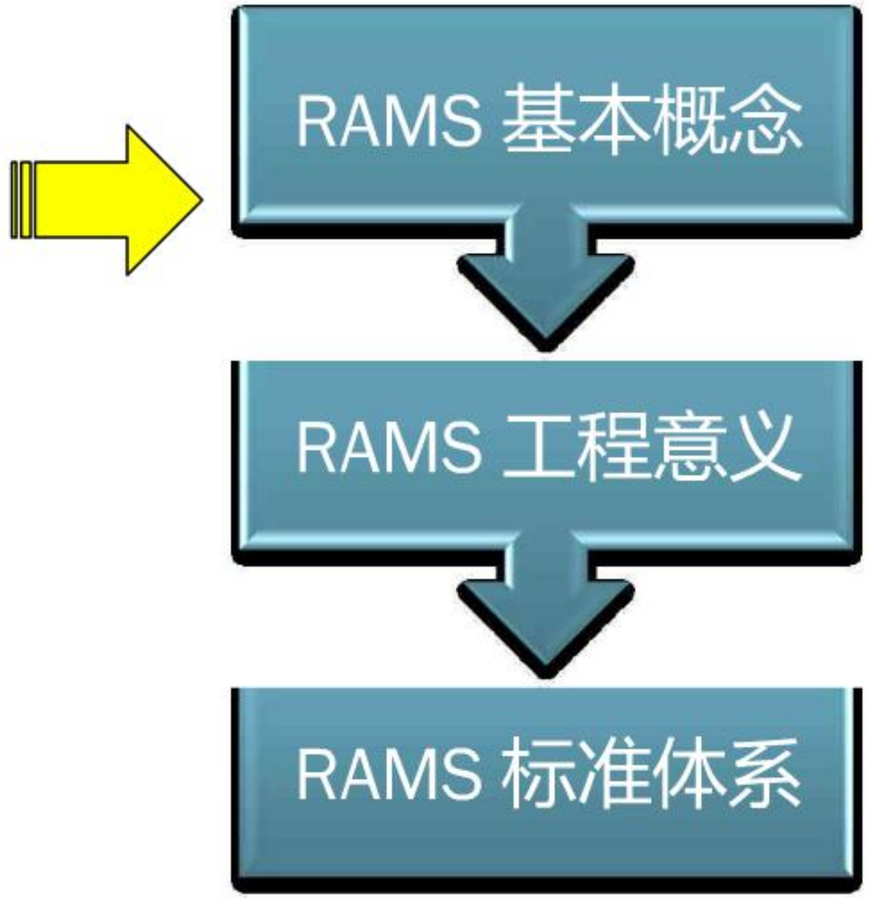
内容安排

1. RAMS 技术基础
2. RAMS 技术要求
3. RAMS 体系框架
4. RAMS 关键技术



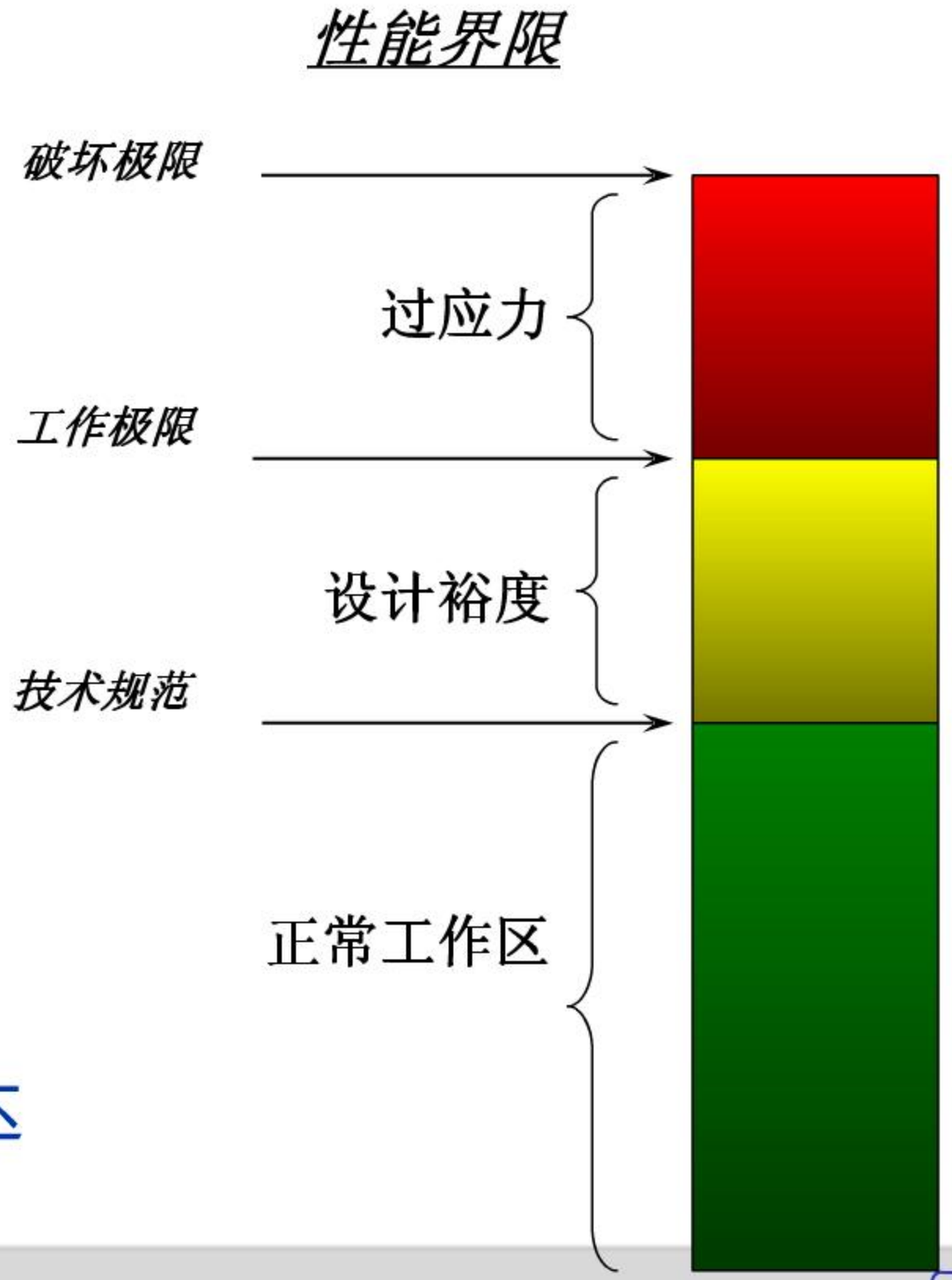
- Reliability - 可靠性
- Availability - 可用性
- Maintainability - 维修性
- Safety - 安全性

“五性” = 可靠性 + 维修性 + 保障性 + 测试性 + 安全性

可靠性（Reliability）

- 可靠性产品的是产品在规定的条件下运行时，在规定的时间内保持规定功能的能力。
- 可靠性的概念有以下特征：
  - 关注故障
  - 判定故障发生的可能性，用定量的形式表达；
  - 评价故障对系统功能的影响程度。
  - 可靠性的定量衡量参数为可靠度或MTBF，是概率参数。
- 可靠性表征产品故障的频繁程度和危害程度，是产品的一种固有属性，主要由设计决定，可靠性设计和分析的主要任务是降低故障发生的概率和降低故障的影响。

- 故障 - 不能满足规定的功能
- 故障的种类：
  - 功能丧失
  - 功能降低
  - Surprise ！
- 故障的可恢复性
  - 软故障 - 没有物理损伤
  - 硬故障 - 有物理损伤
- 规定功能常用故障判据逆向表达



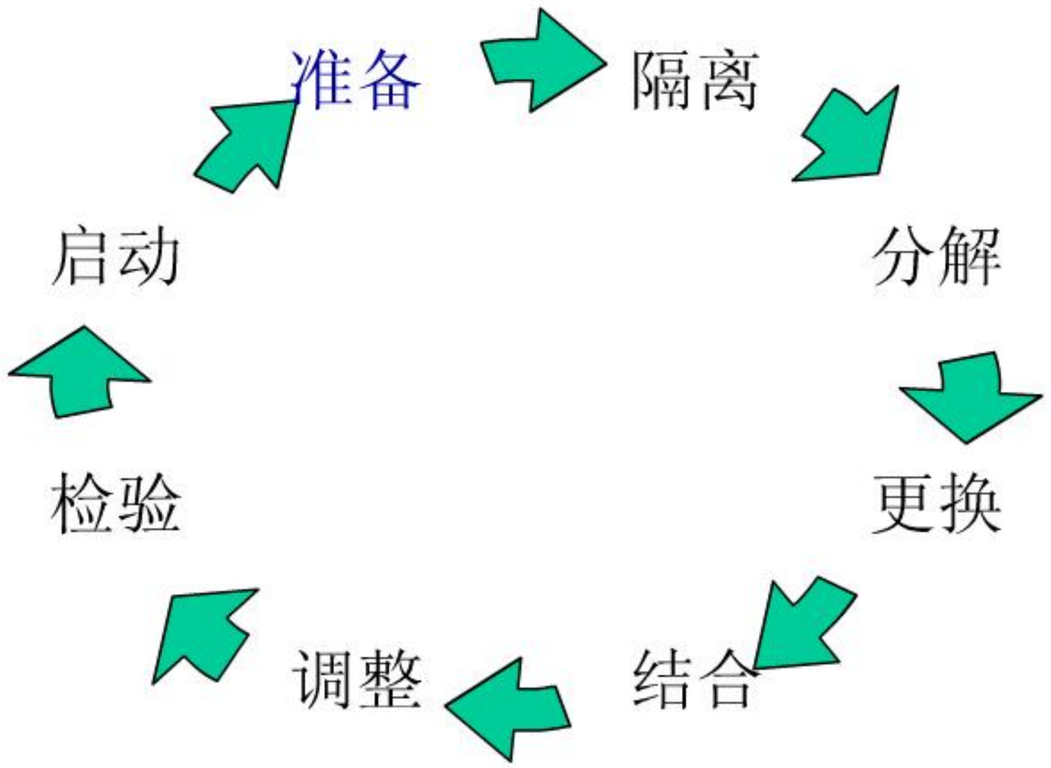
维修性（Maintainability）

- 维修性是产品在规定的条件下和规定的时间内，按规定的程序方法进行维修时，保持或恢复到其规定状态的能力。
- 维修性的概念具有以下特征：
  - 关注故障，是针对故障的一种活动；
  - 维修性的定量衡量参数为平均维修时间（MTTR，MTTM），是时间参数。
- 维修性表征产品预防故障和修复故障的能力，表达产品维修的难易程度，是产品设计所赋予的一种固有属性。
- 维修性设计和分析的主要任务是建立以可靠性为中心的维修设计（RCM - Reliability Center Maintainability），相当于容易发生故障的地方容易修复。

维修类别

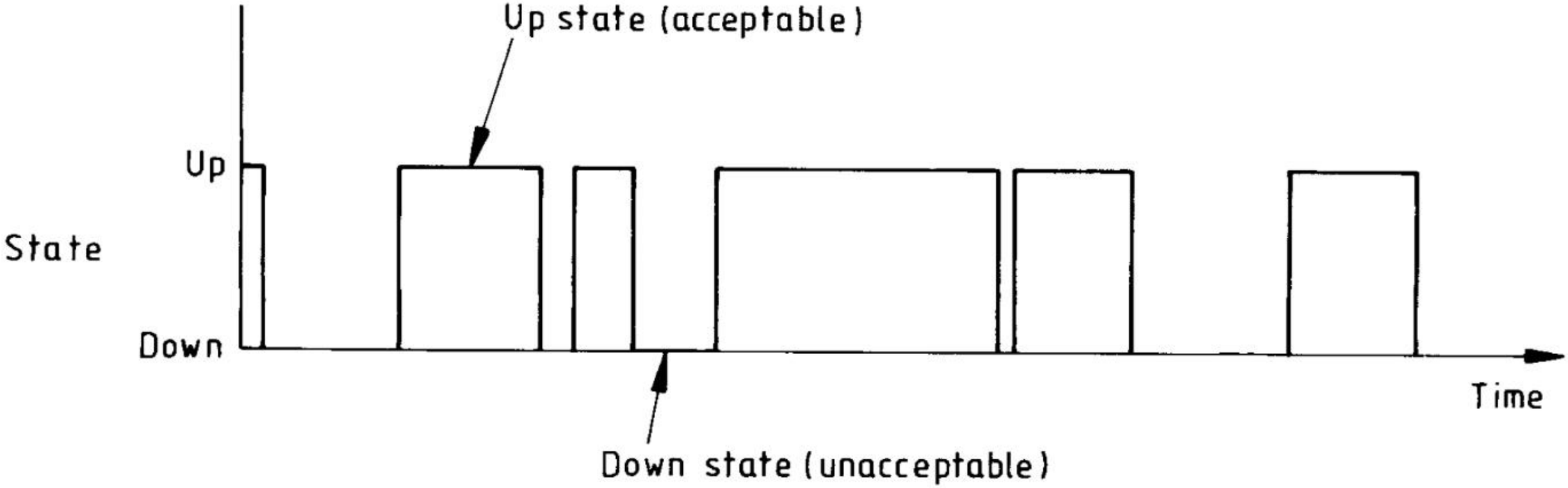
维修类别包括：

- 预防性维修 - 预防故障的维修，是计划性的，常称为维护或保养；
- 修复性维修 - 处理故障的维修，是非计划性的，常称为修理或修复。



可用性（Availability）

- 可用性是产品在任意一个随机时刻处于可用状态的能力。
- 可用性常用可用时间占总时间的比值来描述，即：
  - 可用性 = 可用时间/（可用时间 + 不可用时间）
- 可用性是可靠性、维修性和运用保障的综合特性：
  - 可靠性越好，则可用时间越长；
  - 维修性越好，则维修时间越短，不可用时间越短；
  - 运用保障特性越好，则维修等待时间越短。

