电子设计可靠性工程

第7章 系统级可靠性设计方法

主讲：庄奕琪

本章概要

7.1 可靠性预计与分配

7.1.1 概述

7.1.2 可靠性模型

7.1.3 可靠性预计

7.1.4 可靠性分配

7.1.1 概述

- 可靠性预计与可靠性分配是电子系统可靠性设计的重要任务之一，二者往往需要交互进行，在系统设计的各阶段要反复进行多次
- 可靠性预计是根据组成系统的元器件、部件和分系统的可靠性来推测系统的可靠性，是一个由局部到整体、由小到大、自下而上的综合过程
- 可靠性分配是把系统规定的可靠性指标逐级分配给分系统、部件及元器件，是一个由整体到局部、由大到小、自上而下的分析过程

7.1.2 可靠性模型

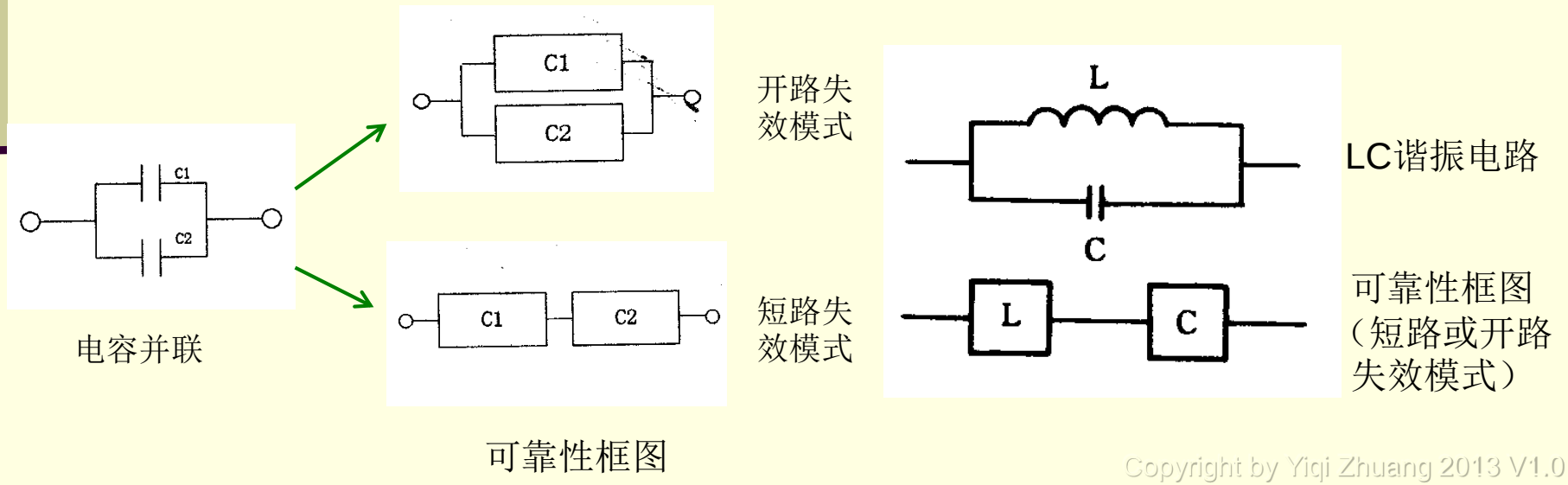
可靠性模型的作用

- 可靠性模型是可靠性预计与分配的基础
- 任何电子系统都是由若干个部件组成。要估算整个系统的可靠性，一方面需求出构成系统的各个部件在相应使用条件下的可靠性特征量，另一方面要知道各个部件的可靠性与整个设备的可靠性之间的关系，这种关系通常用可靠性结构框图来表示
- 可靠性结构框图以及计算得到的系统各部件及其整个系统的可靠性特征量，就构成了所谓”可靠性模型”
- 电子系统只有满足以下条件，才可以用可靠性模型来计算其可靠性
  - 系统只有两种状态，即正常状态和失效状态；
  - 系统各个部件也只有两种状态，即正常状态和失效状态；
  - 各个部件的失效是独立的；
  - 各个部件的可靠性可通过构成部件的元器件的可靠性求得，是已知的

7.1.2 可靠性模型

可靠性框图的建立

- **建立可靠性框图应注意的问题**
  - 功能框图不等于可靠性框图：功能框图中各部件的相对位置是固定有序的，可靠性框图中各部件的先后次序可以在一定条件下更改；功能框图的串联不等于可靠性框图的串联，如LC并联谐振电路在功能上L和C的并联，其可靠性框图却是L和C的串联，因为L和C任一个损坏(开路或者短路)都会造成谐振电路的故障
  - 可靠性框图的形式可能与各个部件的失效模式有关：如两个电容并联应用时，如其主要失效模式是短路，则可靠性框图是串联；如其主要失效模式是开路



7.1.2 可靠性模型

串联系统

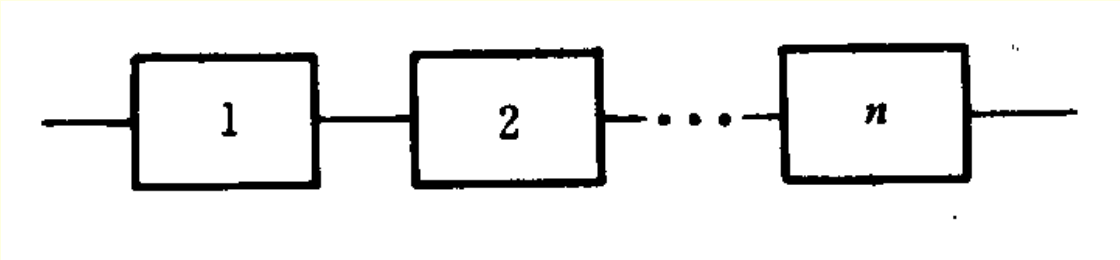
串联系统：组成系统的各个部件中，任一部件的失效都会导致整个系统失效

设系统由n个部件组成，各个部件的失效相互独立，且服从指数分布，第i个部件的可靠性为R_i（t），失效率为λ_i，则

$$R_{system}(t)=\prod_{i=1}^{n}R_i(t)=\prod_{i=1}^{n}e^{-\lambda_i t}=e^{\sum_{i=1}^{n}\lambda_i}=e^{-\lambda_{system}t}$$

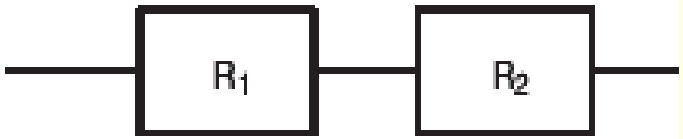
$$\lambda_{system}=\sum_{i=1}^{n}\lambda_i$$

$$\mathrm{MTTF}=\frac{1}{\lambda_{system}}$$



n单元串联系统

可见，在串联系统中，串联的部件单元越多，可靠度越低（R<1），失效率越高



$$R_{system}=R_1\cdot R_2$$

$$\lambda_{system}=\lambda_1+\lambda_2$$

二单元串联系统

7.1.2 可靠性模型

并联系统

并联系统：组成系统的所有部件都失效时系统才会失效

设并联系统由n个部件组成，各个部件的失效相互独立，第i个部件的失效概率为F_i（t），可靠度为R_i（t），则

$$F_{system}(t)=\prod_{i=1}^{n}F_i(t)=\prod_{i=1}^{n}[1-R_i(t)]$$

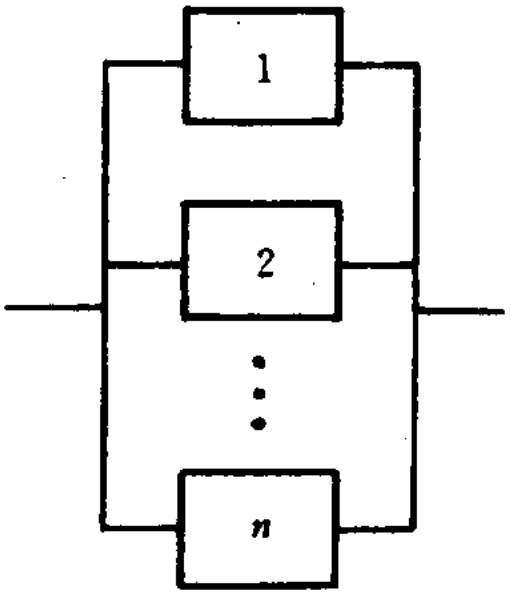
$$R_{system}(t)=1-F_{system}(t)=1-\prod_{i=1}^{n}[1-R_i(t)]$$

若并联的n个单元相同，失效率均为λ，失效服从指数分布，则

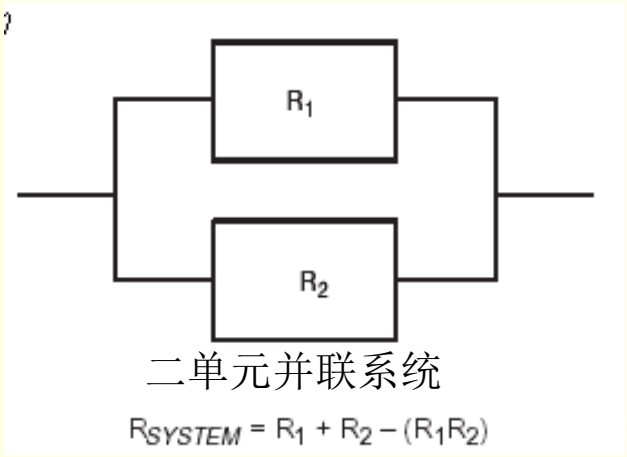
$$R_{system}(t)=1-(1-e^{-\lambda t})^n$$

$$\mathrm{MTTF}=\int_0^{\infty}R_{system}(t)dt=\frac{1}{\lambda}+\frac{1}{2\lambda}+\cdots+\frac{1}{n\lambda}$$

可见，在并联系统中，并联的部件单元越多，失效率越低，寿命越长，故常用于冗余设计（详见本章冗余设计一节）



n单元并联系统



二单元并联系统

7.1.2 可靠性模型

并串联系统

并串联系统：n个各含有m_i个并联部件的子系统再串联起来的系统

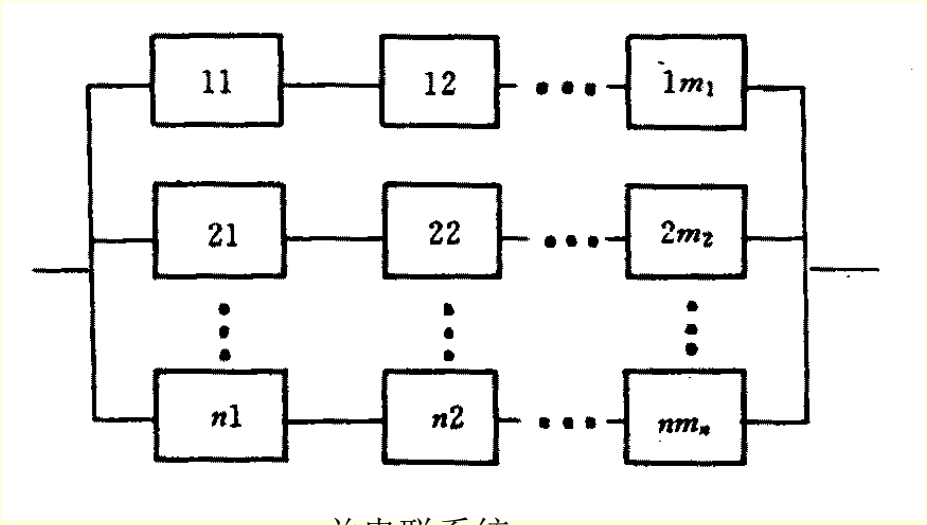
设$R_{ij}(t)$为串联第i个、并联第j个单元的可靠度(i=1,2,…,n；j=1,2,…,mi)，则

$$R_{system}(t)=\prod_{i=1}^{n}\left\{1-\prod_{j=1}^{m_i}\left[1-R_{ij}(t)\right]\right\}$$

若所有单元相同，且并联个数相同，则

$$R_{ij}(t)=R(t),m_1=m_2=\cdots=m_n=m$$

$$R_{system}(t)=\left\{1-\left[1-R(t)\right]^m\right\}^n$$



并串联系统

串并联系统：n个各含有m_i个串联部件的子系统再并联起来的系统

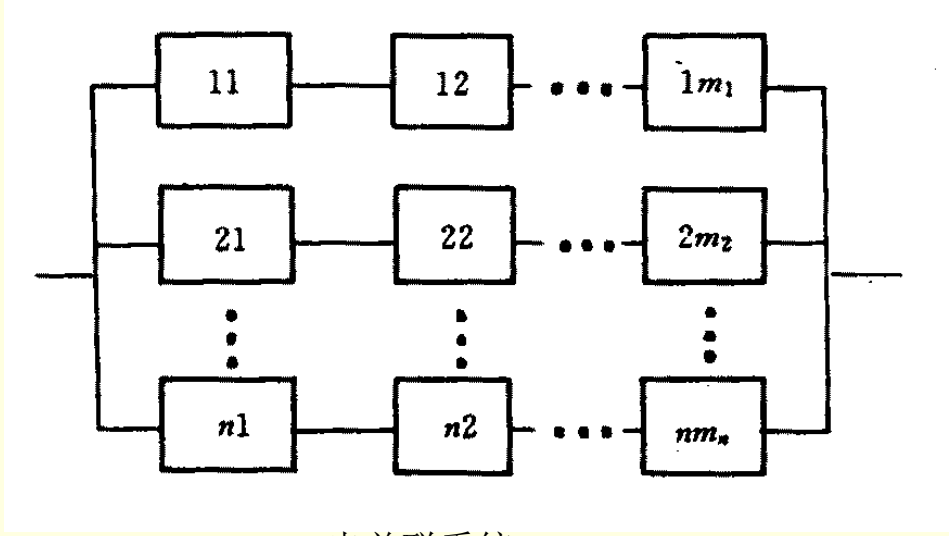
设$R_{ij}(t)$为串联第i个、并联第j个单元的可靠度(i=1,2,…,n；j=1,2,…,mi)，则

$$R_{system}(t)=1-\prod_{i=1}^{n}\left\{1-\prod_{j=1}^{m_i}R_{ij}(t)\right\}$$

若所有单元相同，且串联个数相同，则

$$R_{ij}(t)=R(t),m_1=m_2=\cdots=m_n=m$$

$$R_{system}(t)=1-\left[1-R^m(t)\right]^n$$

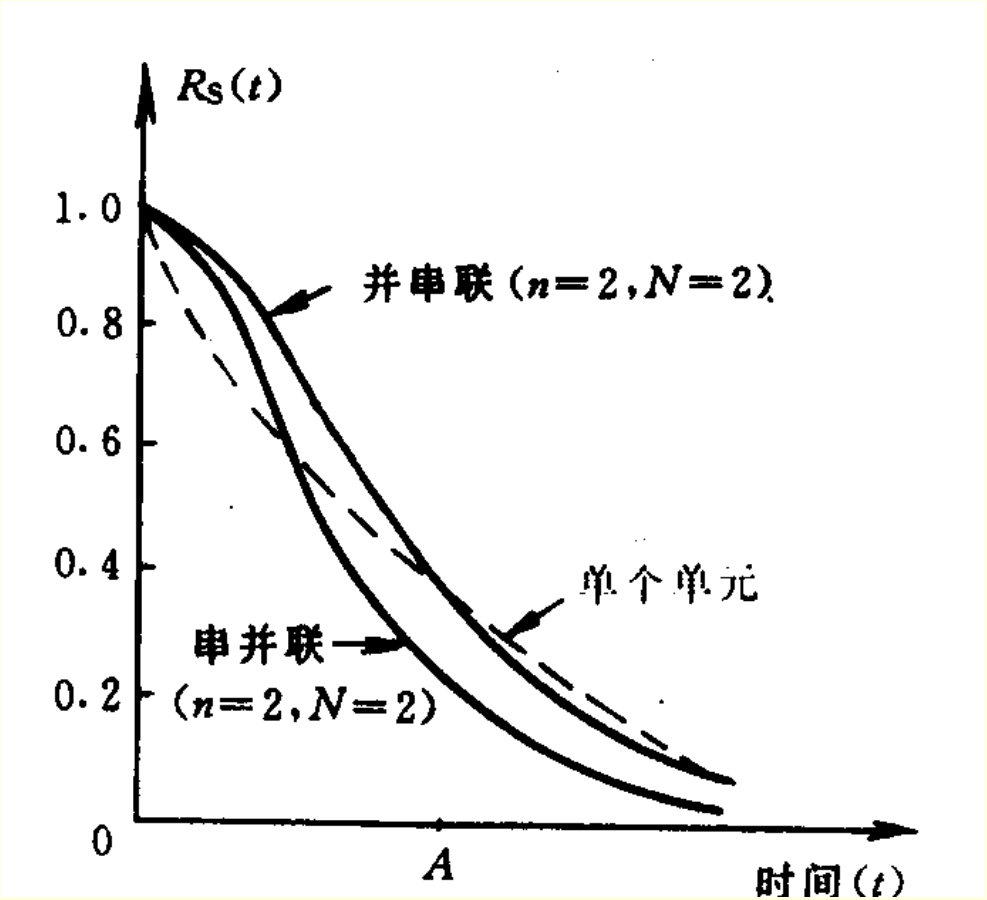


串并联系统

7.1.2 可靠性模型

混联系统的比较

- 短期任务时间（一般工作在单个单元的MTTF之前，图中A点之前），混联系统通常比单个单元的可靠性要好
- 并串联系统的可靠性优于串并联系统
- 串并联系统主要用于对短路故障的保护，并串联系统主要用于对开路故障的保护



2x2单元的混联系统可靠度的比较

混联系统还有表决系统、开关系统、桥联系统等类型，参见“冗余设计”一节

7.1.3 可靠性预计

可靠性预计的目的与依据

- **可靠性预计的目的**
  - 在系统设计阶段，根据系统的功能、使用的元器件及其各部件之间的相互关系，估算系统是否能满足规定的可靠性指标
  - 比较或权衡各种设计方案，亦可为维修性、安全性、保障性分析及试验提供信息
  - 确定影响系统可靠性的关键部位、薄弱环节和潜在问题，确定需改进的部件或单元
- **可靠性预计的依据**
  - 国产元器件：GJB /Z299C-2006 电子设备可靠性预计手册和GJB /Z108 电子设备非工作状态可靠性预计手册
  - 美国元器件：MIL-HDBK-217F 《电子设备可靠性预计手册》

