



系统可靠性设计



可靠性工程师研讨班
第三期



可靠性工程实施内容

可靠性管理

组织机构建立与职责确定
目标规划
制定流程规范，监督控制
培训教育
信息收集与交换
平台建设与框架技术建立
基础技术与工程技术研究
用户服务与保障
技术支持
故障审查与组织
建立故障报告纠正措施系统
(FRACAS)

可靠性设计

可靠性定性定量要求
建立可靠性模型
制定可靠性设计准则
系统可靠性设计
降额设计、余度设计
动态设计、容差设计
潜在通路分析 (SCA)
热设计
静电防护设计
软件可靠性设计
FMEA、FTA

可靠性试验

高加速应力筛选试验
(HASS)
可靠性增长试验、鉴定验收试验
气候环境保护设计
高加速寿命试验



可靠性特征量介绍

可用度 (A-availability) :

产品在一未知时刻，需要执行任务时，处于可工作或可使用状态的概率。

平均无故障间隔时间 (MTBF-mean time between failure) :

指相邻失效间隔工作时间的平均值。

平均失效前时间(MTTF-mean time to failure) :

表示观察到下次失效的期望的时间。

平均拆卸间隔时间 (MTBR-mean time between removals)

系统寿命单位总数与从该系统上拆下的产品总次数比。



可靠性特征量介绍

平均修复时间 (MTTR-mean time to repair) :

是在规定的时间内，修复性维修所造成的累积工作时间除以在同一时间内所完成的修复维修活动总数得到的结果。

可靠度 $R(t)$: 在规定的条件下，规定的时间内，完成规定功能的概率。

基本可靠度 : 是指产品在规定的条件下无故障的概率。它要考虑所有的寿命历程和所有的故障。它反映对产品约束条件和维修资源的要求。

任务可靠度 : 是指产品在规定的任务剖面中完成规定功能的概率。



可靠性特征量介绍

失效率 (λ) : 在规定的条件下和规定的时间内, 产品失效总数与寿命总数之比。

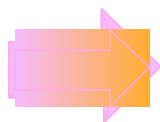
故障检测率 : 被测试项目在规定期间内发生的所有故障, 在规定的条件下用规定的方法能够正确检测出的百分数。

故障隔离率 : 被测项目在规定期间内已被检出的所有故障, 在规定的条件下用规定方法能够隔离到规定个数可更换单元以内的百分数。

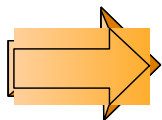
虚警率 : 在规定期间内发生的虚警数与故障指示总次数之比称为虚警率。



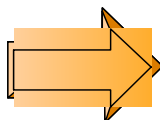
目录



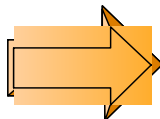
系统可靠性分析的步骤



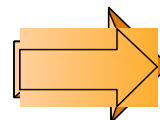
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



系统可靠性模型分析举例

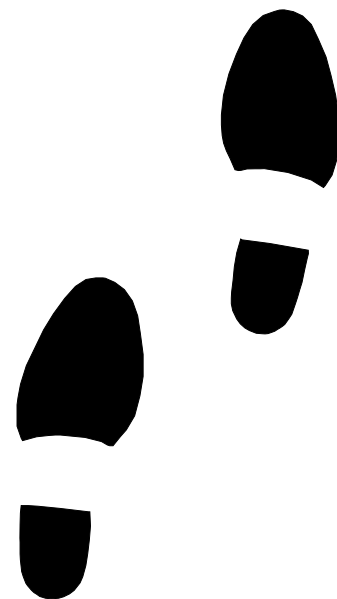


系统可靠性论证分析举例



一、系统可靠性分析的步骤

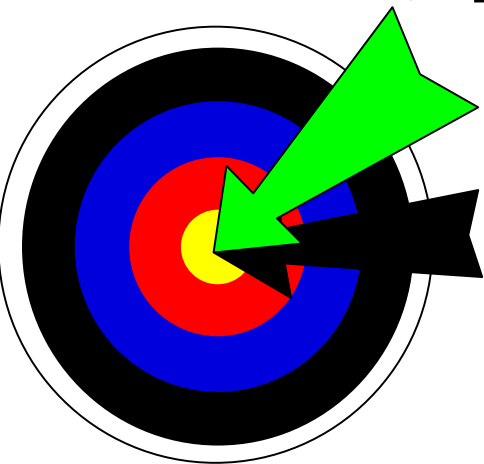
- 1、确定分析目的
- 2、定义系统故障
- 3、定义RAM目标
- 4、结构分析与分解
- 5、结构建模
- 6、确定模型参数
- 7、模型求解和RAM指标计算
- 8、模型参数灵敏度分析
- 9、分析结论





1. 确定分析的目的

- 1. 将规定的系统可靠性指标与目标标准进行比较
- 2. 检查系统结构以确定可靠性薄弱环节
- 3. 优化系统结构
- 4. 优化修理和维护机制





2. 定义系统故障

- 1、常规定义

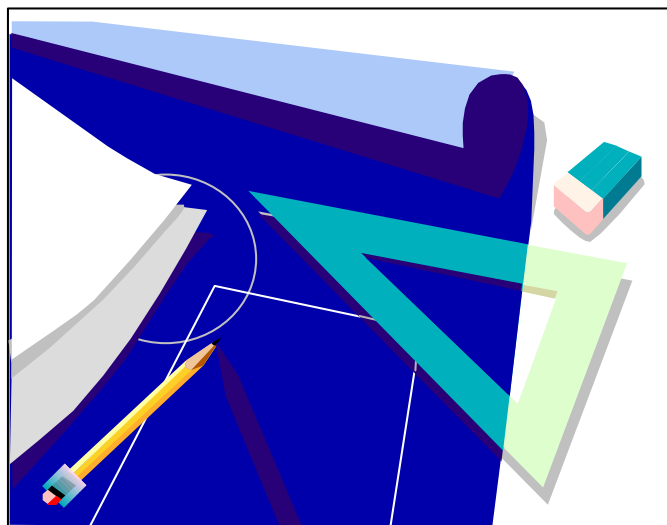
系统故障是指任何将导致系统不可接受的运行状态的单元故障

- 2、系统故障定义中的困难

局部故障、瞬时故障等

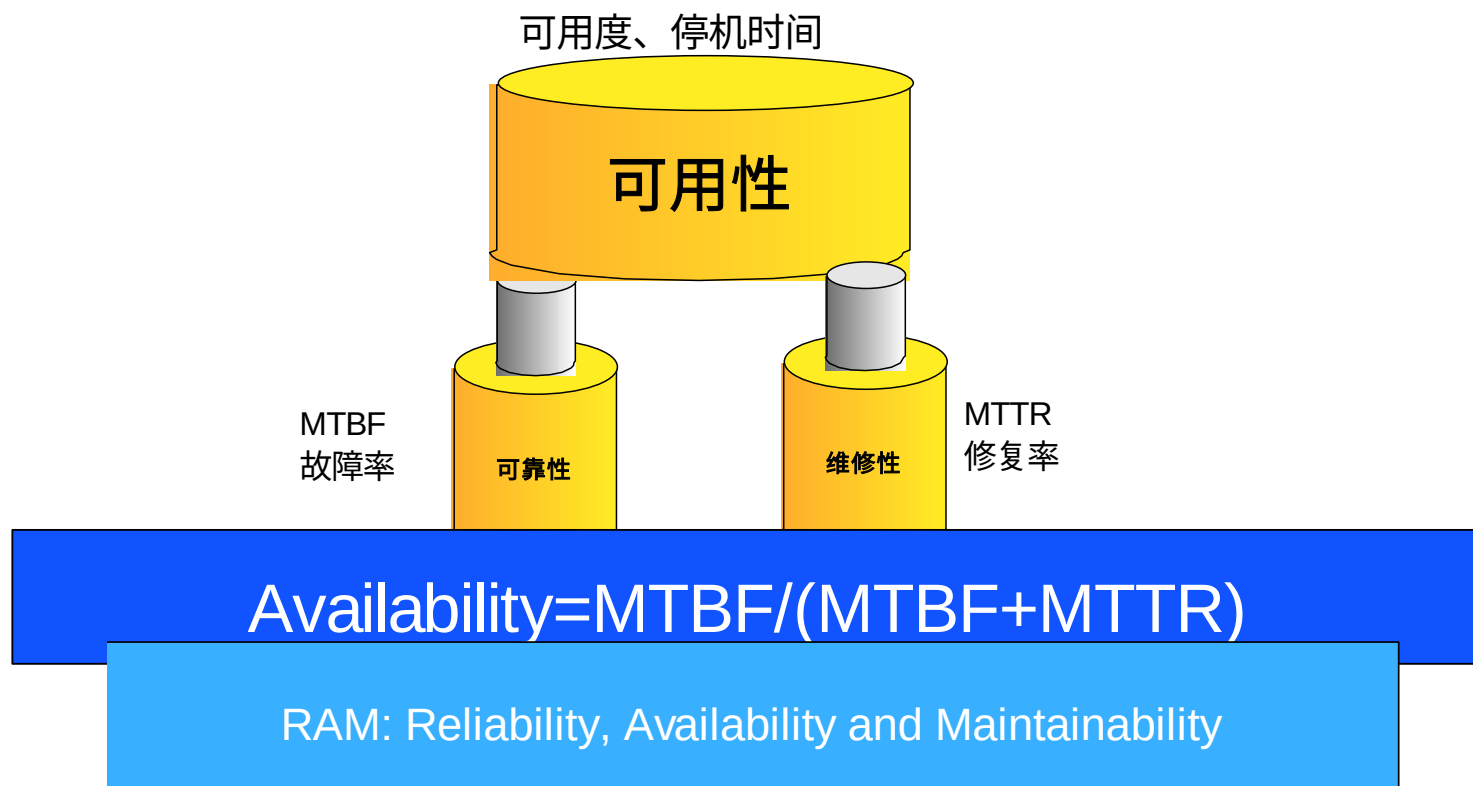
- 3、通常的假设

0-1特性





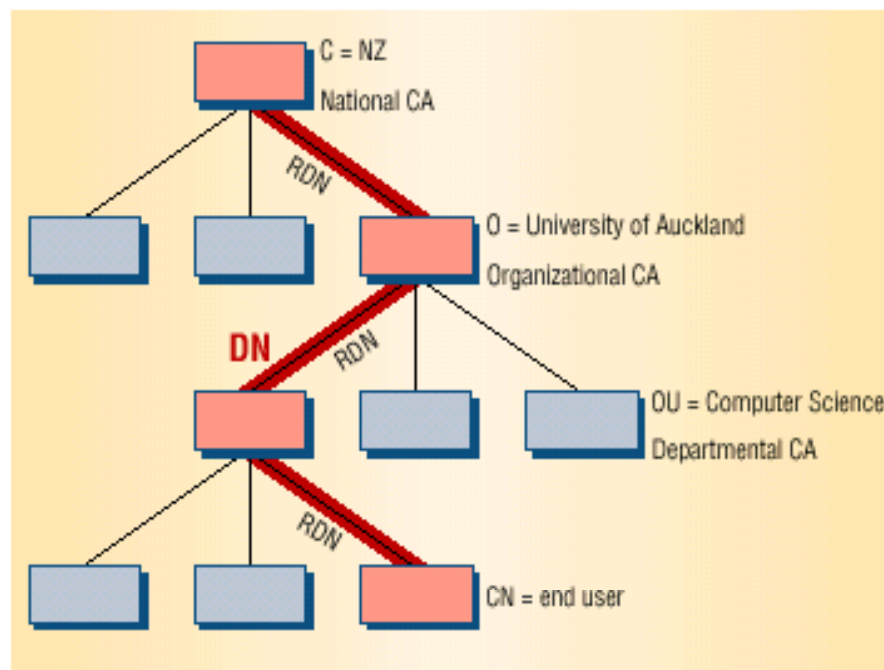
3. 定义RAM目标





4. 结构分析与分解

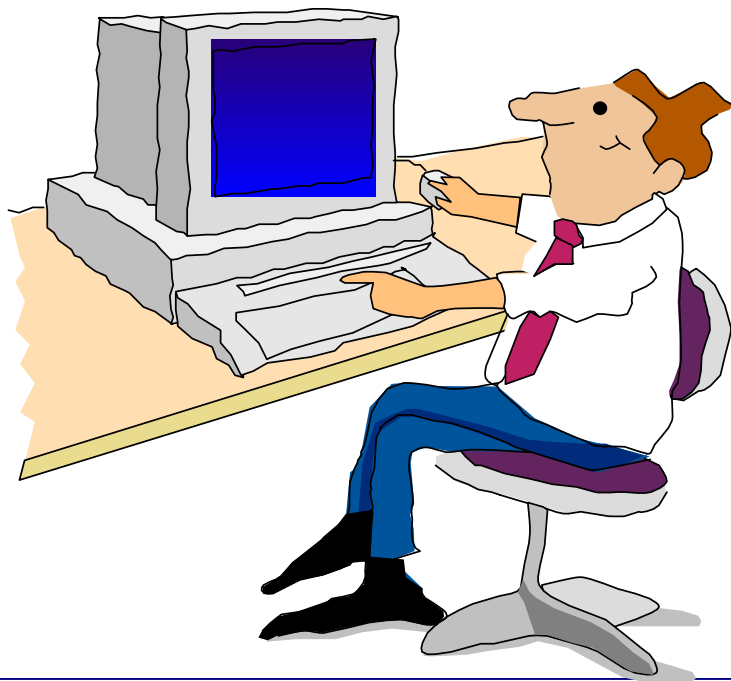
对于大型复杂系统，为了便于分析，可以首先将系统分解为各种独立的单元或工作模式，然后借助一些可靠性分析技术，如FMEA对各单元和工作模式故障造成的影响进行分析