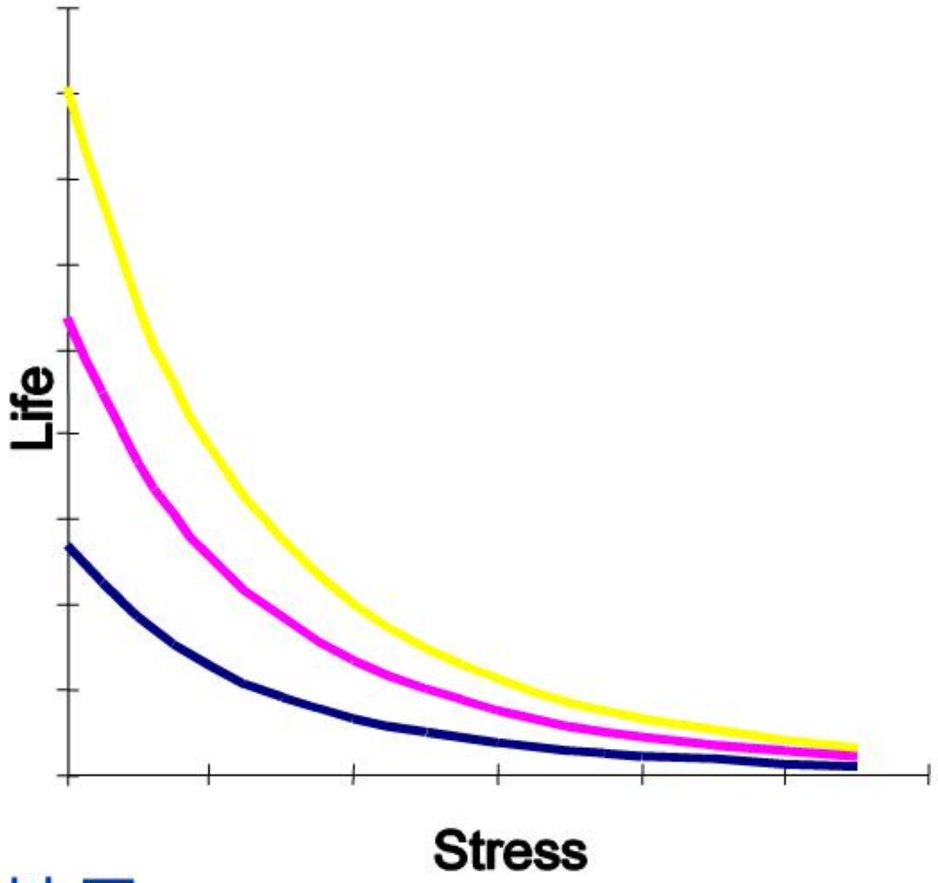

Up state (acceptable)
Up
State
Down
Time
Down state (unacceptable)

安全性（Safety）

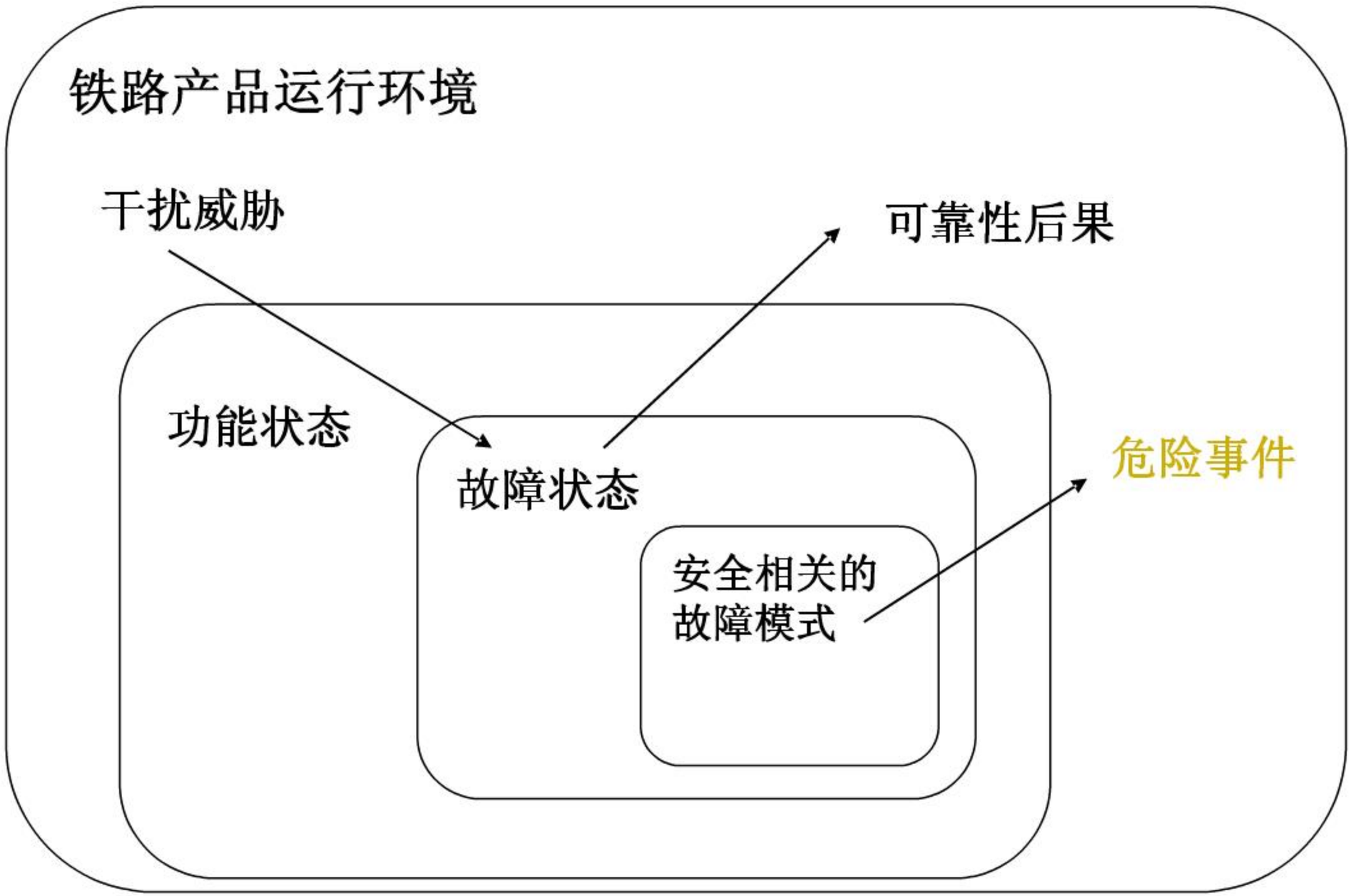
- 安全性是指产品不发生系统危险事件（Hazard Event，也称为事故）的能力。
- 安全性的概念具有以下特征：
- 关注危险，铁路产品的危险包括：
  - 违反政府法规
  - 人员伤亡
  - 重大财产损失
  - 环境破坏
- 涉及到在各种环境条件和工作条件下，在运营、维护和维修过程中发生的所有危险；
- 故障是危险的主要来源，危险性故障是全部故障的子集。

环境应力对可靠性的影响

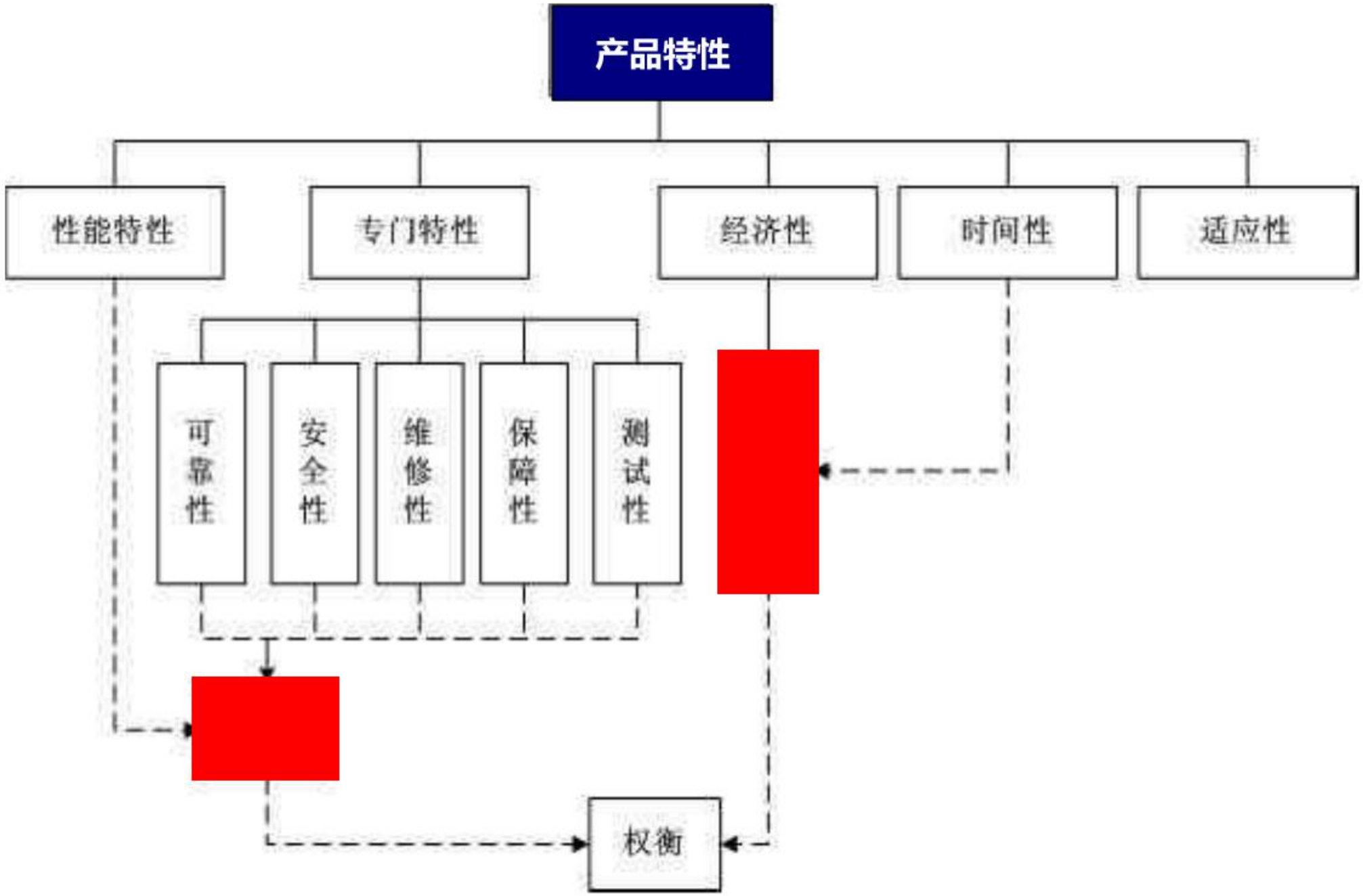
- 环境越恶劣可靠性越差
  - 温度应力会提高产品的故障率
  - 振动应力会加速产品的疲劳
  - 湿度和化学应力会缩短产品的寿命
- 环境应力和可靠性一般是指数关系：
  - 温度 - Arrhenius
  - 振动 - Coffin-Manson
  - 湿度和其他 - Eyring

