电子设计
可靠性工程

第1章 电子可靠性设计基础

主讲：庄奕琪

本章概要

1.1 可靠性概念

1.2 可靠性定量表征

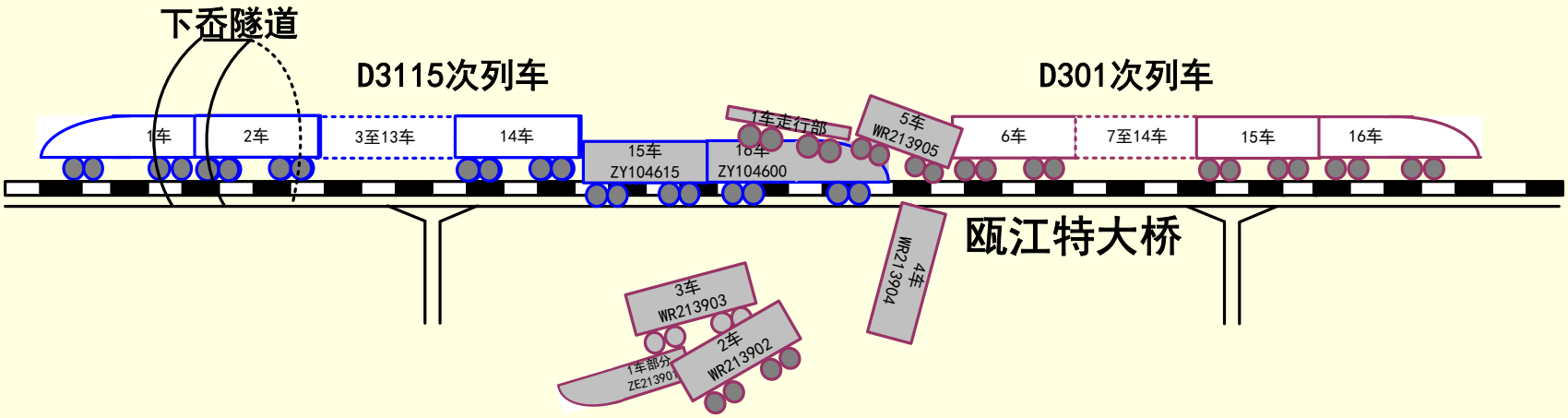
1.3 可靠性技术概要

1.4 可靠性设计

引例

甬温线动车追尾事故:经过

- 2011年7月23日20时30分，由北京开往福州的D301次动车组在浙江省温州市境内，与杭州开往福州的D3115次列车发生列车追尾事故，造成40人死亡、172人受伤，直接经济损失19371.65万元，是中国铁路史上损失最为惨重的安全事故
- 根据国务院调查组于2011年12月25日发布的《“7.23”甬温线特别重大铁路交通事故调查报告》，此事故的发生既有管理方面的原因，也有技术方面的原因，而技术方面的原因可以归结为应用可靠性设计出现了问题



甬温线动车追尾事故现场示意图

引例

甬温线动车追尾事故:技术故障

- 事故当晚，现场雷电频繁。据统计，共发生雷电对地放电（俗称“地闪”）多于340次，其中放电电流幅值超过100kA的就有11次
- 雷击一是导致轨道电路若干部件损坏，包括4个发送盒、2个接收盒和1个衰耗器；二是导致列控中心设备（型号为LKD2-T1）中采集驱动单元的电源保险管烧断（250V/5A）
- 上述故障导致轨道电路与列控中心信号传输的CAN总线阻抗下降，造成轨道电路与列控中心的通信出现异常，发送器的状态在无码、检测码、绿黄码之间随机变化
- 列控中心未能采集到列车的占道状态，导致出现故障后轨道上实际有车占用时，仍然按故障前无车占用状态显示，使区间信号灯错误地显示绿灯，从而最终导致追尾事故的发生

车站列控中心

轨道电路

列车超速防护系统

列车运行控制系统的构成

引例

甬温线动车追尾事故:可靠性设计缺陷

- 防雷设计
  - 铁路设备极易受到雷击的影响，遍布全线的供电与信号电缆、高出地面的钢轨、无处不在的交流电源与变电设备，都将成为雷电侵入的便利途径
  - 可采用防雷电保护接地、内部设备的严格屏蔽、浪涌保护元件等多种可靠性防护手段来防止雷电袭击（本课程第4章和第5章）
- 冗余设计
  - 列控中心采集电路的供电电源只有一路独立电源，一旦失效就会导致系统故障。对于要求高可靠的系统，应同时配备两路独立电源，只有当两路电源同时失效时才会导致系统故障
  - 列控中心采集电路虽然有两路输入，但采集的是同一个源点信号。应采用两路独立采集输入回路，而且对两路采集到的信号进行比较，仅当两路信号相同时，才视为正确信号（本课程第7章）
- 潜在通路分析
  - 采集驱动单元虽然将故障信息传送给了列控中心主机，但传送给主机的状态信息仍然为正常；列控中心主机虽然收到故障信息，但未采取任何防护措施。这些均属于设备设计重大缺陷
  - 设计时，应对设备可能出现的故障类型及其形成通道进行详细分析，并通过硬件和软件的改进，尽可能避免故障的发生。如无法避免，必须能够提供故障信息的发送通道，使设备的管理者及时知晓，及时采取有效措施（本课程第7章）

1.1 可靠性概念

- **可靠性**：产品在规定时间内、规定条件下完成规定功能的能力，是产品质量的重要方面
- **失效或故障**：在规定时间内、规定条件下产品失去了规定的功能
  - 可修复产品（如电子整机，经更换元器件可以修复）为故障，不可修复产品（如电子元器件，只能更换，无法修复）为失效；
  - 短时间内失去规定功能的为故障（如电磁干扰），永久失去规定功能的为失效（如雷电引发烧毁）

1.1 可靠性概念

- **规定功能**
  - 功能：产品所具备的完成指定任务的能力，定性
  - 性能指标：产品完成指定任务时能达到的数量指标，定量
- **规定时间**
  - 平均工作（储存）寿命：不可修复产品在失效前经历的平均工作（储存）时间，亦称平均无故障时间（MTTF， Mean Time to failure，亦称平均故障前时间）
  - 平均故障间隔时间（MTBF，Mean Time Between Failure）：可修复产品在相邻两次故障之间的平均时间
  - 时间单位不只是日历时间，也可能是动作次数（如开关）、重写次数（如存储器）、距离（如汽车的行车公里数）等
- **规定条件**
  - 使用条件：动力负载条件（电源、输出功率、载荷等），使用频率条件（工作频率、速度、数据率等），过电应力条件（静电、浪涌、过电压、过电流、雷击等）
  - 环境条件：气候环境（温度、湿度、空间辐射、气压等），生物和化学环境（霉菌、盐雾、臭氧、污染等），机械环境（振动、冲击、加速度等），电磁环境（电场、磁场、电磁场等）