5. 结构建模

结构建模包括创建描述系统的可靠性模型。诸如不同硬件单元间的兼容性、维护和运行特性以及故障检测和隔离特性，必须全部加以考虑。



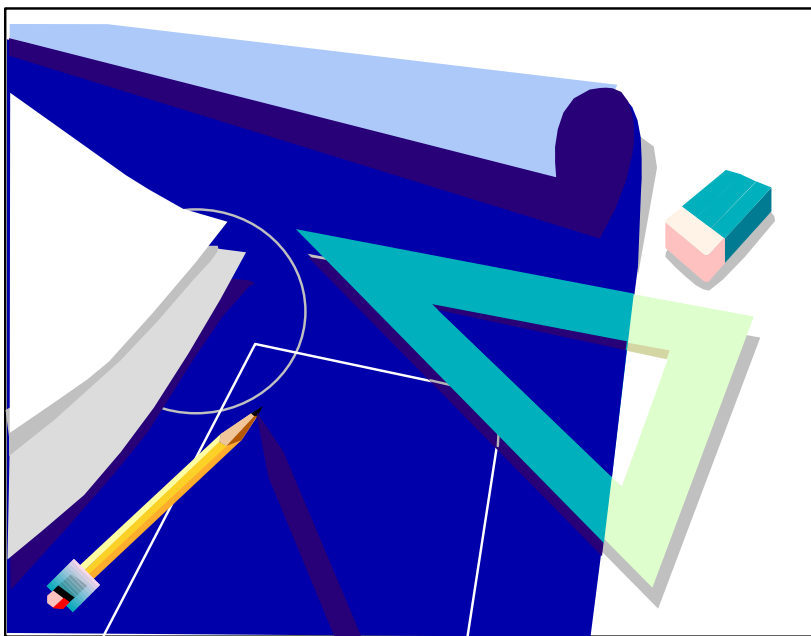


6. 确定模型参数

1. 单元故障参数

2. 修理和维护参数

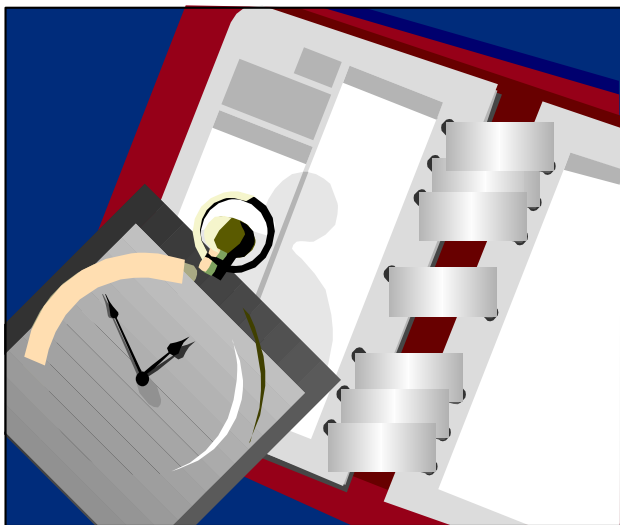
3. 系统管理参数





6.1 单元故障参数

1. 故障时间分布—指数分布
2. 运行条件—设备运行的典型的物理环境
3. 环境描述—设备运行的物理环境的适当的环境故障率修正因子





6.2 修理和维护参数

(1) 修理体制

- A. 维护人员一分配给系统的维护人员数量
- B. 修理优先权—当维护人员不够时的修理顺序。

(2) 修理分布信息

- A. 如果系统每天24小时都要运行，那么每个单元的修理时间将服从的分布。
- B. 无人值守的—如果系统大多数时间是不工作的，下列分布：
 - a. 派遣和路途时间
 - b. 现场修理时间

(3) 维护信息

- A. 时序—周期性维护的时间和持续时间
- B. 影响—周期性维护队系统运行的影响



6.3 系统管理参数

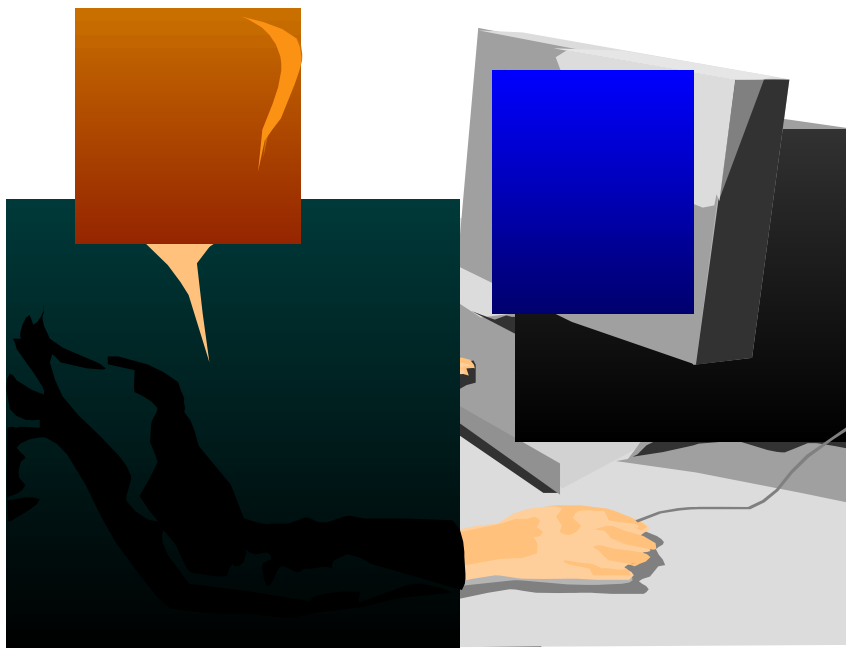
1. 故障检测 — 单元故障无法被检测到的频率，以及直到错误得到修复的时间。
2. 故障覆盖 — 系统无法有效地从故障的主用单元切换到正常工作的备用单元的频率，以及直到错误得到修复的时间。
3. 故障告警 — 单元故障无法及时报告给维护人员造成的延迟时间。





7. 模型求解和RAM指标计算

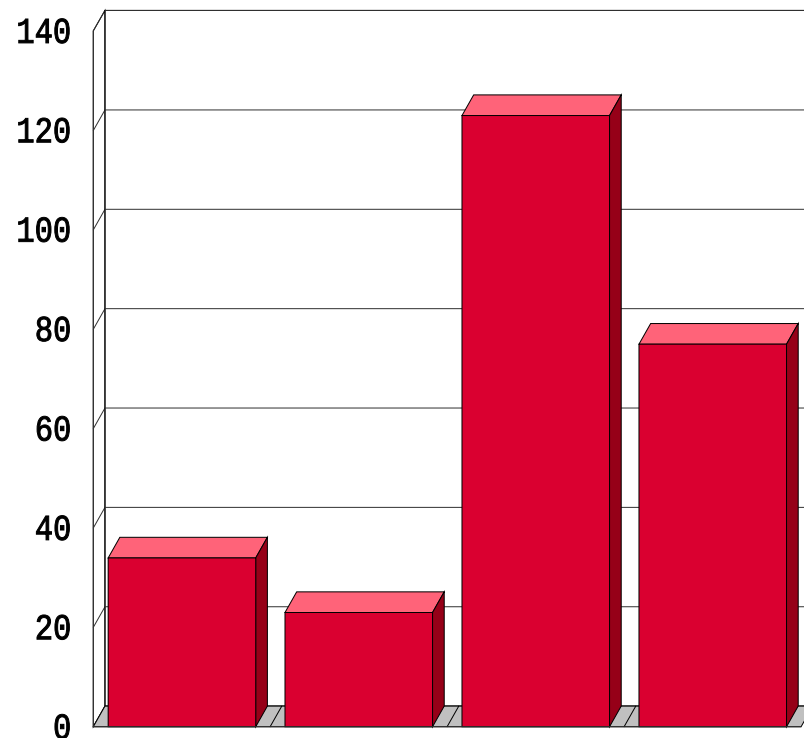
根据建立的系统可靠性模型，采用适当的求解方法，得到
系统可靠性/ 可用性参数





8. 模型参数灵敏度分析

可靠性分析的目的之一是优化系统结构。通常需要确定参数变化对期望的RAM指标的影响，然后找到优化的指标值。另外，很多情况下，模型参数值的正确选取上存在很多不确定性。此时，所选取的参数值对最终可靠性指标计算结果将产生很大影响。灵敏度分析就是一种评估参数变化对期望的RAM指标的影响的方法。这一方法特别适用于支持数据缺乏的参数（例如缺乏倒换率和检测率的支持数据，通常可以采用历史数据确定数值的范围，然后在这个范围内通过判断估计适当的取值。此时，灵敏度分析将可以确定判断对最终RAM指标的影响。





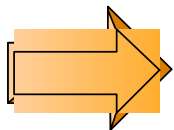
9. 分析结论



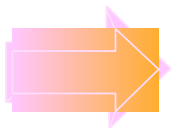
需要描述建模的主要结果。特别是当目标建立后，系统满足这些这些目标的能力。适当的RAM指标必须与这些目标值进行比较，并给出系统满足这些目标值的能力的结论。



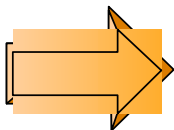
目录



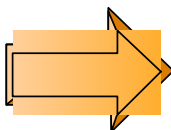
系统可靠性分析的步骤



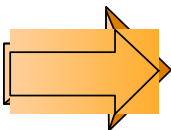
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



系统可靠性模型分析举例



系统可靠性论证分析举例



二、可靠性建模技术

- 1.可靠性方框图(RBD-Reliability Block Diagram)
- 2.状态转移图(Markov模型)
- 3.故障树模型(FT-Fault Tree)
- 4.随机队列(Petri-Net)

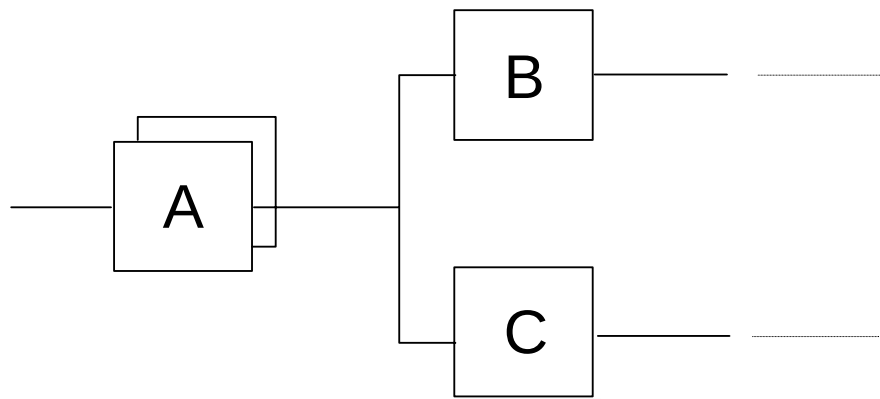


可靠性框图(RBD)