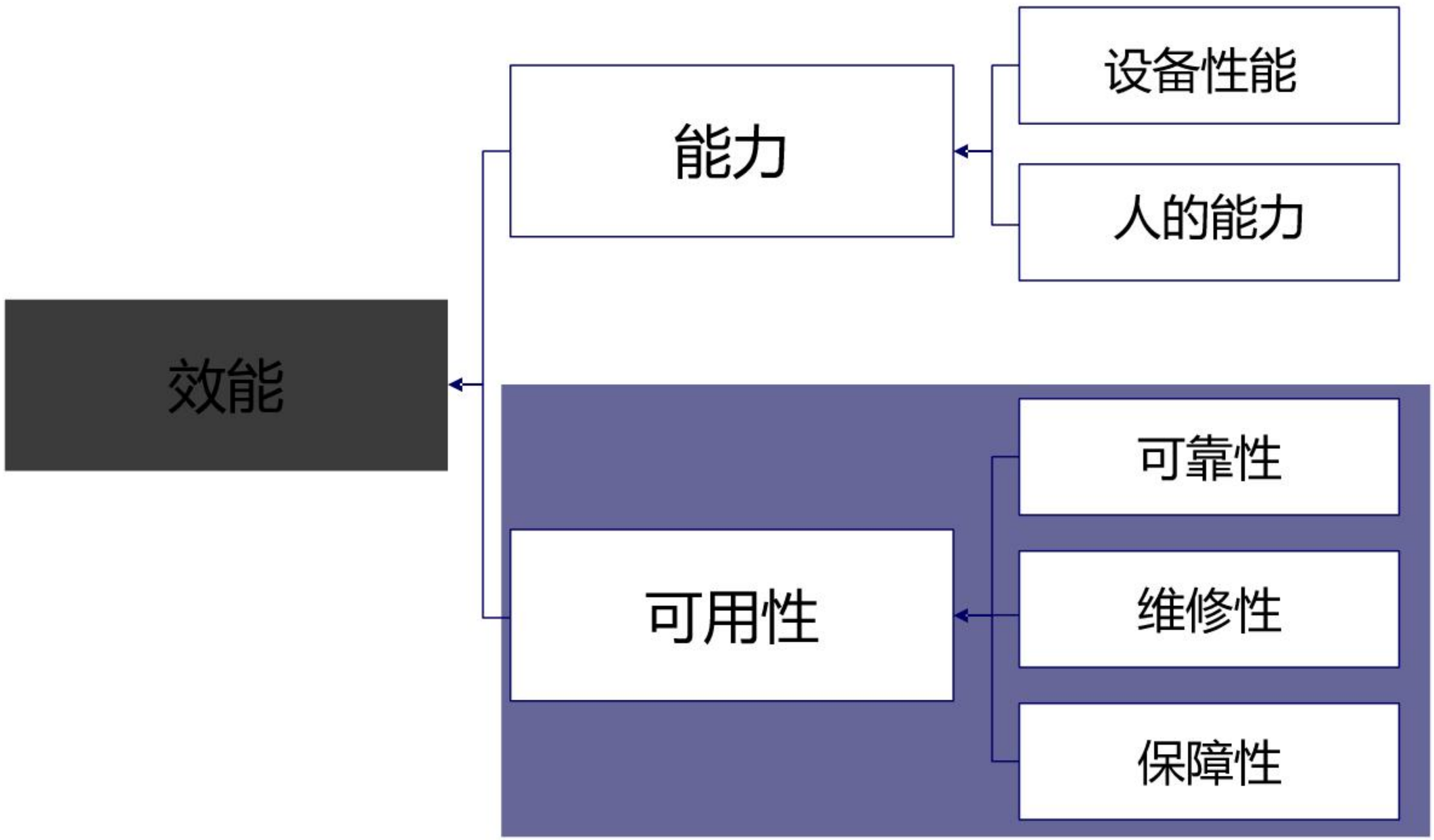


- 有意施加恶劣的环境应力进行试验可以高效地暴露产品缺陷。

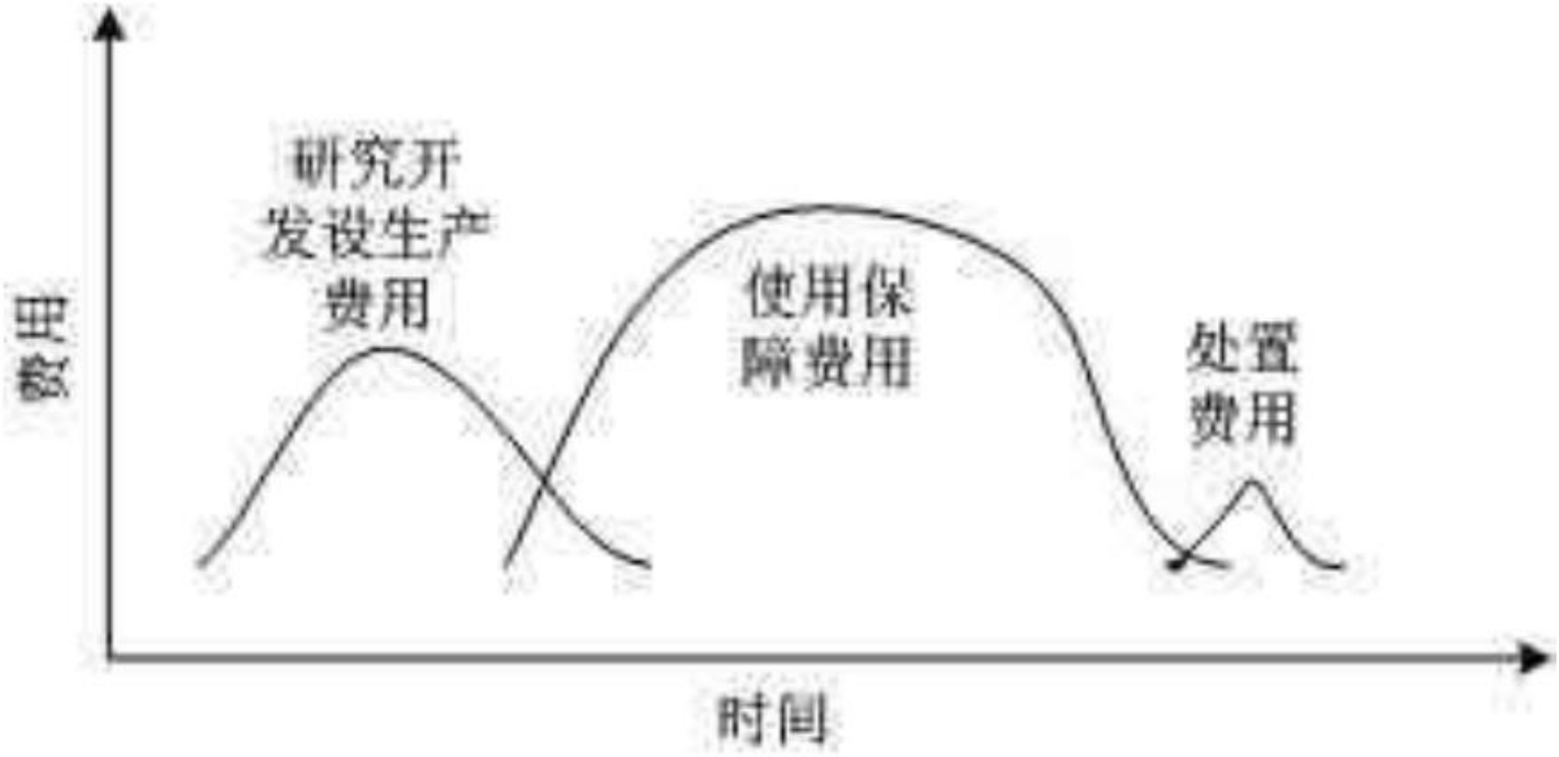

铁路产品运行环境
干扰威胁
可靠性后果
功能状态
故障状态
危险事件
安全相关的
故障模式

1.2 RAMS 的工程意义



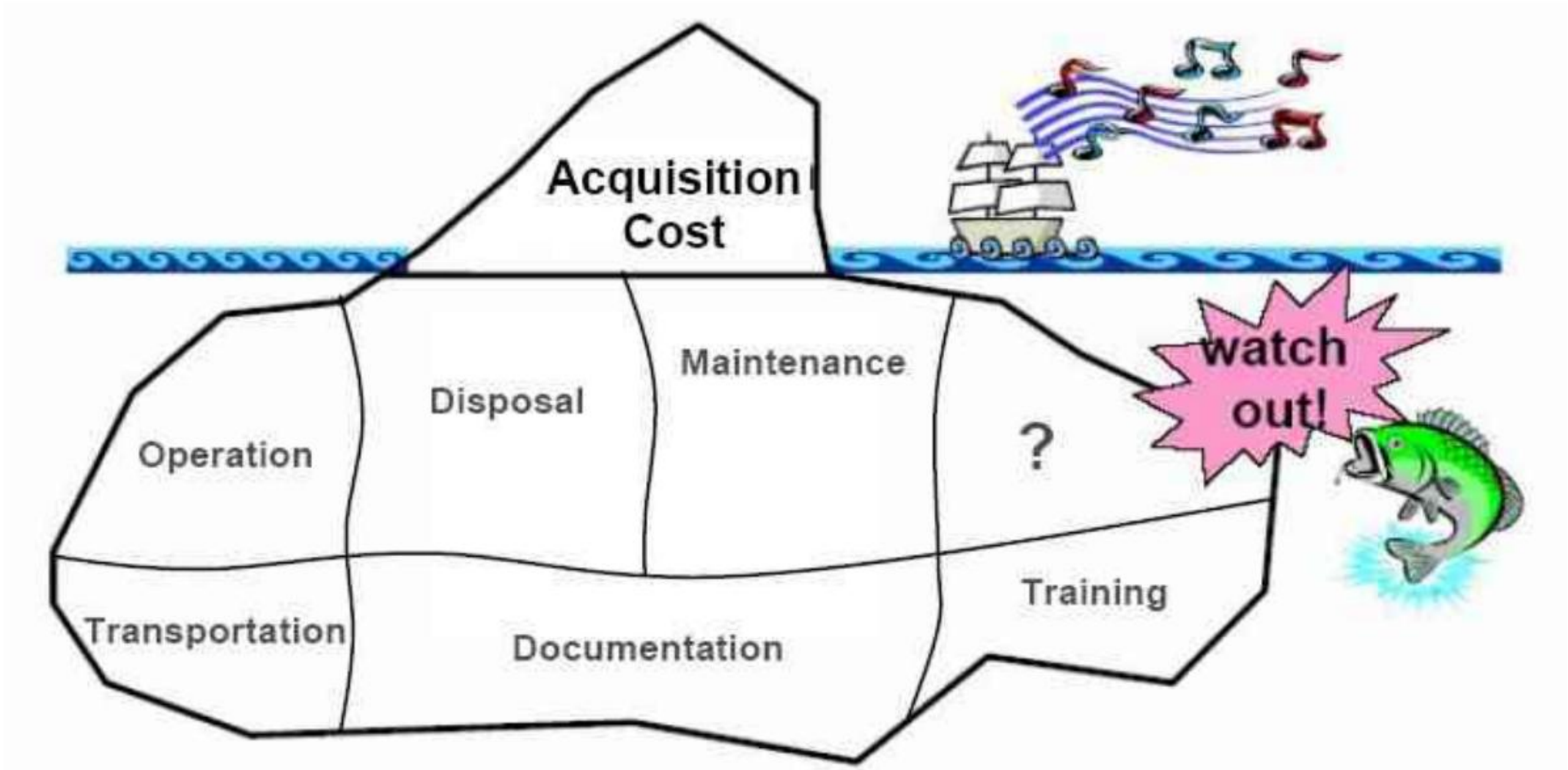

效能
能力
设备性能
人的能力
可用性
可靠性
维修性
保障性

系统的寿命周期费用（Life Cycle Costs，以下简称LCC），是指在系统的整个寿命周期内，为获取并维持系统的运营（包括处置）所花费的总费用。



系统寿命周期费用构成示意图

寿命周期费用


Acquisition
Cost
Maintenance
Disposal
Operation
?
watch
out!
Training
Transportation
Documentation

现代设计思想的转变

- 性能向效能的延伸
- 采购费用向寿命周期费用的延伸

- 发达国家轨道交通行业的RAMS工程已经发展到了一个比较先进的水平，建立了系统的RAMS行业标准，形成了完整高效的工作体系，具备先进的设计分析技术、有效的验证方法等一整套RAMS工程技术支撑。在产品管理过程中，高效地运用RAMS技术，实施全方位的安全性与可靠性管理，有效地控制了产品风险，保证了产品安全性和可靠性，降低产品全寿命周期费用，提高了铁路、地铁、城市轨道等轨道交通工具的质量保证能力和可用性。

- RAMS是系统工程技术之一，也是世界先进轨道交通行业普遍采用的关键技术，法国、日本、英国、德国、美国等发达国家和地区均在轨道机车车辆方面成功地实施了RAMS工程，其中以欧洲国家为代表，不仅建立了RAMS系列标准，使RAMS工程实现了系统化的发展，还在很大程度上推广了RAMS工程，使轨道交通的可靠性、维修性和安全性等指标得到了显著的提高。

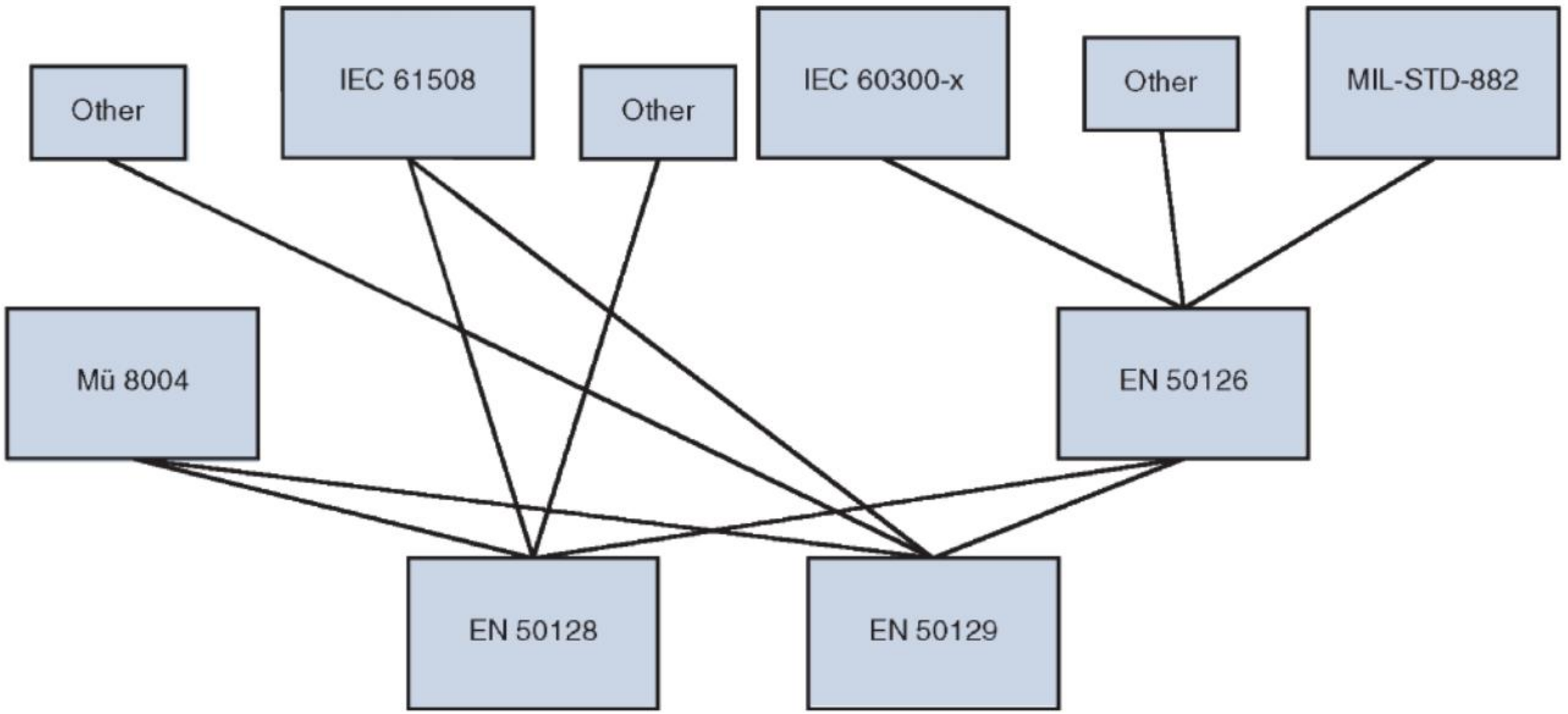
- 我国轨道交通行业的RAMS工程尚处于起步状态，局部建立了质量与可靠性信息系统，利用各研发、生产和使用单位提供的质量与可靠性信息进行分析和评价；重点产品应用了一些RAMS工程技术，例如基于安全系数的可靠性工程设计、故障模式影响分析、故障树分析、可靠性试验等。这些技术的应用对提高轨道交通工具的安全性和可靠性起到了一定作用，还不够系统化，可靠性技术的应用范围还受到很大局限：
  - 没有建立系统的RAMS工程体系
  - 缺乏行业RAMS标准和指导性文件
  - 目前的RAMS工程技术尚不能完全满足行业需要，缺乏RAMS专业人员
  - 缺乏行业RAMS信息数据库
  - 产品的运营故障率较高

- 第一，保障铁路产品的安全运营的需要。
  - 轨道交通安全第一， 机车车辆的工作环境非常严酷，对产品的可靠性水平要求较高；同时由于近年来机车车辆的大幅提速，对机车的安全、可靠、稳定运营提出了进一步的要求。
- 第二，与国际先进水平接轨的需要。
  - 我国大量引进国外的轨道装备产品和技术；伴随着引进，南北车集团的下属企业开始了与国际领先公司的技术合作与配套供应，合作过程中，作为供应链上游的国外厂商，分别对我国内企业提出了相应的RAMS要求，强制要求进行FMECA、FRACAS和LCC等各项工作。
- 第三，降低寿命周期费用（LCC）的需要。
  - 轨道交通产品的使用和维护费用很高，往往超过了采购成本，通过RAMS技术的推动和运用，为LCC的分析和控制提供了技术支持，通过RAMS工程技术的推广应用，权衡产品运营、维护维修策略、备件储备和供应等方面要素，分析寿命费用的关键因素，降低寿命费用水平。

EN 50126 Railway applications – the Specification and demonstration of Reliability, Availability, maintainability and Safety (RAMS)
铁路应用－可靠性、可用性、维修性和安全性技术规格和验证

