如图34所示。

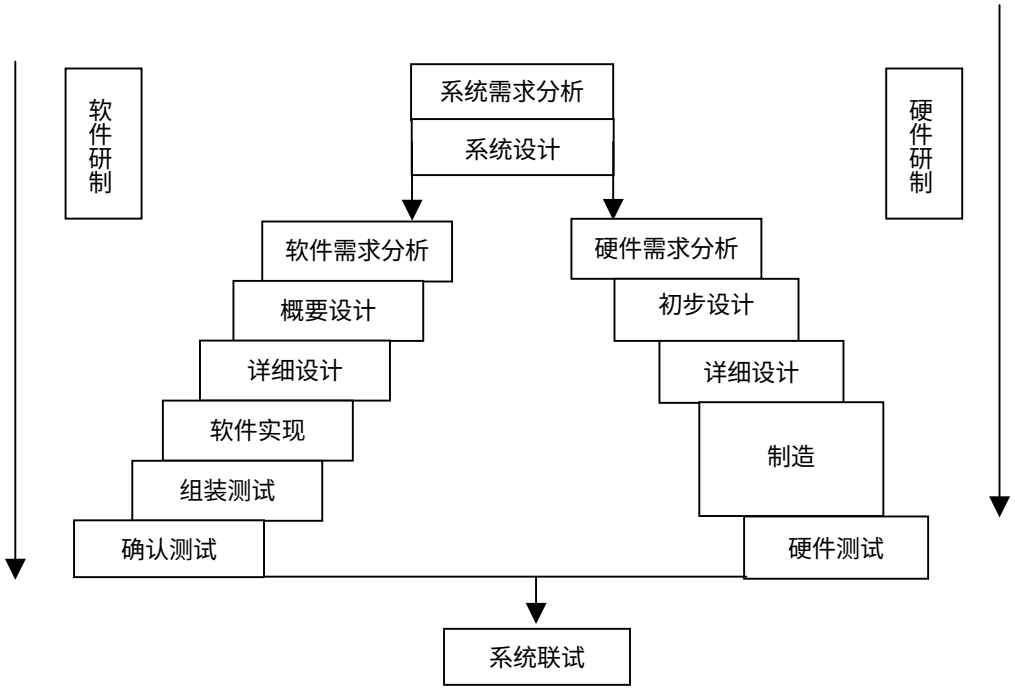


图34　系统研制流程与软件研制程序

软件研制应从从软件需求开始，到软件确认测试终止。软件是作为整个系统的一部分实现的，尤其是在嵌入式系统中，如卫星飞行软件。软件的需求分析与整个系统的需求分析、系统设计有关，软件设计人员应参加系统需求分析、系统设计，从中获取必要的信息。软件确认测试完成后，还应把软件集成到整个系统中。

22.4.1　系统需求分析

22.4.1.1　系统任务

卫星型号系统是一个庞大而复杂的系统工程，由若干个分系统、每个分系统又由若干个子系统、设备、部件或单元等组成，其计算机分系统或其它分系统中的计算机子系统（部件）又由硬件和软件组成。系统分析是研究确定系统中各组成部分的相互关系和作用，主要应由产品设计人员进行，但同时软件设计人员应参与其中，以了解系统任务需求。