7.1.3 可靠性预计

可靠性预计的步骤与层次

- **可靠性预计的步骤**
  - 建立系统可靠性模型
  - 计算各个元器件和部件单元的可靠性指标
  - 根据可靠性模型和各个元部件的可靠性数据，计算系统的可靠性指标
- **可靠性预计的类别与方法**
  - 可行性预计：用于产品方案论证阶段，作为预计依据的信息只有产品的总体规格，只能借助以往的工程经验、相似产品的可靠性历史数据来预计待研制产品的可靠性。预计方法有相似产品法、相似电路法、有源组件法等
  - 初步预计：用于产品详细设计阶段早期，作为预计依据的信息有设计草图、产品构成框架以及主要元器件的种类和数量。预计方法主要采用部件计数法，求得部件失效率后，再根据系统可靠性模型来求得系统总体的失效率
  - 详细预计：用于产品详细设计阶段中后期。此时已知产品各个组成部分及元器件的工作环境和应力条件。预计方法主要采用元器件应力分析法

7.1.3 可靠性预计

系统可靠性的初步估算通常采用相似产品法和相似电路法

- **相似产品法**
  - 借助于已知的相似产品的可靠性经验数据（$MTBF_0$），根据所要设计的产品可能的差别加以修正
  - 待设计产品的平均无故障时间

$$MTBF = MTBF_0 \cdot \pi_1 \cdot \pi_2 \cdot \pi_3$$

π_1为新产品不成熟因子，$0<\pi_1\leq 1$

π_2为复杂性修正因子，如新产品复杂性提高，则$\pi_2\leq 1$，否则$\pi_2 \geqslant 1$

π_3为综合修正因子，考虑到采用采用新技术、新部件、新元器件以及人员素质变化、可靠性管理水平提高等因素对可靠性的影响

- **相似电路法**
  - 如果能够知道系统中各个电路的失效率和数目，则产品的失效率可以通过求和估计
  - 设系统由失效率分别为λ_i、数量为N_i的k个类型电路所组成，则系统的失效率近似为

$$\lambda = \sum_{i=1}^{k} N_i \lambda_i$$

7.1.3 可靠性预计

部件可靠性的估算

- 部件单元可靠性的估算通常采用元器件计数法。它假定该部件是由失效率不同的N种元器件构成，元器件可靠性之间的关系满足串联模型或者近似串联模型，而且元器件的失效分布为指数型，该部件的失效率可表示为

$$\lambda_{system} = k_1\lambda_1 + k_2\lambda_2 + \cdots + k_N\lambda_N$$

式中，k_i和λ_i是该部件中第i个元器件的数量和失效率（$i = 1,2,\cdots,N$）

实例:某一系统部件由以下6种元器件构成，其失效率和MTBF为

项目 / 元器件	元件失效率 λ_i	元件数量 K_i	总失效率 $K_i\lambda_i$
集成电路	3.7×10^{-7}	3600	1.33×10^{-3}
晶体管	10^{-7}	3500	3.5×10^{-4}
电阻、电容	10^{-8}	7750	0.78×10^{-4}
厚膜电路	2.4×10^{-8}	50	1.2×10^{-6}
接插点	10^{-8}	10000	1.0×10^{-4}
焊接点	10^{-9}	83000	0.83×10^{-4}

$$\lambda = (13.3 + 3.5 + 0.78 + 0.01 + 1.0 + 0.83)\times10^{-4} = 1.9422\times10^{-5}/\text{h}$$

$\text{MTBF} = 1/\lambda = 515\text{h}$　　该部件实测值为500h，与预计值基本一致

7.1.3 可靠性预计

元器件可靠性的估算

- 不同类型的元器件由于工作机理和失效模式不同，在系统中使用时所加应力条件和所处环境也不一样，因此不宜用统一的失效率来表征。为此，元器件可靠性的估算可采用应力分析法。它首先根据温度、电压和负载情况得出基本失效率λ_b，再考虑其它因素（如环境、质量等级等），引进不同的系数π，与λ_b相乘得到实际工作失效率λ_p
- 不同类型的元器件工作失效率的计算公式以及各个系数的值会有所不同，可参照GJB299C。对于大多数元器件，失效率的计算公式大体如下

工作失效率

$$\lambda_P = \lambda_b \pi_E \pi_Q \pi_A \pi_V \pi_C$$

基本失效率：取决于工作温度、电压或负载

环境系数：取决于工作环境类型（如数字IC取1～50，电容器取1～30）

质量系数：取决于质量等级，一般取0.5～10

降额系数：取决于工作电压（或功率）与额定电压（或功率）的比

应用系数：取决于元器件在电路中的功能及其重要性，一般取0.75～5

复杂度系数：取决于器件的规模和复杂度（如数字IC内部的门数），约为0.7～1.5

- 元器件的失效率也可以采用有关元器件生产厂家提供的数据，或者采用以前的相似系统中同类元器件现场使用的数据

7.1.4 可靠性分配

可靠性分配的目的与准则

- **目的**

  根据系统设计任务书中规定的系统可靠性指标，分解到构成系统的各个部件（可以是子系统、设备，甚至是元器件、接插件）中去，使设计人员在设计各个部件时能够明确其可靠性要求并采取相应的可靠性保证措施，以确保整个系统可靠性指标的实现

- **准则**

  - 假定系统由n个部件构成，其可靠性分别为R_1，R_2，…，R_n，则系统可靠性分配的准则是使

$$R_{system预估} = f(R_1, R_2, \cdots R_n) \geq R_{system指标}$$

  - 若系统为无冗余的简单串联系统，上式成为

$$R_{system预估} = R_1(t) \cdot R_2(t) \cdots\cdots R_n(t) \geq R_{system指标}$$

  显然，如果没有约束条件的话，上述不等式可以有无数个解。为了找到相对最优的解，必须对各个部件的特点（包括电路结构、使用环境和成本考虑等）进行分析，给出各自的权重因子。在此约束条件下来求出各个部件的可靠性指标

7.1.4 可靠性分配

等分法和等比例法:算法

- **等分法**
  - 给各个部件分配完全相同的可靠性指标，如由n个部件构成的简单串联系统，

$$R_{system}(t)=\prod_{i=1}^{n}R_i(t)\Rightarrow R_i(t)=R_{system}^{\frac{1}{n}}$$

  - 这种分配最为简单，但不甚合理，因为它未考虑各个部件可靠性特性的差别以及在系统中所起作用的不同
- **等比例法**
  - 根据部件的预估可靠性的相对大小，将系统指标按比例分配到各个部件中
  - 设第i个部件初始预计的不可靠度为Fi预估，据此预计出的系统不可靠度为Fs预估，系统总体要求的不可靠度为Fs指标，则为了达到此指标，各个部件的不可靠度必须提升到

$$F_{i指标}=F_{i预估}\cdot\frac{F_{S指标}}{F_{S预估}}$$

7.1.4 可靠性分配

等分法和等比例法:示例

- **示例**

  假定某系统由A、B、C、D四个串联单元构成

  - 系统要求的可靠性指标： $F_S=0.16$， $R_S=0.84$
  - 各单元的预计不可靠度：$F_A'=0.04$， $F_B'=0.08$， $F_C'=0.12$， $F_D'=0.08$
  - 系统的预计不可靠度： $F_S'=F_A'+F_B'+F_C'+F_D'=0.32$
  - 按等比例法求得的各单元不可靠度指标应为： $F_A=0.02$， $F_B=0.04$，$F_C=0.06$， $F_D=0.04$
  - 按等比例法求得的各单元可靠度指标应为：$R_A=0.98$， $R_B=0.96$， $R_C=0.94$，$R_D=0.96$
  - 按等分法求得的各单元可靠度指标应为： $R_A=R_B=R_C=R_D=0.84^{1/4}=0.962$

  可见，等比例法比等分法更为合理，但需要对各个部件的可靠性进行初步的预计

7.1.4 可靠性分配

权重法:权重的确定

- **权重法**

  根据各个部件的特点，给出不同的权重因子，并由此来计算各自的可靠性指标要求。通常对以下类型的部件应分配更低的可靠性指标：

  - **复杂性**高的部件。该部件包含更多的元器件而且连接关系复杂，因此要达到高可靠要求比较困难，并且更加费钱
  - **重要性**低的部件。该部件失效对整机的可靠性影响程度相对较小，或者不会带来致命的后果
  - **环境**恶劣的部件。该部件所处环境比别的部件恶劣，因而更容易失效
  - **标准化**程度低的部件。该部件采用非标准件、新研制的、不成熟的元器件多，可靠性更加难以保证
  - **维修**不便的部件。该部件不容易维修或更换，难以通过维修保障来延长其寿命
  - 元器件**质量**较差的部件。该部件所使用的元器件的可靠性水平较低，因而导致部件可靠性较低

7.1.4 可靠性分配

权重法:定量表征

若某个整机的平均故障间隔时间的设计指标为$MTBF_s$，该整机由N个单元组成，分配可靠性指标时需考虑n个加权因子，设第j个单元的第i个加权因子为k_{ji}（一般设某一个单元的$k_{ji}=1$，作为其它单元的参照基准），则第j个单元的平均故障间隔时间为

$$MTBF_j = \frac{\sum_{j=n}^{N}\prod_{i=1}^{n} k_{ji}}{\prod_{i=1}^{n} k_{ji}} MTBF_{system}$$

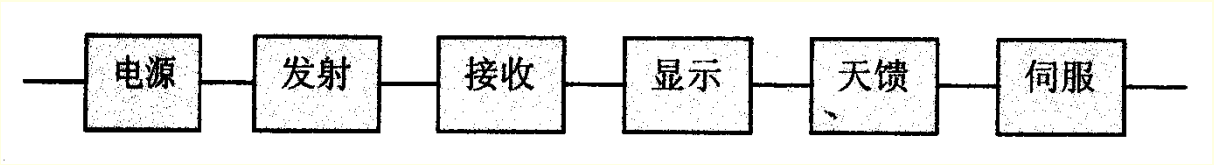
如果认为可靠性分配的结果不合理，或者实际上难以实现，可以通过改变系统功能结构或者各部件的可靠性因子来加以调整和优化

式中，加权因子可分为复杂因子、重要因子、环境因子、标准化因子、维修因子和元器件质量因子（i=1,2,3,4,5,6）。加权因子越小，则说明根据该因素分配给该单元可靠性指标越低

7.1.4 可靠性分配

权重法:示例

某舰载综合火控雷达系统的总可靠性指标为$MTBF_{system}$=400h



系统构成及系统可靠性模型

可靠性分配的计算

分机	电源	发射	接收	显示	天馈	伺服
复杂因子 k_{j1}	1	0.5	2	3	0.2	0.5
重要因子 k_{j2}	1	1	1	1	1	1
环境因子 k_{j3}	1	1	2	1	2	1.5
标准化因子 k_{j4}	1	3	2	2	2	1
维修因子 k_{j5}	1	0.5	0.6	0.6	0.4	0.5
元器件质量因子 k_{j6}	1	1.5	1	1	0.5	2
$K_j=\prod_{i=1}^{6}k_{ji}$	1	1.125	4.8	3.6	0.16	0.75
$K=\sum_{j=1}^{6}K_j$	11.435					
$MTBF_j=\frac{K}{K_j}MTBF_{system}$	4570h	4070h	950h	1270h	28590h	6100h

- 以电源单元作为其它单元的参照基准，即令k_{1i}=1（i=1,2,3,4,5,6)
- 发射单元、天馈单元和伺服单元的元器件较少，故复杂因子较小
- 接收单元对环境干扰敏感，天馈单元易对外界形成干扰，故环境因子较高
- 电源部分维修相对困难，故维修因子较大
- 分配结果表明接收和显示部分是该系统的可靠性薄弱环节

7.2 冗余设计

7.2.1 概述

7.2.2 平行冗余

7.2.3 开关冗余

7.2.4 表决冗余

7.2.5 混合冗余

7.2.1 概述

冗余的概念与作用

- 什么是冗余？
  - 冗余设计也称余度设计或容错设计。它通过增加冗余资源使系统具备多于一种手段执行同一种规定功能的能力，即使系统局部出错或发生故障，其功能仍然能不受影响，从而提高整个系统的可靠性。如在电路设计时，对于容易产生短路的部分，以串联形式复制；对于容易产生开路的部分，以并联形式复制
- 何时需采用冗余？
  - 采用了可获得的最好元器件和其它可靠性设计方法后，系统可靠性仍然达不到要求时，只能采用冗余设计
  - 无法获得所需的高可靠元器件时，采用冗余设计可以降低对构成系统的部件或者元器件的可靠性要求
  - 选用高可靠元器件比采用冗余设计的经济代价更高时，比如欲将失效率降低一个数量级，有可能要更新90%以上的元器件

7.2.1 概述

冗余的局限性

- 冗余会增加系统的复杂性、重量、体积、功耗和成本，从简化设计和低功耗设计的角度来看对可靠性是不利的，为此应在高可靠性和高安全性系统中采用冗余，或者只在系统的关键部件（如电源）采用冗余
- 不是所有系统层次都可以采用冗余设计，在较低的系统层次（如电路级）采用冗余设计比在较高层次更为有效，但给故障测试和电路设计带来的困难也越大。譬如，对于数字逻辑电路，多级冗余电路的设计极为困难甚至不可能，故只能采用部件级和系统级冗余
- 因实现冗余而增加的故障检测和通道切换装置的可靠性必须高于受控部分

7.2.1 概述

冗余的主要类型

- 按冗余的实现层次，可分为系统级冗余、部件级冗余和电路级冗余
- 按冗余的体系结构，可分为平行冗余、开关冗余、表决冗余以及混合冗余
- 按冗余的实现载体，可分为硬件冗余和软件冗余等
- 按冗余元件的贮备状况，可分为热贮备、冷贮备和温贮备冗余系统
- 按冗余结构是否随故障情况的变化而变化，可分为静态冗余（亦称被动冗余）、动态冗余（亦称动态冗余）

7.2.1 概述

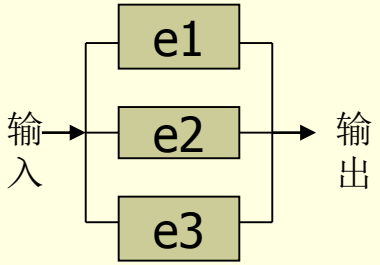
冗余的实现方式

- **硬件冗余**：复制硬件单元，当工作硬件发生故障时，用备份硬件替换。或者，通过表决和比较，屏蔽系统中的错误。适用于模拟和数字的硬件系统。本节之后所述的冗余即指硬件冗余
- **信息冗余**：将重要数据或文件存储于存储区的不同位置，可备份多份。一旦在用数据或文件被破坏或丢失，则自动从备份空间复制。需增加存储空间容量
- **时间冗余**：重复执行某一操作或某一程序，并将执行结果与前次执行结果比较。一旦发现有所不同，即再运行一次。如仍然有误，则初步判断出现了硬件永久性故障。此法会耗用系统计算时间，从而降低了系统运行速度。另一种时间冗余是通过直接降低电路的速度来增加系统的可靠性
- **程序冗余**：采用多个独立设计的程序模块，采用表决方式决定正确结果
- **信息容错**：增加数据码位，构成各种检错与纠错码（如采用奇偶校验码检错、汉明码纠错），使信息或数据在存储、传输、运算和处理过程中的错误得以自动纠正，通常只适用于数字系统

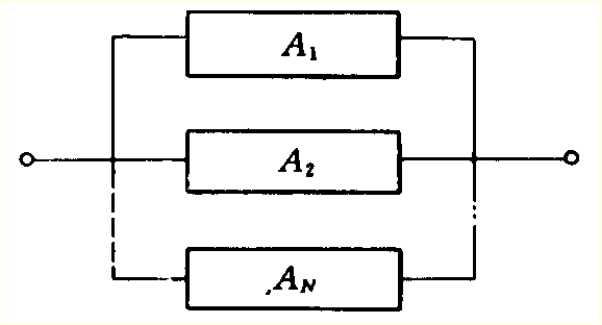
7.2.2 平行冗余

特点

多个相同单元并联构成系统，每个单元执行同样功能，只要有一个单元工作，系统就能正常工作；只有所有单元失效，系统才能失效



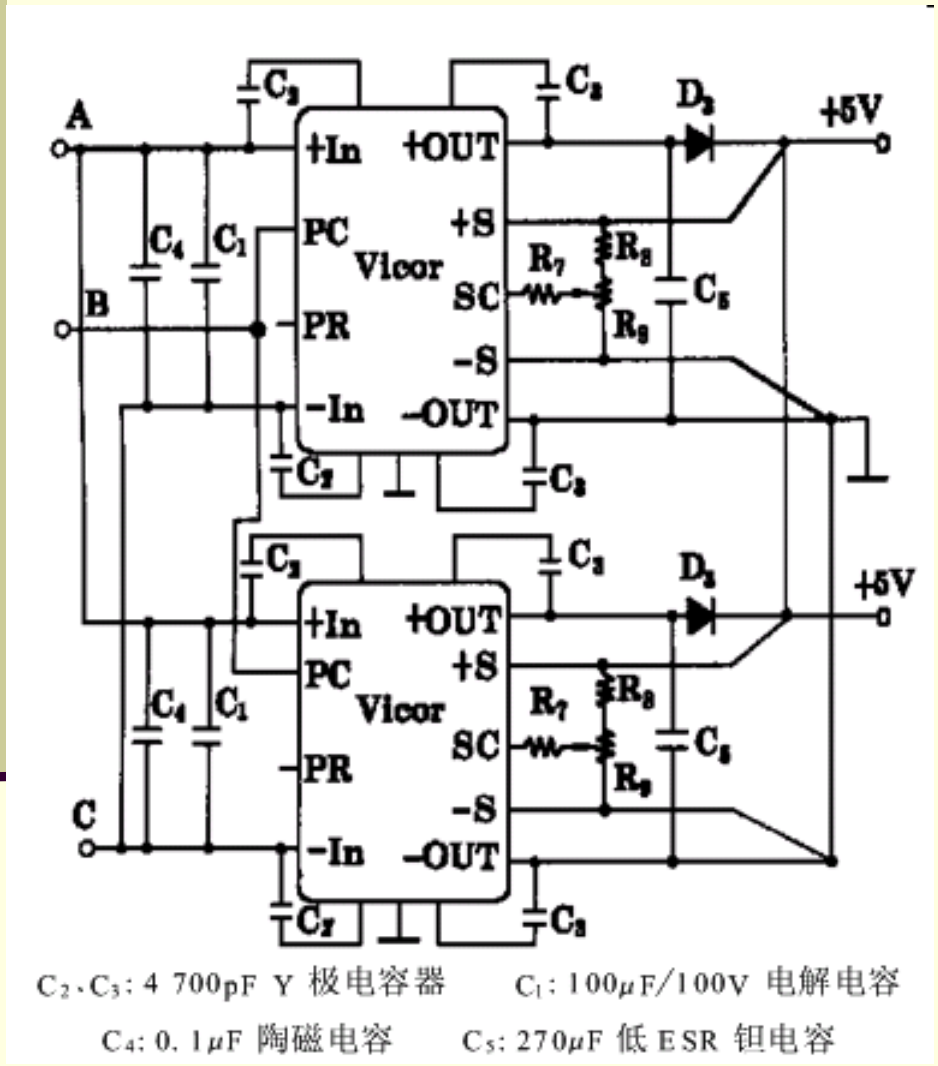
- 优点：构造简单，并联系统的可靠性比构成系统的各个单元的可靠性高，且随单元数↑而↑
- 缺点：
  - 在用单元工作时，冗余单元也在工作并消耗寿命（称为工作贮备系统，或者热贮备系统）
  - 增加输入负载，n个单元并联的电流负载是单个单元的n倍
  - 要求一个单元的失效不会影响到其它单元的正常工作，为此可增加故障检测单元，一旦发现某单元发生故障，即断开该单元