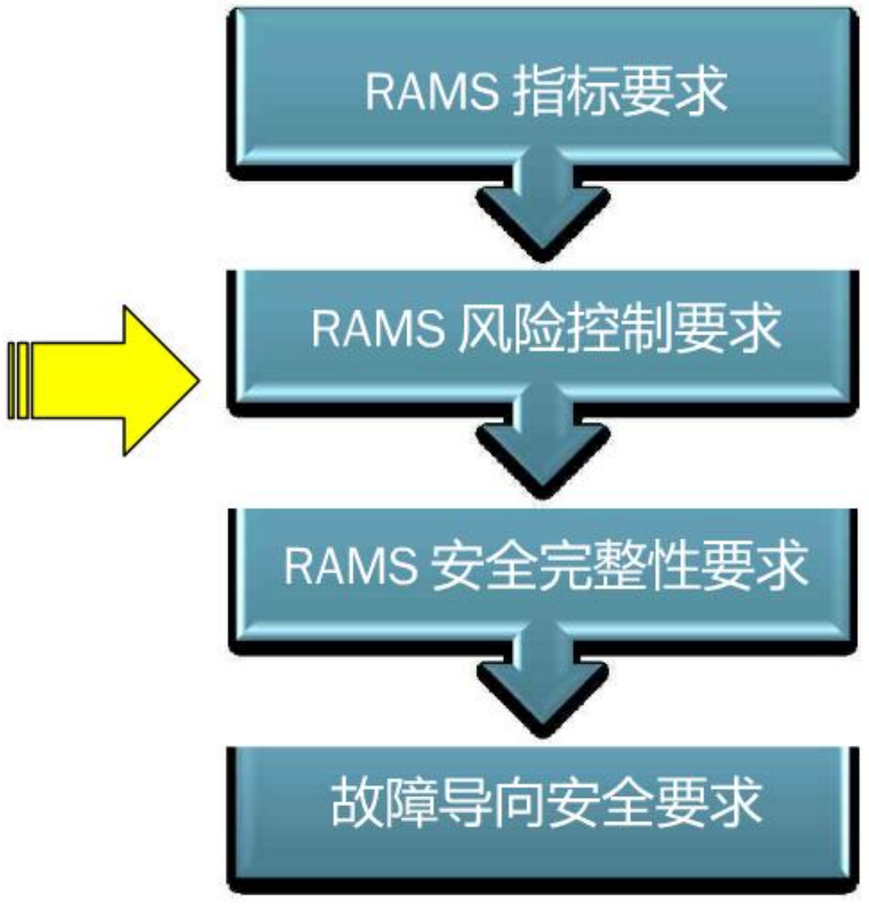
EN 50128 Railway applications – Software for railway control and protection systems
铁路应用－铁路控制和保护系统软件

EN 50129 Railway applications – Safety related electronic systems for signalling
铁路应用－与安全性相关的信号传送电子系统


Other
IEC 61508
Other
IEC 60300-x
Other
MIL-STD-882
Mü 8004
EN 50126
EN 50128
EN 50129

内容安排

1. RAMS 技术基础
2. RAMS 技术要求
3. RAMS 体系框架
4. RAMS 关键技术



- 对于铁路产品的“系统要求”阶段，需要提出并确定系统RAMS技术要求，并形成文档，随后将系统要求分配到分系统和设备中去。
- 铁路产品各级产品的RAMS 活动都是围绕RAMS要求进行的，包括定义、分配、实现、评估和验证等活动。
- RAMS要求分类：
  - 定性要求 - 提出了应当开展的RAMS 的工作项目和工作要求，通常采用评审的方法进行确认；
  - 定量要求 - 是基于RAMS的技术参数提出的，一般通过评估和验证的方法进行确认。

故障类别定义

序号	故障分类	系统故障模式	运行影响	说明
1	重大	完全失效	铁路产品不能运行	造成服务延误超过规定时间或产生超过规定水平的费用
2	主要	致命性功能失效	紧急运行 1	为使系统达到规定的性能必须做出调整
3	较小	非致命性功能失效	紧急运行 2	没有妨碍系统达到规定的功能，但有非致命性功能缺失。
4	轻微故障	可以忽略的功能失效	正常运行	产生非计划性维修

- RAMS 参数是产品RAMS定量化描述的数学属性，RAMS 参数体系是某种产品RAMS 的参数的集合；

- RAMS指标是产品某一RAMS 参数的要求值，RAMS指标体系是所有RAMS 参数的要求值。

参数	符号	量纲	备注
平均故障间隔时间	MTBF	时间，距离，周期	当量纲取距离时，也可以用 MDBF 表示 当量纲取周期时，也可以用 MCBF 表示
故障率	λ	故障 / 时间，距离，周期	
平均首次故障时间	MTTF	时间，距离，周期	当量纲取距离时，也可以用 MDTF 表示
可靠度	R(t)	无量纲	

- MTBF 针对不同的故障类型进行分类：
  - 1类故障 - MTBF1
  - 2类故障 - MTBF2
  - 3类故障 - MTBF3
  - 4类故障 - MTBF4
  - 1，2，3类故障 - MTBF

平均故障间隔时间 - MTBF

MTBF(Mean Time Between Failures) 是铁路产品主要的可靠性参数，适用于铁路产品的整车系统及下属各级产品，为累积工作时间除以累积故障次数。

平均故障间隔时间（MTBF）的计算公式如下：

$$MTBF=\frac{\sum_{i=1}^{n} t_{ci}}{r_a}$$

式中：

n – 产品总数

t_{ci} – 第 i 个产品的工作时间

r_a – 累积故障次数

MTBF 不是寿命！

寿 命: 产品能有价值存活的时间长度，是时间特性。
MTBF: 它体现了在寿命期内的发生故障的强度，是概率特性。

例如:

产品	典型设计寿命	典型MTBF
继电器	15,000 次	55,000 次
按钮	3 million	12 million
电视机	15 years	68 years
人	（71,74）年	39年

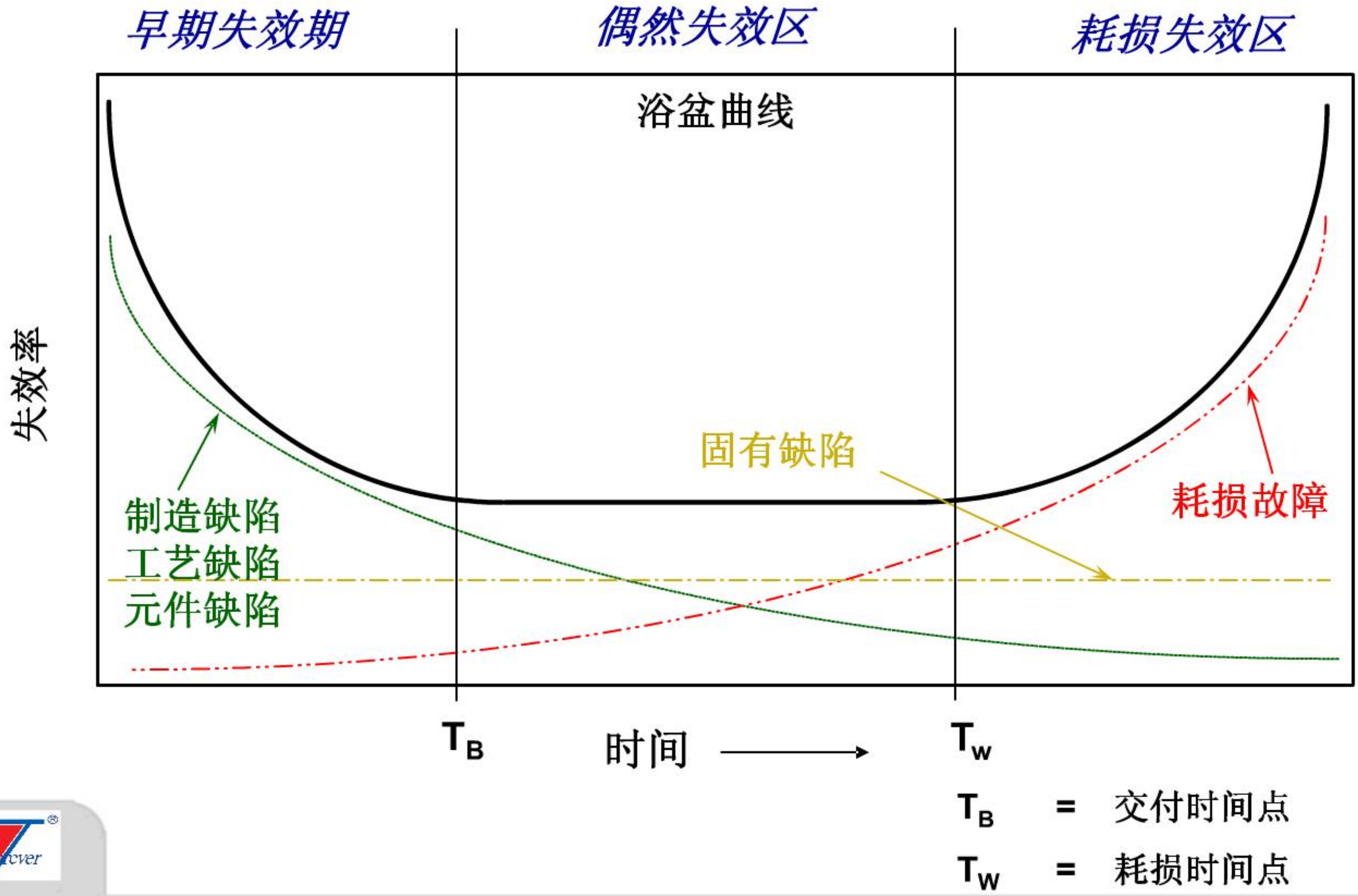
千万不能搞混

- 故障率（Failure Rate）：
  - 定义：工作到某时刻尚未发生故障的产品，在该时刻后单位时间内发生故障的概率。
  - 单位：一般为10^{-6}/小时或10^{-9}/小时（fit）
  - 计算：故障次数除以总工作时间

- 是MTBF 的倒数：

$$\lambda = \frac{1}{MTBF}$$

浴盆曲线

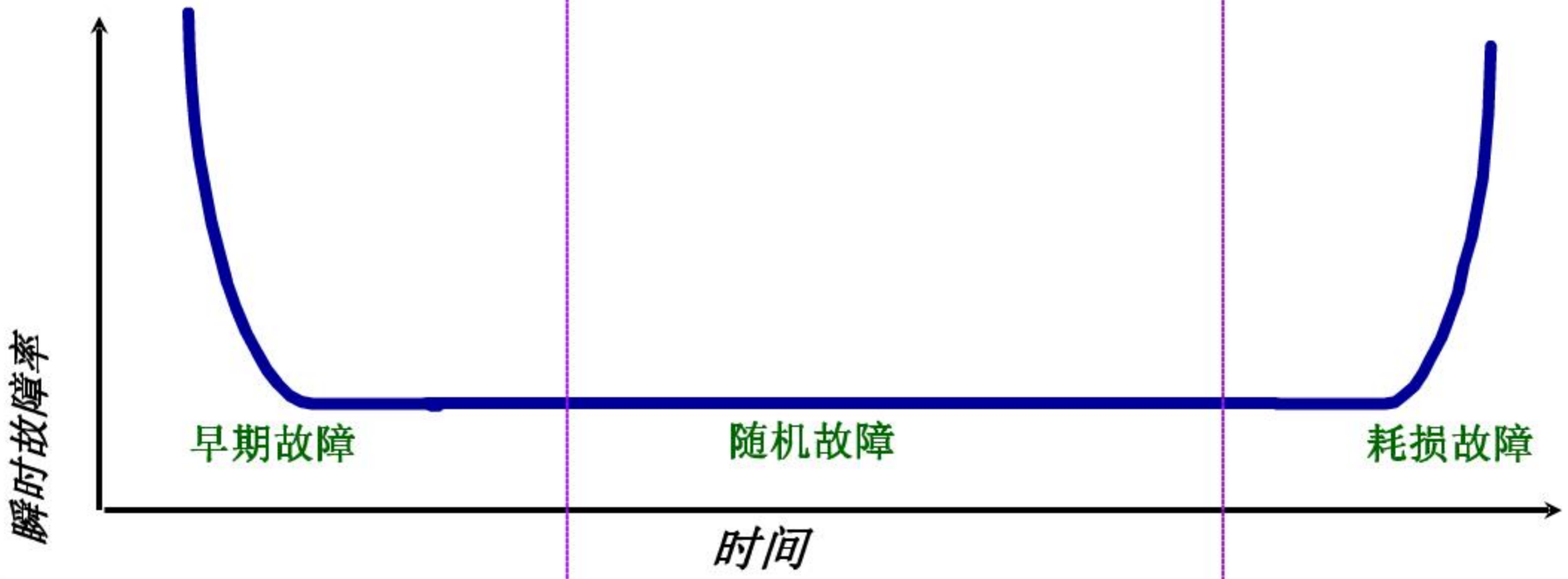


T_B = 交付时间点

T_W = 耗损时间点

浴盆曲线

制造和筛选	可靠性预计和验证	耗损机理分析
增加检查点	可靠性评估	材料特性
改善抗恶劣环境设计	可靠性预计	使用数据积累和分析
老化试验	可靠性增长试验	加速寿命试验
环境应力筛选试验	高加速寿命试验	系统寿命模型