1.1 可靠性概念

可维修性和可保障性

可用度（表征可用性Availability）

平均故障间隔时间（表征可靠性Reliability）

$$A = \frac{MTBF}{MTBF + MTTR + MLDT}$$

平均维修时间（表征可维修性Serviceability）

平均保障延误时间（表征可保障性）

- **可用性**是指可维修、可保障产品在某时刻具有或维持规定功能的能力，它比可靠性表征的范围更广。可用性有时称为可信性
- **可维修性**是指产品在固定的时间内，按规定的程序和方法进行维修时，恢复到能完成规定功能的能力
- **可保障性**是指产品在规定的时间内，按规定的程序和方法进行保障时，保持完成规定功能的能力

1.1 可靠性概念

安全性和健壮性

- 安全性（Safety）：正确地安装、维护和使用设备，使之不会危害人、家畜和财产
- 健壮性（Robustness）：系统从各种出错条件下恢复原有功能的能力。亦称鲁棒性或坚固性

与电子设备有关的安全危险

危险	可能结果	原因
电击	电死，由于肌肉收缩或燃烧至伤	接触有压部件
加热或可燃气体	失火、烧伤	高温元件、散热、损坏的或过载的元件和导线
毒气或冒烟	中毒	损坏的或过载的元件和导线
移动部件、结构不牢	物理损坏	电机、机械强度不足的部件，重的或锋利的部件
内爆/外爆	由碎片造成伤害	CRT，真空管，过载电容和电池
电离辐射	辐射曝露	高压 CRT，辐射源
非电离辐射	射频烧伤，可能是慢性的	功率射频电路，无线发射机，天线
激光辐射	眼睛损害，烧伤	激光
声辐射	听力损害	扩音器，超声波传感器

1.2 可靠性定量表征

可靠度与失效概率

可靠性可用定量的指标来表征。我们无法准确预计产品在何时失效，只能得到产品在何时失效的可能性高低，故可靠性的定量表征指标均为概率

- **可靠度R(t)**
  - 产品在t时间内不失效的概率　R(t)=P{τ>t}　τ为产品的寿命
  - 若N个产品工作到t时间有n(t)个失效，N(t)个未失效，则R(t)的估计值（实际的可靠性定量指标只能通过试验或现场观测得到其近似值，亦称观测值）

$$\hat{R}(t)=\frac{N-n(t)}{N}=\frac{N(t)}{N} \qquad (\text{如} N>>n(t))$$

  - R(0)=1（产品在刚投入使用时不会失效），R(+∞)=0（产品只要使用时间足够长，最终一定会失效）
- **失效概率F(t)**
  - 产品在t时间内失效的概率　F(t)=P{τ≤t}　τ为产品的寿命
  - 显然　F(t)+R(t)=1　（F(t)亦称不可靠度）
  - 若N个产品工作到t时间有n(t)个失效，则 $\hat{F}(t)=1-\hat{R}(t)=\frac{n(t)}{N}$ $(\text{如} N>>n(t))$
  - F(0)=0，F(+∞)=1

1.2 可靠性定量表征

失效密度与失效率

- **失效密度（亦称累积失效率或失效概率密度）f(t)**
  - 产品在t时刻附近的单位时间段发生失效的概率

$$f(t)=\frac{dF(t)}{dt} \qquad \hat{f}(t)\approx\frac{1}{N}\frac{\Delta n(t)}{\Delta t}$$

$$F(t)=\int_0^t f(x)dx \qquad R(t)=\int_t^\infty f(x)dx \qquad (\because \int_0^\infty f(x)dx=1)$$

- **失效率（瞬时失效率）λ(t)**
  - 在t时刻尚未失效的产品在t时刻附近的单位时间段内发生失效的概率

$$\lambda(t)=\frac{F'(t)}{R(t)}=\frac{f(t)}{R(t)}=\frac{1}{R(t)}\frac{dR(t)}{dt} \qquad \hat{\lambda}(t)=\frac{\hat{f}(t)}{\hat{R}(t)}=\frac{1}{N(t)}\frac{\Delta n(t)}{\Delta t}$$

  - λ(t)的单位：1Fit=10^{-9}/h（每十亿个小时的失效元件数）或者1Fpmh=10^{-6}/h(每百万个小时的失效元件数)