22.4.1.2　软件任务书

通过系统分析所获得的系统需求应以任务书形式确定下来。

软件任务书应由软件交办方在进行系统需求分析和任务分解工作之后组织编写。承制方应参加任务的分解和任务书的讨论，协助交办方的工作。

软件任务书是待研制软件的开发、测试和验收的依据，其主要内容应包括：

a）　任务书的主要内容组成；

b）　软件的功能和性能，每个配置项的输入、处理和输出；

c）　软件的外部环境，如硬件接口和运行环境等；

d）　软件的外部信息交换和协议；

e）　软件设计的限制和约束，如语言、工具、方法等；

f） 可靠性要求；

g） 验收、交付方式，如验收环境和方式，交付后的维护等；

h） 时间进度和经费等。

22.4.1.3 系统需求评审

应对系统需求进行评审，包括：

a） 系统需求应满足：可跟踪性，与型号系统所分配功能的一致性，可测试性，设计、操作和维护的可行性。

b） 系统设计应满足：技术途径可行，软件、硬件、人工操作功能分配的折中考虑恰当，可跟踪性，与系统需求的一致性，设计和所用标准恰当，以及操作和维护的可行性。

c） 软件研制任务书应对软件的所有主要功能、性能技术指标进行定义，与系统需求和系统设计一致。

d） 软件的接口说明完整、一致，满足可测试性。

e） 软件安全性分析和关键性分级正确。软件独立测试工作有安排。

f） 软件验收和交付内容全面、明确、可检查。

g） 软件承办方最终向交办方交付的内容清单以及后续服务必须在软件研制任务书上明确，并经双方确认。

h） 进度和经费安排合理。

i） 系统需求阶段还可能需要形成：可行性研究报告、系统需求规格说明、系统设计说明、初步项目开发计划等文档。

22.4.2 软件需求分析

应获得的软件需求包括：功能需求、性能需求、接口需求、操作需求、资源需求、验证需求、验收测试需求、文档需求、保密性需求、可移植性需求、可靠性需求、维护性需求、安全性需求等。

每项软件需求的属性应包括：标识、优先级、稳定性、来源、清晰性、验证性等。

应制定项目开发计划、方法和工具等以及编制《软件需求规格说明》。

22.4.3 软件设计

22.4.3.1 概要设计

软件的概要设计工作应满足以下技术要求：

a） 设计完整：软件概要设计说明应完整，覆盖软件需求规格说明中描述的所有软件需求。

b） 接口清晰：必须定义软件的主要部件和它们之间的接口，必须定义和引用所有外部接口。

c） 详细一致：概要设计说明必须详细，各部件之间的详细程度应一致，以便制定详细实现计划。

d） 弱耦合。

e） 高内聚。

f） 作用范围在控制范围之内：软件的各个模块中有许多判定，这些判定决定了某些操作是否要执行。一个判定的作用范围（影响范围）是指所有受这个判定影响的模块。只要模块中含有一些依赖于这个判定的操作，那么该模块就在这个判定的作用范围之中。控制范围属结构特点，而与模块的功能无关。

g） 控制软件规模和扇入扇出数：设计员应估计每个模块的规模，检查它是否因包含了多个功能而使规模过大。模块的扇出（Fan－Out）表示一个模块对它的直属下级模块的控制范围，扇出数指其

直属的下级模块的个数。模块越多，内聚度就可能越低。模块的扇入（Fan－In）表示一个模块与其直接上级模块的关系，扇入数指其直接上级模块的个数。应尽可能地加大模块的扇入数。

22.4.3.2 详细设计

从顶层开始，逐级将概要设计产生的软件体系结构中的每一个软件部件分解细化，将设计进行到低层，直至形成若干个软件单元（可编程模块）。

软件的详细设计工作应满足以下技术要求：

a） 按结构化程序设计原则进行设计；

b） 采用规定的工具来描述软件单元；

c） 符合可靠性设计准则；

d） 详细地规定各单元间的接口；

e） 对每个单元确定所有的输入、处理、输出；

f） 对符号命名确定统一的规则并按规定使用；

g） 只使用基本控制结构来描述各软件单元的过程；

h） 详细设计与软件需求可追踪；

i） 详细设计与概要设计一致；

j） 在各部件和单元的需求之间内部一致；

k） 单元测试的要求和方法正确。

22.4.4 软件实现

应采用结构化编码方法进行代码编制。在进行软件单元编码时，必须构造下列特性：完整性、功能单一、入口/出口单一、转移有条件、防错处理完备、变量值域检查、循环需终止、标号和名字易辨识、避免全局变量和共享变量、模块规模不宜大等。

22.4.5 软件测试

按照QJ 3027—1998的要求对卫星用软件进行测试。

中华人民共和国航天行业标准

卫星可靠性设计指南

QJ 2172A－2005

*

中国航天标准化研究所出版

北京西城区月坛北小街 2 号

邮政编码：100830

北京航标印务中心印刷

中国航天标准化研究所发行

*

2005 年 7 月出版

定价：70.00 元