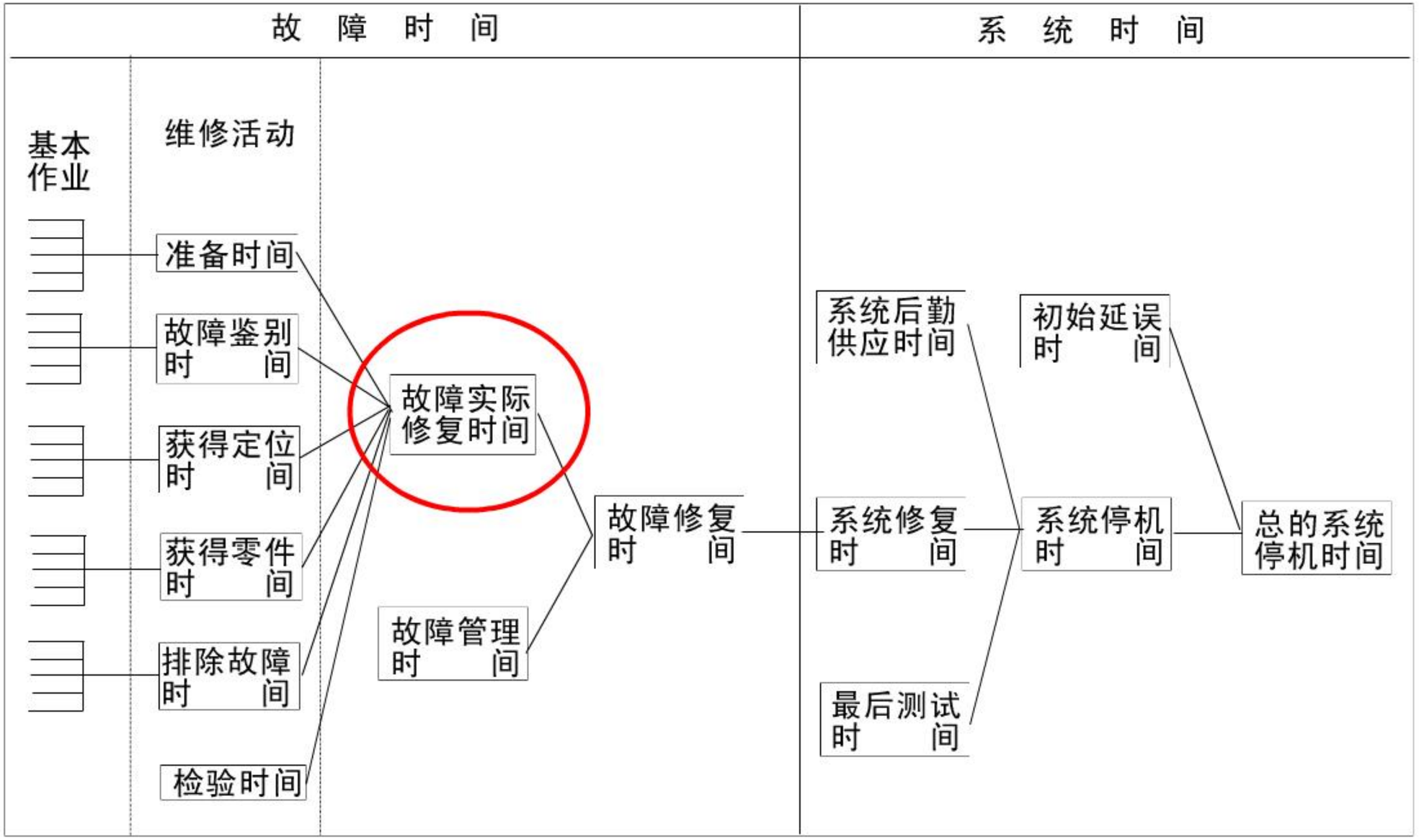
...开箱合格率	...预计和试验	与环境和应力相关的疲劳和衰减机

参数	符号	量纲	备注
平均修复时间	MTTR	时间	
平均维修时间	MTTM	时间	当表示平均预防性维修时间时，用 $MTTM_p$ 表示
平均维修间隔时间	MTBM	时间，距离，周期	当量纲取距离时，也可以用 MDBM 表示 当量纲取周期时，也可以用 MCBM 表示 当表示平均预防性维修间隔时间时，用 $MTBM_p$ 表示

平均故障间隔时间 - MTTR

- MTTR（Mean Time To Restore）表示针对发生故障的产品，平均恢复产品功能所需的时间
- MTTR 是一个时间参数，需要考虑各个维修活动所占用的时间
- MTTR 是铁路产品主要的维修性参数，通常情况下，也是唯一的维修性参数。与MTBF相似，MTTR 也是可以分类计算的，一般按维修级别（现场级、中间级和车间级）进行分类。

MTTR的时间


故障时间
系统时间
基本作业
维修活动
准备时间
故障鉴别时间
获得定位时间
获得零件时间
排除故障时间
检验时间
故障实际修复时间
故障管理时间
故障修复时间
系统后勤供应时间
初始延误时间
系统修复时间
系统停机时间
总的系统停机时间
最后测试时间

参数	符号	量纲	备注
可用度	A	无	
固有可用度	Ai	无	
可达可用度	Aa	无	
工作可用度	Ao	无	

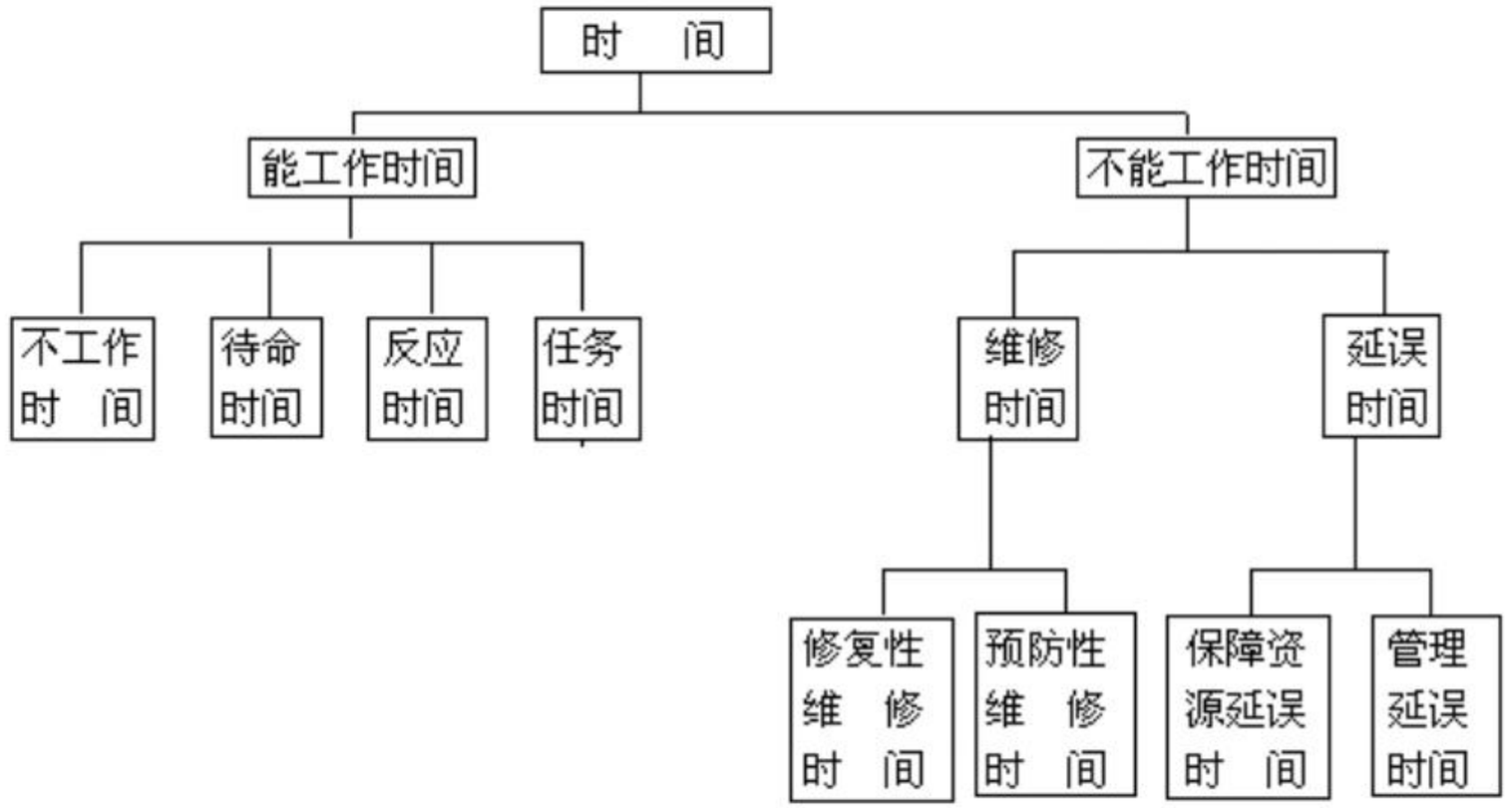
可用度的参数含义

可用度—A

可用度为在任意随机时刻，产品处于可运行状态的概率。

用以下公式计算：

$$A=\frac{\text{可工作时间（MUT）}}{\text{可工作时间（MUT）}+\text{不可工作时间（MDT）}}=1-\frac{\text{MDT}}{\text{MUT}+\text{MDT}}$$



可用度的参数

固有可用度－A_i

A_i（inherent Availability）指只考虑到故障修复情况，不进行预防性维修（保养），没有资源延迟，也没有管理延迟。

A_i的计算方法为：

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

可达可用度－A_a

A_a（achieved Availability）考虑到故障修复和预防性情况，没有考虑备件和管理延迟

A_a的计算方法为

$$A_a = \frac{MTBM}{MTBM + MTTM}$$

运行可用度－A_o

A_o（operational Availability）考虑到故障修复和预防性情况，并考虑到保障延迟。

A_o的计算方法为：

$$A_o = \frac{MTBM}{MTBM + MDT}$$

可用度计算举例

某型号电子铁路产品每 120 天保养一次，平均每次保养时间为 3 天。该产品的故障率为 2 次/年，故障的平均修复时间为 4 小时，备件供给延迟和管理延迟的累积时间为 1.5 天。

按每年 360 天运营计算，已知参数和中间参数如下：

λ ＝2 次/年 ＝0.0055 次/天

$$MTBF=\frac{1}{\lambda}=\frac{1}{2}=0.5\text{年}=180\text{天}$$

$MTBM_p$=120 天

$MTTM_p$＝3 天

MTTR＝4 小时＝0.167 天

可用度计算举例

$$MTBM = \frac{1}{\frac{1}{MTBF} + \frac{1}{MTBM_p}} = \frac{1}{\frac{1}{180} + \frac{1}{120}} = 72.46\text{天}$$

$$\text{MTTM} = \text{MTBM} * \left(\frac{MTTR}{MTBF} + \frac{MTTM_P}{MTBM_p} \right) = 72.46(\frac{0.167}{180} + \frac{3}{120}) = 1.87\text{天}$$

备件延迟(SDT)＋管理延迟(ADT)＝1.5 天

MDT＝1.5+1.87=3.37 天

于是，

固有可用度：

$$A_i = \frac{MTBF}{MTBF + MTTR} = \frac{180}{180 + 0.167} = 99.91\%$$

可达可用度：

$$A_a = \frac{MTBM}{MTBM + MTTM} = \frac{72.46}{72.46 + 1.87} = 97.48\%$$

运行可用度：

$$A_o = \frac{MTBM}{MTBM + MDT} = \frac{72.46}{72.46 + 3.37} = 95.56\%$$

参数	符号	量纲
平均危险故障间隔时间	MTBF(H)	时间，距离，周期
平均安全系统故障间隔时间	MTBSF	时间，距离，周期

MTBF(H)是平均危险故障间隔时间（Mean Time Between Hazard Failure），除了故障定义为特定的危险故障外，计算方法与 MTBF 一致。同故障率类似，MTBF(H)的倒数称为危险率（也称为事故率），用 H(t)符号表达。

一般来说，MTBF(H)是铁路产品唯一的安全性参数，但有时也称为 MTBHE（Mean Time Between Hazard Event）。

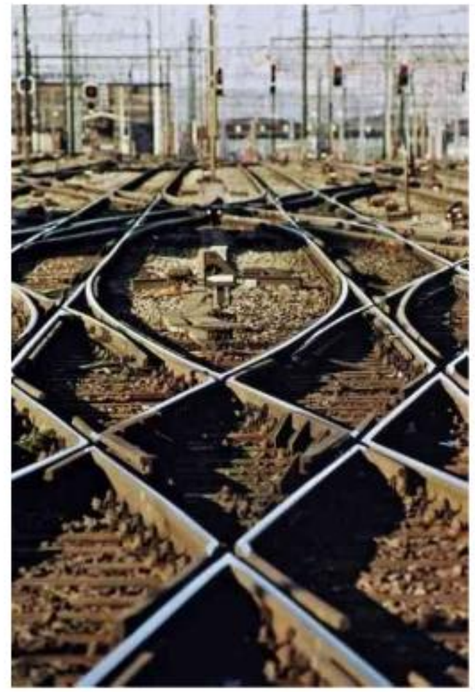
MTBSF 是平均安全系统故障间隔时间（Mean Time Between Safe System Failure），除了故障定义安全系统的故障外，计算方法与 MTBF 一致。值得注意的是，MTBSF 与安全系统的 MTBF 是不同的。

CENELEC规定的RAMS要求

- RAMS 指标要求
- 风险控制分析要求
- 安全完整性要求
- 故障导向安全要求

危险（Hazard）

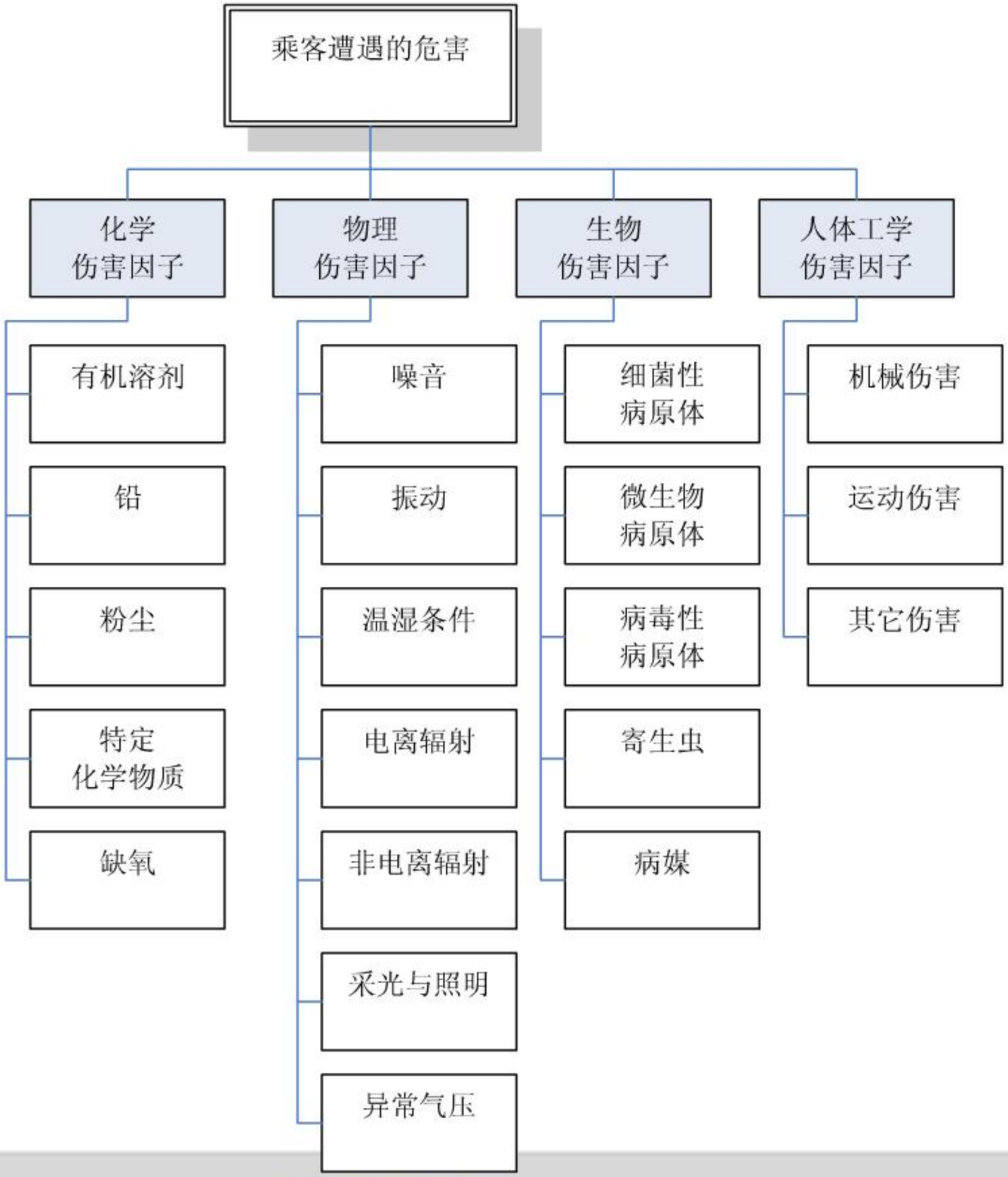
- 导致下列后果的产品状态：
  - 违反政府法规
  - 人员伤亡
  - 重大财产损失
  - 环境破坏
- 危险事件 = 事故 = Hazard Event