1.2 可靠性定量表征

寿命:计算公式

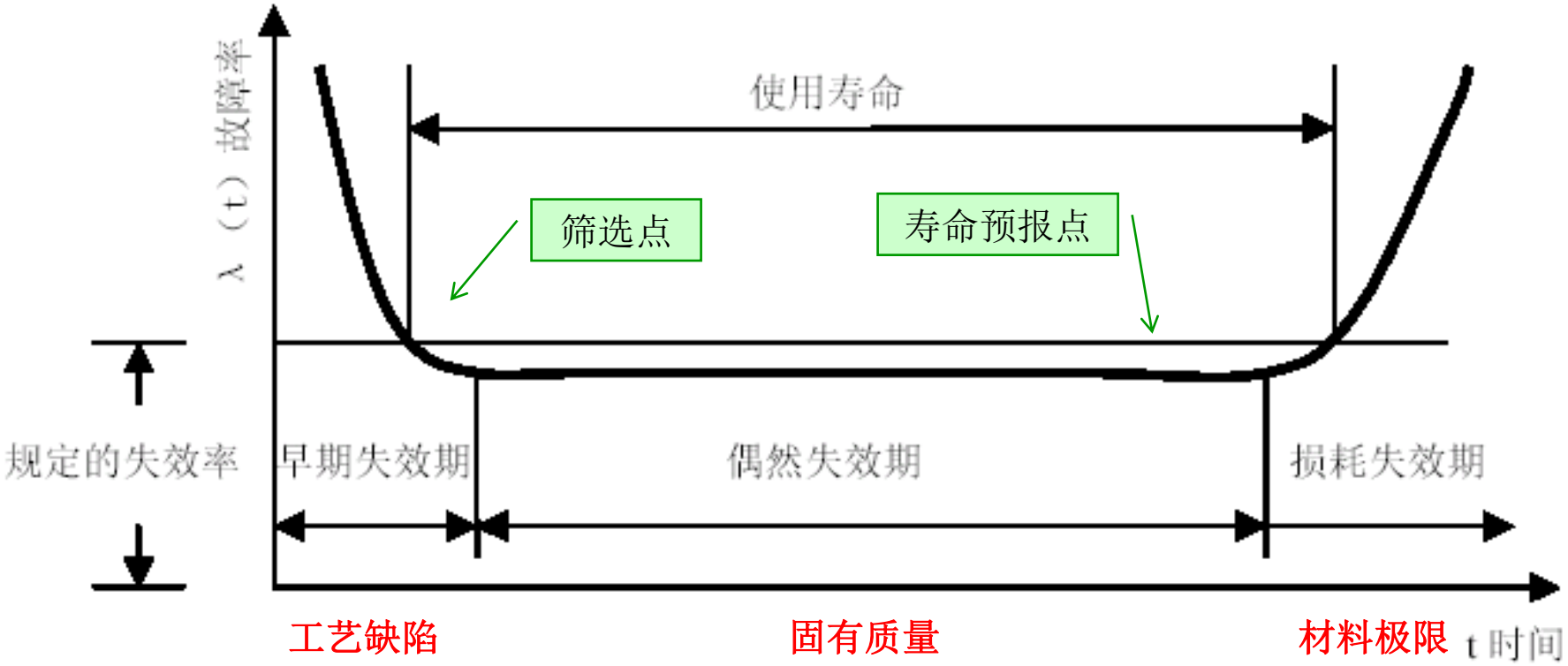
平均寿命 $$\theta = \int_0^\infty t f(t)dt = \int_0^\infty R(t)dt$$

寿命方差 $$\sigma^2 = \int_0^\infty (t-\theta)^2 f(t)dt$$

可靠寿命 $$r = t\Big|_{R=R_0} \begin{cases} \text{中位寿命} r = t\Big|_{R=0.5} \\ \text{特征寿命} r = t\Big|_{R=1/e=0.368} \end{cases}$$

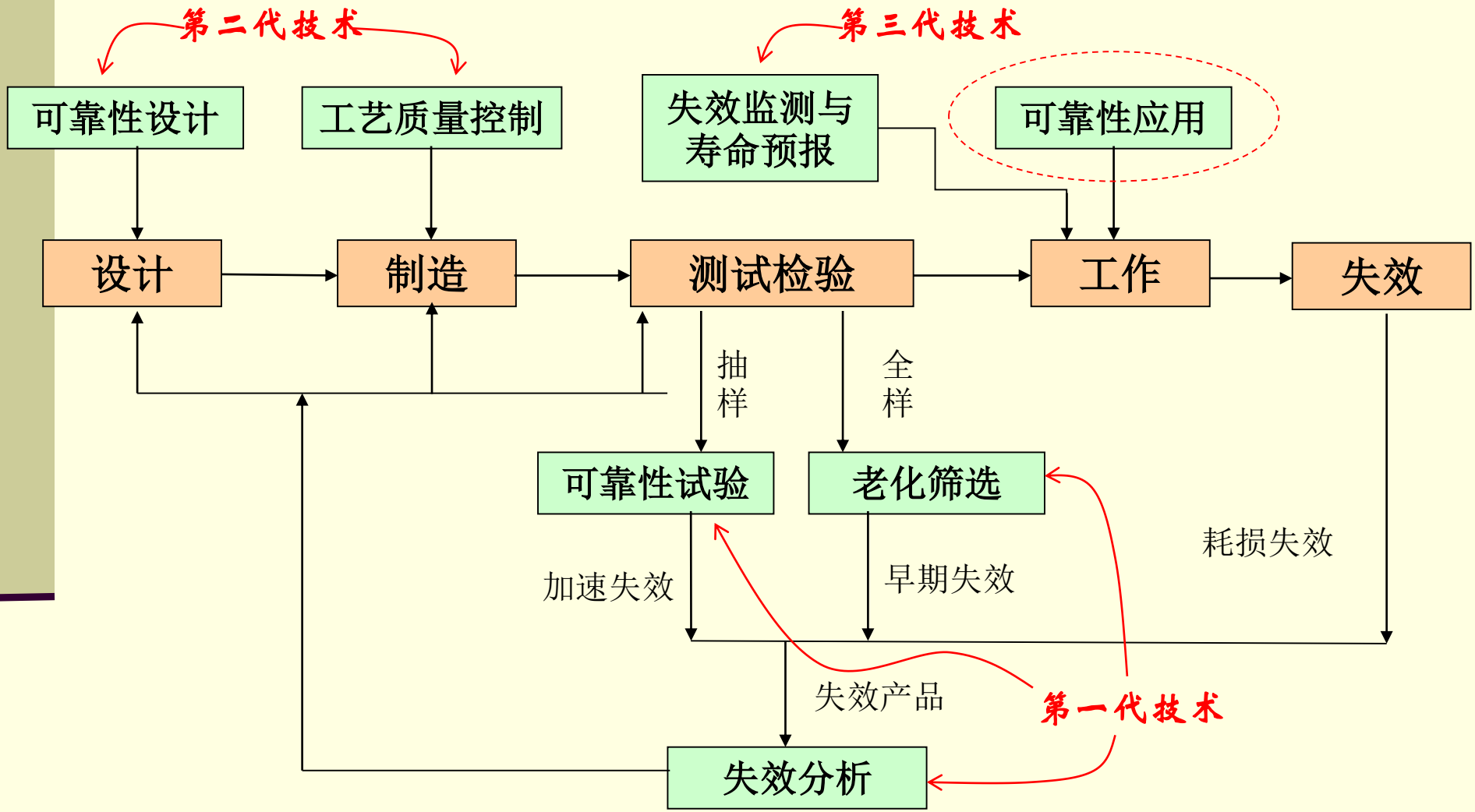
1.2 可靠性定量表征

“浴盆”曲线



- **早期失效期**：失效率较高且呈下降趋势，主要是由于设计错误、工艺缺陷、装配问题、管理不当等原因引起的，但可以通过筛选老化的方法来剔除部分早期失效的产品，提高出厂产品的可靠性
- **偶然失效期**：失效率较低且基本保持常数，是产品的最佳工作阶段。在此阶段的失效大多数是由于产品的固有质量或者偶然因素引起的
- **耗损失效期**：失效率再度呈现上升趋势，这是由于元器件材料磨损、疲劳、老化等原因造成的，只能采取更换元器件等方法来解决，相对于一般电子设备或电子元器件，半导体器件在损耗期的上升更缓慢一些