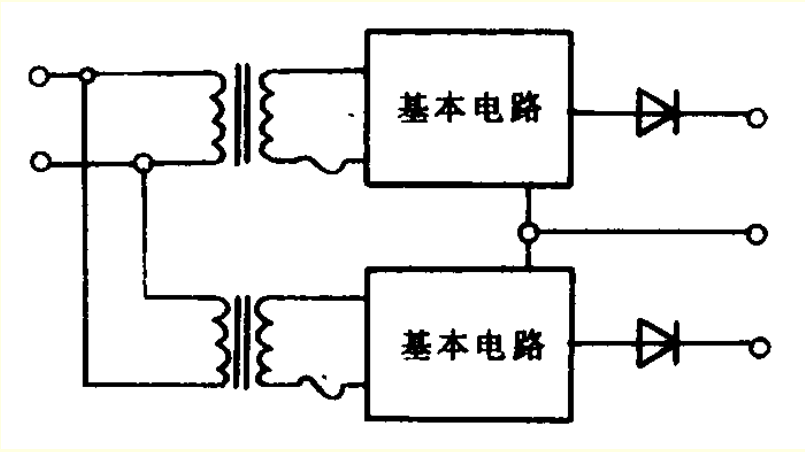
工作贮备并联系统可靠度和MTTF的计算公式见本章“可靠性预计与分配”一节。在以多个相同单元构成的系统中，如每个单元的MTTF=1/λ，则2单元并联系统的 MTTF=3/2λ，3单元并联系统的MTTF=11/6 λ

7.2.2 平行冗余

双电源系统



并联贮备+5V直流电源的结构



并联贮备交流电源的结构

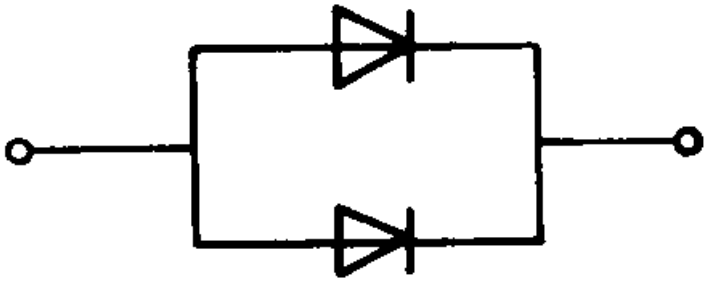
- 仅当两个电源都出现故障时，才会对系统停止供电
- 组合电源的失效率等于两个电源单元失效率之和
- 为防止相互干扰，加有隔离二极管以及开通控制引脚（PC）

若单个电源的失效率为$\lambda=1.055\times10^{-4}/h$，则单电源的MTTF=$1/\lambda$=9479h，双冗余电源的MTTF=$3/2\lambda$=14218h

7.2.2 平行冗余

二极管两倍冗余电路

串联



并联

- 若二极管开路失效概率>短路失效概率，则并联电路可靠性>单个器件可靠性>串联电路可靠性
- 若二极管短路失效概率>开路失效概率，则串联电路可靠性>单个器件可靠性>并联电路可靠性
- 若二极管短路失效概率=开路失效概率，则无论串联还是并联都不能提高电路的可靠性

可见，冗余电路改善可靠性的程度与失效模式有关

逻辑门级电路的串并联将会改变电路功能或者因时延不同引发“冒险竞争”，因此其多倍冗余电路的设计比较困难，所以对数字电路而言，硬件冗余多用于模块级或系统级

7.2.2 平行冗余

混合并联

设二极管的开路故障概率为P_o，短路故障概率为P_s，则

串并联电路可靠工作概率$P_{SPG} \approx 1-2P_s^2-4P_o^2$　　并串联电路可靠工作概率$P_{PSG} \approx 1-2P_o^2-4P_s^2$

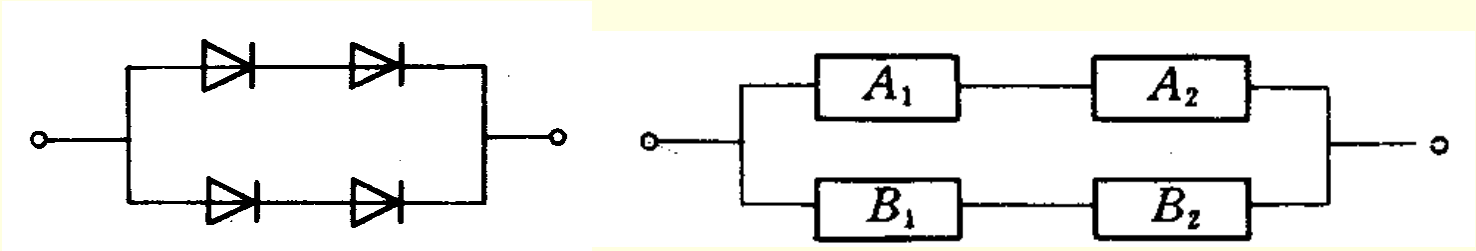
若$P_o < P_s$，则$P_{SPG} > P_{PSG}$，串并联结构较好;若$P_S < P_O$，则$P_{PSG} > P_{SPG}$，并串联结构较好

若$P_o = P_s = P$，则$P_{SPG} = P_{PSG} = 1-6P^2 >$单个二极管的可靠工作概率$1-2P$

$$\frac{\text{冗余电路的故障概率}6P^2}{\text{单管的故障概率}2P} = 3P << 1$$

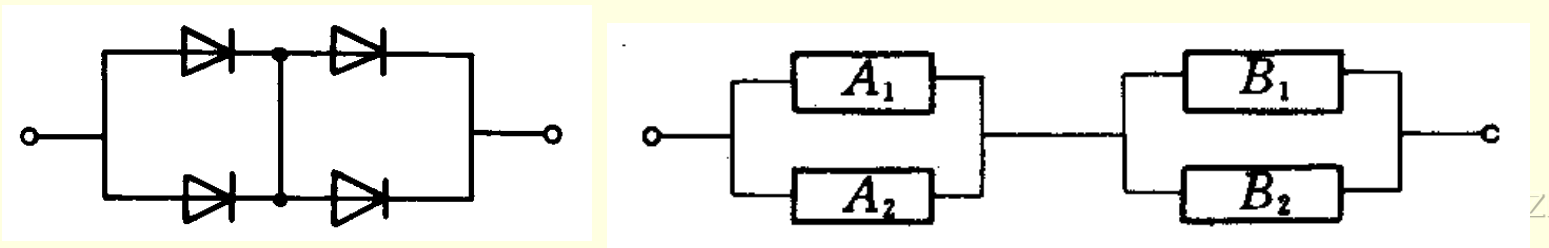
如$P = 10^{-6} \Leftarrow 3P = 3\times10^{-6} \Rightarrow$冗余电路的故障概率减少到单管的300万分之一

当元件以开路失效为主时，可采用并串联冗余；以短路失效为主时，可采用并串联冗余。不论哪一种情况，冗余电路都显著改善了可靠性，但所用元器件数量也大为增加，连接关系更为复杂，从简化设计的角度看，对可靠性又会带来不利影响



串并联

(先串后并)

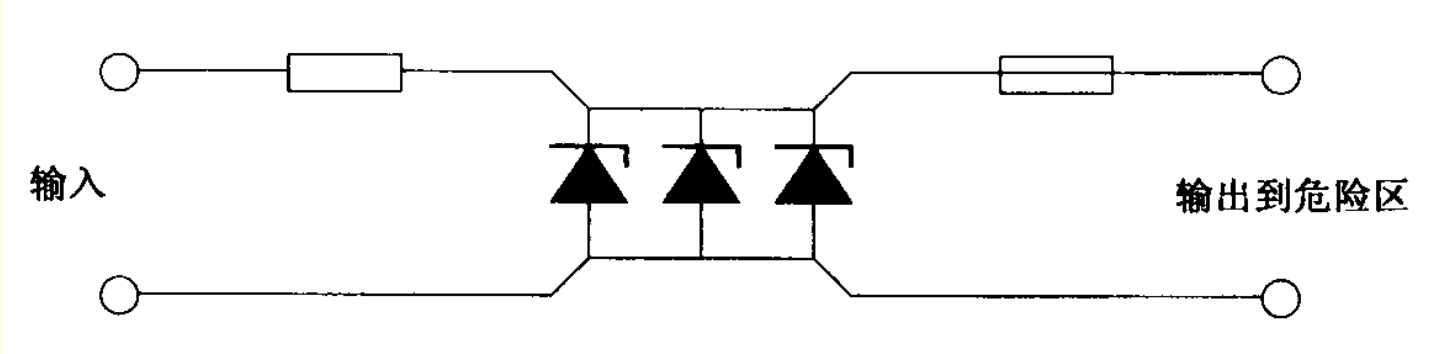


并串联

（先并后串）

7.2.2 平行冗余

- 如果防护元件的失效率太高，则可根据失效模式采取多个防护元件并联或者串联的方式

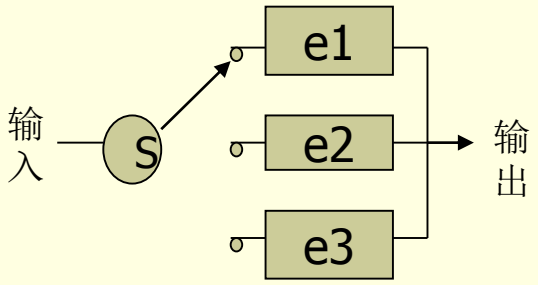


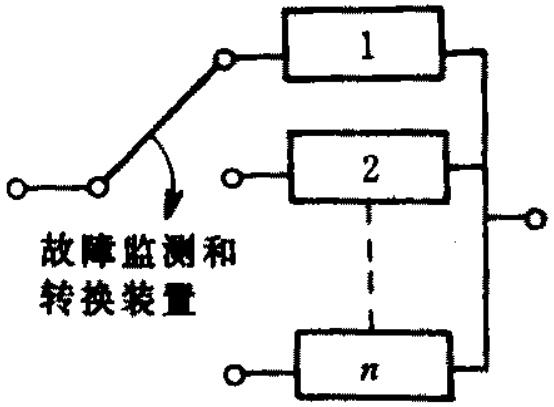
即使三个二极管中有两个出现开路故障，仍然能够实现箝位的功能

7.2.3 开关冗余

特点

- 开关系统：系统由n个单元组成，其中只需一个单元工作，其余n-1个单元贮备。当工作单元失效时，贮备单元通过转换开关去逐个顶替工作，直到所有单元都失效或者转换开关失效为止
- 非工作贮备系统：在用单元工作时，冗余单元不工作。在贮备期中，冗余单元可能不失效（冷贮备，冗余单元处于断电状态），也可能失效（温贮备，冗余单元处于待机状态）；开关可能不失效（理想开关），也可能不失效（非理想开关）
- 效果
  - 理想开关冷贮备系统的寿命是所有单元寿命之和
  - 不考虑开关可靠性时，非工作贮备系统的可靠性优于工作贮备系统
  - 温贮备切换单元时中断运行的时间短，但需消耗一定的功率；冷贮备平时不消耗功率，但切换时间相对较长。对于卫星系统，能量储备有限，可采用冷贮备；对于过程控制系统，重组时间应尽可能短，故应采用温贮备





非工作贮备模型

7.2.3 开关冗余

转换开关完全可靠情形

设转换是瞬时的，n个单元寿命T_1，T_2,…，T_n独立，则

系统寿命$T_{system}=T_1+T_2+T_3+\cdots+T_n$

系统可靠度$R_{system}(t)=1-F_1(t)*F_2(t)*\cdots F_n(t)$

若$T_i(i=1,2,\cdots,n)$服从参数为λ的指数分布，则

$$R_{system}(t)=\sum_{k=0}^{n-1}\frac{(\lambda t)^k}{k!}e^{-\lambda t}$$

$$\text{MTBF}=\frac{n}{\lambda}$$

转换开关不完全可靠情形

以两单元冷贮备系统为例，设两个单元及其转换开关的失效率分别为λ_1、λ_2、λ_{SC}，则可以证明

$$R_{system}(t)=e^{-\lambda_1 t}+\frac{\lambda_1}{\lambda_{sc}+\lambda_1-\lambda_2}\left[e^{-\lambda_2 t}-e^{-(\lambda_1+\lambda_{sc})t}\right]$$

$$\text{MTBF}=\frac{1}{\lambda_1}+\frac{\lambda_1}{\lambda_2(\lambda_1+\lambda_{SC})}$$

7.2.3 开关冗余

温贮备系统

以两单元温贮备系统为例，设两个单元及其转换开关的工作失效率分别为λ_1、λ_2、λ_{SC}，
单元1首先工作，失效后切换到单元2，单元2的贮备失效率为λ_y，λ_1、λ_2、λ_{SC}、λ_y均服从指数分布

转换开关完全可靠情形（$\lambda_{sc}=0$）

$$R_{system}(t)=e^{-\lambda_1 t}+\frac{\lambda_1}{\lambda_1+\lambda_y-\lambda_2}\left[e^{-\lambda_2 t}-e^{-(\lambda_1+\lambda_y)t}\right]$$

$$\mathrm{MTBF}=\frac{1}{\lambda_1}+\frac{\lambda_1}{\lambda_2(\lambda_1+\lambda_y)}$$

转换开关不完全可靠情形（$\lambda_{sc}>0$）

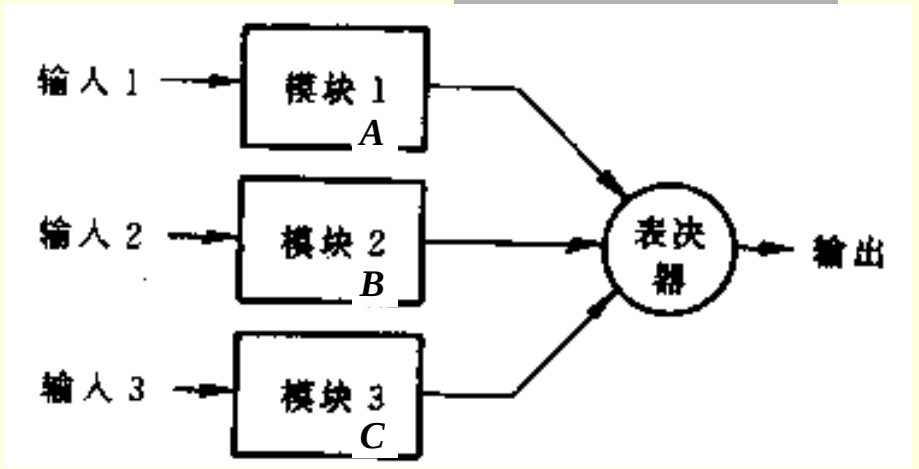
$$R_{system}(t)=e^{-\lambda_1 t}+\frac{\lambda_1}{\lambda_{sc}+\lambda_y+\lambda_1-\lambda_2}\left[e^{-\lambda_2 t}-e^{-(\lambda_y+\lambda_1+\lambda_{sc})t}\right]$$

$$\mathrm{MTBF}=\frac{1}{\lambda_1}+\frac{\lambda_1}{\lambda_2(\lambda_1+\lambda_{sc}+\lambda_y)}$$

7.2.4 表决冗余

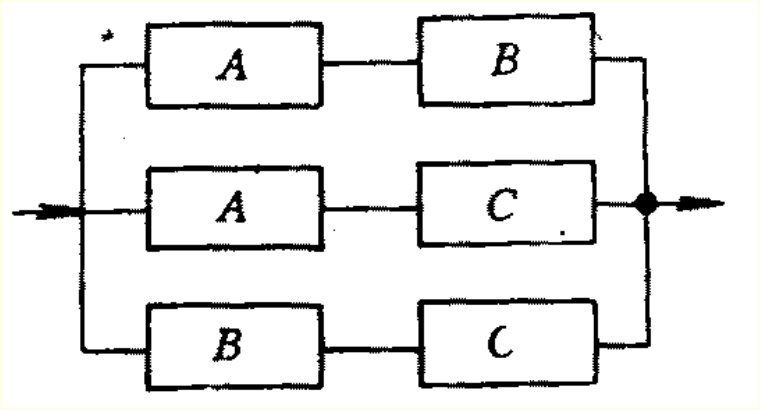
三模表决

多数表决系统：一个系统将三个及以上（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。若并联单元为3，则称为三模冗余（或称2/3表决系统）；若并联单元为N>3，则称为N模冗余