Point Track Element

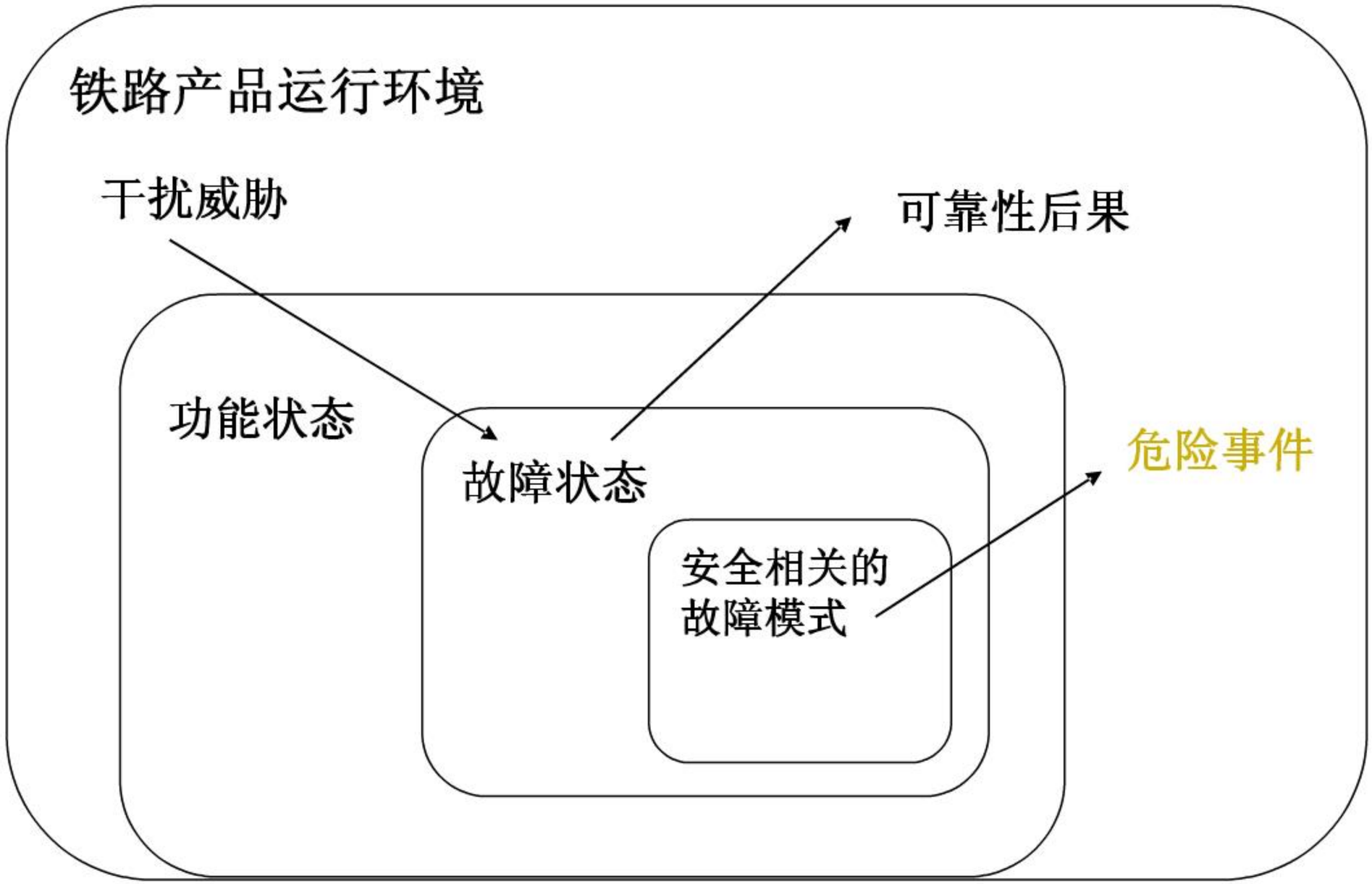
危险原因	激发因素	预防和控制
产品故障	产品缺陷，偶然故障	可靠性、安全性设计和控制
操作失误	人的特性，程序错误	人素工程、容错设计、人员培训
不可抗拒力	地震、洪水、人为破坏等	不可预防

危险来自于...


乘客遭遇的危害
化学伤害因子
物理伤害因子
生物伤害因子
人体工学伤害因子
有机溶剂
铅
粉尘
特定化学物质
缺氧
噪音
振动
温湿条件
电离辐射
非电离辐射
采光与照明
异常气压
细菌性病原体
微生物病原体
病毒性病原体
寄生虫
病媒
机械伤害
运动伤害
其它伤害

危险的类别

- MIL-STD-882C 定义的危险类别：
  - 加速器或辐射器
  - 放射性材料
  - 爆炸物
  - 激光
  - 化学毒性材料
  - 电
  - 机械危险
  - 非电离辐射
  - 热危险
  - 压力危险
  - 噪音
  - 环境危险
  - 火灾
  - 其它危险


铁路产品运行环境
干扰威胁
可靠性后果
功能状态
故障状态
安全相关的
故障模式
危险事件

风险（Risk）

- 风险是危险的评价参数
  - 危险导致的后果 - 危险严重性（Severity）
  - 危险发生的频繁程度 - 危险可能性（Occurrence）

- Risk = Severity × Occurrence

危险严重性

符号	严重程度	对人和环境的后果	常用系数
I	灾难的	导致多个人员死亡或多重严重伤害 严重破坏环境	10
II	危急的	导致单人死亡或严重受伤 明显破坏环境	1
III	临界的	人员轻伤 对环境有明显威胁。	0.1
IV	轻微的	对人可能的轻微伤害	0.01

危险可能性

符号	分类	衡量参考	描述
A	频繁发生	每年10次	很可能经常发生，将持续经历危险
B	可能发生	每年1次	将发生几次，预期危险经常发生
C	偶然发生	10年1次	可能发生几次，预期危险发生几次
D	很少发生	100年1次	在系统寿命周期内可能发生，有理由预期危险将发生
E	几乎不可能	1000年1次	不太可能发生，可以设想预期的危险可能发生。
F	不会发生	小于1000年1次	极不可能发生，可以认为危险不会发生

风险的计算

危险严重性

符号	严重程度	常用系数
I	灾难的	10
II	危急的	1
III	临界的	0.1
IV	轻微的	0.01

危险可能性

符号	分类	衡量参考
A	频繁发生	每年10次
B	可能发生	每年1次
C	偶然发生	10年1次
D	很少发生	100年1次
E	几乎不可能	1000年1次
F	不会发生	小于1000年1次

可能性等级	风险控制类别			
A				
B				
C				
D				
E				
F				
	Ⅳ	Ⅲ	Ⅱ	Ⅰ
	严重性等级			

风险接受

不可接受

不希望的

可容忍的

可忽略的

危险风险控制（Risk Control）

- 最小风险设计 - 降低危险风险的设计措施、如冗余设计、故障导向安全设计等
- 安全装置 - 自动的或其它安全防护装置，使风险严重性降低。
- 报警装置 - 采用报警装置检测危险状况，并向有关人员发出适当的报警信号。
- 专用规程 - 制定专用的规程和进行培训。

安全完整性等级（SIL）

- 安全完整性（Safety Integrity） - 与安全相关的系统达到规定的安全性要求的能力
- 安全完整性等级（SIL-Safety Integrity Level） - 对铁路产品或功能达到某种级别的安全性的一种分类要求。
- SIL 分为1、2、3、4共四个等级，SIL等级越高说明安全性完整性水平越高，危险的风险越小，相应的需要开展的安全性工作就越多，系统安全性的要求也就越严格。

EN50129 给出的SIL表

THR per hour per function	Safety Integrity Level
10^{-9}<=THR<10^{-8}	4
10^{-8}<=THR<10^{-7}	3
10^{-7}<=THR<10^{-6}	2
10^{-6}<=THR<10^{-5}	1

- THR- Tolerable Hazard Rate(可容忍的危险率）
- 铁路产品的用户会为承包商提出SIL 要求，承包商需将SIL 要求分配给各个子承包商和供应商。

- 故障导向安全（Fail-Safe）是当故障发生时，使故障转向安全策略，或者说使产品尽可能发生不引起危险的故障。

例如，当铁路产品上的速度显示装置发生指示错误时，只允许它发生不指示或速度指示值比实际运行速度值高的错误，不允许发生速度指示值比实际运行速度值低的错误。

- 故障导向安全是在铁路行业应用广泛的技术，主要是一种设计技术，通过设计控制使故障导向安全。
- 对故障导向安全要求的评估通常需结合FTA、FMEA等分析技术进行。

内容安排

1 RAMS 技术基础

2 RAMS 技术要求

3 RAMS 体系框架

4 RAMS 关键技术

3.1 RAMS 管理平台

- RAMS 管理组织
  - RAMS 责任体系
  - RAMS 管理结构
  - RAMS 专业机构
- RAMS 工作体系
  - RAMS 保证大纲
  - RAMS 工作计划
- RAMS 工作资源
  - 专业软件
  - 试验设备
  - 数据

RAMS大纲和计划

项目阶段	RAMS 工作项目
预先研究	● 评估在规定条件下应用的 RAMS 目标
可行性研究	● 评估 RAMS 要求 ● 评估 RAMS 历史经验数据 ● 确定特别应用施加到安全性的影响 ● 与用户协商 RAMS（如必要）
邀请招标	● 施行初步 RAMS 分析（最坏状况） ● 分配系统 RAMS 要求（子系统 / 部件，其他相关系统等） ● 进行系统危险风险分析 ● 进行与 RAM 相关的风险分析 ● 准备将来的 RAMS 数据评估 ● 关于 RAMS 的逐条讨论
合同谈判	● 审查 / 更新初步的 RAMS 分析和 RAMS 分配
定义系统要求	● 制定项目 RAMS 管理 ● 确定系统 RAMS 要求 ● 制定 RAMS 大纲 ● 分配 RAMS 要求到子承包商和供应商。 ● 定义 RAMS 验收标准
设计和实现	● 可靠性分析（FMEA、建模、预计） ● 安全性分析（FMECA、FTA、ETA、HAZOP） ● 维护 / 维修分析；定义维护 / 维修策略 ● 基于维护 / 维修策略的可用性分析 ● RAMS 评审 ● 评估寿命周期成本 ● RAMS 验证，证据收集 ● 设计 / 生产 FMEA ● 可靠性和维修性试验，如可采用
采购	● 提供 RAMS 技术规范给子承包商和供应商
生产试验	● 与 RAMS 相关的质量保证 / 工序保证
试车 / 验收	● 进行 RAM 验证 ● 准备安全性应用案例 ● 开始 RAMS 数据评估 ● 在早期运行中进行 RAM 试验，数据筛选和评估
运行 / 维护	● 临时运行和维护（维护 / 修理策略） ● 运行和维护人员培训

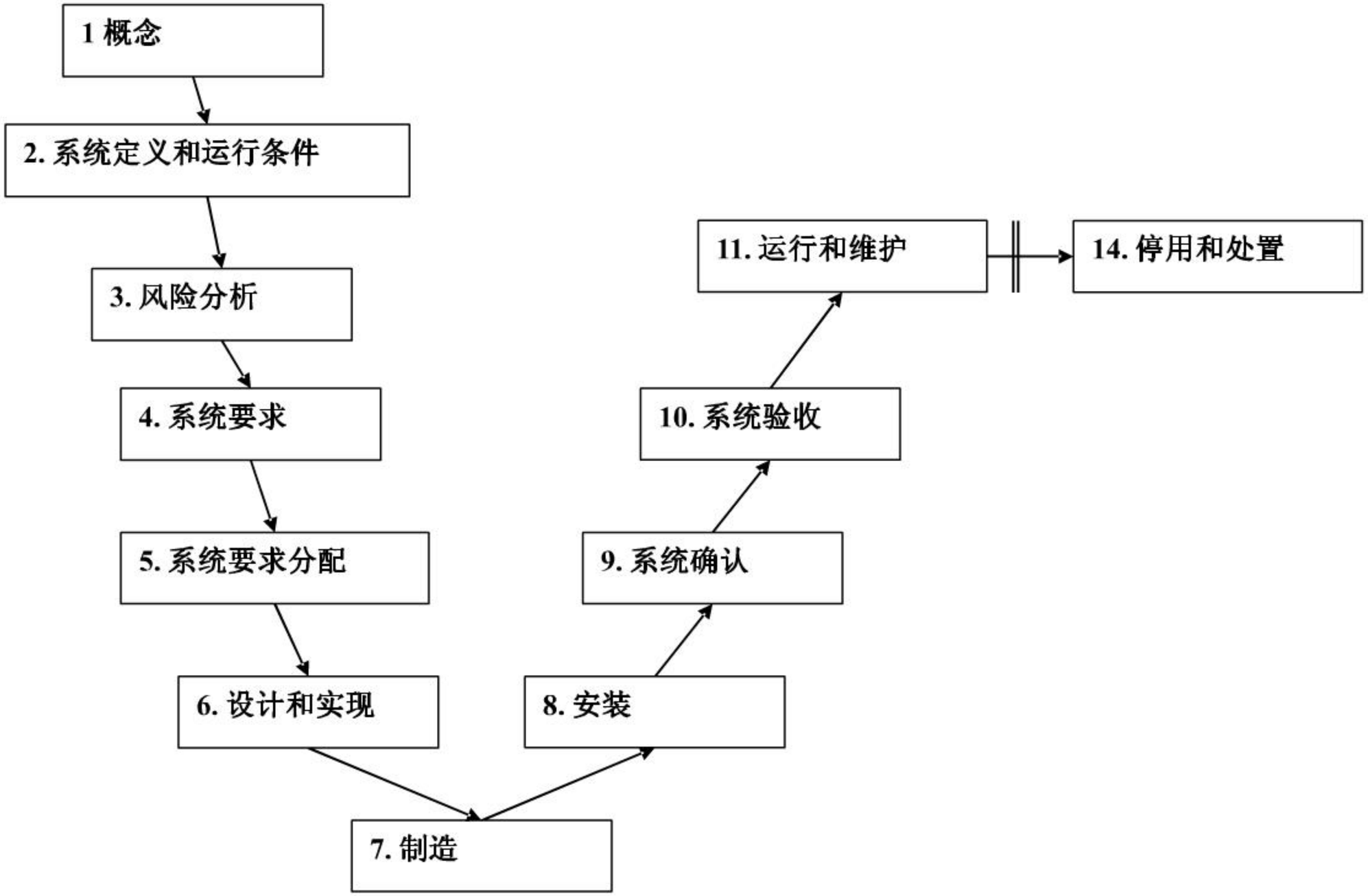
- **工作要求**
- **工作责任**
- **时间节点**
- **评审要求**