1.3 可靠性技术概要 全寿命周期的可靠性保证技术



在不同的阶段，必须采用不同的可靠性技术手段来保证电子产品的可靠性

1.3 可靠性技术概要

- 可靠性筛选是对元器件进行100%的非破坏性测试与应力试验，用以剔除早期失效的元器件。
- 可靠性筛选项目通常包括高温存储、功率老化、热冲击、振动与冲击、潮热、密封检漏、抗潮湿和电气参数测试等，具体项目和方法见相关文献
- 可靠性筛选的效果可以由以下参数表征：
  - 筛选效率：设一批产品的总数为N，其中早期失效的产品为R，筛选后共淘汰了n个产品，其中包括实际淘汰的早期失效产品r个，则筛选效率为

$$\eta = \text{应淘汰的早期失效的产品实际被淘汰的比率} - \text{不应该被淘汰的产品被淘汰的比率}$$

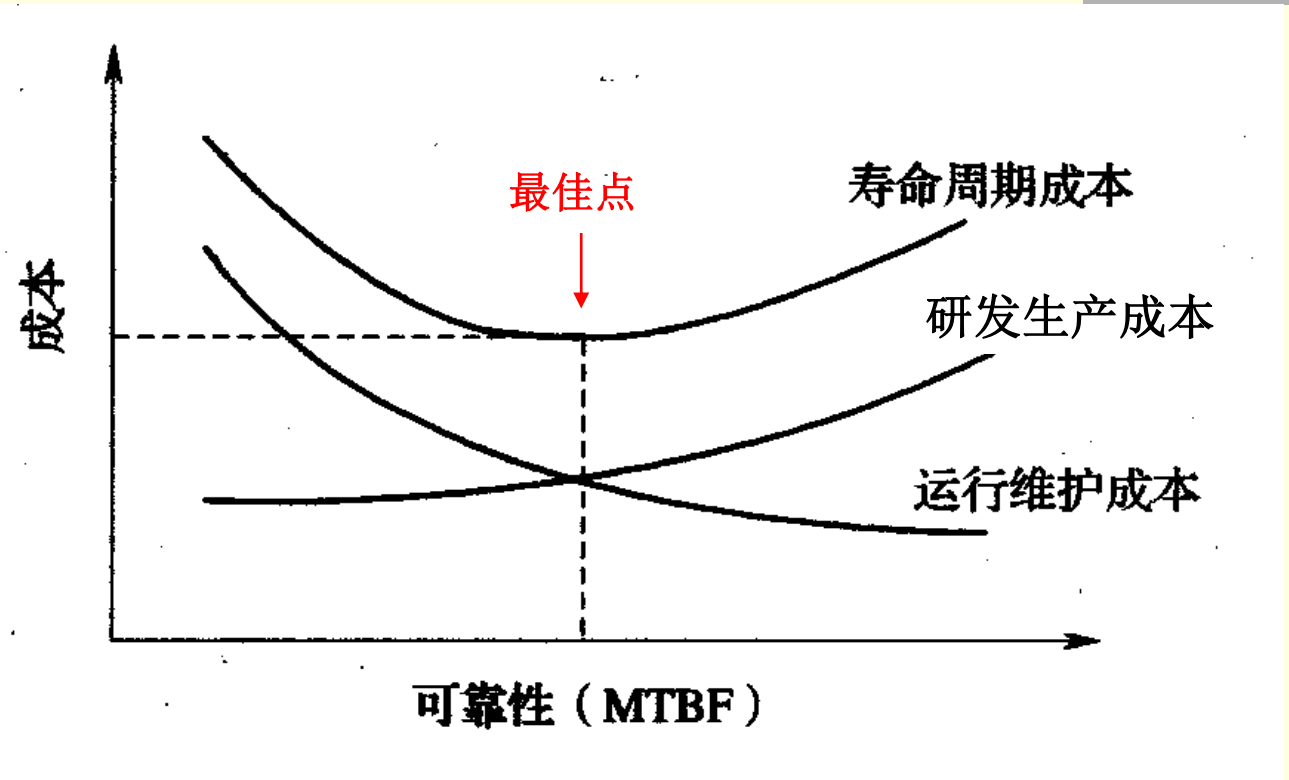
$$= \frac{r}{R} \cdot \left(1 - \frac{n-r}{N-R}\right) = 0 \sim 1$$