1. 系统功能框图

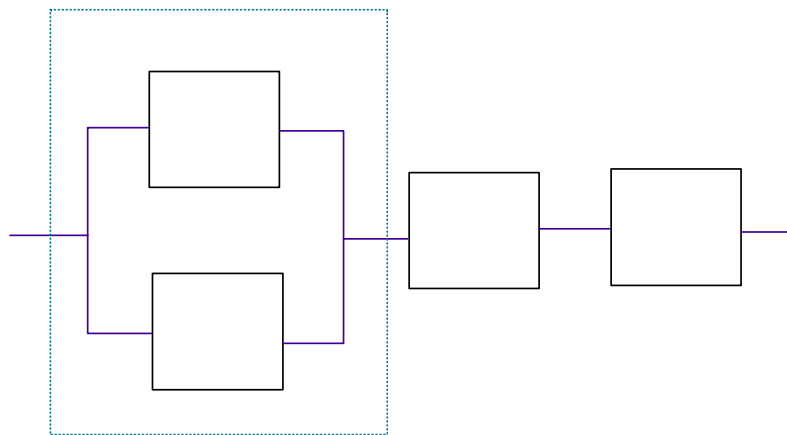
功能框图是最简单的一种图形描述方法。它描述了硬件单元间的电子物理连接关系，而不是SRMA要求的逻辑关系。它描述了数据或控制在系统中的流向，描述了各种单元彼此间是如何相互关联的。例如，下图给出了一个通讯系统简化的功能框图示例。





2. 可靠性方框图(RBDs)

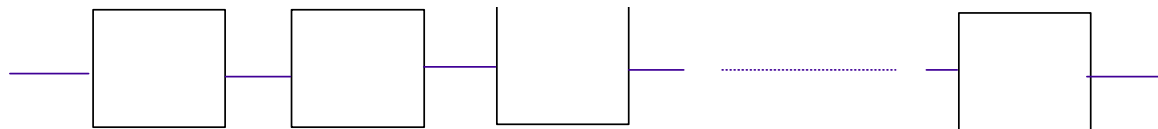
可靠性方框图(RBDs)通常用于表示系统的可靠性结构。RBDs是一种简单地表示所有可能的功能结构以及故障的单元对系统功能影响的图形方法。可靠性框图通常由表示基本的系统组成单元的方框组成。方框图通常都有一个起点和一个终点。其中至少要有一条从起点到终点的路径是通的，且没有通过一个故障的单元，系统才是正常的。以下是最常见的的基本结构(串、并联)RBD示例。





2.1 RBD-串联模型

组成系统的所有单元中任一单元故障就会导致整个系统故障的系统称串联系统。



系统可靠
度：

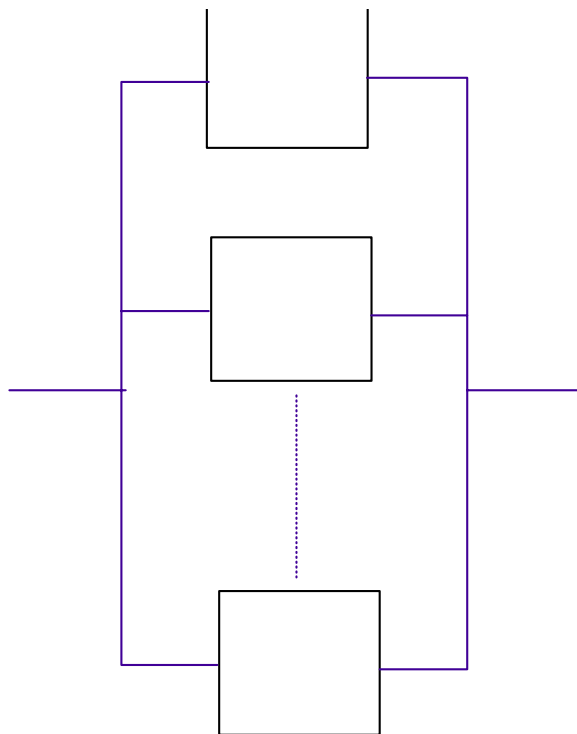
$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \cdot \dots \cdot R_n(t) = \prod_{i=1}^n R_i(t)$$

系统故障
率：

$$\lambda = \lambda_1 + \lambda_2 + \dots + \lambda_n = \frac{1}{\theta}$$



2.2 RBD-并联模型



系统的不可靠度：

$$Q_S = Q_1 \cdot Q_2 \cdot \dots \cdot Q_n = \prod_{i=1}^n Q_i$$

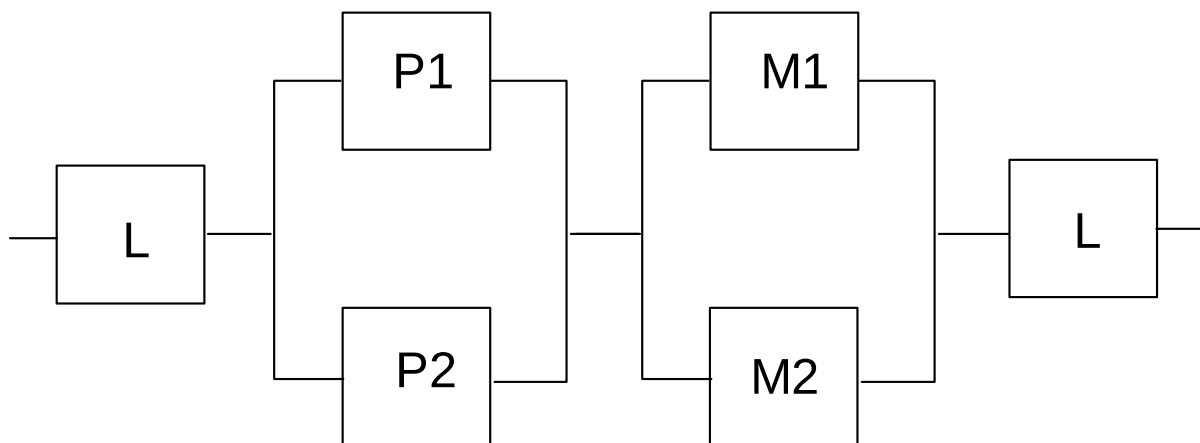
系统的MTBF：

$$MTBF_S = \frac{1}{\lambda} + \frac{1}{2\lambda} + \dots + \frac{1}{n\lambda}$$



2.2 可靠性方框图(RBD)(续)

复杂系统的RBD示例：





2.3 RBD-r/n模型

组成系统的n个单元中，不故障的单元数不少于r(r为介于1和n之间的某个数)，系统就不会故障，这样的系统称r/n系统。

系统的可靠度：

$$R_S(t) = R^n(t) + C_n^1 R^{n-1}(t) \cdot [1 - R(t)] + C_n^2 R^{n-2}(t) \cdot [1 - R(t)]^2 + \cdots + C_n^{n-r} R^r(t) \cdot [1 - R(t)]^{n-r}$$

系统的MTBF：

$$MTBF_S = \frac{1}{n\lambda} + \frac{1}{(n-1)\lambda} + \frac{1}{(n-2)\lambda} + \cdots + \frac{1}{r\lambda}$$



2.4 RBD-多数表决模型

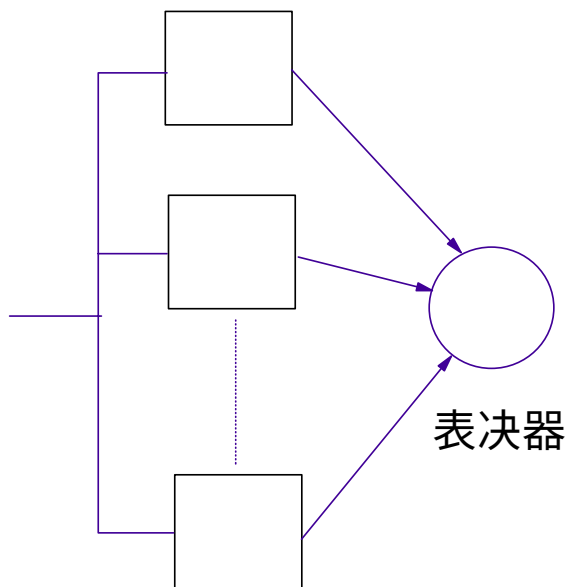
一个系统将三个以上(必须是奇数)并联单元的输出进行比较,把多数单元出现相同的输出作为系统的输出,这样的系统称多数表决系统。

优点：

- (1) 可以用来显示有缺陷的单元；
- (2) 对于短期任务时间(一般工作时间在单个单元的MTBF之前),可靠度有显著提高。

缺点：

- (1) 要求表决器的可靠度大大高于单元可靠度；
- (2) 若任务时间较长(大于单个单元的MTBF),其可靠度反而低于单个单元的可靠度。





状态转移图(MARKOV)

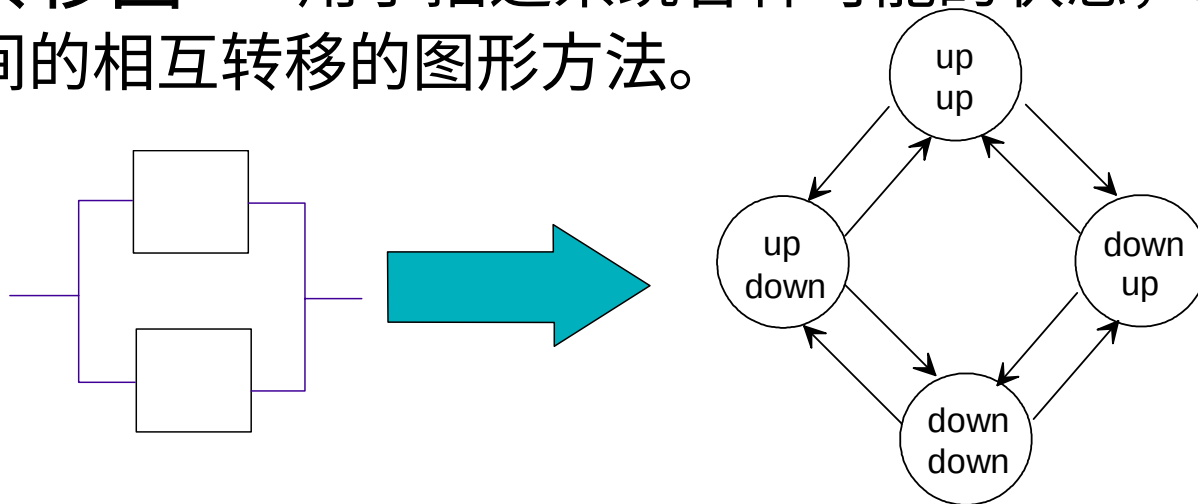


3. 状态转移图

“状态”：系统可能出现的一种工作模式。包括除正常、故障外的功能降级模式。

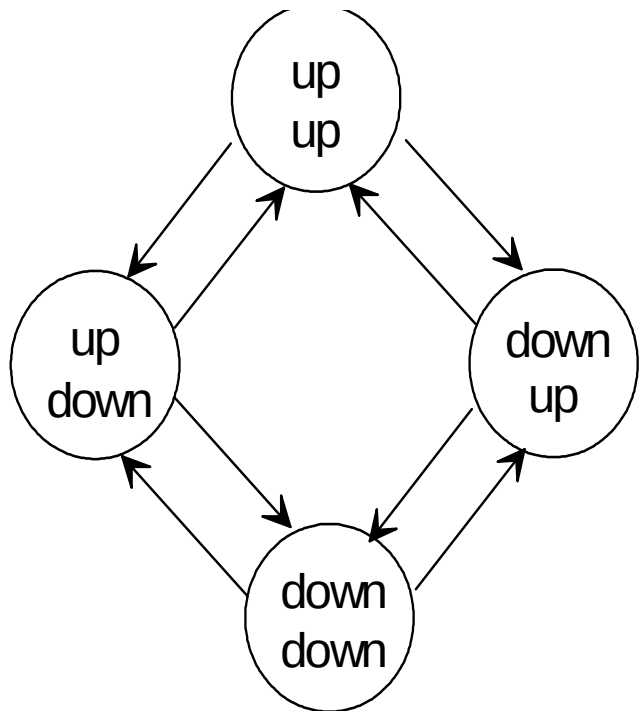
“状态空间(state space)”：系统一系列的状态组合

“状态转移图”：用于描述系统各种可能的状态，以及这些状态间的相互转移的图形方法。

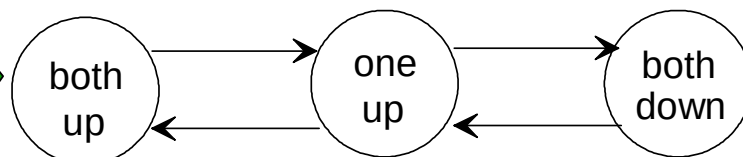
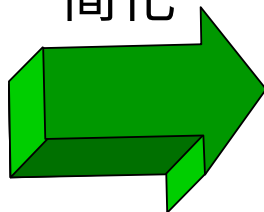