3.2 RAMS 工作项目

RAMS 工作类别	RAMS 工作项目
RAMS 管理	提出并确定 RAMS 要求
	建立 RAMS 工作大纲
	建立 RAMS 工作计划
	确定 RAMS 的组织和责任
	RAMS 数据管理
RAMS 设计与分析	历史数据和经验的积累和分析
	RAMS 设计分析工具的使用
	风险分析和控制
RAMS 试验	为了改进 RAMS 特性的试验
	环境应力筛选试验
	RAMS 验证试验
RAMS 验证	RAMS 评估和评审
	RAMS 试验验证
	RAMS 使用验证

RAMS 分析项目

序号	工作项目	覆盖内容	工作输入	工作输出
1	系统功能分析和故障定义	系统结构树 功能框图 故障定义和故障判据	任务剖面 RAMS 要求 系统功能原理 系统组成清单	系统功能分析和定义报告
2	可靠性框图建模(RBD)	可靠性框图分析	系统功能分析和定义报告	可靠性框图模型报告
3	可靠性预计分析	可靠性预计分析 最坏情况分析 敏感性分析和权衡分析	可靠性框图 BOM 清单 设计资料	可靠性预计分析报告
4	故障模式影响及危害性分析(FMECA)	故障模式影响分析 危害性分析	系统功能分析和定义报告 可靠性框图报告 可靠性预计报告	FMECA 报告
5	故障树分析(FTA)	故障树分析 重复故障分析 共因故障分析	系统功能分析和定义报告 顶事件定义	FTA 报告
6	事件树分析（ETA）	事件树分析	初步危险分析报告	ETA 报告
7	操作危险研究(HAZOP)	操作危险分析	初步危险分析报告 FMECA 报告	HAZOP 报告
8	维修性预计	维修性预计	系统功能分析和定义报告 可靠性预计报告	维修性预计报告
9	可用性分析	可用性分析 权衡分析	可靠性预计报告 维修性预计报告 FTA 报告	可用性分析报告
10	初步危险分析	确定危险源 危险初步分析和评价	系统功能分析和定义报告 可靠性框图报告 FMEA 报告	初步维修分析报告
11	设备危险分析	设备危险分析	初步危险分析报告 可靠性预计分析报告 FMECA 报告 FTA 报告 ETA 报告 初步危险分析报告	设备危险分析报告
12	接口危险分析	接口危险分析	系统功能分析和定义报告 HAZOP 报告 FMECA 报告	接口危险分析报告


1 概念
2. 系统定义和运行条件
3. 风险分析
4. 系统要求
5. 系统要求分配
6. 设计和实现
7. 制造
8. 安装
9. 系统确认
10. 系统验收
11. 运行和维护
14. 停用和处置

寿命周期阶段	阶段 RAM 工作	阶段安全性工作
1. 概念阶段	审查以前产品的 RAM 能力 考虑项目 RAM 含义	审查以前产品安全性能力 考虑项目安全含义 审查安全策略和安全目标
2. 系统定义和应用条件	评估过去的 RAM 数据 进行初步 RAM 分析 设定 RAM 策略 确定长期运行＆维护条件 确定现有设施制约对 RAM 的影响	评估过去的安全数据 进行初步安全分析 设定安全策略 定义可容许的风险标准 确定现有设施制约对安全的影响
3. 风险分析		进行系统危险风险分析 建立危险日志 进行风险评估
4. 系统要求.	确定系统ＲＡＭ 规格要求和验收标准 定义系统功能结构 建立ＲＡＭ 大纲 建立ＲＡＭ 管理	确定系统安全性规格要求和验收标准 定义安全相关的功能性要求 建立安全管理
5. 系统要求分配	分配系统 RAM 要求，确定子系统＆部件 RAM 要求和验收标准	分配安全目标和要求，确定子系统＆部件安全性要求和验收标准 更新系统安全计划

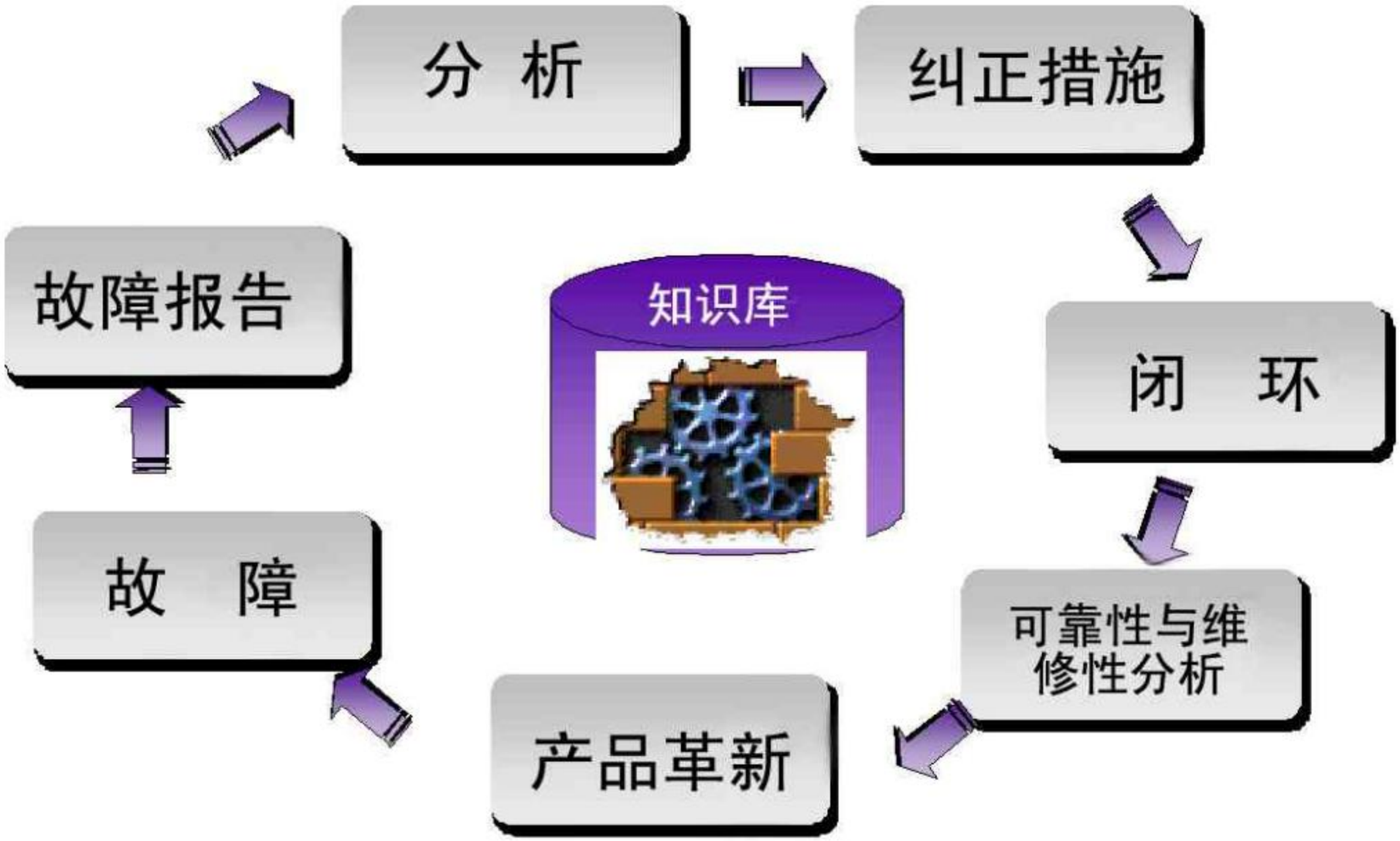
寿命周期阶段	阶段 RAM 工作	阶段安全性工作
6. 设计和执行	通过审查、分析、试验和数据评估执行 RAM 工作项目，包括： 1. 可靠性和可用性 2. 维护和维修性 3. 优化维护策略 4. 后勤支持	通过审查、分析、试验和数据评估执行安全计划，包括： 5. 危险日志 6. 危险分析和风险评估 7. 验证安全相关的设计决定
7. 生产	进行环境应力筛选 RAM 改进试验 启动故障报告和纠正系统	通过审查、分析、试验和数据评估履行安全计划 使用危险日志
8. 安装	对维修人员进行培训 建立备件和工具供应	建立安装程序 执行安装程序
9. 系统确认	进行 RAM 验证	建立试车程序 执行试车程序 准备安全案例

寿命周期阶段	阶段 RAM 工作	阶段安全性工作
10. 系统验收	进行 RAM 验证	评审安全性案例
11. 运行和维护	获得备件和工具 进行可靠性维护和后勤支持	执行以安全性为中心的维修 监控和维护危险日志
12. 性能监控	采集，分析，评估和使用性能&RAM 统计数值	采集，分析，评估和使用性能&安全统计数值
13. 改进和更新	考虑改进和更新的ＲＡＭ含义	考虑改进和更新的安全性含义
14. 停用和处理	无 RAM 活动	建立安全计划 进行危险分析和风险评估 执行安全计划

- FRACAS 是 “Failure Report Analysis and Corrective Action System” 的缩写，是“故障报告、分析及纠正措施系统” ，
- FRACAS 通常也称为“故障信息闭环管理系统” 。
- FRACAS 有多种称法，如“归零管理” 、 “PRACAS”、 “8D”等。

- 利用“信息反馈，闭环控制”的原理，通过一套规范化的程序，使发生的产品故障能得到及时的报告和纠正，从而实现产品可靠性的增长，达到对产品可靠性和维修性的预期要求，防止故障再现。