  - 筛选剔除率：被淘汰的产品占产品总数的比率

$$P = \frac{n}{N}$$

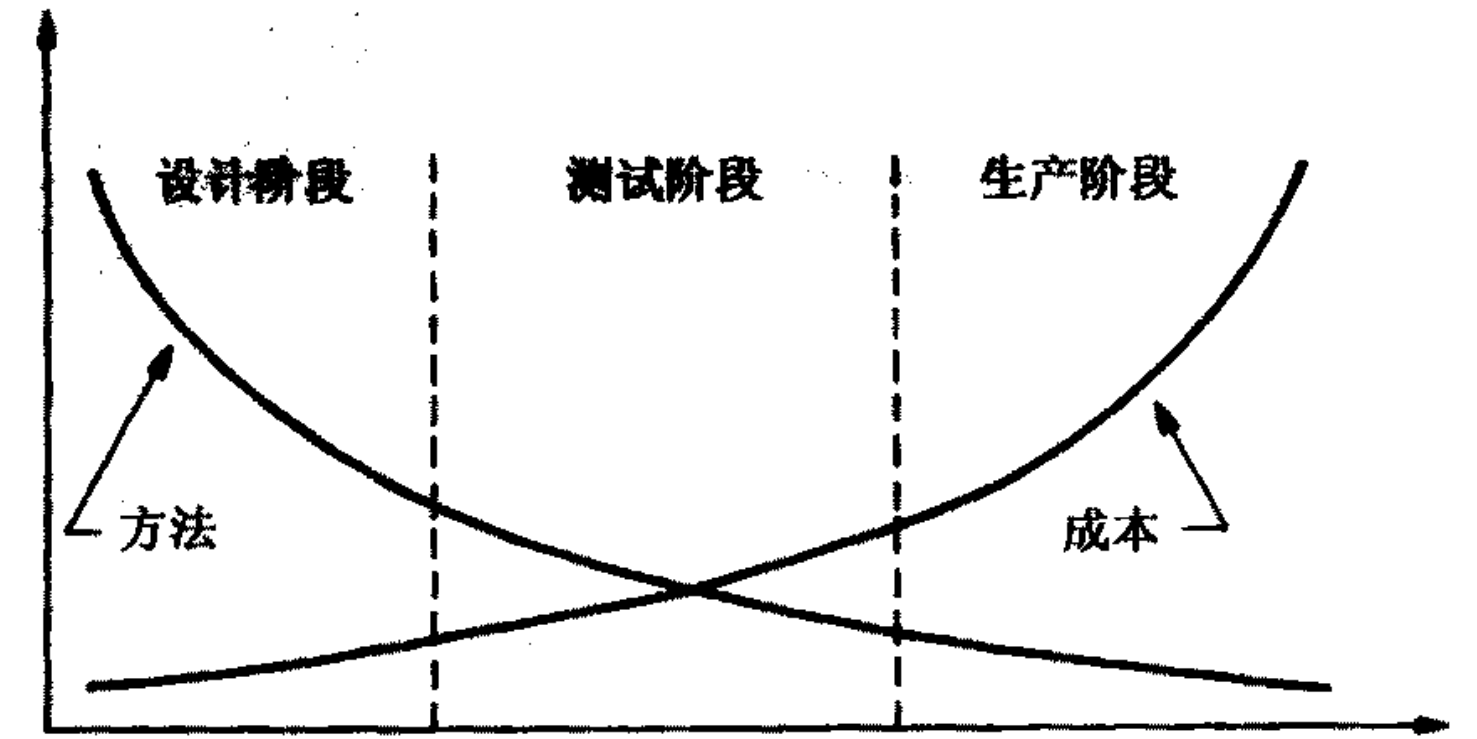
1.3 可靠性技术概要

可靠性与成本的权衡



- 研发生产成本包括原材料采购、设计、工艺改进等方面的成本，运行维护成本包括修理、备件和保障等方面的成本，二者之和为寿命周期成本
- 随着产品可靠性要求的提高，在前期开发中必然要投入更多的研发生产成本，但会降低后期的维护保障成本，因此性价比最好的是寿命周期成本的最低点

1.3 可靠性技术概要



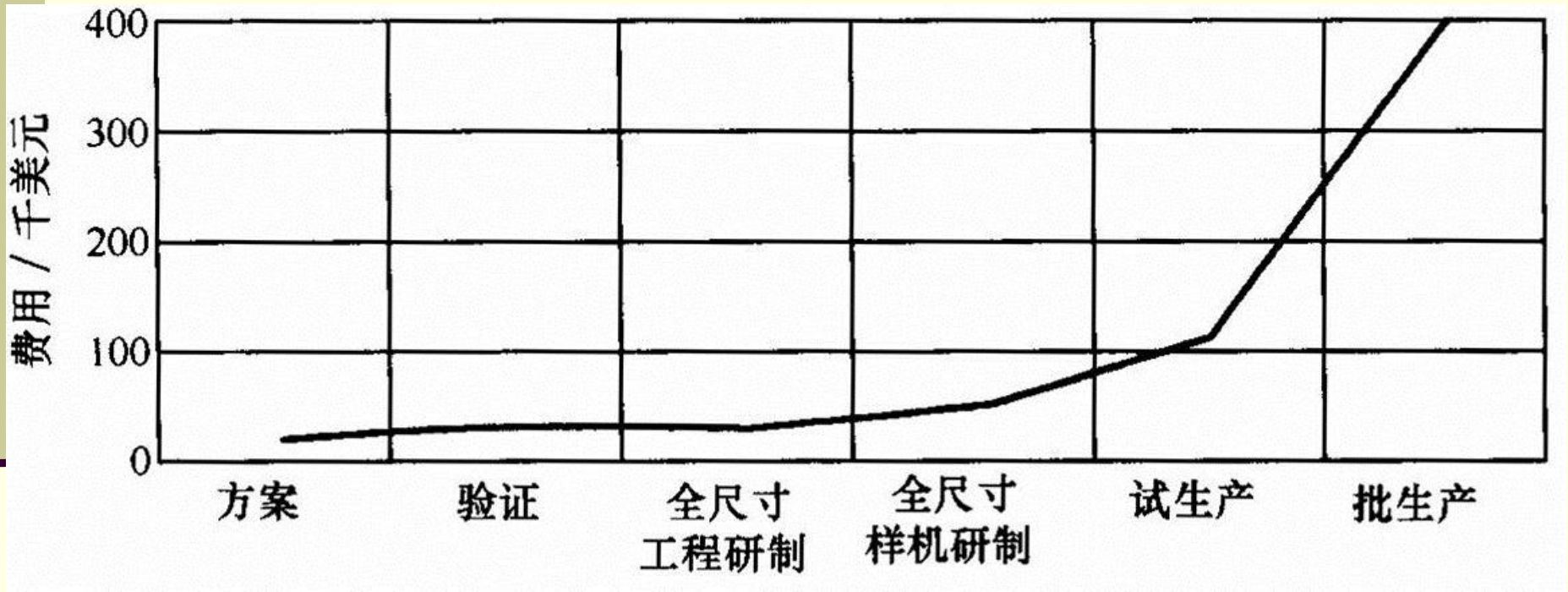
产品开发进程

- 内建可靠性理念认为，可靠性是被“设计”到产品中去的，而不是被“附加”进去的，或是“筛选”出来的
- 在设计阶段来解决可靠性问题，要比在测试乃至生产阶段来解决，不仅可用的技术手段多，而且投入经济成本少得多