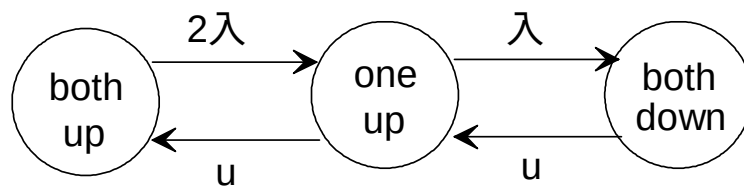
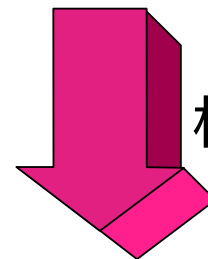
3.1 状态转移图的标注与简化



简化



标注





3.2 Markov建模技术理论

一、Markov模型的基本概念

Markov模型是描述复杂系统可用性的一种数学模型，它由两个基本的要素组成：

状态state

两态与多态问题

状态转移transition

由于故障从正常状态变为故障状态

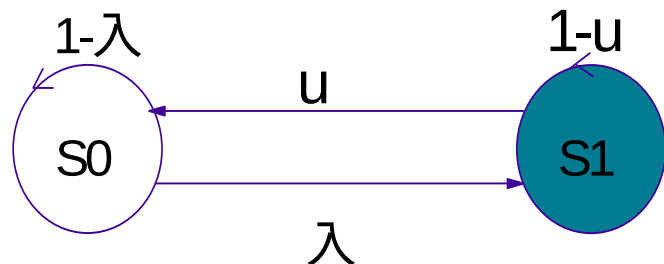
由于修理从故障状态恢复到正常状态





3.2.1 单个单元的Markov模型

该单元的可用度即为处于S₀状态的概率：



$$A(t) = P_0(t)$$

$$P_0(t) = e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu} \left[1 - e^{-(\lambda+\mu)t} \right]$$

其中：

S₀：单元正常工作

S₁：单元故障，正在修理

λ：故障率

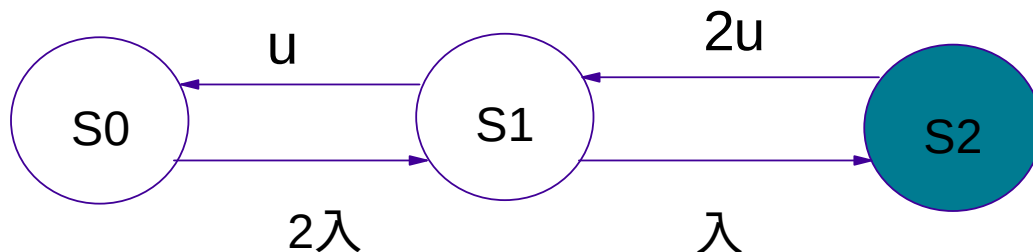
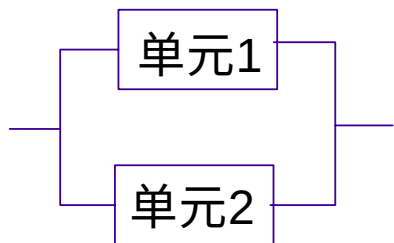
μ：修复率

单元的稳态可用度(t趋于无穷大)：

$$A_s = \frac{\mu}{\lambda + \mu} = \frac{1}{1 + \frac{\lambda}{\mu}}$$



3.2.2 两并联单元的Markov模型



其中：

S0：两个单元都正常工作，系统正常工作

S1：其中一个单元故障，系统正常工作

S2：两个单元都故障，系统故障

入：故障率

u：修复率



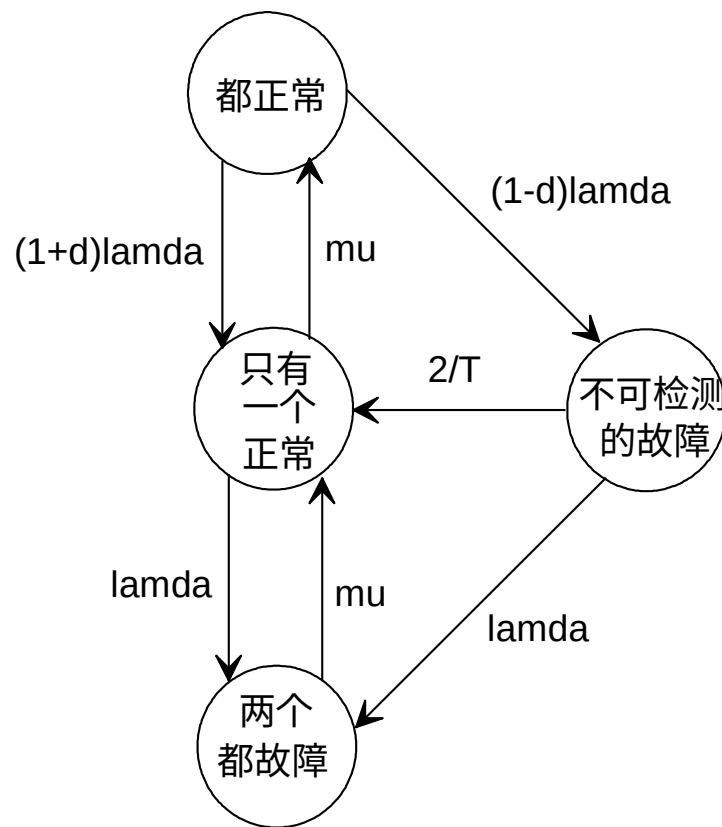
马尔可夫模型举例(一)

1. 考虑故障检测的马尔可夫模型

d : 故障检测率

T : 系统执行例行诊断的时间间隔

隔





马尔可夫模型举例(二)

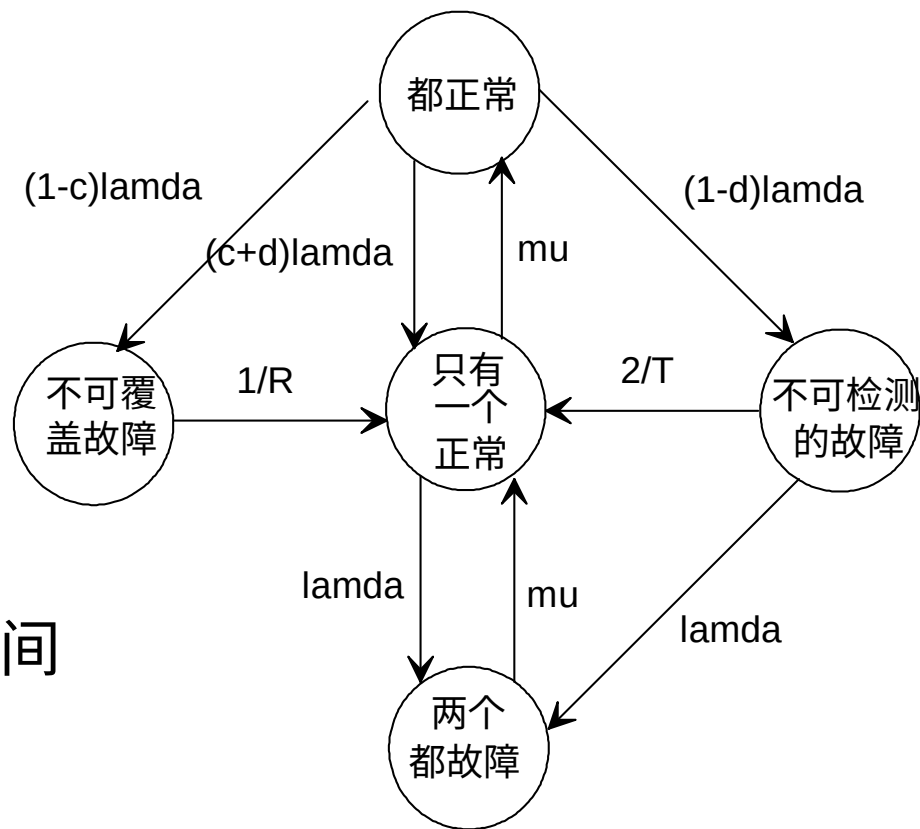
2. 考虑故障检测和故障倒换

的马尔可夫模型
d：故障检测率

c：冗余结构倒换成功率

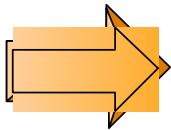
T：系统执行例行诊断的时间间隔

隔

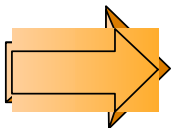




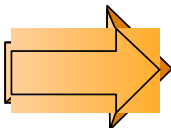
目录



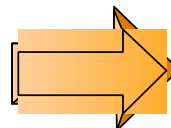
系统可靠性分析的步骤



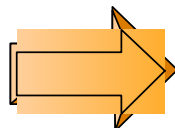
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



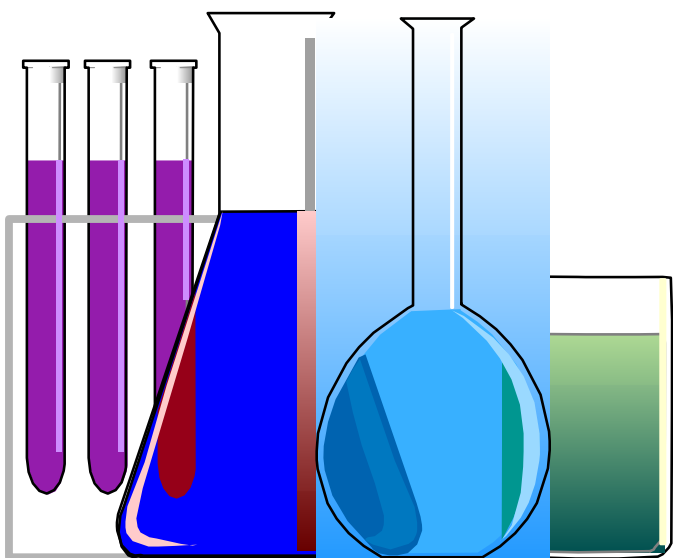
系统可靠性模型分析举例



系统可靠性论证分析举例



三、系统可靠性建模中考虑的要素

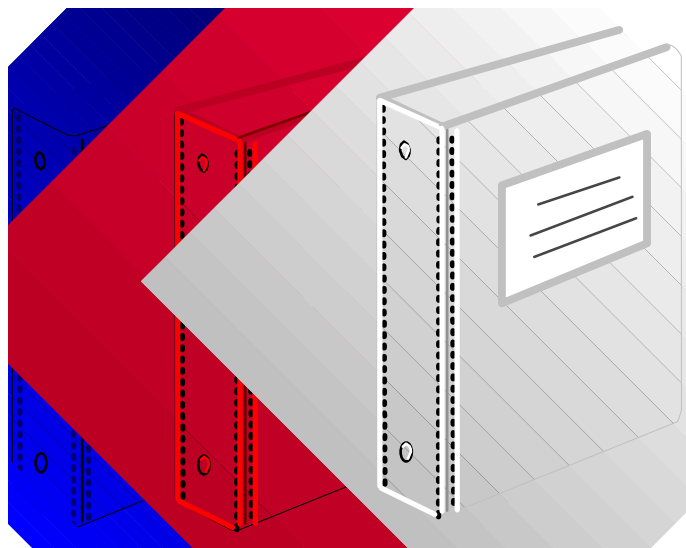


1. 故障率预计
2. 故障检测
3. 故障检测频率
4. 故障隔离和恢复
5. 故障倒换
6. 维护机制
7. 维修过程
8. 计划性维修活动



3.1 故障率预计

- MIL-HDBK-217
- BELLCORE TR 332(SR 332)
- GJB 299B





3.2 故障检测

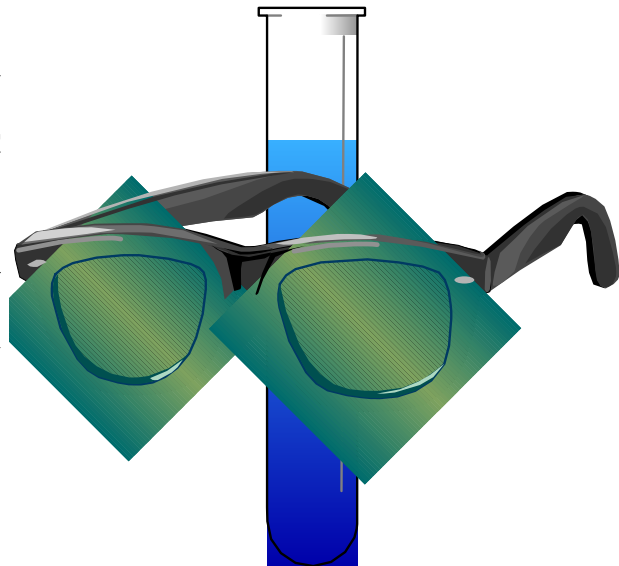
系统故障检测、隔离和恢复的能力是系统可靠性的一个重要方面。理想情况下，系统应能够立即检测到系统中的任何故障(硬件或软件)并启动恢复过程。常见的故障检测方法包括：