2/3表决系统

三模冗余：由3个相同模块和1个表决器构成，将2个模块出现相同的输出作为系统的输出，可以容忍一个模块出故障



2/3表决系统的等效串并联模型

若三个模块的可靠度均为R，则可以证明三模冗余的可靠度为

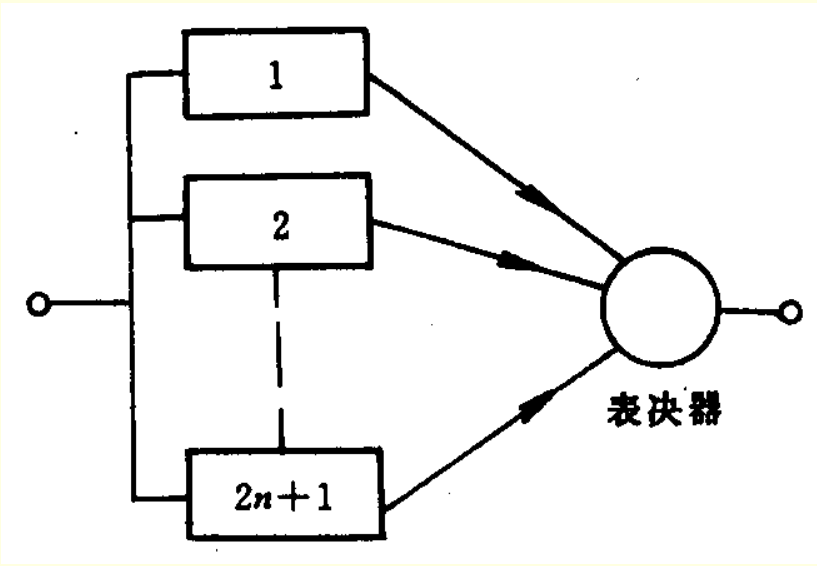
$R_{3,2} = 3R^2 - 2R^3 > R$（$R > 0.5$时）

只有当单模可靠性较高时，2/3系统才具有比单模更高的可靠度

7.2.4 表决冗余

N模表决

N模冗余：由N=2n+1（n=正整数）个模块和1个表决器构成，将(N+1)/2个模块出现相同的输出作为系统输出，可以容忍（N-1）/2个模块出故障



若在构成系统的2n+1（n=1,2,…）个单元中，使系统正常工作必须的最小单元数为k，每个单元的可靠度、失效率均为R(t)、λ，表决器的可靠度、失效率为R_m、λ_m，且都服从指数分布，则

$$R_{system}(t)=\left\{\sum_{i=0}^{2n+1-k}C_{2n+1}^{i}R^{2n+1-i}(t)\cdot[1-R(t)]^{i}\right\}R_m=\left[\sum_{i=0}^{2n+1-k}C_{2n+1}^{i}e^{-\lambda t(2n+1-i)}\cdot\left(1-e^{-\lambda t}\right)^{i}\right]\cdot e^{-\lambda_m t}$$

7.2.4 表决冗余

n中取k(G)系统

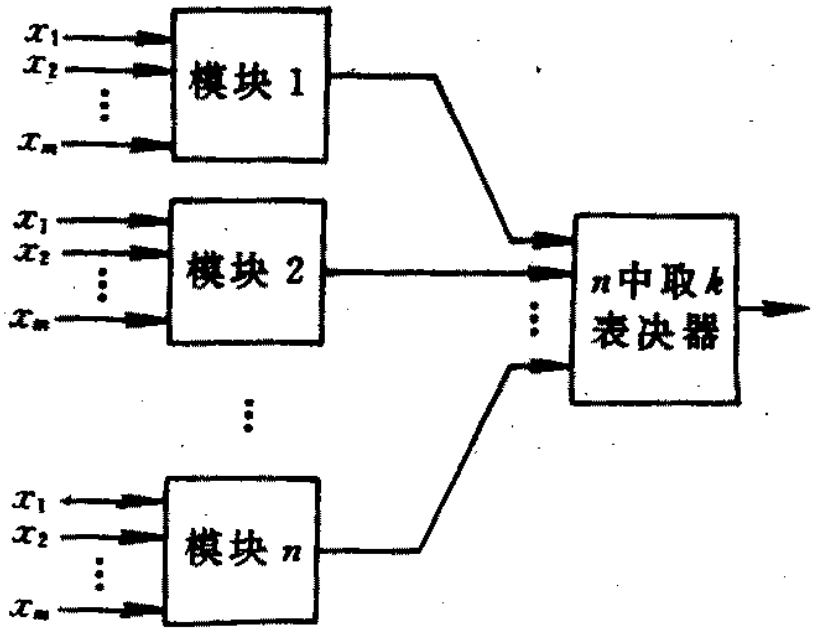
系统由n个部件构成，而系统成功地完成任务只需要其中的k个部件正常工作。这种系统称为k/n(G)系统（G表示系统完好），或称为n中取k表决(1≤k≤n），当失效部件数≥n-k+1时，系统即失效

实际上，k=1时的1/n(G) 系统就是并联系统； k=n时的n/n(G)系统就是串联系统；k≥(n+1)/2的k/n(G)系统就是多数表决系统

若构成系统的n个单元的失效率均为λ，可靠度均为R且符合指数分布，即$R=e^{-\lambda t}$,并假定表决器的可靠度远大于冗余单元的可靠度，则可证明$k/n(G)$系统的

$$\mathrm{MTTF}=\frac{1}{n\lambda}+\frac{1}{(n-1)\lambda}+\frac{1}{(n-2)\lambda}+\cdots+\frac{1}{k\lambda}$$

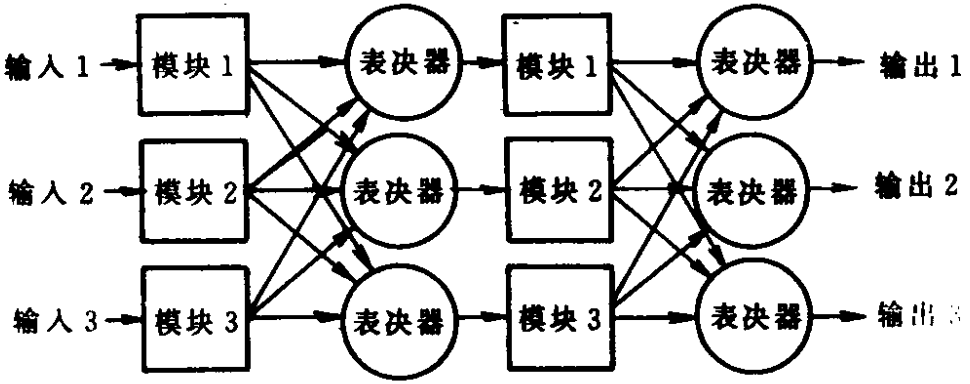
$$R_{n,k}=\sum_{i=k}^{n}C_n^i R^i(1-R)^{n-i}$$

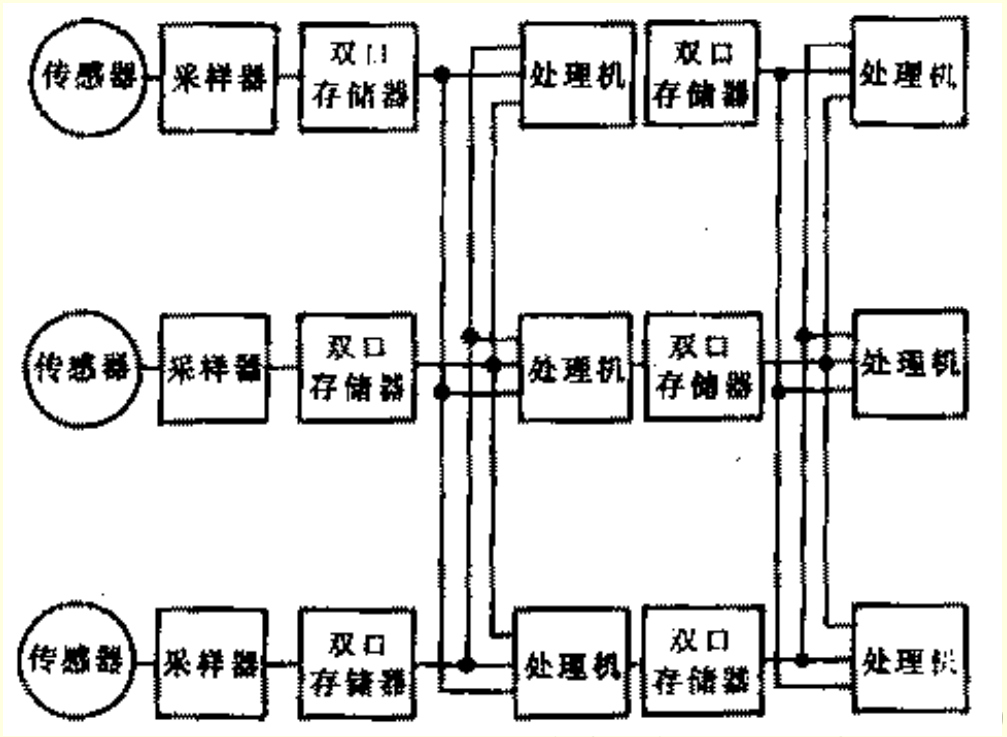


7.2.4 表决冗余

三重表决冗余系统

- 表决器的可靠性一定要远优于模块的可靠性。如果表决器的可靠性比单一模块的可靠性差，则无论几模冗余，其可靠性都不会比单一模块的可靠性好。在这种情况下，可采用右上图所示的三重冗余表决结构，右下图是一个三重冗余表决系统的实例



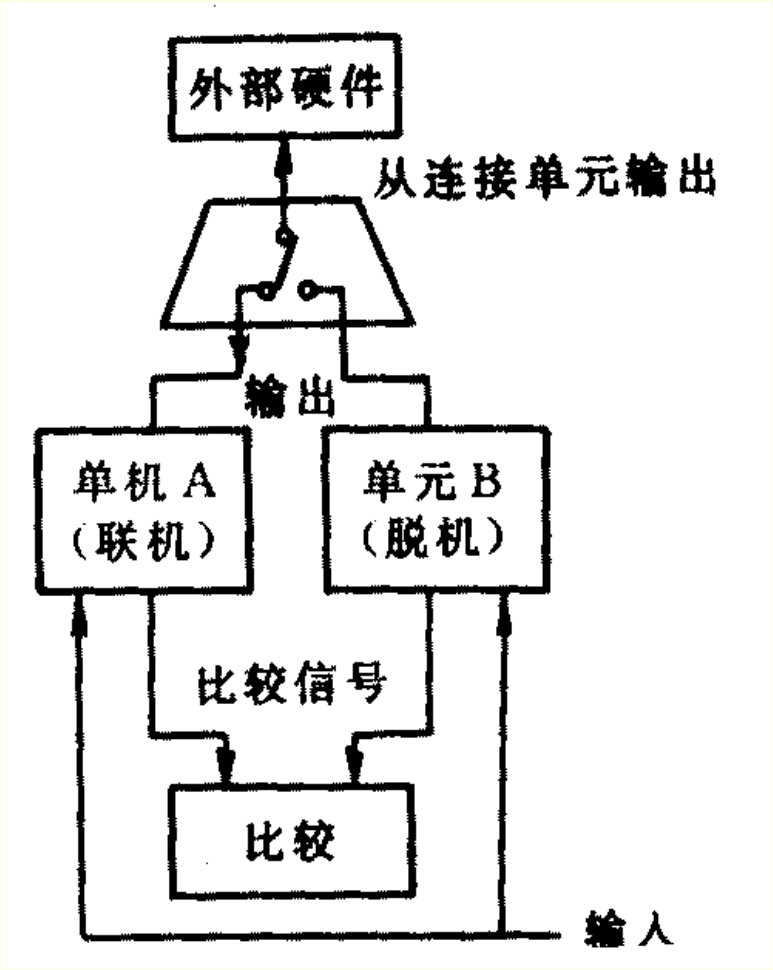


计算机数据采集三重表决冗余系统→

7.2.4 表决冗余

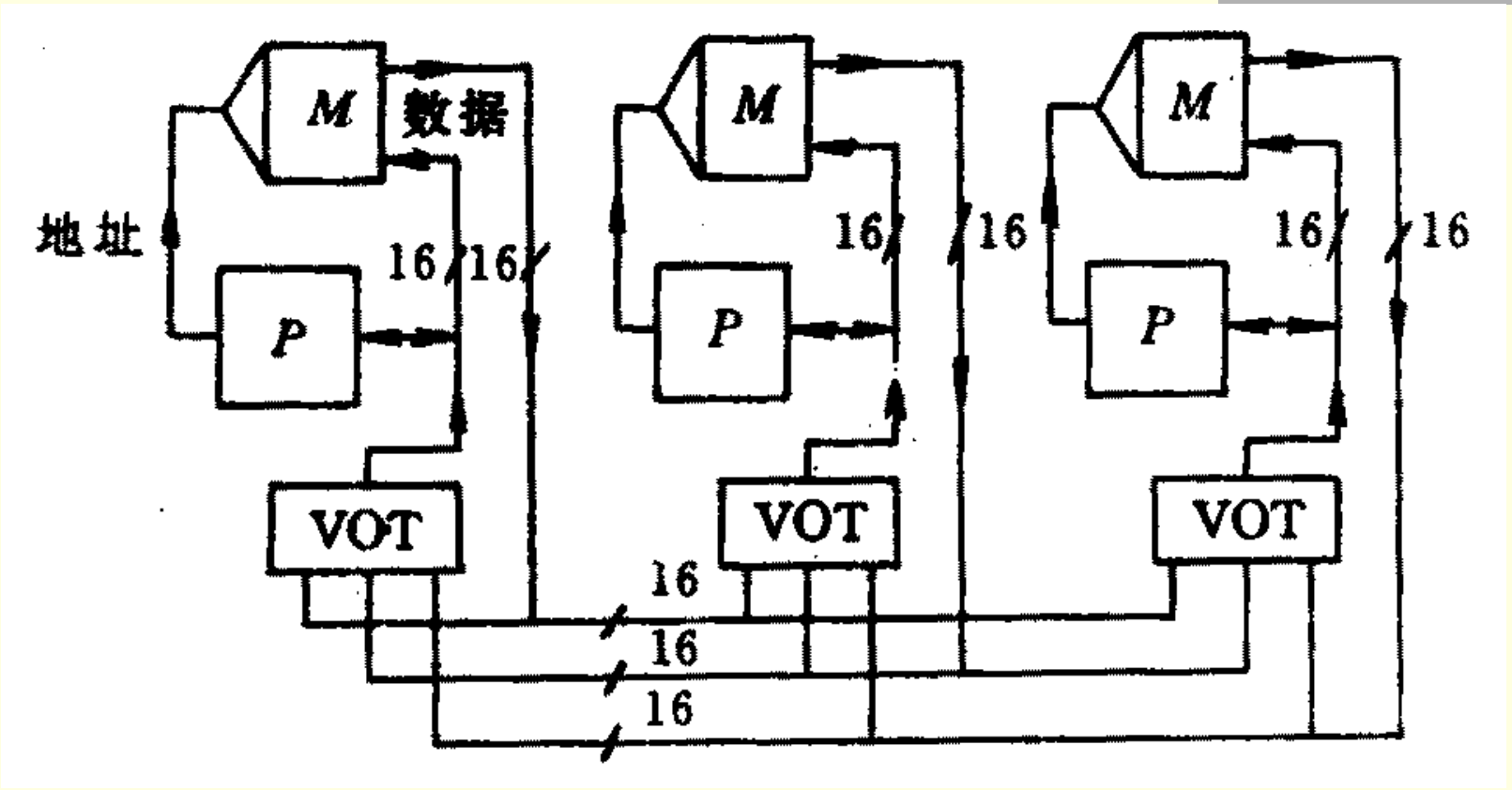
双机比较

- 双机比较可视为一种简化的表决冗余系统。两个相同的单元执行相同的任务，但只有一个连接到系统的输出。在系统工作的同时，每个单元都会输出一个比较信号，如果发现两个单元的比较信号不一致，说明至少有一个单元有故障，然后可通过自诊断程序或是外部仲裁器来判断哪一个单元出现了故障



7.2.4 表决冗余

2/3冗余系统示例

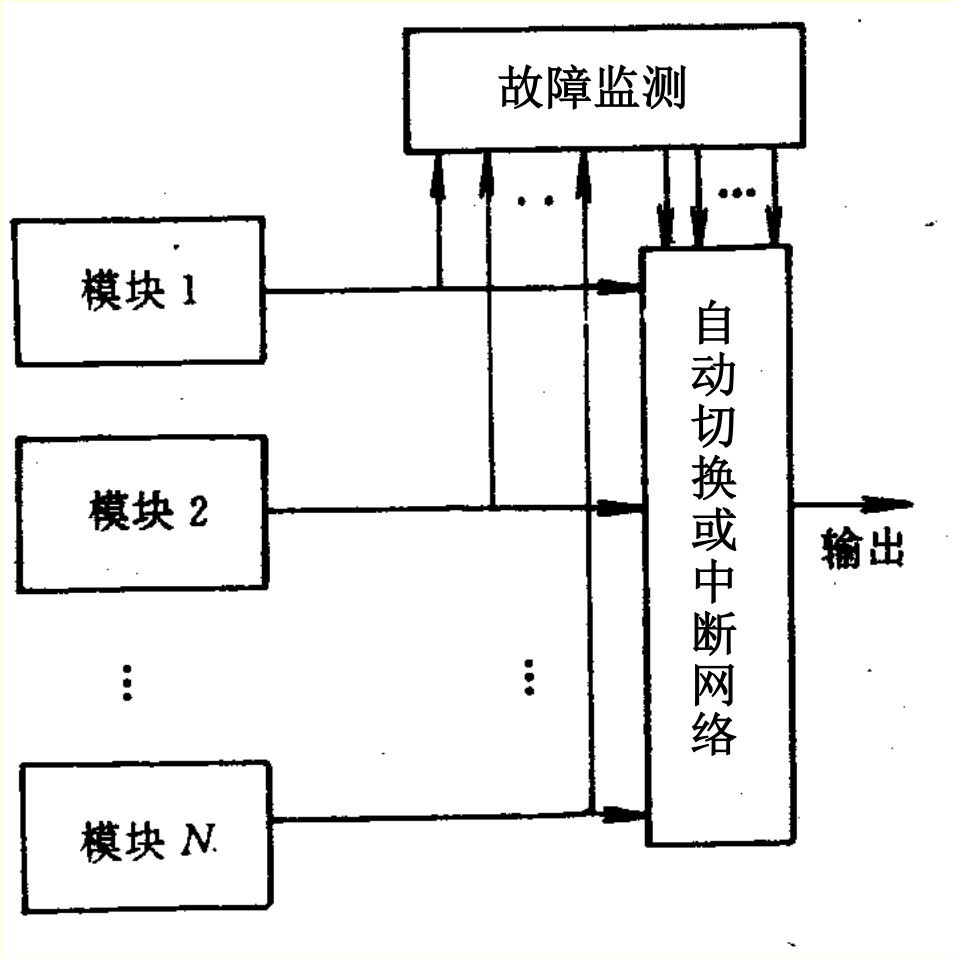


由存储器（M）取出的数据经表决器（VOT）后送往处理器（P），处理运算后的数据分别送回各自的存储器。数据如果出现单个错误，就会在此系统中自动得到纠正。图中的数据传输线均为16位