1.3 可靠性技术概要

可靠性与研发成本

国外某短程导弹项目在研制阶段的七个节点进行设计修改所付出的平均花费



在产品研发中，越早考虑可靠性设计，投入的成本就会越低

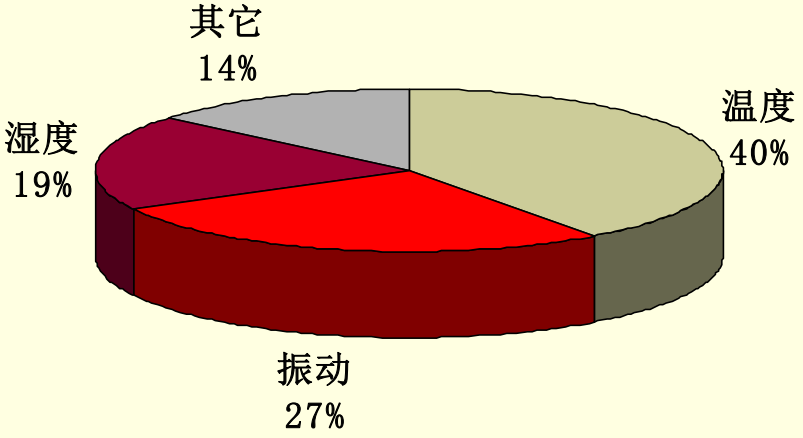
1.4 可靠性设计

影响可靠性的使用应力

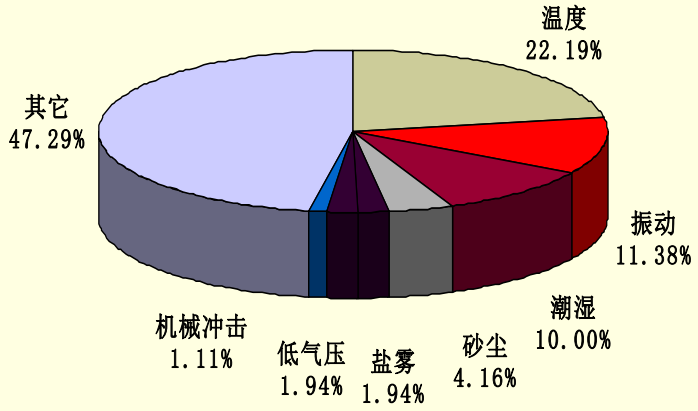
- **按应力类型分**

应力类别	应力形式	应用场合
电应力	静电、浪涌、过电压、电磁干扰	工作、安装、测量
温度应力	高温、低温、温度循环	大功率工作、间歇工资、高寒地区、焊接
机械应力	振动、冲击、加速度	安装、运送、航天器、航空器、移动设备
气候应力	高湿度、盐雾、低气压	储存、海上、沿海、亚热带地区

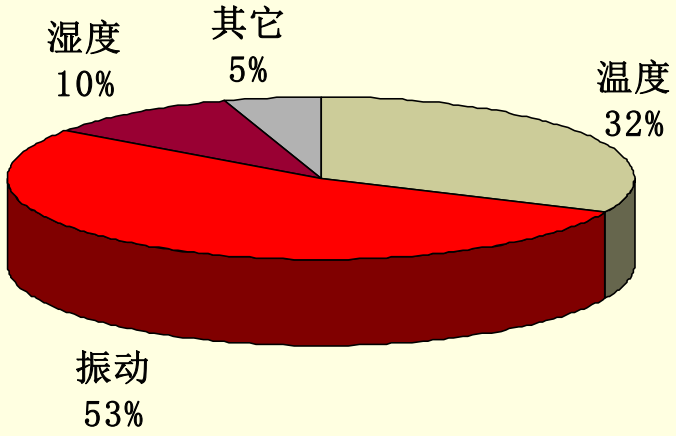
1.4 可靠性设计 引起电子设备故障的环境应力分布



野外地面电子设备



机载电子设备



航空电子设备

1.4 可靠性设计

影响可靠性的使用应力(续)

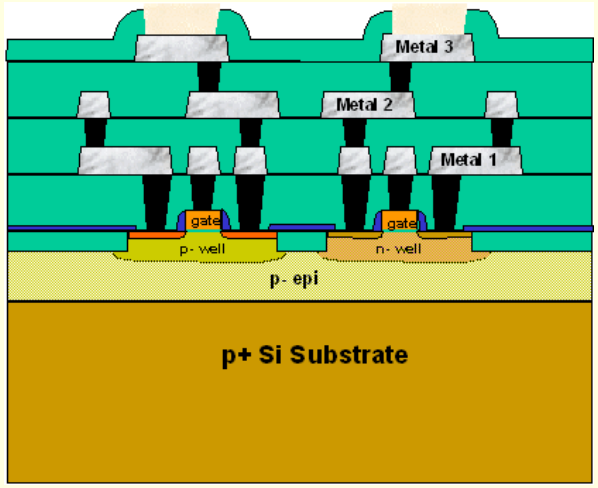
- **按应力强度（从小到大）及产生的后果分**
  - A级：设备仍然能在规定的环境中实现正常功能，但性能有所下降（如电脑运行速度变慢）
  - B级：设备出现误动作或丧失局部功能，但设备总体上仍在正常运转，干扰消失后，设备可以自动恢复正常状态，不再出现误动作或局部功能失常（如电脑个别软件无法运行）
  - C级：设备运行停止，需要外部干预（如操作者重新启动）才能重新开始运行（如电脑死机，重新开机可恢复正常）
  - D级：故障现象同上，但已给设备引入不可恢复的潜在损伤，设备的寿命及抗环境应力能力已下降（如电脑死机后重新开机可正常运行，但之后会频繁死机）
  - E级：设备即时永久丧失功能，必须进行维修（如电脑死机后再也无法开机）

如应力类型为电应力，则产生上述后两种情况的通常叫做“电过应力”（如浪涌、静电放电、雷击、核辐射等），通常由元器件的永久性失效所致；产生前三种情况的通常叫做“干扰”（如电磁干扰、噪声等），通常由元器件的暂时功能失常所致