1. 输出比较检测。
2. 纠错码(ECC-Error Correcting Code)检测”
3. 自动诊断程序
4. 人工例行检测



3.3 故障检测频率

故障检测频率是系统检测机制的一个重要特性，因此必须在可靠性模型加以认真考虑。上面介绍的比较、奇偶和错误纠正码这些方法都是连续检测的方法，且通常从故障发生到被检测到之间不会存在延迟。然而，自动或人工诊断或检查则不是连续的，且并不是所有的故障都有必要立即检测到。这种“检测延迟”在工作在主备用方式的冗余结构中通常表现在备用单元。备用单元的某些故障直到常规检查时才被发现，而当主用单元故障时就会导致更加严重的后果。





3.4 故障隔离与恢复

故障隔离和恢复是指系统能够确认并更换单元，使之对服务影响最小的能力。

常见的故障隔离和恢复方法包括：

自动重新配置：系统能够自动使故障的硬件单元从服务中脱离，并将其功能转移到另一个单元的能力。这种方法通常用于那些从主用单元切换到备用单元，而对服务影响很小或没影响的冗余结构。

纠错码允许系统在一个或多个bit错误的情况下继续运行。这一点必须在可靠性模型中考虑。



3.5 故障倒换

如果主用单元故障的恢复机制中包括切换到备用单元，通常无法正常切换是一个小概率事件。无法正常切换的结果就是系统故障。正常切换的概率称为故障倒换率。可靠性模型中应考虑这个因素。一些系统允许通过远端控制来实现这种故障恢复。这样就比通常的人员到达和修理的过程时间要短得多。





3.6 维护体制

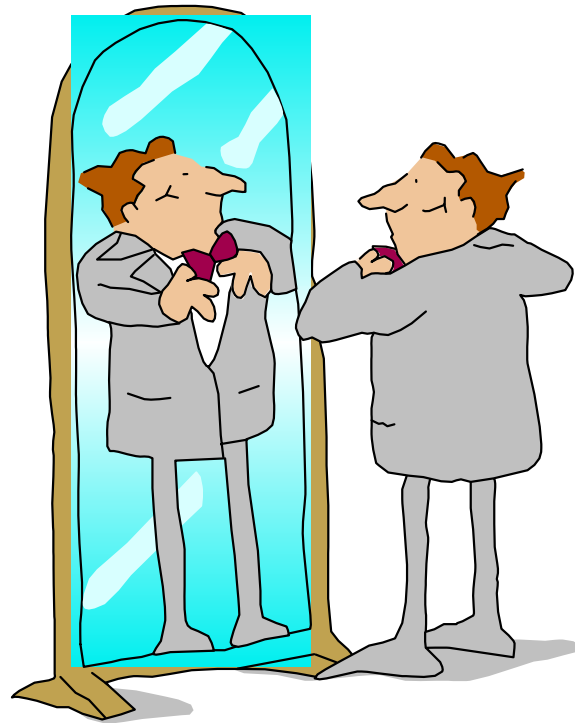
系统一个重要的方面是提示维护人员故障发生以便于定位和更换的能力。那些告警不够充分，导致不能产生立即提示的单元都应在可靠性模型中体现。由维护人员恢复故障的机制(如周期性测试或维护)也应在模型中考虑。应提供维护人员检测的时间估计以便在模型中考虑。





3.7 维修过程

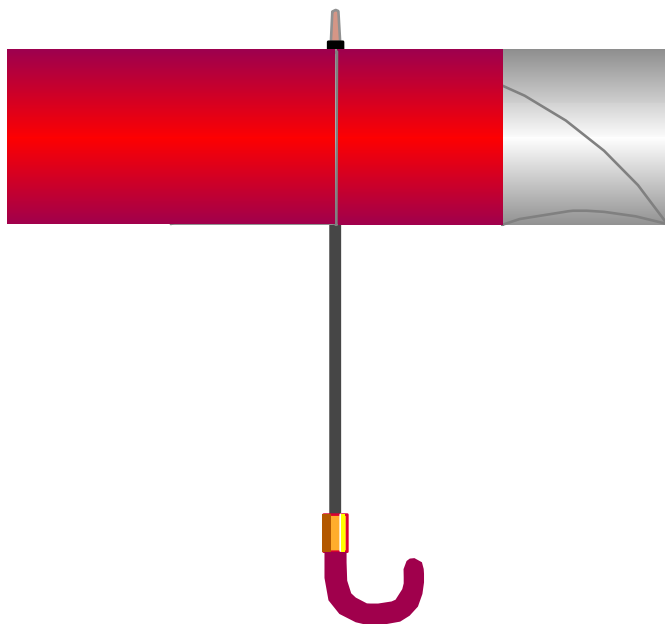
- ❑ 有人值守与无人值守
- ❑ 现场维护与远程恢复
- ❑ 维护人员数量与 vs. 故障数量
- ❑ 维修过程错误导致的系统故障





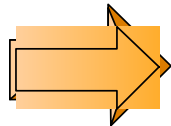
3.8 计划性维护活动

应对计划性维护硬件和软件活动进行评估，如周期性诊断和一般的升级。

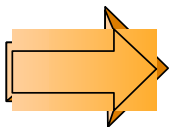




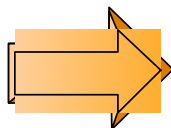
目录



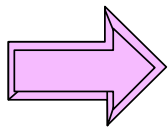
系统可靠性分析的步骤



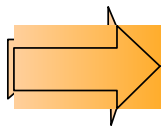
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



系统可靠性模型分析举例



系统可靠性论证分析举例



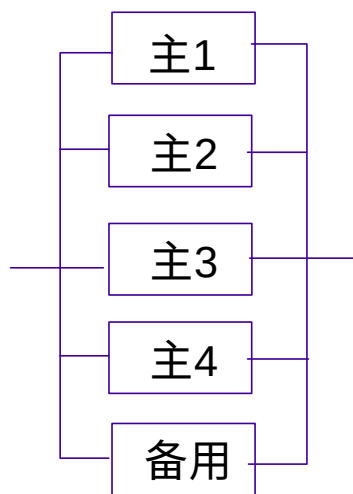
系统可靠性分析实例(一)

利用马尔可夫模型对电源冗余方案进行论证

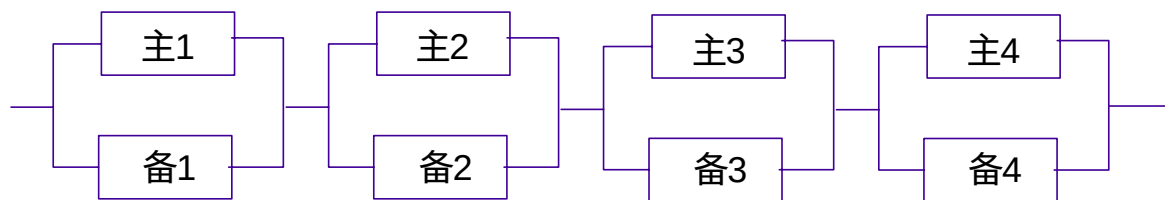
1. 问题的提出

在某通讯系统中，为保证电源的可靠性，拟对4个电源模块进行冗余。在考虑冗余方案时，有两种选择：

- (1) 4+1冗余(如图a)
- (2) 4个电源模块分别采用1+1冗余(如图b)



图a.4+1冗余



图b.4个1+1冗余

问题：综合考虑可靠性和成本，哪一种方案最优？

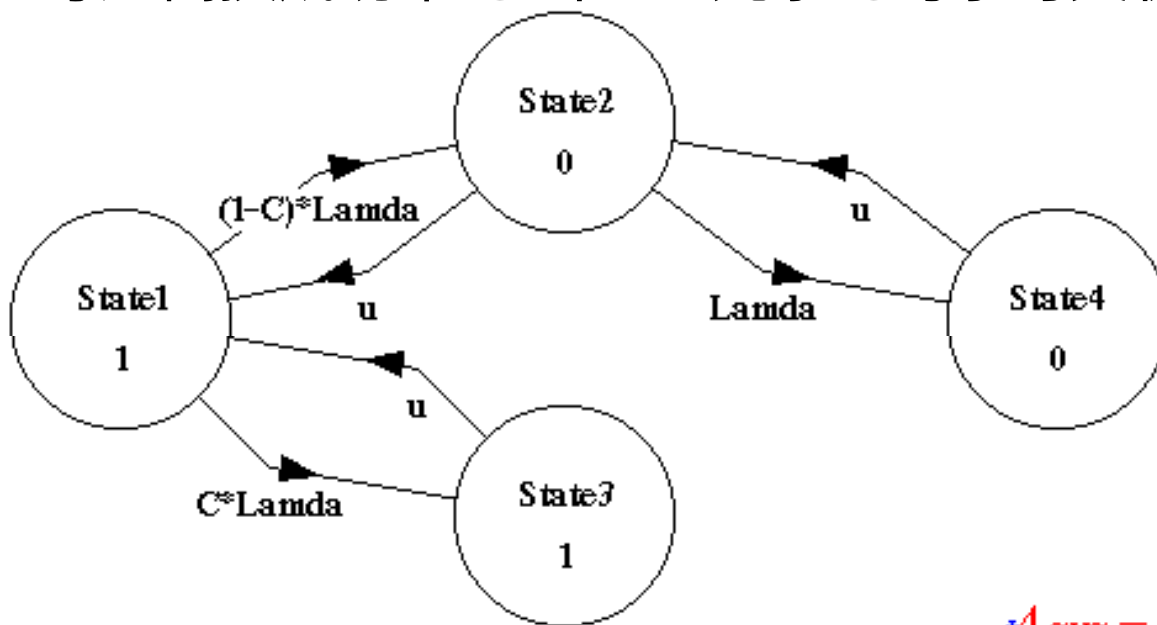


系统可靠性分析实例

利用马尔可夫模型对电源冗余方案进行论证(续)

2. 问题的求解一

考虑倒换成功率的4个1+1冗余的马尔可夫状态转移图：



$$A_{SYS} = P_1 + P_3 = \frac{c\lambda\mu + \mu^2}{\mu^2 + \lambda\mu + c\lambda^2}$$