7.2.4 表决冗余

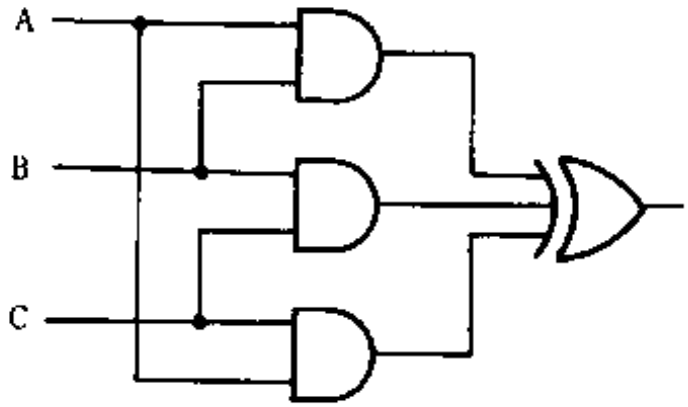
三模-单模系统

- 在三模冗余系统中，某一模块出现永久性故障时，必须及时切除，否则当另一模块又出现瞬间故障时，表决失误，反而使可靠性降低。若只切除出现永久性故障的那一模块，则当剩下的两个模块之一再出现故障时，表决器无所适从。所以，此时应切除两个模块，成为单机系统运行。这样的冗余系统称为三模-单模系统
- 对于三模-单模系统以及更复杂的冗余系统，应增加故障检测和通道切换单元，以便能够及时获得故障信息，并及时切除故障模块或者自动投入备用模块



7.2.4 表决冗余

- 对于数字系统，可采用硬件表决和软件表决两种方式。硬件表决速度快，但需增加硬件，造成成本、功耗、重量和体积的上升，而且算法固定；软件表决速度慢，但成本低，算法灵活，而且只能用于带处理器的数字系统
- 对于故障监测和自动切换，也可以采用硬件与软件两种方式来实现。硬件方式速度快，但会增加开销；软件方式不能及时发现瞬态故障，而且在软件进行故障监测期间，系统工作要短时中断



一位数字量的硬件2/3表决器

7.2.5 混合冗余

开关冗余+表决冗余

示例:此混合冗余系统由3工作、2备份的开关冗余系统与2/3表决系统结合而成。差异比较检测器用于比较各模块的输出与表决器的输出是否一致，从而选择正确的单元输出为系统输出。一旦发现三个工作模块之一发生故障，则由备用模块替换

作为一般情况，设开关冗余为n工作、s备份（总模块数N=s+n），表决冗余为k/n(G)，k=(n+1)/2，各个单模块的可靠度均为R，忽略开关网络、表决器和检测电路的失效率，则此系统的可靠度为

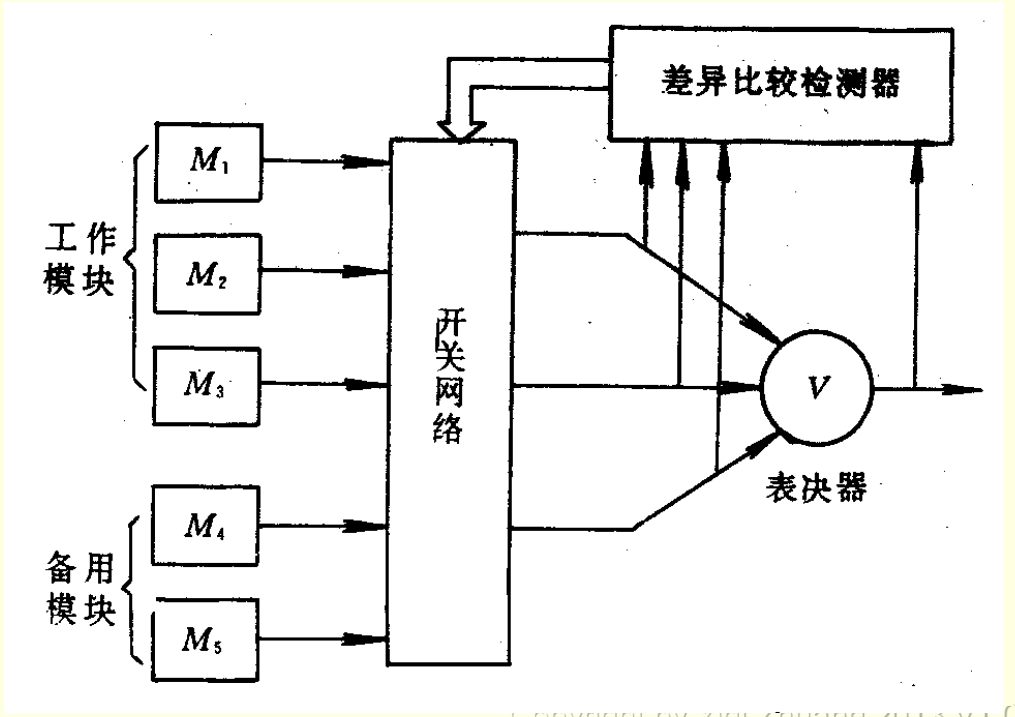
$$R_{混合}=\sum_{i=k}^{N}C_N^iR^i(1-R)^{N-i}$$

对图例，n=3, s=2，N=5, k=2, 并设R=0.9，可计算得到

$$R_{混合}=\sum_{i=2}^{5}C_5^iR^i(1-R)^{5-i}=0.99854$$

明显大于单纯的2/3表决系统可靠度

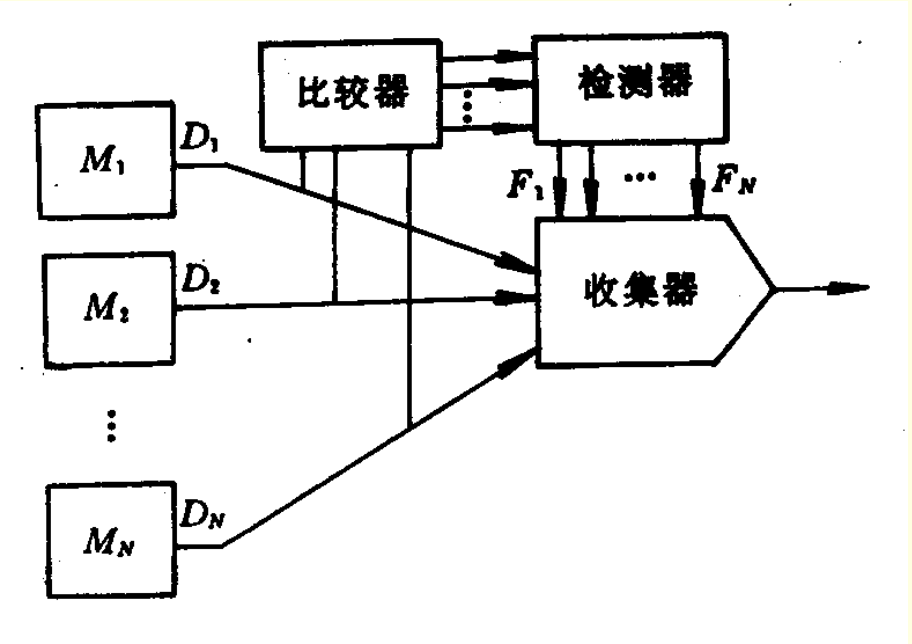
$$R_{3,2}=\sum_{i=2}^{3}C_3^iR^i(1-R)^{3-i}=0.972$$



7.2.5 混合冗余

筛模冗余

- 由N个模块组成相同的工作通道，各通道的模块相同并同时工作，形成N通道冗余结构。比较器不断地比较各通道的输出信号。若某一通道的输出与其它不同，即被筛选除去，系统就变成了N-1冗余结构。直至仅剩两个通道，这时系统的两个通道仍可进行相互比较，校验是否一致。因此，该系统运行N-2个通道（模块）出现故障



- 三通道的筛模系统与三模表决系统具有相同的可靠性和容错能力，但前者可使故障通道自动退出系统，并给出该通道的故障信息，这比一般的三模表决系统更便于维修。
- 多余三通道的筛模系统比n>3的k/n(G)表决系统的可靠度高，但它不允许同时发生两个以上的故障，否则将引起检测器工作混乱，而k/n(G) 系统允许(n-k)个模块同时发生故障

7.3 潜在通路分析

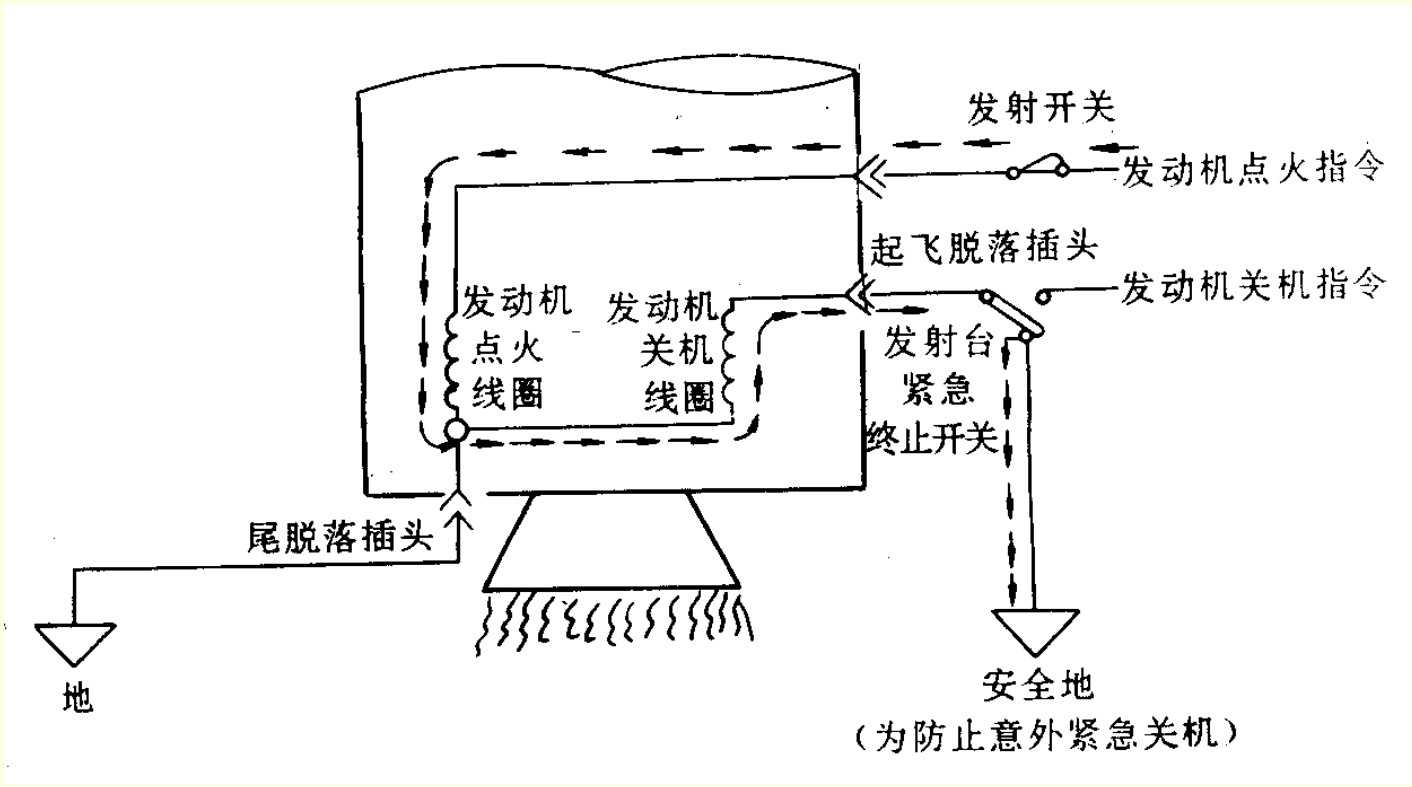
7.3.1 来源与类型

7.3.2 分析方法

7.3.1 来源与类型

引例

美国红石火箭有着50次以上成功发射的记录，但在1959年11月21日发射时，给出发射命令和发动机点火后，火箭升离发射台几英寸后发动机突然熄火，导致发射失败。事后发现这是由于发动机控制线路中存在潜在通路所致



如果火箭尾部脱落插头和起飞脱落插头同时脱落，则系统将会正常工作；如果前者比后者先脱落，就会出现如图中虚线所示的潜在通路，点火指令诱发关机线圈（继电器初级）流过反向电流，从而启动关机指令，导致发动机异常关机

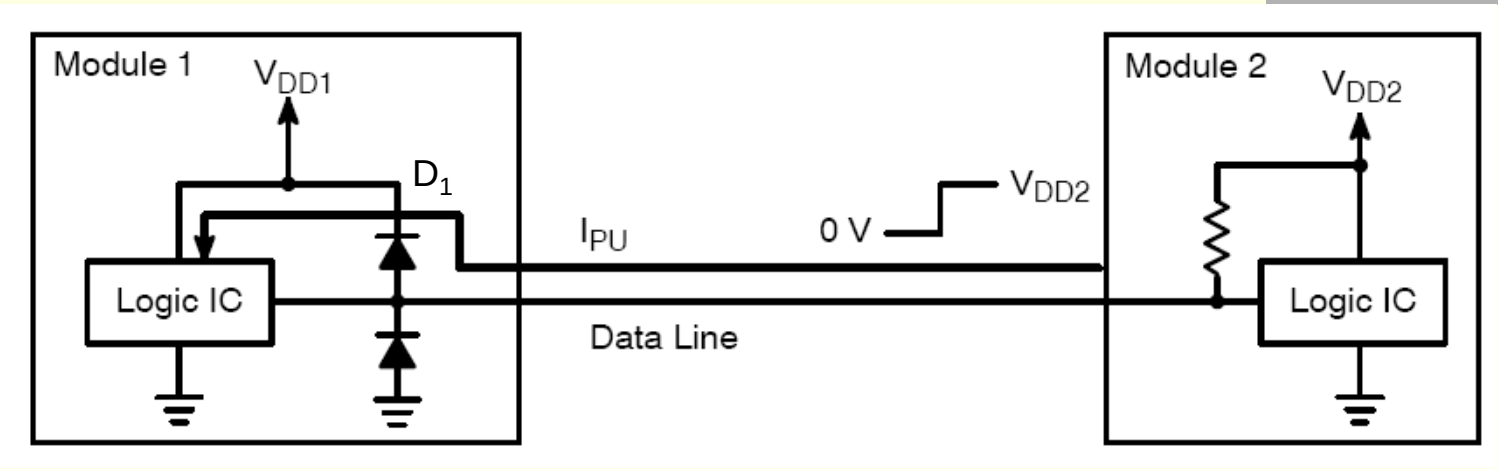
7.3.1 来源与类型

潜在通路的来源

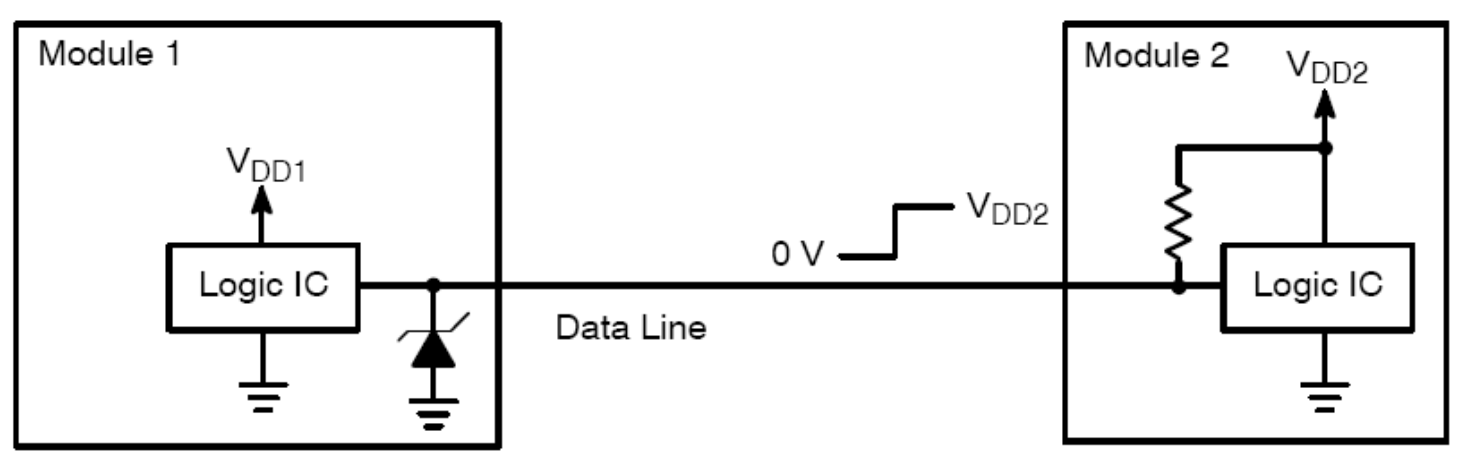
- 定义
  - 潜在通路：在某种条件下，系统或电路出现的未预期（通常也是不希望有的）的通路。它的存在会使期望功能异常，或者产生非期望功能
  - 潜在通路可以出现在控制电路、数字逻辑系统和软件系统中
- 表现形式
  - 潜在电路：潜在的电流通路，它的存在会引起不希望的功能发生或者抑制一个规定功能的发生
  - 潜在时间：某功能在不希望的时间内存在或发生
  - 潜在指示：引起混淆或不正确的状态指示，导致错误的操作
- 形成原因
  - 分系统设计人员对系统整体缺乏全面、深入的认识
  - 对设计评审后所做的更改将对各系统带来的影响未进行充分的审查
  - 其它设计失误（设计缺陷、设计图错误等）