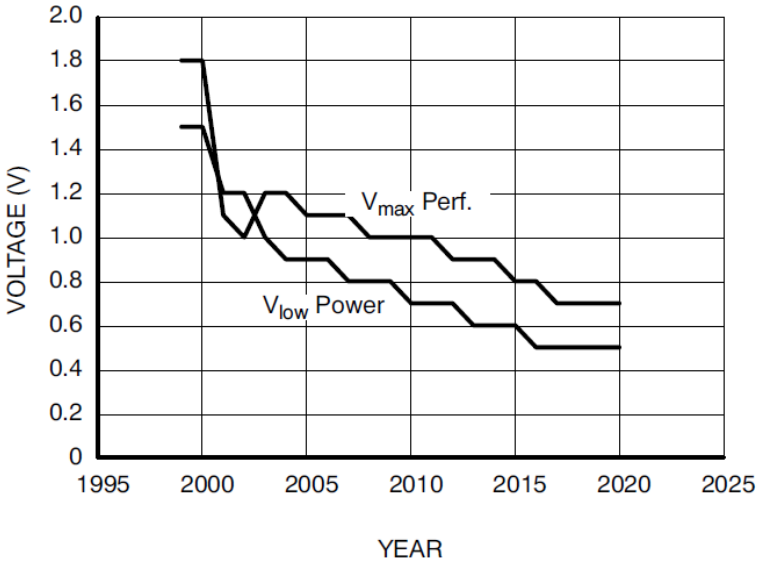
1.4 可靠性设计

元器件使用失效增多的原因

- 片内原因
  - 芯片集成度↑→工艺尺寸↓，工艺层次↑→片内电流密度↑，电场强度↑，热不匹配性↑
  - 芯片工作电压↓→噪声容限↓→抵抗外界过电压的余度↓
  - 数字电路工作频率↑、模拟电路灵敏度↑ →片内防护电路设计制造难度↑
- 片外原因
  - 系统高频高速化：电过应力与干扰的传播路径多样化、复杂化
  - 应用环境多样化：如航天、航空、车载、手持移动设备等
  - 保护手段低成本化：如采用无屏蔽作用的塑料机箱取代金属机箱，用塑料封装取代高可靠的金属、陶瓷封装等