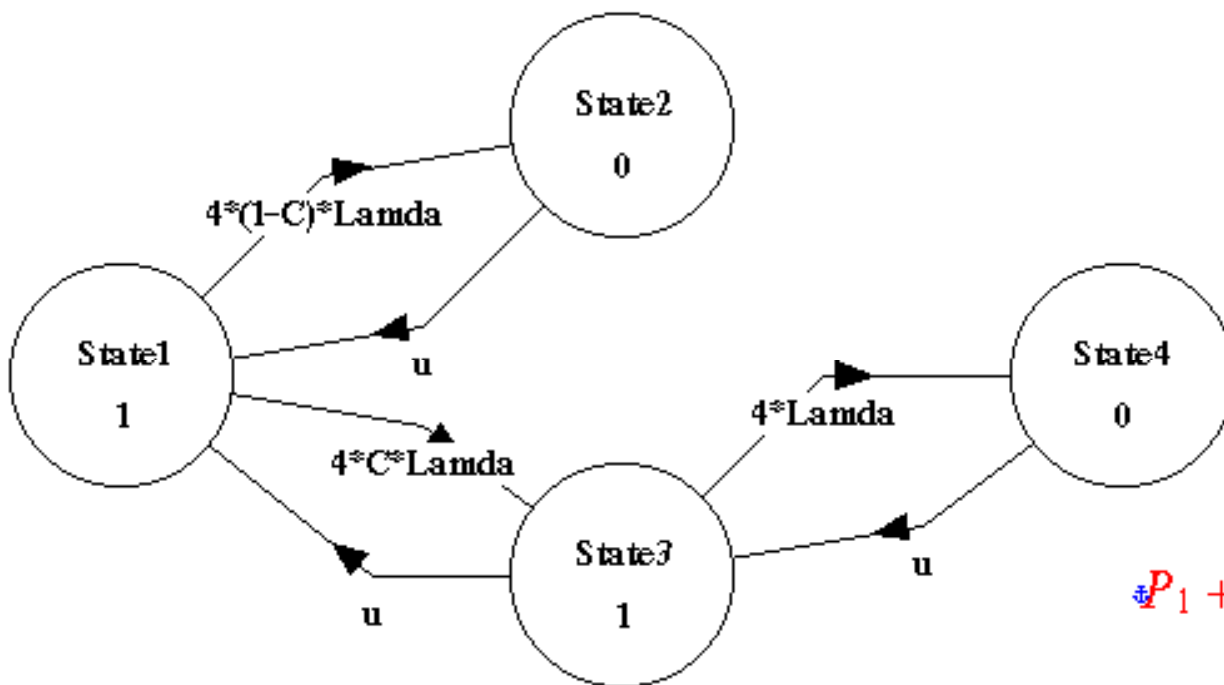


系统可靠性分析实例(一)

利用马尔可夫模型对电源冗余方案进行论证(续)

2. 问题的求解(续)一

考虑倒换成功率的4+1冗余的马尔可夫状态转移图：



$$P_1 + P_3 = \frac{4c\lambda\mu + \mu^2}{\mu^2 + 4\lambda\mu + 16c\lambda^2}$$



系统可靠性分析实例(一)

利用马尔可夫模型对电源冗余方案进行论证(续)

3. 结论

通过上面的建模和计算，两种冗余方案的可用度计算结果非常接近，方案1(为每个电源模块都增加一个备份，组成4个1+1主备用的结构)的可用度为0.999999599997，而方案2(4+1主备用)的可用度为0.999999599987，前者比后者要高，但差异非常小。但从成本的角度考虑，方案1显然是不经济的，因为它比方案2要多增加3个电源模块，同时使系统结构变得更加复杂，而在可用度的提高上却并不明显。

方案	冗余方案	可用度
1	4个1+1	0.999999599997
2	4+1	0.999999599987



系统可靠性分析实例(二)

根据客户需求确定系统方案

1. 问题的提出

客户对某产品的可靠性提出的要求是：产品MTBF必须大于5年。在产品的早期设计阶段，就必须对这一需求的可行性加以论证。因为产品的可靠性很大程度上取决于早期的系统方案设计，如果早期的系统方案可靠性相对需求差距太大，那么则很难在后期的设计、生产过程中加以弥补。



**客户要求产品MTBF
必须在5年以上**



系统可靠性分析实例(二)

根据客户需求确定系统方案

单元名称	配置数量	故障率 (FITs)	MTBF(hr s)
单板1	1	4000	250000
单板2	1	4000	250000
单板3	2	944	1059322
单板4	1	553	1808318
单板5	1	4000	250000
单板6	2	185	5405405
单板7	1	130	7692308
单板8	2	131	7633588
电源	3(2+1冗余)	1000	1000000
风扇	3	10000	100000
背板	1	143	7000000
硬盘	1	833	1200000

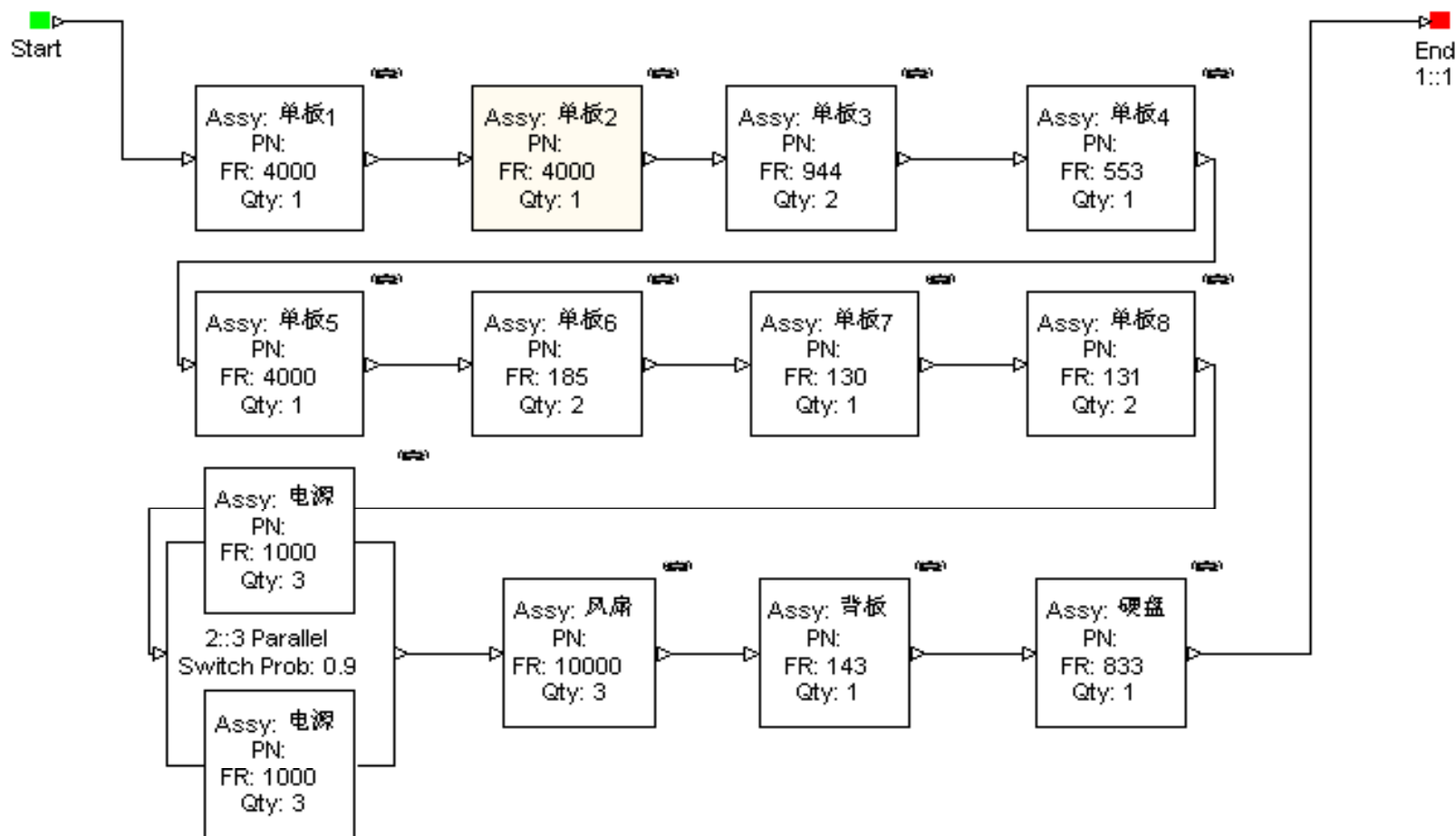
2. 原设计方案

该产品原设计方案中各组成单元及其相关可靠性指标如右表所示：

系统可靠性分析实例(二)

根据客户需求确定系统方案

3. 原方案可靠性框图



系统可靠性分析实例(二)

根据客户需求确定系统方案

4. 原方案系统可靠性计算结果

RBD Calculation Results

MTBF (simulated): 21515.618579 Results at time 1000.00:
MTTF: 21515.618579 Reliability: R 0.954678
Steady-State Availability: $A_i(\infty)$ 0.999953 Availability: A 0.999953
Operational Availability: A_o 0.999953 Unreliability: F 0.045322
Cost of Configuration: C_{rbd} NA Unavailability: Q 0.000047
Cost of Spares: C_{sp} NA Failure Rate: λ_{sys} 46384.028482
Achieved Availability: A_a NA
Confidence Level (Reliability): NA
Confidence Level (Availability): NA
Calculation Method: Analytical

Time	Availability	Reliability	Failure Rate	Unavailability
0	1.000000	1.000000	46379.000048	5.551115e-
100.00	0.999953	0.995373	46379.503931	0.000
200.00	0.999953	0.990767	46380.007584	0.000
300.00	0.999953	0.986182	46380.511005	0.000
400.00	0.999953	0.981619	46381.014194	0.000
500.00	0.999953	0.977077	46381.517153	0.000
600.00	0.999953	0.972555	46382.019880	0.000
700.00	0.999953	0.968055	46382.522376	0.000
800.00	0.999953	0.963575	46383.024642	0.000
900.00	0.999953	0.959116	46383.526678	0.000
1000.00	0.999953	0.954678	46384.028482	0.000

采用前面介绍的建模、计算方法，计算得到系统的可靠性指标为：

MTBF=2.4年

不能满足客户的要求。

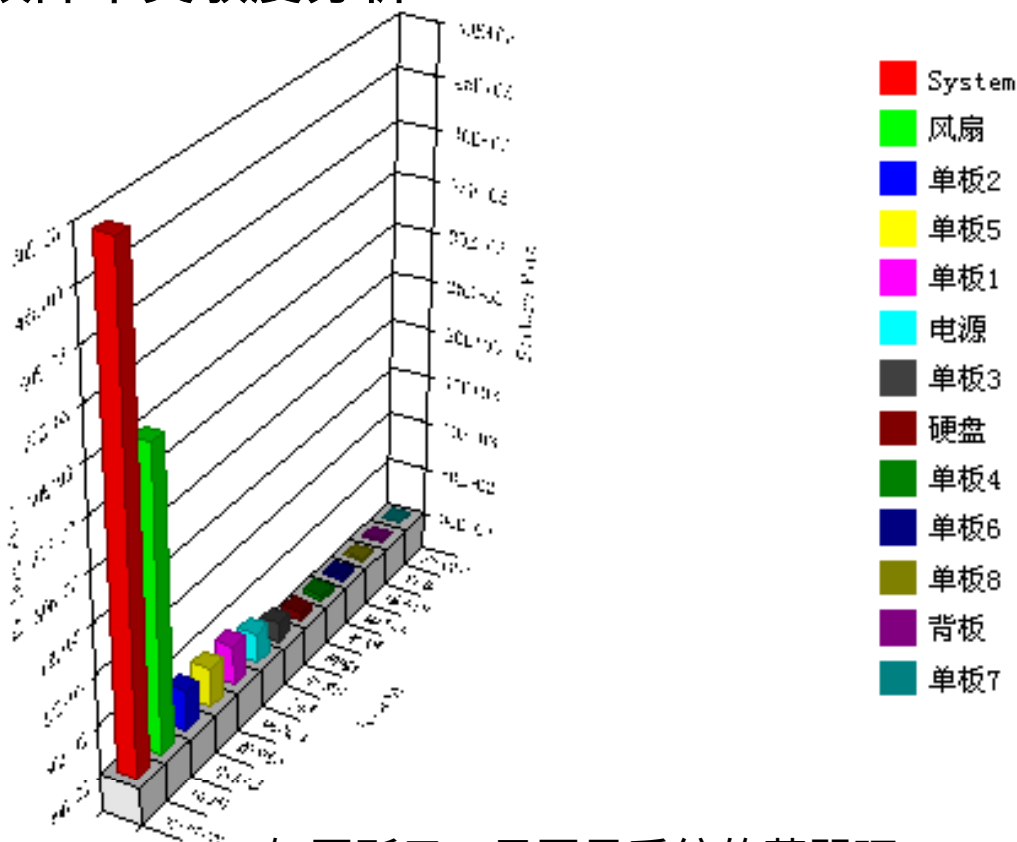


系统可靠性分析实例(二)