7.3.1 来源与类型

潜在电路



若模块2的电源电压高于模块1（V_{DD2}>V_{DD1}），则当模块1输入高电平时，模块1的输出保护二极管D_1就会导通，导致模块2给模块1供电，并形成从模块2到模块1的供电电流I_{PU}，可能会导致模块1功能失控。此类通道称为“潜在通道”。

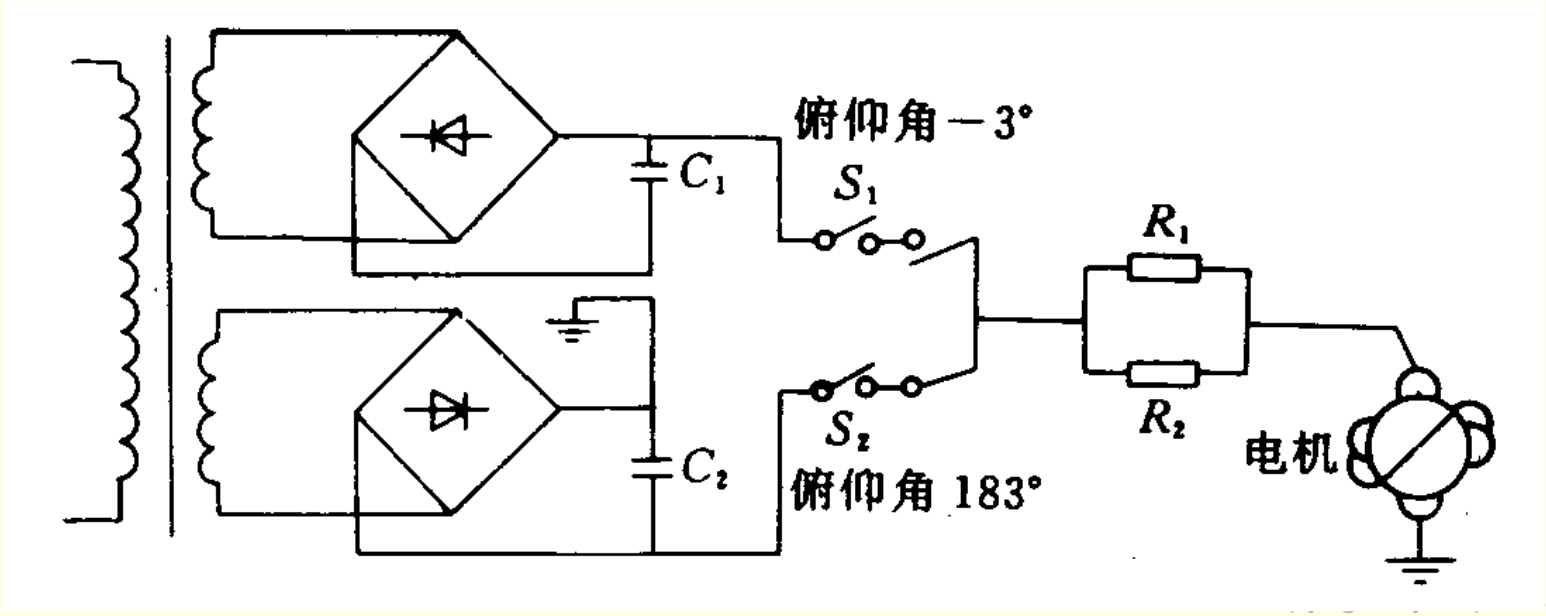


采用箝位二极管作为模块1的输出保护，可避免上述问题的发生

7.3.1 来源与类型

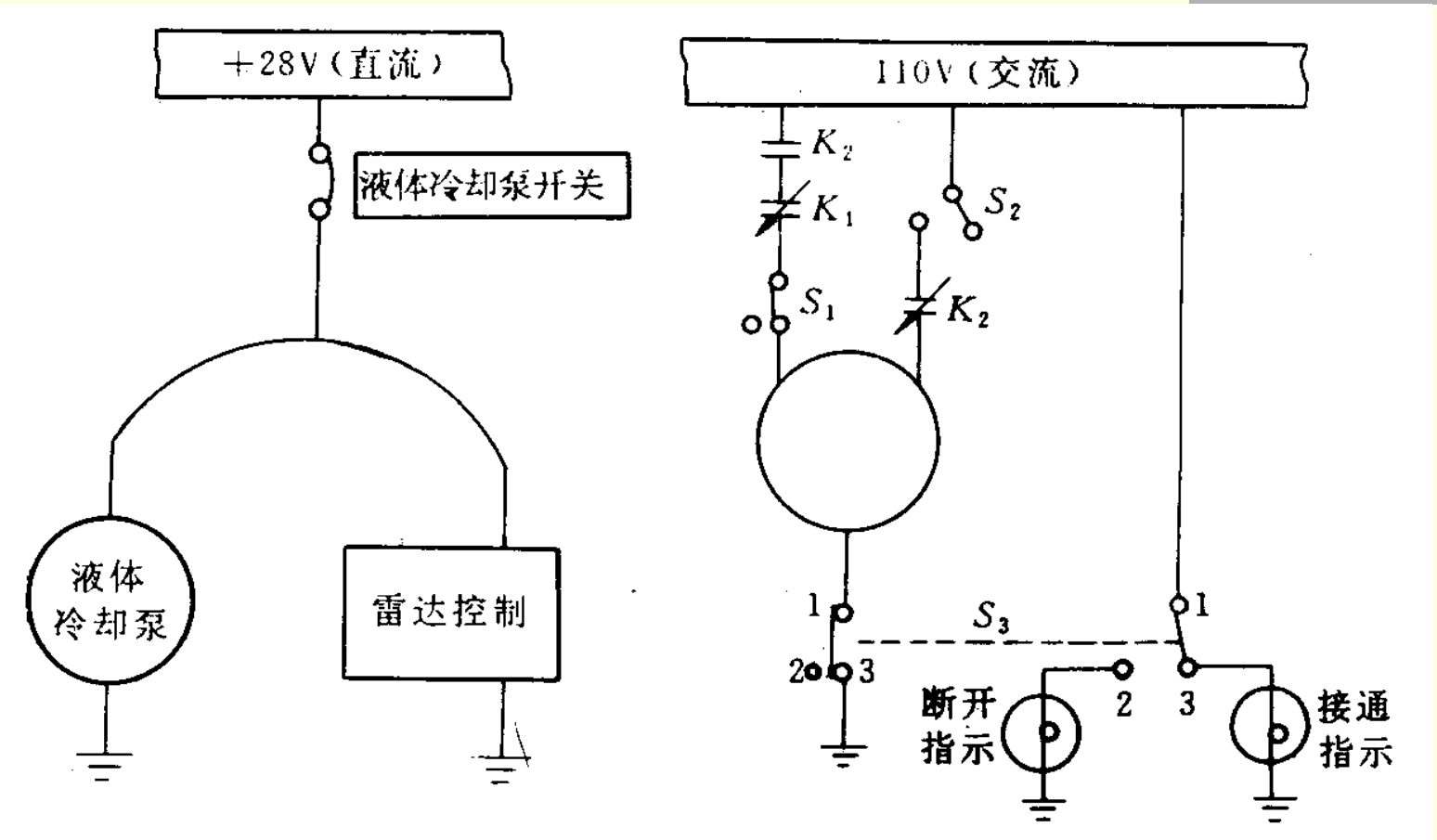
潜在时间

- 某观测雷达系统的保护控制电路，用于防止天线在俯仰时因超过角度界限而损坏
- 正常功能：控制天线在-3°~+ 183 ° 间俯仰
  - 天线转到-3° 时，微动开关S1接通，使天线顺时针旋转；一旦离开-3° 时，S1断开，使天线俯仰方向不受控制电路的影响
  - 天线转到183 ° 时，微动开关S2接通，使天线逆时针旋转；一旦离开183 ° 时，S2断开，使天线俯仰方向不受控制电路的影响
- 潜在时间危害：天线俯仰齿轮箱的速比设计发生差错时，S1和S2有可能在某一特定时间和特定位置上同时接通，使电源负载短路，从而烧毁整个控制系统的电源



7.3.1 来源与类型

潜在指示



某机载雷达：K仅标志为液体冷却泵开关，实际同时控制着雷达电源，当操作人员断开液体冷却泵时，无意中将雷达电源也切断了

声纳供电系统的指示灯：S3的位置使接通指示灯亮，似乎表明电机电源接通，但事实上电机电源是否接通还与开关S1、S2状态有关（图中状态使电机不接通）

7.3.2 分析方法

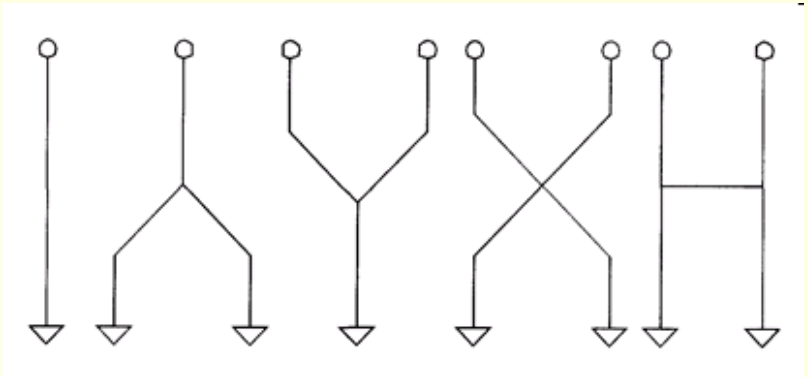
潜在通路分析的目的与步骤

- 潜在通路分析（Sneak Circuit Analysis，SCA）的目的

  在假定所有部件都正常的条件下，找出哪些南引起功能异常或者抑制正常功能的潜在通路，为改进设计提供依据

- 潜在通路分析的步骤

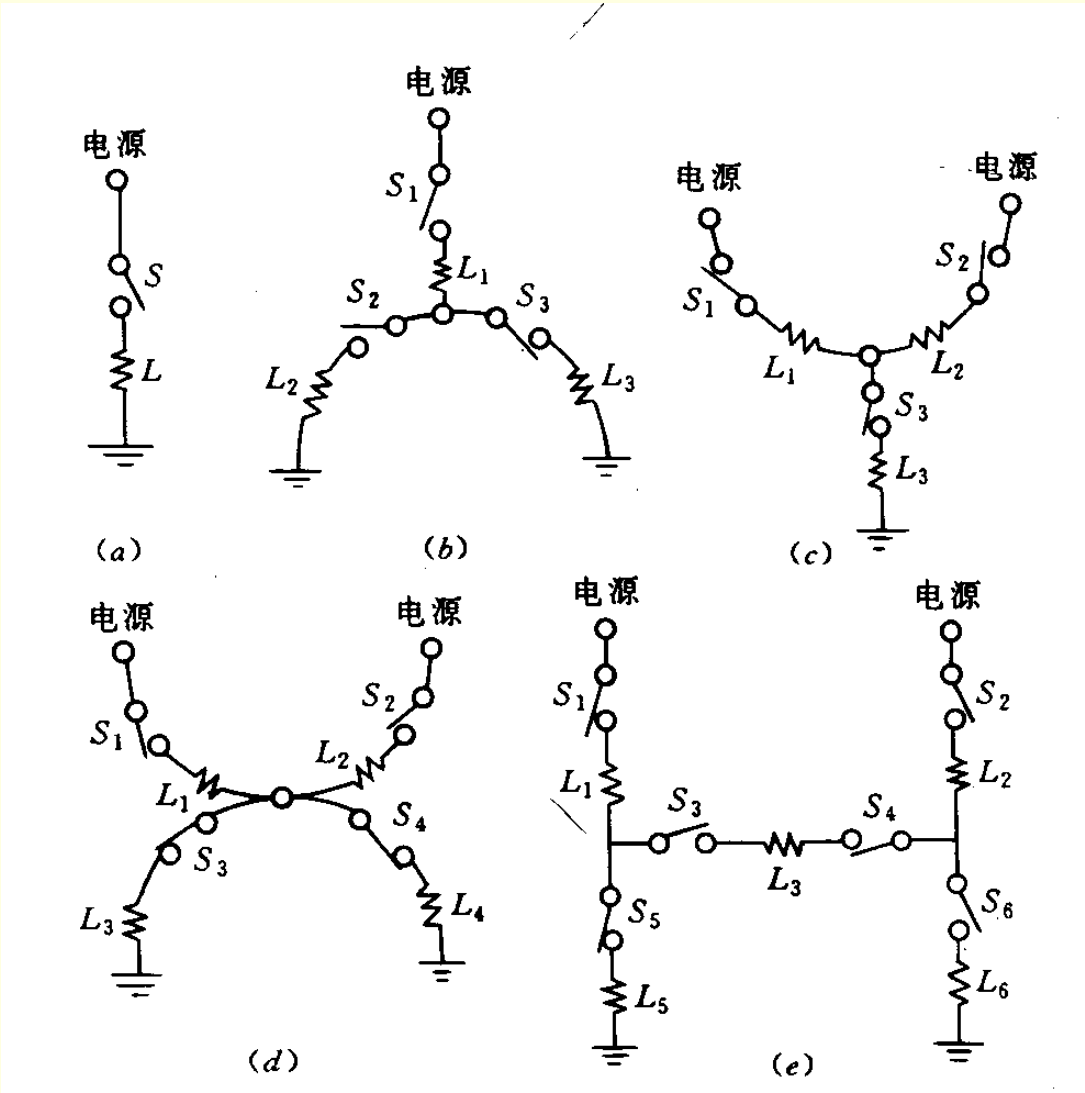
1. 获取电路所存在的一切通路的信息：保留接通电源和接地线的通路，略去其它无关的路径（如保留开关、阻容元件、有源器件、继电器等，略去只起电路连接作用终端板和接插件等），使电路简化，便于分析
2. 网络树的绘制：将所有电源置于顶端，把接地置于底部，并使电路按电流自上而下的规律排列，形成网络树。网络树实际上代表着简化后的电路拓扑结构。任何电路的网络树均可用下图所示的五种基本拓扑图形的组合表示
3. 功能仿真与分析：通过静态与动态仿真，确定网络树上各元件的工作状态，找到可能的潜在路径以及由此路径导致的电路功能缺陷
4. 设计的改进与优化：修改与优化设计，切断潜在通路



网络树的五种基本拓扑结构。自左到右：单线，接地圆弧，电源圆弧，组合圆弧，H形

7.3.2 分析方法

网络树结构示例



- 单线结构可能出现的潜在通路
  - 当需要负载L时，开关S处于断开状态
  - 当不需要L时，S处于闭合状态
  - L接入电路时，S显示断开
  - L脱离电路时，S显示闭合
- H形结构可能出现的潜在通路>100条，其中6个开关的组合状态可能出现的潜在通路就有64种之多
- 目前所识别出来的潜在通路，将近50%是来自H形网络（如本节引例），因此设计时应尽量避免这种结构

7.3.2 分析方法

潜在通路分析的特点

- 潜在通路分析是在假定所有元器件与电路部件正常工作的前提下进行的，不考虑由于元器件质量缺陷或者不期望的环境应力所引起的潜在电路
- 潜在通路分析只注重系统将发生何种故障，不注重系统如何正常工作；只注重构成系统的各个元器件之间的连接关系及其相互影响，不考虑元器件自身的可靠性
- 潜在通路分析应针对系统最终完成的底层具体电路（如生产图、安装图、布线图等），而不是设计中间层次的逻辑图、功能框图和电源图。在较高一级图纸转换到较下一级图纸的过程中，引入潜在状态的可能性较大
- 潜在通路分析的计算工作量通常很大，一般都借助计算机和EDA工具来完成

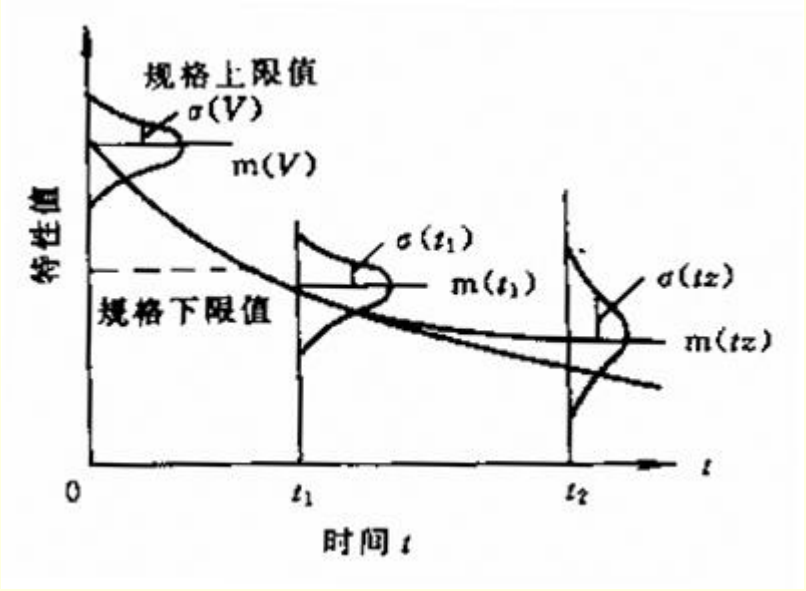
7.4 容差设计

7.4.1 作用

7.4.2 方法

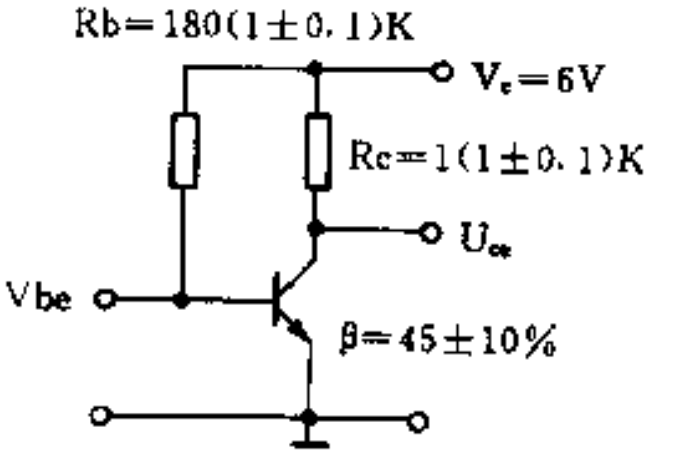
7.4.1 作用

- **容差**
  - 元器件参数值相对于额定值的偏差
- **容差的来源**
  - 初始偏差：元器件工艺一致性无法达到理想化程度，导致不同批次元器件性能参数存在一定的差异（通常文献中所称“容差”仅指初始偏差，为狭义的容差，本书定义的容差为广义的容差，包括了初始偏差、温度漂移和时间漂移等）。多数元器件参数的初始偏差满足正态分布，它可由均值m和标准差σ来表征
  - 环境条件：环境条件的变化导致元器件参数的变化，最典型的是元器件参数随温度的漂移
  - 退化效应：经过若干时间的工作或者存储后，元器件参数逐渐发生不可逆的变化，即元器件参数随时间的漂移
- **容差导致的后果**
  - 电路功能部分失常或者全部失常
  - 电路性能指标变化或下降