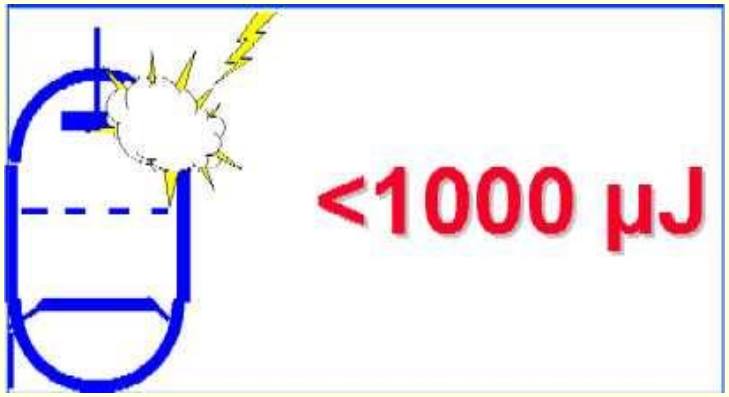
集成电路内部物理结构示意图



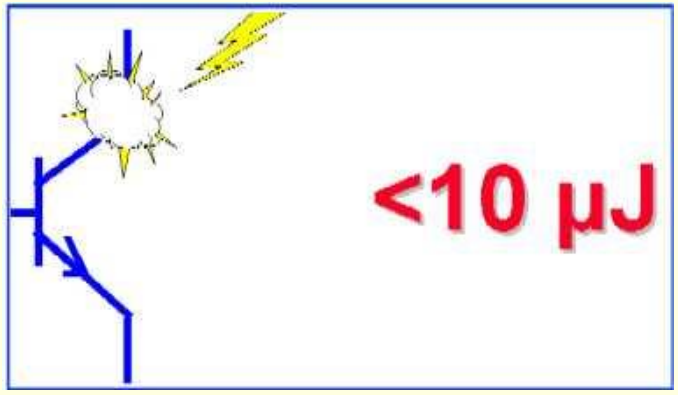
集成电路的工作电压逐年下降

1.4 可靠性设计

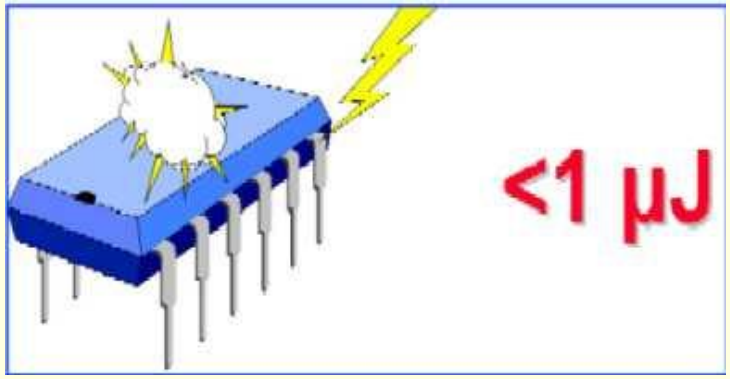
尺寸缩小→抗应力强度↓



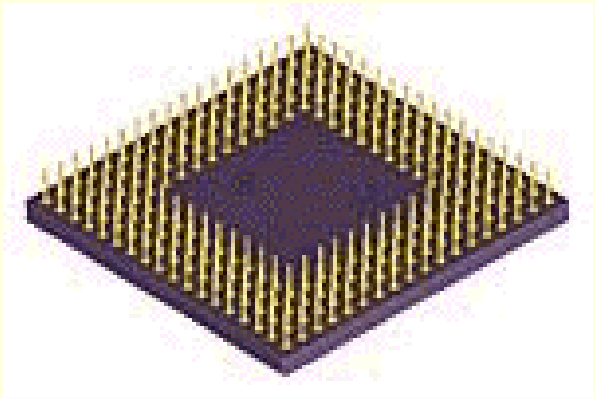
电子管



晶体管



集成电路

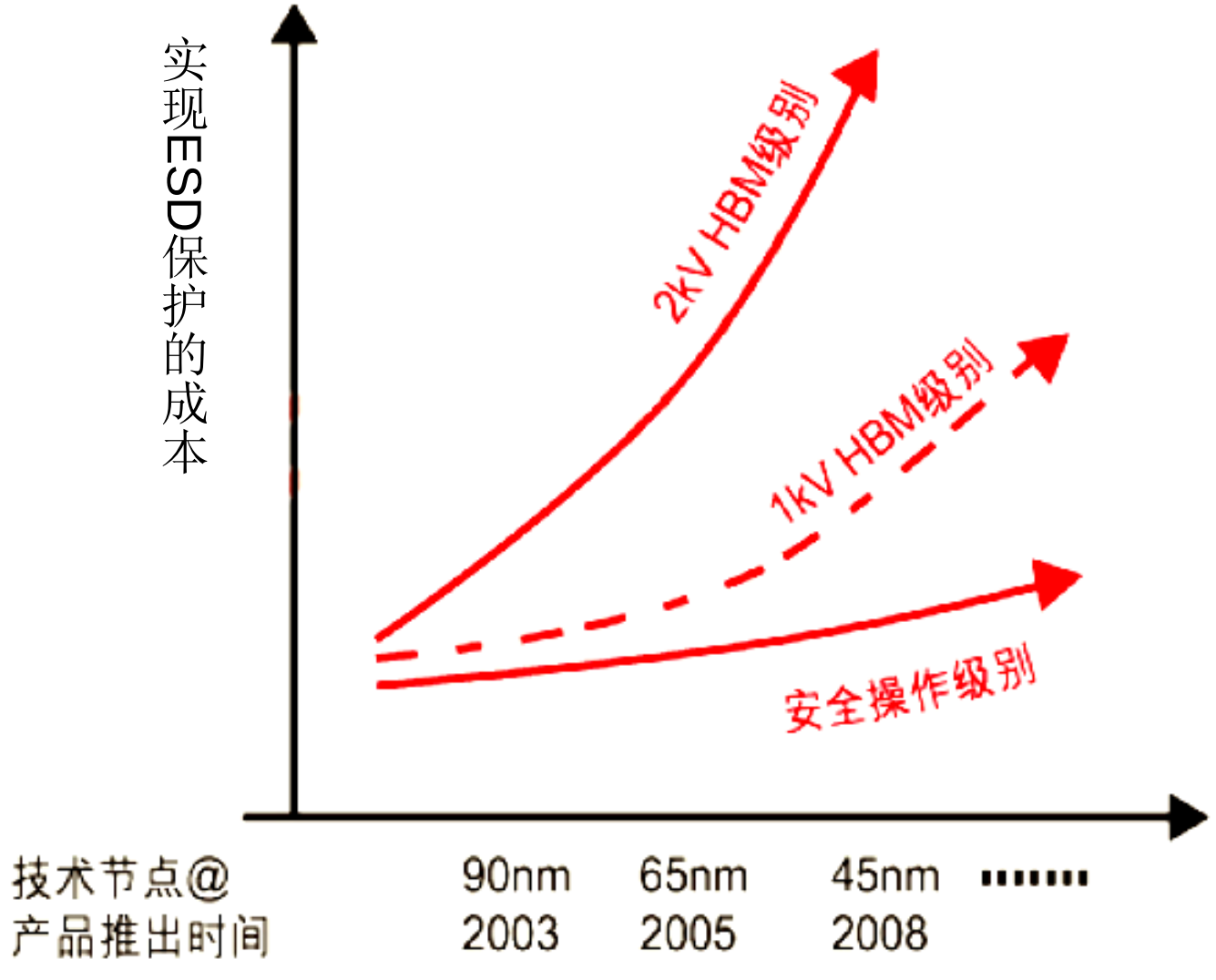


<0.1uJ

超大规模集成电路

1.4 可靠性设计

片内防护成本不断上升

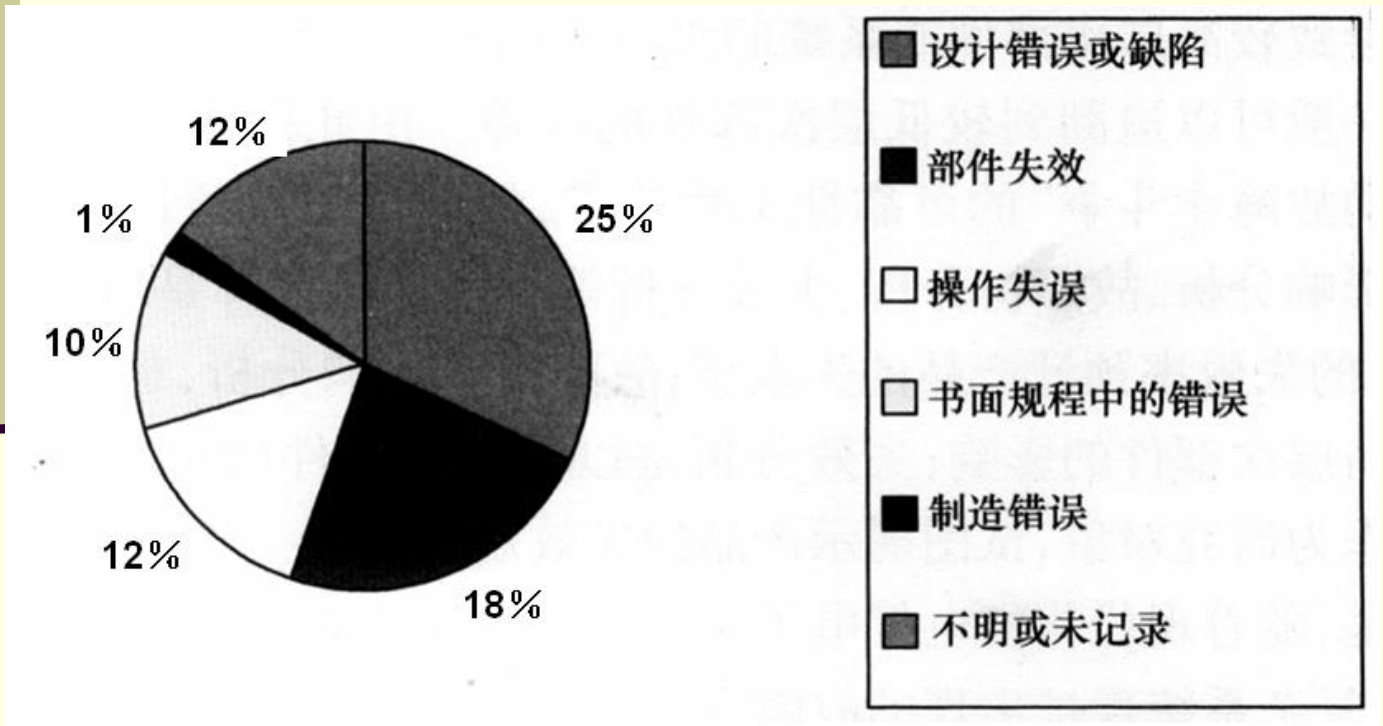


- 随着集成电路工艺尺寸的缩小、集成电路工作电压的降低和集成电路速度的提升，要保证同样的片内静电防护级别，所需的成本将会按指数规律上升
- 从成本和良率考虑，芯片制造厂已将片内防护标准从2kV降低到500V，而转为靠片外保护来达到所需的高防静电等级要求

1.4 可靠性设计

可靠性设计的重要性

- 整机的可靠性设计比元器件的可靠性设计更为重要
  - 国外卫星系统级故障的最终原因是设计错误或缺陷，其比例高于部件或元器件失效导致的故障比例



世界五个商业核电站安全事故原因的统计结果

END

第1章 电子可靠性设计基础

主讲：庄奕琪