根据客户需求确定系统方案

Failure Rate

5. 单元故障率灵敏度分析



如图所示，风扇是系统的薄弱环节



系统可靠性分析实例(二)

根据客户需求确定系统方案

6. 改进措施—改进风扇方案后，系统可靠性的提高

RBD Calculation Results

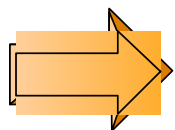
MTBF (simulated): 51055.868764 Results at time 1000.00:
MTTF: 31787.720625 Reliability: R 0.980326
Steady-State Availability: $A_i(\infty)$ 0.999980 Availability: A 0.999980
Operational Availability: A_o 0.999980 Unreliability: F 0.019674
Cost of Configuration: C_{rbd} NA Unavailability: Q 0.000020
Cost of Spares: C_{sp} NA Failure Rate: λ_{sys} 20352.044592
Achieved Availability: A_a NA
Confidence Level (Reliability): NA
Confidence Level (Availability): NA
Calculation Method: Analytical

Time	Availability	Reliability	Failure Rate	Unavailability
0	1.000000	1.000000	19379.000763	2.220446e-
100.00	0.999980	0.998059	19479.085974	0.000
200.00	0.999980	0.996112	19578.537636	0.000
300.00	0.999980	0.994159	19677.361724	0.000
400.00	0.999980	0.992199	19775.564135	0.000
500.00	0.999980	0.990234	19873.150696	0.000
600.00	0.999980	0.988264	19970.127158	0.000
700.00	0.999980	0.986287	20066.499202	0.000
800.00	0.999980	0.984305	20162.272440	0.000
900.00	0.999980	0.982318	20257.452412	0.000
1000.00	0.999980	0.980326	20352.044592	0.000

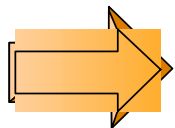
原方案中3风扇个
风扇中不能有一个故障，因为一旦一个风扇故障，将使系统温度过高而导致故障，现增加一个风扇，实际上使风扇变为一个3/4结构，可使系统MTBF从原来的2年多提高到接近6年



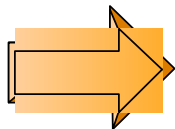
目录



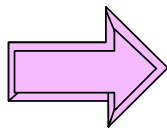
系统可靠性分析的步骤



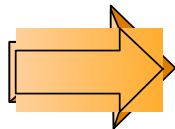
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



系统可靠性模型分析举例



系统可靠性论证分析举例



系统可靠性分析举例（电源产品）





系统可靠性分析举例（电源产品）

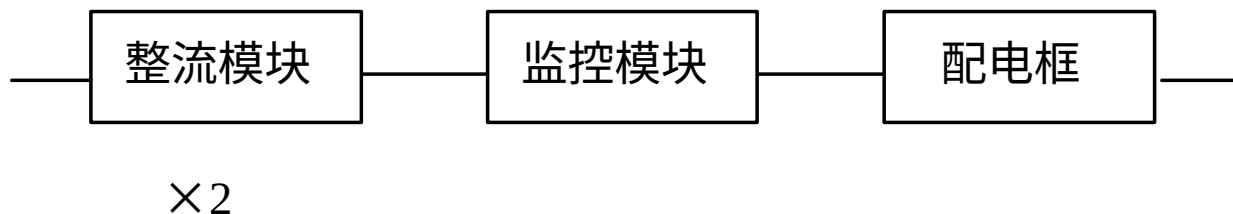
电源产品可靠性要求

指标	量值	条件	备注	
模块、单板平均故障间隔时间MTBF	整流模块	10	25°C, 额定输入, 满载输出 Bellcore 应力法预计	可靠性预计报告
	监控模块	20		
	配电单元	50		
系统	15 万小时			
系统不可用度	$<1 \times 10^{-6}$			
2. 寿命：10年				



系统可靠性分析举例（电源产品）

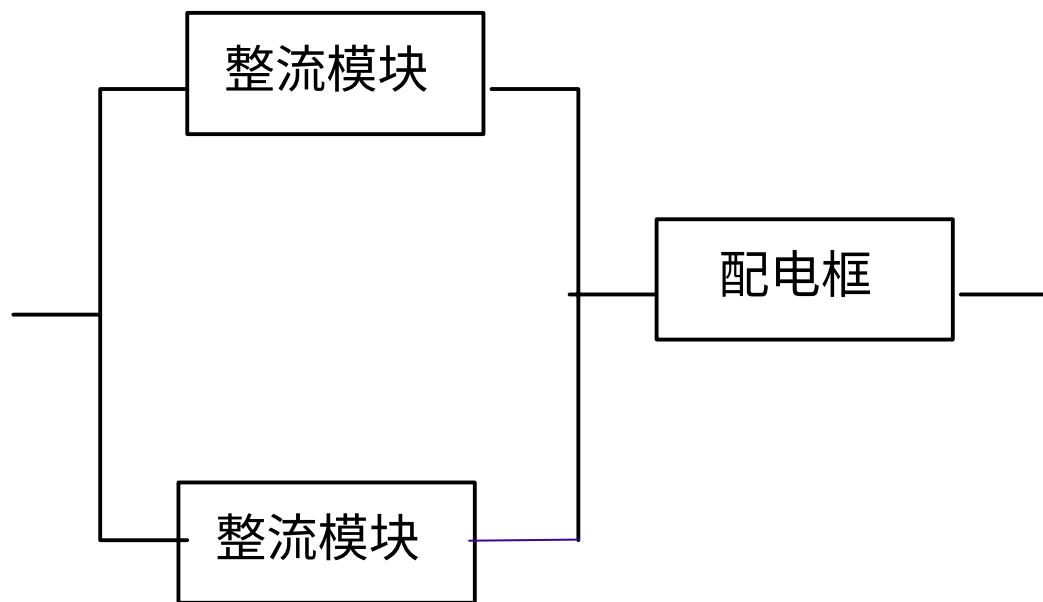
216电源系统整机基本可靠性模型框图





系统可靠性分析举例（电源产品）

根据上面关于任务可靠性的定义，在216电源系统中，其中的监控模块故障不会直接导致电源系统故障，因此在216电源系统的任务可靠性模型中将只包括整流模块和配电框两部分。由此可以建立系统的任务可靠性模型框图如下：





系统可靠性分析举例（电源产品）

根据上面介绍的评分原则，采用重要度、复杂度、成熟度和环境因子4个属性，并对它们分别评分如下：

模块名称	重要度	复杂度	成熟度	环境条件
整流模块	10	10	7	10
监控模块	1	7	10	2
配电框	10	1	1	1

表1. 216电源系统各模块评分表



系统可靠性分析举例（电源产品）

整机MTBF=15万小时，转换为故障率（FITs）和返修率分别为：

整机故障率= $1/150000=6666.67\text{FITs}$

整机年返修率= $6666.67/10000000000 \times 8760=5.84\%/年$

采用以上介绍的分配方法论可以得到各模块单元的分配结果如下表：

单元名称	配置数量	分配的返修率
整流模块	2	1.91%
监控模块	1	0.11%
配电框	1	0.08%



系统可靠性分析举例（电源产品）

对任务可靠性模型进行分配结果如下表：

单元名称	配置数量	分配的故障率 (FITs)	单板 MTBF(hrs)	单板 MTBF(yrs)
整流模块	2	5952.4	168000	19.2
配电框	1	714.3	1400000	159.8



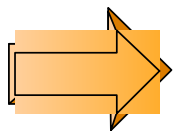
系统可靠性分析举例

针对本公司产品举例说明并讨论

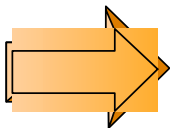




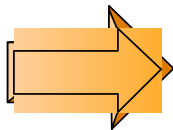
目录



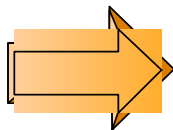
系统可靠性分析的步骤



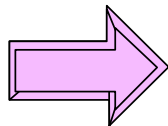
系统可靠性建模技术



系统可靠性建模分析中考虑的要素



系统可靠性模型分析举例



系统可靠性论证分析举例



系统可靠性分析举例（接入设备）

根据国家通信行业标准《YD/T 1045-2000 多业务接入交换机（NAS）技术规范》的要求，系统MTBF需大于69000h，系统MTTR需小于1h。即要求系统可用度A为99.99855%，系统年中断时间7.62min。具体的故障定义基本确定为：标准中给出的可靠性指标指的是系统瘫痪，即一半以上的业务中断时的指标，并且是综合考虑了软件、硬件问题的指标。

系统年中断时间为7.62min，参照BELLCORE标准（SR-TSY-001171：METHODS AND PROCEDURES FOR SYSTEM RELIABILITY ANALYSIS）中系统指标和硬件指标的关系——即硬件指标是系统指标的1/5，所以确定多业务接入交换机的硬件年中断时间为1.524min。假设系统MTTR仍为1h，则产品硬件部分可用度应为99.9997% MTBF=3333332h。



系统可靠性分析举例（接入设备）

利用可靠性分析软件RELEX 对各单板进行了初步的可靠性指标预计。

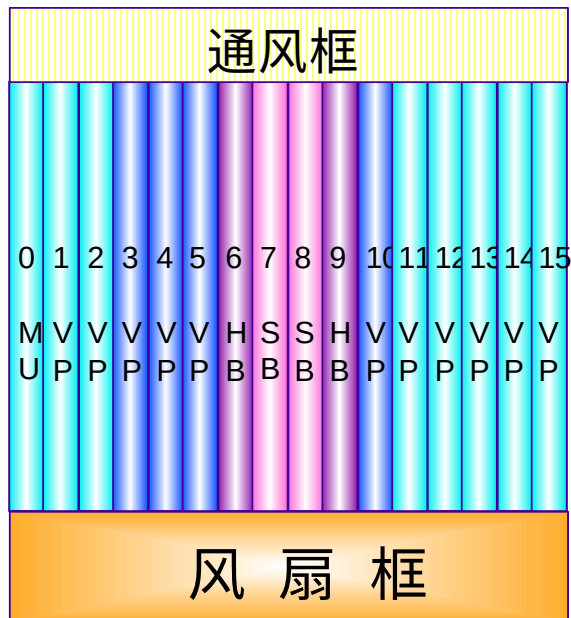
表1 产品各模块可靠性指标

单板名称	预计失效率 (FIT)	修正失效率 (FIT)	单板年返修率	备注
4875	6,666.67	2,963	2.56%	失效率为厂家提供资料, TR-332 预计值
MU	4,842.75	2,152.33	1.87%	
VP	5,633.17	2,503.63	2.17%	
HB	5,204.54	2,313.13	2.01%	
MB	6,609	2,937.33	2.54%	