7.4.1 作用

1. 系统设计：确定电路的结构，实现电路的功能。如图电路，通过确定其电路的拓扑结构，就可以确定其输入电压与输出电压的关系（ $U_{ce} = V_c - \beta R_c \frac{V_c - U_{be}}{R_b}$ ）
2. 参数设计：确定电路各元件参数的中心值，实现电路的性能指标。如图电路，通过确定各个电路元件的额定值（均值），就可以确定其在固定的输入电压（如0.7V）下，输出电压的额定值（如4.675V）
3. 容差设计：保证一定参数分布条件下的电路性能指标。进一步，在保证电路性能指标的前提下，如何使允许的元器件参数变化范围达到最大？如图电路，在各电路元件的容差确定之后，可算出输出电压值的最大变化范围为 4.02~5.157V



7.4.1 作用

- 若电路的允许容差大，则电路的可靠性高，且对电路元件参数的精度和稳定性要求低，元件成本低，但设计难度大；若电路的允许容差小，则电路的可靠性差，且对电路元件参数的精度和稳定性要求高，元件成本高
- 使电路的性能对于元器件参数的离散以及使用环境的变化（如温度、辐射、振动）不敏感的设计叫做健壮设计（robust design）。容差设计是健壮设计的一种
- 参数设计是容差设计的基础。当容差设计发现难以解决的矛盾时，往往再重做参数设计，甚至修改系统设计，以求得系统在功能、性能指标、可靠性和成本方面的最佳平衡

7.4.2 方法

标准差综合法

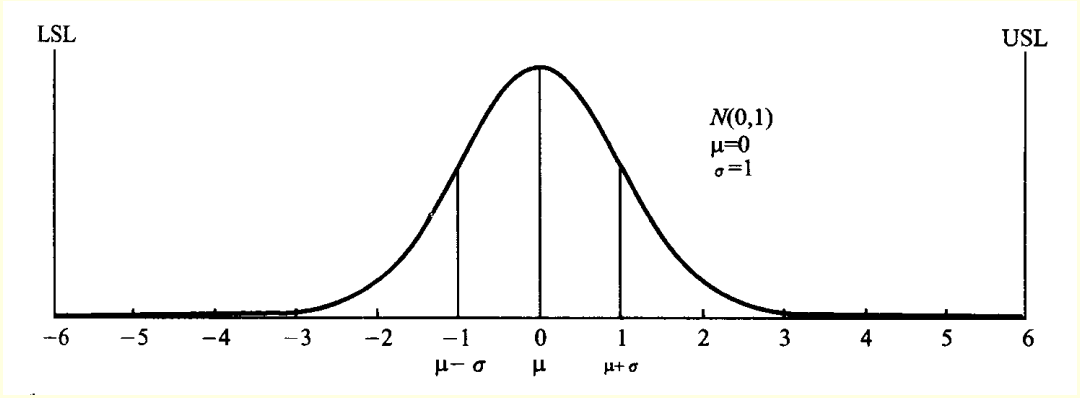
- 方法：假定元器件参数离散符合正态分布，根据电路灵敏度，计算电路性能指标离散的分布范围及规律，从而判断是否能够满足要求
- 基本关系式：若元器件的参数是相互独立的随机变量Xi，则电路的性能参数也是一个随机变量Y

当$Y=f(X_1,X_2,\cdots,X_n)$，各$X_i(i=1,2,\cdots,n)$相互独立，且均值和方差分别为μi和σ_i^2时，

Y的均值 $\mu_Y=f(\mu_1,\mu_2,\cdots\mu_n)$

Y的方差 $\sigma_Y^2=\sum_{i=1}^{n}\sigma_i^2\left[\frac{\partial}{\partial X_i}f(X_1,X_2,\cdots,X_n)\right]^2$ 式中，$\frac{\partial f}{\partial X_i}$是电路灵敏度

- 特点：比最坏情况法更接近实际情况，因为可以证明在组成整机的元器件很多，且元器件是稳定、批量生产的产品时，元器件参数近似地服从正态分布。不过，使用此方法必须事先知道元器件参数的正态分布参数（均值u，标准差σ），而且并非所有元器件参数均严格符合正态分布

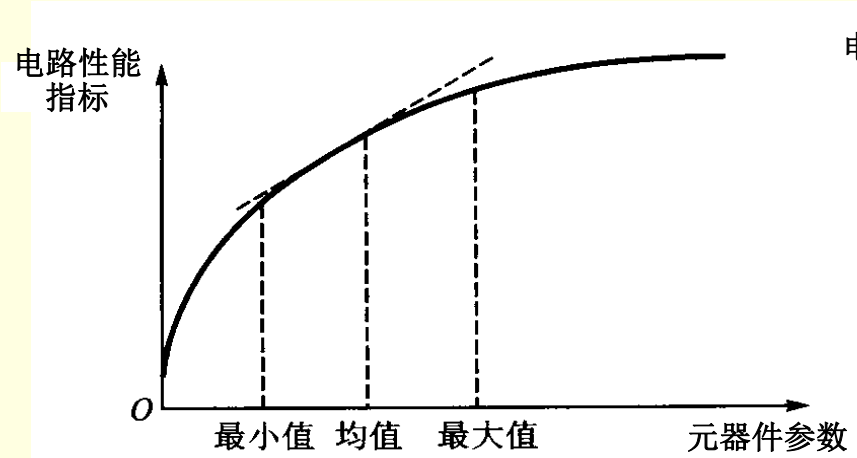


正态分布图

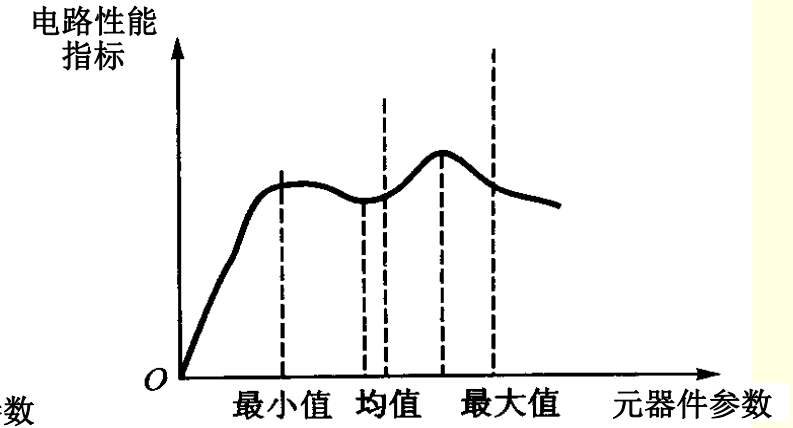
7.4.2 方法

最坏情况法

- **方法**：元器件参数Xi取最大变化值（最大值，最小值），根据电路性能指标Y随元器件参数变化而变化的规律（灵敏度$\partial Y/\partial X_i$），计算电路性能指标Y离散的最大变化值，从而判断是否能够满足要求（也称为最坏情况电路分析WCCA或极差综合法）。若$\partial Y/\partial X_i>0$，则在决定Y的最大值时，$X_i$应取最大值；在决定Y的最小值时，$X_i$应取最小值。反之，若$\partial Y/\partial X_i<0$,$X_i$的取值相反
- **特点**：计算最为简单，得到的结果最为悲观，电路实现成本最大，但也许实际上根本不会出现（如对上述电路，采用最坏情况法得到的Uce变化范围为4.02～5.157V，采用标准差综合法得到的Uce变化范围为4.325～5.025V，后者出现的概率可达99.73%，因此超出此范围的可能性就很小了



灵敏度为单调函数



灵敏度为非单调函数

7.4.2 方法

最坏情况法(续)

片状多层陶瓷电容器的容差

测试项目	C0G	X7R	X7R	测试项目	C0G	X7R	X7R
初始误差	2.5%	10%	20%	高湿偏置	3.0%	12.5%	12.5%
温度漂移	2.5%	15%	15%	使用寿命	3.0%	12.5%	12.5%
耐温特性	2.5%	10%	10%	热冲击	2.5%	10%	10%
温度周期	2.5%	10%	10%	实测误差	7%	33%	37%
耐湿特性	3.0%	12.5%	12.5%				

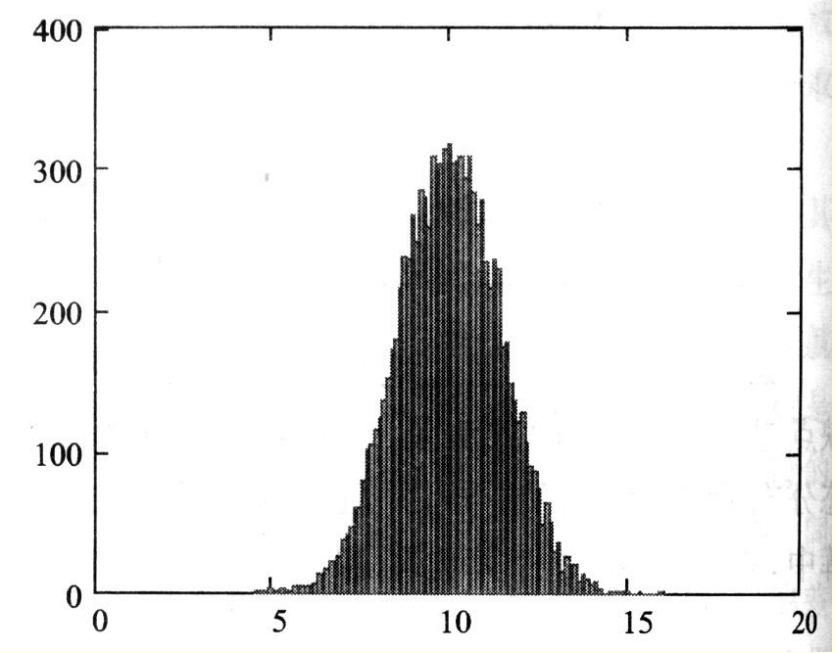
可见：

- 产生容差的因素有初始偏差、温度、湿度、偏置电压、热冲击、老化时间等
- 实测容差远小于所有容差项的和，这说明最坏情况法事实上无法出现，因为不同因素引起的容差项的变化方向不可能相同

对于元器件很少的简单电路，最坏情况法和标准差综合法的计算结果差别不大，故为计算简单可用最坏情况法；对于元器件很多的复杂电路，最好采用标准差综合法，以免无谓地增加对元器件参数精度与稳定性的要求；对于高可靠电路，为提高保险系数，可采用最坏情况法

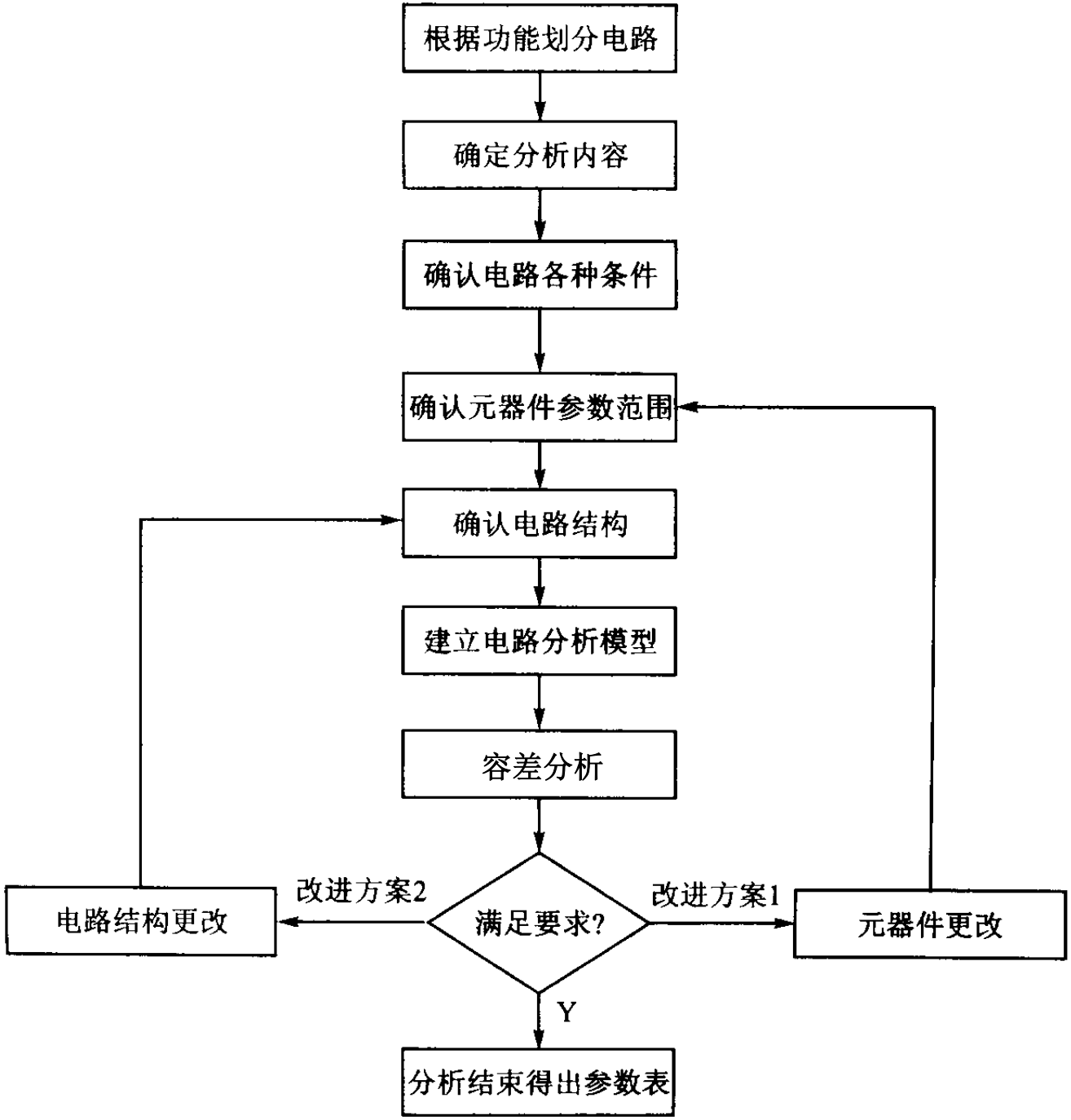
7.4.2 方法

- 方法：元器件参数在一定的概率分布范围（可取正态分布、高斯分布、均匀分布等）内随机取值，根据电路灵敏度，计算得到电路性能指标的概率分布，从而判断是否能够满足要求
- 特点：最接近实际情况，而且能获得电路性能指标的概率分布，这是其它方法所不及的，但计算复杂，运算时间长，无法手工计算，必须采用计算机仿真模拟



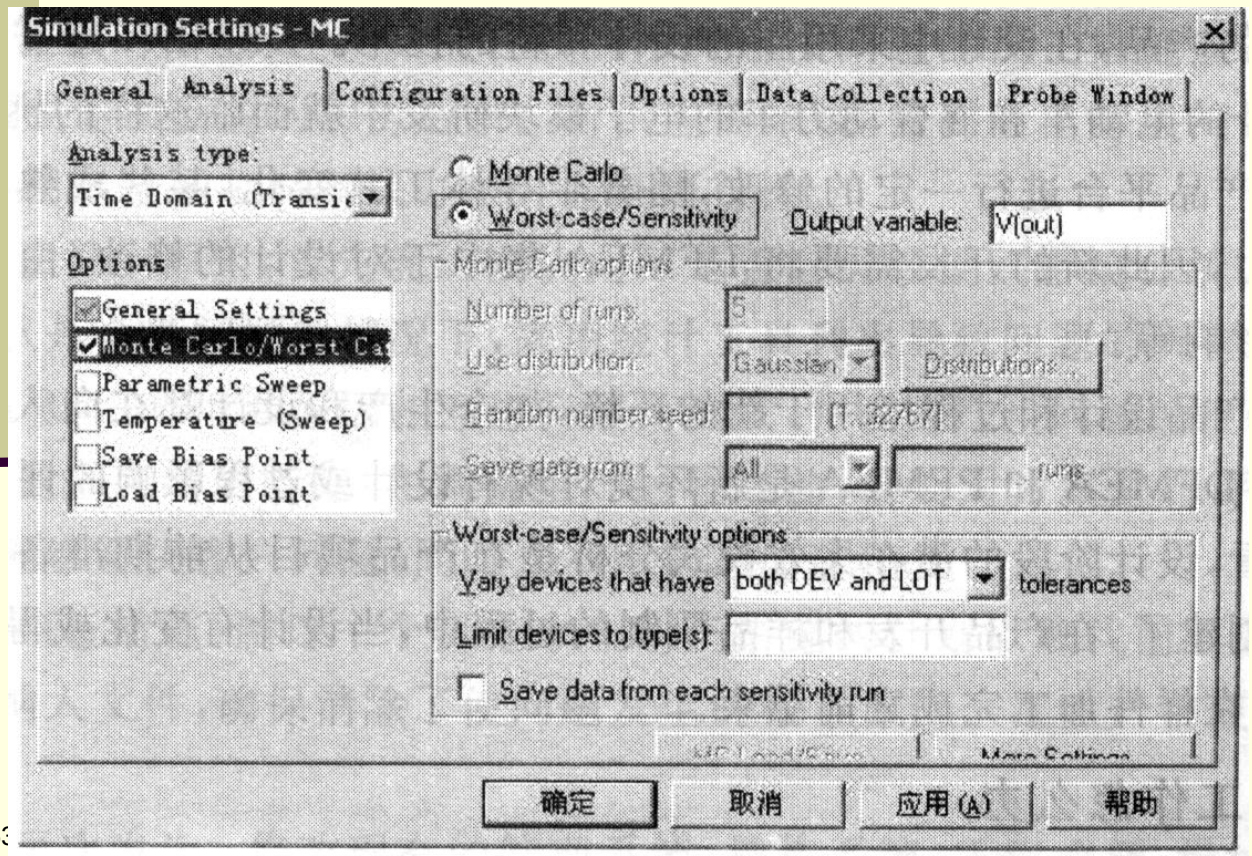
正态分布蒙特卡洛计算的电路参数分布柱状图

容差设计流程



7.4.2 方法

- 直接计算：简单直观，但只适用于规模小的电路，可借助MATHCAD等计算软件
- 计算机仿真：借助诸如PSPICE之类软件来完成，适用于规模大、拓扑结构复杂的电路



PSPICE软件容差分析界面，可选择分析方法（蒙特卡洛法还是最坏情况法）、分析类型（如时域还是频域分析）、随机取点数、分布类型等

7.5 容错设计

7.5.1 基本方法

7.5.2 常用校验码

7.5.1 基本方法

缺陷、错误和故障

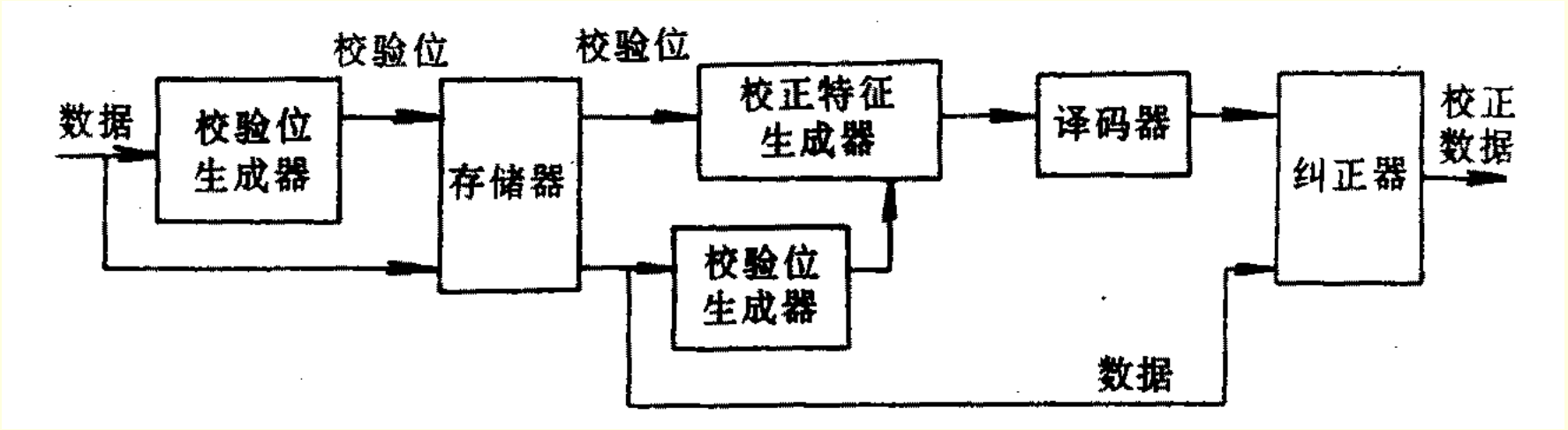
- **电子系统故障发生的过程**
  - 缺陷（fault）：一是系统的硬件或者软件中存在的内部缺陷，二是来自外部环境的过应力（雷击、静电放电、热冲击等）或者干扰（电磁噪声、辐射、振动等）
  - 错误（error）：由于缺陷而造成的系统信息或者状态的不正确
  - 故障（failure）：由于错误的发生，使得系统未能正确地提供预先指定的服务
- **缺陷、错误、故障之间的关系**
  - 缺陷引起错误，而错误导致失效。但不是所有的缺陷都引起错误，不是所有的错误都导致失效；也不是只要存在缺陷就会立即造成错误，一旦出现错误就会出现失效
  - 例如，假定系统中某根信号线由于物理短路而固定为逻辑1，那么这是一个缺陷。如果系统在运行至某个时刻，需要这根信号线传递逻辑0，但这根信号线仍然保持逻辑1，这就是一个错误。如果这根信号线与系统中的另一个信号线共同控制一个阀门，那么此信号线的错误在系统的某些状态下就可能导致阀门不能按预期的要求启闭，从而造成系统的失效

7.5.1 基本方法

- **错误的类型**
  - 先天性的固有缺陷引起的错误：俗称“硬故障”，是由元器件自身的物理缺陷、电路设计失误以及生产过程的工艺缺陷引起的错误，如数字系统中某些存储单元不能写入、某些逻辑节点固定于逻辑1或0等。此类属于永久性错误，只能通过更换元器件或者硬件冗余来纠正
  - 后天性的外在原因引起的错误：俗称“软错误”，如外界过应力或者电磁干扰引发的读、写错误。此类错误常常引发系统的瞬间性或是间歇性故障，随机出现或是偶尔出现。对数字系统中出现的此类错误，可以通过容错设计来加以纠正
- **数字信号传输中的错误**
  - 在数字信号的传输、存取、运算过程中，由于各种干扰，接收端收到的数据不可避免地会出现错误，如数据丢失、0变1、1变0等
  - 不同的用户，对数据的准确度要求是不同的。一般而言，对于传输数字话音，要求误码率为10^{-3}~10^{-4}；传输计算机之间的数据，要求误码率<10^{-8}
  - 实际能够实现的误码率，与传输所依据的通信协议、传输速率以及传输距离有关。如有线通信信道的误码率约在10^{-4}~10^{-6}，无线通信信道的误码率约在10^{-2}~10^{-3}

7.5.1 基本方法

- **容错设计的目的**
  - 容错设计用于纠正数字系统的数据错误或者降低误码率。它在发送端给待传送的数据序列（称为信息元）增加多余码元（称为监督元、校验码、检错码或者纠错码），作为接收端判断数据是否正确的依据。一旦发现错误可采取一定的方法自动纠正，也可要求发送端重发
  - 容错设计是广义的冗余设计的一部分，亦称信息容错，通常只适用于数字系统，具体的容错算法可以通过硬件逻辑电路或者软件程序来实现



带检错纠错功能的数字存储容错系统的构成框图

7.5.1 基本方法

容错设计的基本方法

- **前向纠错（FEC）**

  发送端发出带纠错码的数据序列，接收端收到后能根据编码规律自动纠正错误。此法无需反馈通道，能用于单向通信，但所需纠错码的数量会随着数据序列长度的增加而加大。

- **检错重发（ARQ）**

  发送端发出带检错码的数据序列，接收端收到后如果判断出有错误发生，就会反馈信息到发送端，要求其重发。此法只需少量的冗余码元（一般为总码元的5%~20%），就能获得很低的误码率，而且检错译码器比FEC采用的纠错译码器要简单得多，但需要反馈通道，无法用于单向传输系统，反馈也会降低系统的有效传输速率

- **混合纠错（HEC）**

  发送端发送具有自动纠错和检错能力的码，接收端对进行译码。如果错误在码的纠错能力之内，就自动进行纠错；如果错误较多，超出了码的纠错能力，就要求发送端重发。此法是FEC和ARQ的结合，兼具二者的优点，应用比较广泛

7.5.2 常用校验码

校验码的类型与数量

- **校验码的类型**
  - **线性码：**监督元和信息元之间具有线性关系，可用一组线性方程来表示
  - **分组码：**一个码字（分组）内的监督元仅与本码字内的信息元相关，主要用于数字系统和计算机内部的检错/纠错，如奇偶校验码就是一种线性分组码
  - **卷积码：**一个码字内的监督元不仅与本码字内的信息元相关，还与相邻的前N-1个码字内的信息元相关，主要用于数字通信或者数字信号较远距离传输
- **校验码的数量**
  - 校验码的检错/纠错能力与其数量有关
  - 检错只需知道一组或若干组传输数据码中是否出现错误，而无需知道错误发生在哪一个数据位，因此校验位的数量可以远小于数据位，如奇偶校验码；纠错则需知道错误发生在哪一位，因此校验位的数量必须达到一定的要求，如海明码
  - 以四位校验码为例，可以表示2^4个状态，除去表示无错误的“0000”状态外，尚有2^4-1个状态可用于判断信息码的正误，其中还包含四位校验码本身，因此最多能够判断的信息码位为

    （2^4-1）-4=11位
  - 推广至一般情况，若校验位数为K，信息位数为S，则K和S之间应满足以下关系（海明不等式）

    $2^K-1 \geqslant K+S$

7.5.2 常用校验码

奇偶校验码

奇偶校验码是一种最简单的检错码，多用于数字系统内部作为检错手段，是系统自检测的常用办法

- **一维码**
  - 发送时，在传输信息序列后增加一个校验位，使所形成的码组中的“1”或“0”的数目为奇数，称为奇数校验；若为偶数，则为偶数校验
  - 接收时，把各码元的所有位相加，对于偶数校验，若结果为“1”则说明有错误，若为“0”则说明无错；对于奇数校验，则反过来判断
  - 奇偶校验能查出任意奇数个错误，不能查出任意偶数个错误，只能检错，不能纠错，适用于信道干扰不严重、码长不大、出错概率比较小的系统

7.5.2 常用校验码

奇偶校验码(续)

- **方阵码**
  - 发送时，将信息码元分成若干小组（称为分组），每组一行，形成方阵。每行加一奇偶校验码，构成行校验码；每列也加一奇偶校验码，构成列校验码；为检查校验列和校验行本身的错误，还生成一个总校验位
  - 接收时，先按行进行奇偶校验，再按列进行奇偶校验
  - 方阵码亦称二维乘积码。与一维奇偶校验码相比，它能够检查出在连续传送的多个码元中出现的多个错码；不仅能检查出奇数个错误，也有可能检查出个别偶数个错误；不仅能检错，在错误不多的情况下能纠正部分错误

- 若信息元阵列有单个错误，则对应的行和列均不满足校验要求，而总校验位正确，据此可查出错误的码元并予以纠正
- 若信息元阵列出现多个错误，只要任意一个行和列最多只有单个错误，则仍然可以确定出出错的位置并予以纠正
- 若信息元阵列出现多个错误，而且单行或则单列中出现多个错误，则只能判定有错，但无法明确定位
- 若只有校验码本身出现错误，则可通过总校验位判断。此类情况在接收端还原时不一定需要校正

信息元阵列

1	0	0	1	1	0	0	1	0
0	1	0	0	1	0	1	1	0
1	1	0	1	1	0	0	1	1
1	0	1	1	0	0	0	0	1
0	1	1	0	1	1	0	1	1
1	0	0	0	1	1	1	0	0
0	1	0	1	1	0	0	0	1

行校验码

列校验码　　总校验码

7.5.2 常用校验码

海明校验码

- **海明校验码**
  - 在传输数据中按码距近似均匀拉大的某种规律，加入若干校验位。如果某一位出错，就会引起与之相关的校验位的值发生变化，由此不仅可发现错误，还能指出是哪一位错误，从而实现自动纠错
- **示例：**假定需传输的8位二进制码为

$D_1D_2D_3D_4D_5D_6D_7D_8$

增加4位奇偶校验位P_1、P_2、P_3、P_4，其中第i个校验位的位置为2^i-1（i=0,1,2,3），以及总校验位P_5，构成13位海明码

$P_1P_2D_1D_2P_3D_3D_4P_4D_5D_6D_7P_5$

以偶校验算法为例，各个校验位可由下式算出

$$P_1 = D_1 \oplus D_2 \oplus D_4 \oplus D_5 \oplus D_7$$
$$P_2 = D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7$$
$$P_3 = D_2 \oplus D_3 \oplus D_4 \oplus D_8$$
$$P_4 = D_5 \oplus D_6 \oplus D_7 \oplus D_8$$

$$P_5 = D_1 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_5 \oplus D_6 \oplus D_7 \oplus D_8 \oplus P_4 \oplus P_3 \oplus P_2 \oplus P_1$$

其中，每一个数据位D_j(j=0,1,2,3, …;7）都至少出现在三个P_i关系式中（P_5就是因此而追加的校验位），因此从P_i的变化可以推断出哪一个D_j出现了错误，从而为自动纠错提供了依据。具体的检错判据如下：

7.5.2 常用校验码

海明校验码(续)

- 偶校验的海明检错码及出错判断表如下

$$S_1 = P_1 \oplus D_1 \oplus D_2 \oplus D_4 \oplus D_5 \oplus D_7$$
$$S_2 = P_2 \oplus D_1 \oplus D_3 \oplus D_4 \oplus D_6 \oplus D_7$$
$$S_3 = P_3 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_8$$
$$S_4 = P_4 \oplus D_5 \oplus D_6 \oplus D_7 \oplus D_8$$
$$S_5 = P_5 \oplus D_1 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_5 \oplus D_6 \oplus D_7 \oplus D_8 \oplus P_4 \oplus P_3 \oplus P_2 \oplus P_1$$

校正位	P_5	D_8	D_7	D_6	D_5	P_4	D_4	D_3	D_2	P_3	D_1	P_2	P_1
海明码位号 / S位	H_{13}	H_{12}	H_{11}	H_{10}	H_9	H_8	H_7	H_6	H_5	H_4	H_3	H_2	H_1
S_5	1	1	1	1	1	1	1	1	1	1	1	1	1
S_4	0	1	1	1	1	1	0	0	0	0	0	0	0
S_3	0	1	0	0	0	0	1	1	1	1	0	0	0
S_2	0	0	1	1	0	0	1	1	0	0	1	1	0
S_1	0	0	1	0	1	0	1	0	1	0	1	0	1

- S_1~S_5全为0，则所有数据位未出错
- S_1~S5的编码值与表中哪一列相同，则表明哪一位海明码出错，将该位海明码改为其反码，即可纠正其错误
- S1~S5中只有一位不为0，表明是某一校验位出错，出错位就是该Si位对应的Pi位，或者是三位海明码同时出错，但后者出现的概率远小于前者

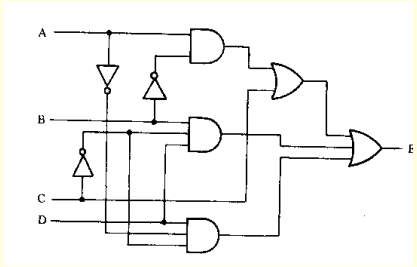
7.6 其它可靠性设计方法

简化设计

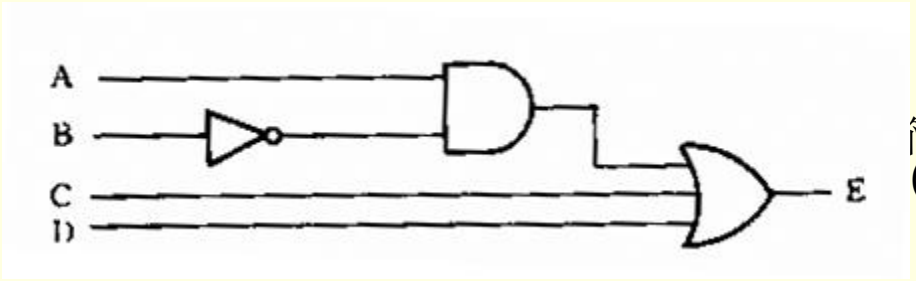
- 原理
  - 可靠性是电路及结构复杂性的函数
  - 减少元器件数及其元器件之间的互连书就能减少整体失效率，最高的可靠性来自最简单的电路
- 途径
  - 尽可能减少产品组成部分的数量及其相互间的连接关系
  - 尽可能实现元器件、零部件的标准化、系列化与通用化
  - 尽量减少元器件的规格、品种数，争取用较少的元器件实现多种功能
  - 尽可能采用经过考验的可靠性有保证的元器件
  - 尽可能采用模块化、层次化设计
- 方式
  - 算法，逻辑，线路，布图，走线。越往顶层，简化的效率越高

实例：美国F-4战斗机改型为F/A-18A战斗机时，对发动机作简化设计，使其元件数从22000个减少到14300个，在获得同样推力的同时，可靠性提高了4倍

简化前
(8个门)



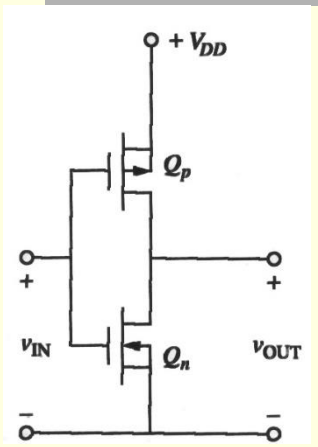
$$E = A\bar{B} + C + \bar{A}\bar{C}D + B\bar{C}D$$



简化后
(3个门)

$$E = C + D + A\bar{B}$$

7.6 其它可靠性设计方法



- 意义
  - 提高系统可靠性：功耗↓ → 温升↓ →可靠性↑
  - 实现便携产品的需要：可采用电池供电
  - 增强系统抗干扰能力：无电源线干扰，自身噪声↓
- 要点
  - 能用CMOS器件实现的，不用NMOS或双极电路来实现。因为CMOS电路的功耗远低于NMOS和双极电路
  - 能用软件完成的，不用硬件实现。这样一可以降低硬件电路的规模和复杂度，二有利于提升系统的可靠性，因为一般而言软件的可靠性比硬件要高得多，三在相同的硬件系统中，更多的功能用软件来实现，会降低系统的功耗，但同时会降低系统的工作速度
  - 能低频工作的，不要使之高频工作
  - 能低电源电压工作的，不要采用较高电压工作
  - 能采用节能工作方式的，不要采用标准工作方式

7.6 其它可靠性设计方法 电路实现形式的考虑

- 多个通道共用一个电路或器件，但要注意减少元器件不能增加其他器件的负担（应力、负载能力等），因保护、冗余和容错等目的增加的电路不能省，共用器件应能满足多个通道的性能及可靠性要求
- 多采用集成电路，少采用分立器件。集成电路与完成同样功能的分立元件PCB组件相比，焊点少，一致性高，密封性好，失效率要低的多
- 多采用规模大的芯片，少采用规模小的芯片。同样可减少互连线和焊点数量，也有利于提升可靠性
- 能用数字电路实现的，不用模拟电路完成。数字电路的噪声容限高，抗干扰能力强，失效率优于同等规模的模拟电路

END

第7章 系统级可靠性设计方法

主讲：庄奕琪