系统可靠性分析举例（接入设备）

表1. 典型配置的单元配置数量表



单元名称	典型配置数量 (块)
4875电源系统	1套
MU	1
VP	11
SB	2
HB	2



系统可靠性分析举例（接入设备）

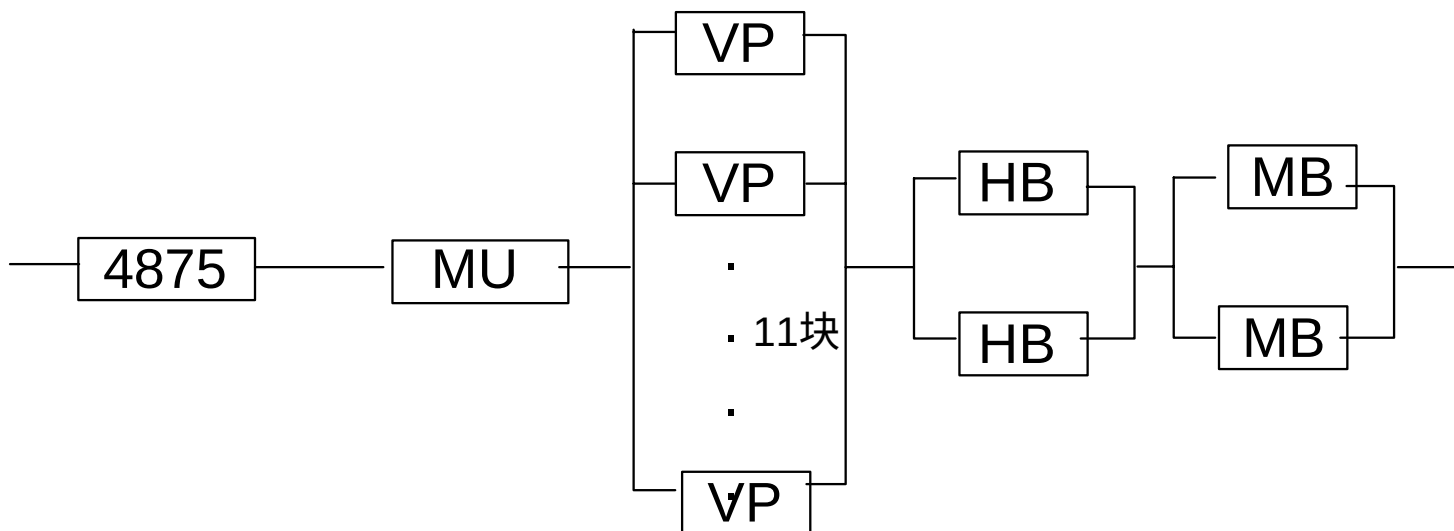
任务可靠性指标是相对与以下的故障定义和可靠性模型确定的。
多业务接入交换机严酷度定义分为以下四类：

- I. 这种故障会导致整个系统崩溃或主要功能受到严重影响，
- II. 这种故障会导致系统主要功能受到影响、任务延误的系统轻度损坏或存在较大的故障隐患，
- III. 系统次要功能丧失或下降，须立即修理，但不影响系统主要功能的实现的故障。
- IV. 部分功能下降，只须一般维护的，不对功能实现造成影响（一般告警或指示灯故障等）。



系统可靠性分析举例（接入设备）

任务可靠性模型



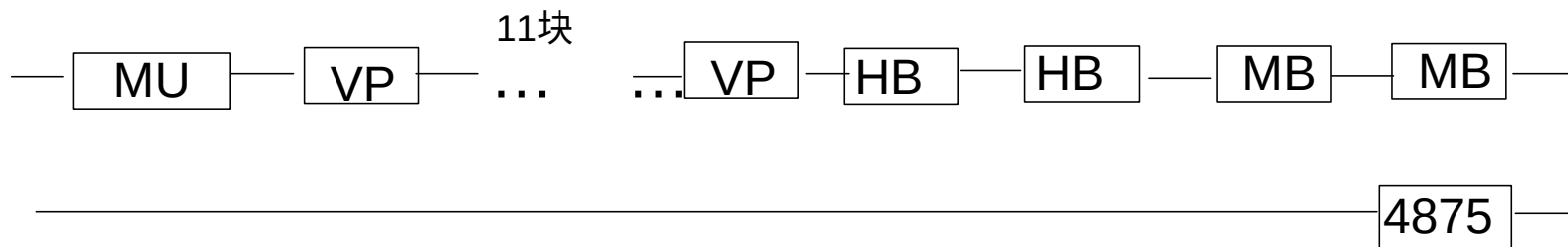


系统可靠性分析举例（接入设备）

对于存在冗余系统的产品，不但要考虑任务可靠性指标，还应该考虑基本可靠性指标。

基本可靠性指标主要考虑所有引起维修的故障，即使这些故障并不一定影响产品执行功能。对于基本可靠性指标，主要考虑产品平均年返修率。

产品年平均返修率定义为产品运行一年的时间里，故障部件数与产品所有部件数之比，用F表示。根据以往产品现场运行的经验，多业务接入交换机典型配置为1块MU、11块VP、2块HB、2块MB，即单板发货时按照此比例发货，年返修率指标定义为0.3%。
产品的基本可靠性指标是相对于以下的可靠性模型得到





系统可靠性分析举例（接入设备）

可靠性分配方法

单板返修率 vs. 产品平均年返修率

产品的基本可靠性指标——产品平均年返修率，可通过串联各单元的年返修率得到。

$$F_s = \sum_{i=1}^n (N_i \times F_i) / \sum_{i=1}^n N_i$$

其中：

N_i 为典型配置中的第*i*中单板的配置数

F_i 为第*i*种单板的年返修率

F_s 为产品平均年返修率

n 为产品的单元类型总数

返修率 vs. 故障率(FIT)

单板的年返修率等于该单板运行1年时的不可靠度：

$$F = 1 - e^{-\lambda \times t}$$

其中：

λ 为单板的失效率FIT

t 为1年的小时数， $t=365 \times 24=8760h$ 。



系统可靠性分析举例（接入设备）

利用可靠性分析软件RELEX对各单板进行了初步的可靠性指标预计。

表1 产品各模块可靠性指标

单板名称	预计失效率 (FIT)	修正失效率 (FIT)	单板年返修 率	备注
4875电源系统	6,666.67	2,963	2.56%	失效率为厂家提供资料，TR—332预计值
MU	4,842.75	2,152.33	1.87%	
VP	5,633.17	2,503.63	2.17%	
HB	5,204.54	2,313.13	2.01%	
MB	6,609	2,937.33	2.54%	



系统可靠性分析举例（接入设备）

（2）基本可靠性指标

首先，产品的基本可靠性指标——产品平均年返修率，可通过串联各单元的年返修率得到。

$$F_s = \frac{N_{MSTU} \times F_{MSTU} + N_{CPU} \times F_{CPU} + N_{DPU} \times F_{DPU} + N_{MPU} \times F_{MPU}}{N_{MSTU} + N_{CPU} + N_{DPU} + N_{MPU}}$$

这里， N_{MSTU} 为典型配置中MSTU的配置单板数， F_{MSTU} 为MSTU单板的年返修率。其他同理。各单板的年返修率：

$$F = 1 - e^{-\lambda \times t}$$

其中， λ 为单板的失效率； t 为1年的小时数， $t=365 \times 24=8760h$ 。

可得， $F_s=2.18\%$ 。

这里，根据经验数据，“修正失效率”为“预计失效率”的1/2.25倍。

根据上表数据，可计算产品的可靠性指标。

（1）任务可靠性指标

首先计算出各模块的可用度指标，对于并联部分，根据下面公式计算A：

$$A = 1 - \{C \times [1 - a^N \times (N+1 - N \times a)] \div N + (1 - C) \times (1 - a^N) \div N\}$$

其中：

A——1：N冗余系统的可用度

C——倒换率——成功倒换的概率， $C = C_A \times C_S$ ， C_A 为主用侧的故障检测率， C_S 为备用侧的故障检测率，在此C取0.7。

a——N+1个单元中每个单元的可用度。

对于VP板的11中取6系统，模块可用度可假设为1。



系统可靠性分析举例（接入设备）

	单个模块可用度	整个模块（任务）可用度
4875电源系统	0.999997037008779	0.999997037008779
MU	0.999997847674633	0.999997037008779
VP	0.999997496376268	1
HB	0.999997686875351	0.99999930605886
SB	0.999997062678628	0.999999118797549

其次，计算产品任务可用度指标。产品任务可用度等于各模块任务可用度相乘。产品任务可用度 $A=0.999995462$ 。



系统可靠性分析举例（接入设备）

1、接入设备现时的任务可靠性指标为0.999995462，未达到既定任务可靠性目标0.999997的要求。

2、基本可靠性指标为年返修率2.18%，与既定基本可靠性目标——一年返修率0.3%有较大差距。

所以在可靠性指标分配中，主要考虑满足基本可靠性指标。若满足了基本可靠性指标而不能满足任务可靠性指标（冗余单元倒换成功率不变），则再主要考虑满足任务可靠性指标。

根据经验，选取不同的复杂性因子和重要性因子组合，给各单板确定需要达到的年返修率目标值



系统可靠性分析举例（接入设备）

分配方案一					
	预估单板年返修率	重要性因子	复杂性因子	分配的返修率	对应失效率(FIT)
MU	1.87%	0.2	0.2	0.25%	281.34
VP	2.17%	0.2	0.2	0.25%	281.34
HB	2.01%	0.3	0.2	0.37%	422.28
MB	2.54%	0.3	0.3	0.55%	634.00
对应系统	0.99999672				
分配方案二					
	预估单板年返修率	重要性因子	复杂性因子	分配的返修率	对应失效率(FIT)
MU	1.87%	0.1	0.2	0.18%	203.12
VP	2.17%	0.2	0.2	0.36%	406.61
HB	2.01%	0.2	0.1	0.18%	203.12
MB	2.54%	0.2	0.1	0.18%	203.12
对应系	0.999996915				
分配方案三					
	预估单板年返修率	重要性因子	复杂性因子	分配的返修率	对应失效率(FIT)
MU	1.87%	0.2	0.2	0.17%	195.86
VP	2.17%	0.3	0.2	0.26%	293.92
HB	2.01%	0.3	0.3	0.39%	441.16
MB	2.54%	0.3	0.4	0.51%	588.60
对应系统 A	0.999996728				



系统可靠性分析举例（接入设备）

分配方案四					
	预估单板年返修率	重要性因子	复杂性因子	分配的返修率	对应失效率(%)
MU	1.87%	0.3	0.2	0.29%	325.98
VP	2.17%	0.5	0.1	0.24%	271.58
HB	2.01%	0.5	0.1	0.24%	271.58
SB	2.54%	0.5	0.3	0.71%	816.69
对应系统A	0.999996711				
分配方案五					
	预估单板年返修率	重要性因子	复杂性因子	分配的返修率	对应失效率(FIT)
MSTU	1.87%	0.3	0.4	0.24%	278.96
VSP	2.17%	0.6	0.2	0.24%	278.96
HRB	2.01%	0.6	0.3	0.37%	418.69
SMB	2.54%	0.7	0.4	0.57%	651.96
对应系统A	0.999996716				



系统可靠性分析举例（接入设备）

分析结论：

但从各种不同分配方案的计算结果来看，可以要求各单板的基本可靠性达到较高的要求来使产品平均年返修率达到既定要求，此时，各单板的基本可靠性已经很高了。若为了满足产品任务可靠性指标要求，再对单板基本可靠性值进行要求，已不太可能。

以分配方案1为例，若各单板基本可靠性指标达到分配值，此时系统可用度为0.99999672。

(1) 即使假设我们冗余单元（SB、HB单板）的故障检测做得很好，倒换成功率很高，达到90%，此时的系统可用度为0.999996931，仍然不能达到既定目标系统可用度99.9997%的要求。

(2) 从产品任务可靠性模型可以看出，影响产品任务可靠性指标的主要是MU单板的基本可靠性指标，但即使MSTU单板基本可靠性指标失效率等于100FIT（可靠性指标已相当高），此时系统的可用度(0.99999672)仍达不到既定目标要求；



系统可靠性分析举例（接入设备）

分析结论：

(3) 还有一个因素我们一直没有考虑，那就是平均修复时间，通信行业标准要求MTTR小于1h，但即使我们的产品仅能将MTTR减小到0.9h，此时对应的系统可用度为0.999997048112597，已达到既定目标要求，若能将MTTR减小到0.5h，则此时系统可用度为0.99999836，大大超过了既定目标要求。

综上所述，产品各单板的基本可靠性指标要求可根据实际情况从上节的分配方案中选择，而影响产品任务可靠性指标的主要是平均修复时间。所以，任何有益于减少MTTR的手段，如：重要故障检测、例测、远程监控、故障上报策略、故障记录策略等故障管理策略对于产品而言都是非常有意义的。



系统可靠性实际分析

利用RELEX软件RBD模型,对以下部件组成一个计算机系统
进行系统建模, 并使可用度达到 $A=99.999\%$, 输出报告。
练习过程 (40min)

光驱	MTBF=10000	MTTR=20min
----	------------	------------

硬盘	MTBF= 20000	MTTR=30min
----	-------------	------------

显示器	MTBF= 5000	MTTR=5min
-----	------------	-----------

主板	MTBF= 6000	MTTR=40min
----	------------	------------



系统性可靠性设计

谢谢大家！