- 通过FRACAS 建立企业问题/故障信息数据库，为可靠性设计和分析以及关于维修策略、保障策略和备件策略的制定提供数据支持。


分 析
纠正措施
故障报告
知识库
闭 环
故 障
可靠性与维修性分析
产品革新

利用 FRACAS，可以：

1. 及时有效地处理当前故障

2. 过去发生的故障不再重现

3. 建立企业的可靠性经验

FRACAS代表两个系统

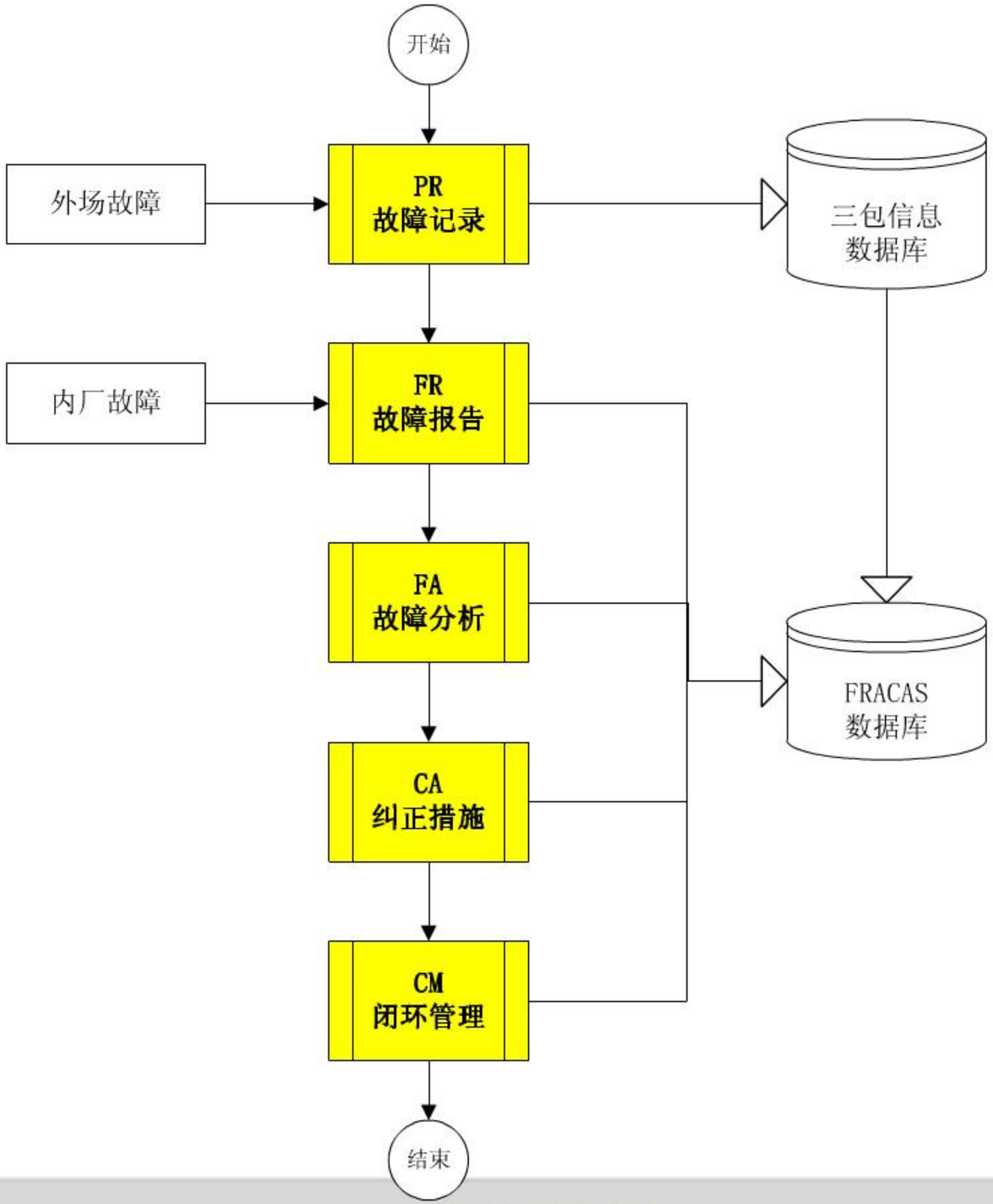
FRACAS是一个工作系统

- 组织机构(各方代表)
- 人员职责分工
- 工作的流程
- 资源保障

FRACAS是一个信息系统

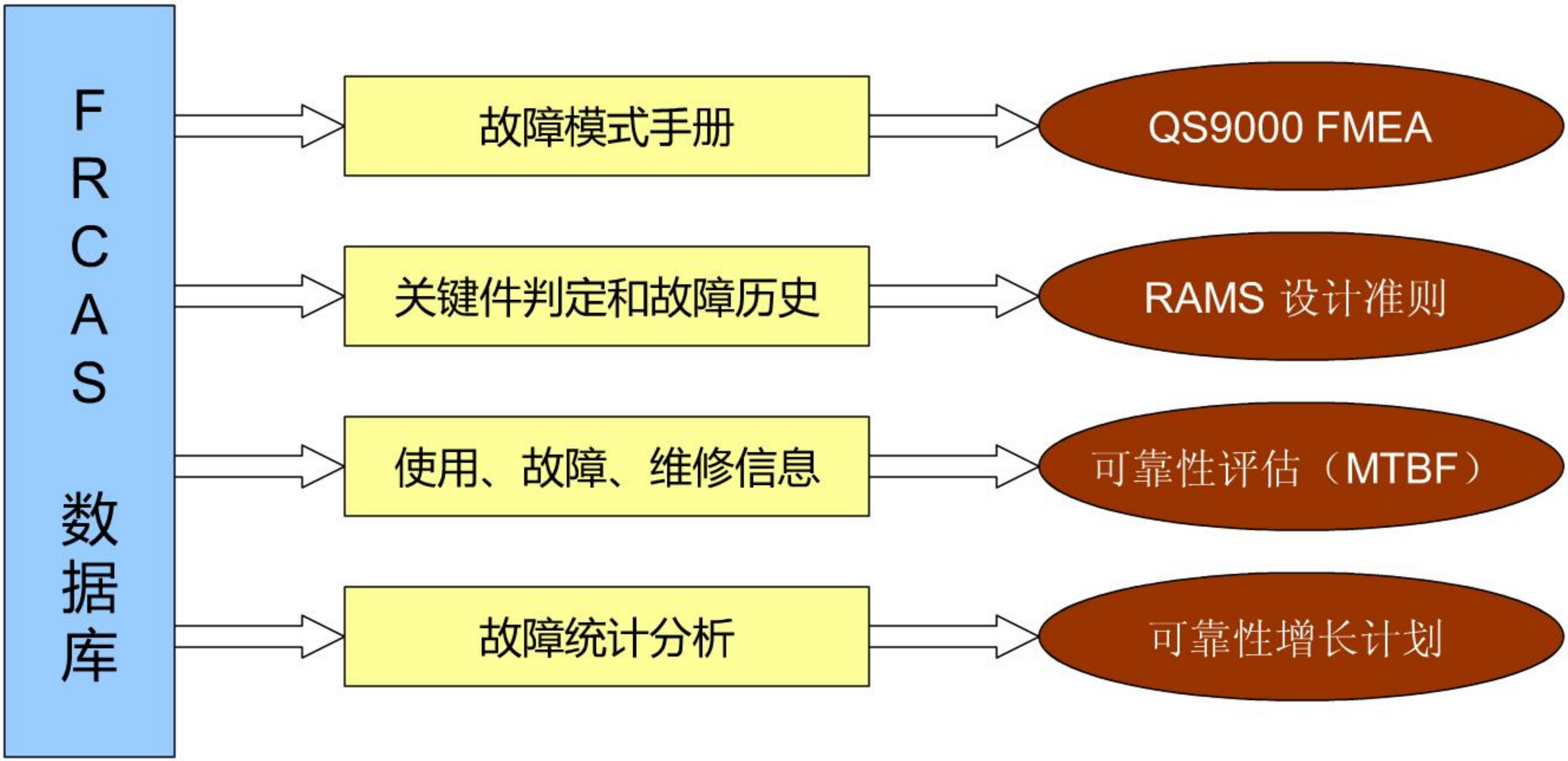
- 与可靠性信息系统的关系
- 信息准确与完整性
- 及时性、正确性
- 可追踪性

FRACAS 流程



- 故障记录表
- 故障报告表
- 故障分析表
- 纠正措施表
- 闭环管理表

FRACAS故障信息的利用



内容安排

1 RAMS 技术基础

2 RAMS 技术要求

3 RAMS 体系框架

4 RAMS 关键技术

- 可靠性建模（RBD）
- 可靠性预计
- 维修性预计
- 可用性计算
- 故障模式影响与危害性分析（FMECA）
- 初步危险分析 (PHA)
- 故障树分析 (FTA)
- 事件树分析 (ETA)

4.1 可靠性框图模型（RBD）

- 可靠性框图模型包括：
  - 可靠性框图
  - 数学模型
- 可靠性框图模型分析的程序是：

1. 系统定义（任务和功能、组成与接口、工作模式等）
2. 任务定义和故障判据
3. 建立可靠性框图
4. 建立可靠性数学模型
5. 可靠性模型计算
6. 结果分析和设计调整

系统可靠性度

System Rel = *f* (Subsys Rel)

Goals *Analysis*

子系统可靠度

SubSys Rel = *f* (Asm Rel)

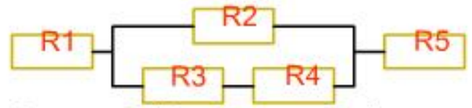
组件可靠度

Asm Rel = *f* (Comp Rel)

零件/元器件可靠度

Comp Rel = *f* (可靠度)

可靠性关系模型

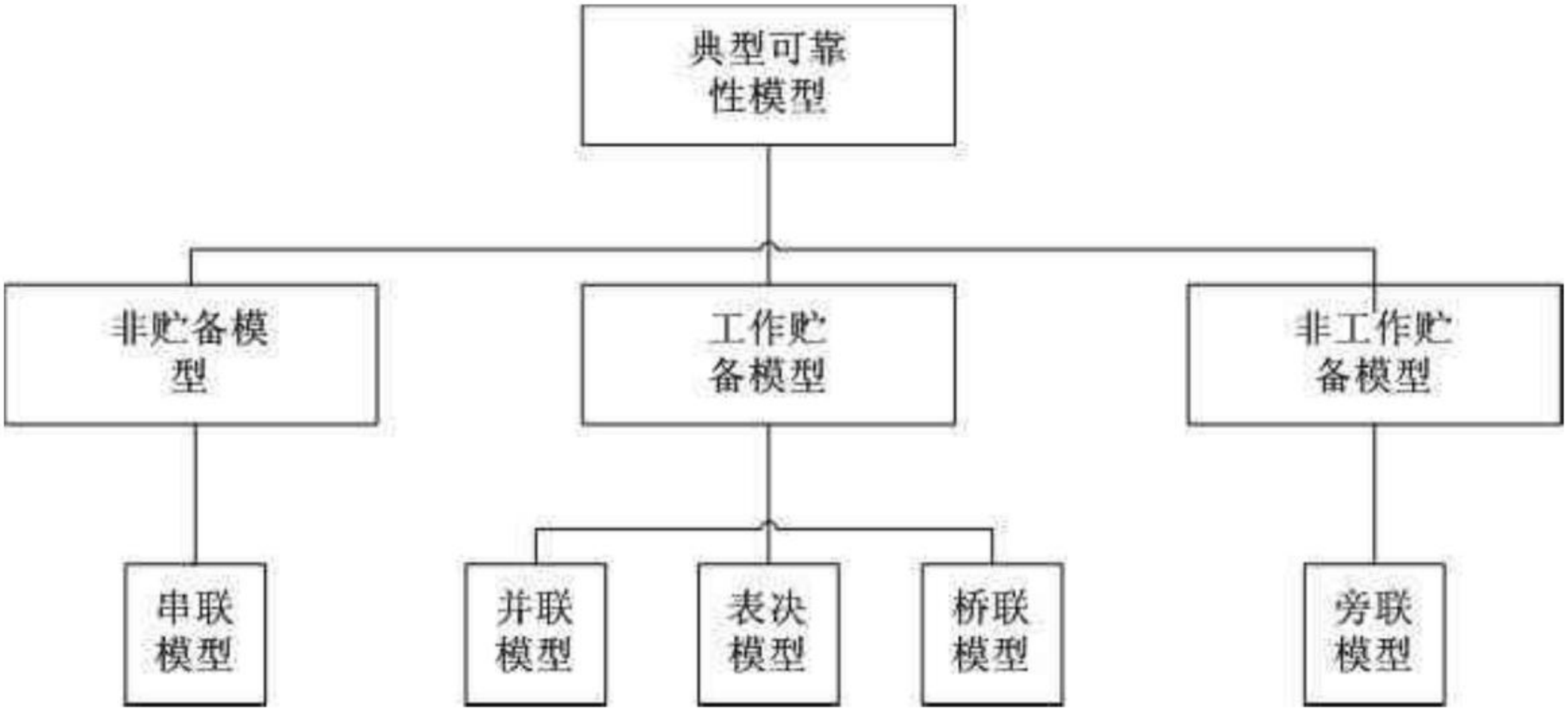


$R_{Total} = f(R_1, R_2, \ldots R_N)$

$R = e^{(\lambda)(-t)}$

$\lambda = \frac{Ln(R)}{-t}$

典型的可靠性框图模型

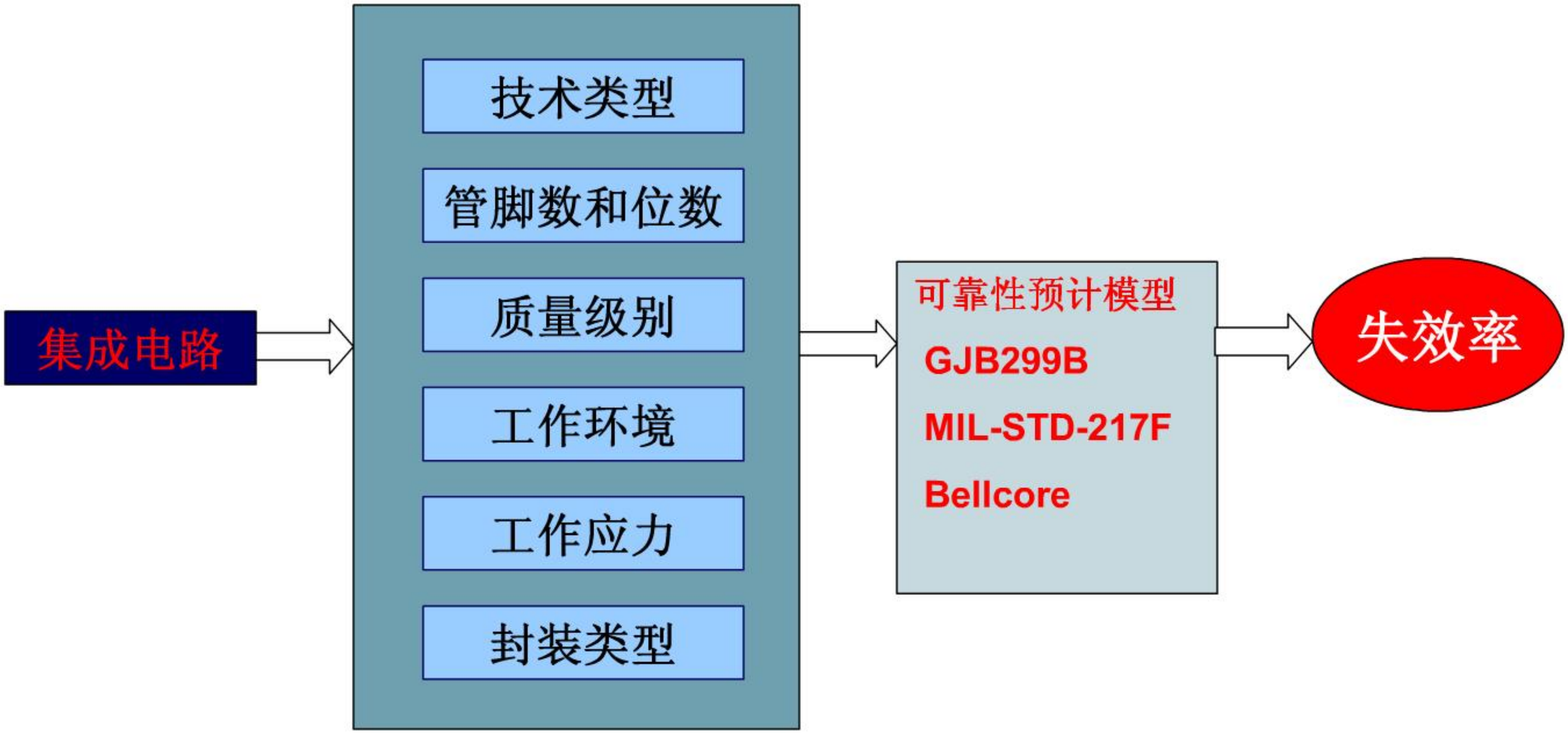


Demonstration

演示

4.2 可靠性预计

- 可靠性预计：根据产品结构和使用特性来评估产品可靠性水平的方法；
- 可靠性预计的目的：评估产品可靠性水平是否达到要求，并根据预计结果指导可靠性设计，提高产品可靠性；
- 可靠性预计方法：
  - 电子产品：元件计数法、应力分析法
  - 机械产品：概率分析法
- 可靠性预计参数：
- MTBF1,MTBF2,MTBF3,MTBF4,
- MTBF,MDBF;


集成电路
技术类型
管脚数和位数
质量级别
工作环境
工作应力
封装类型
可靠性预计模型
GJB299B
MIL-STD-217F
Bellcore
失效率

国外的电子产品的可靠性预计标准

标准编号	标准名称	发布机构	说明
MIL-HDBK-217F	电子设备可靠性预计手册	美国军方	该标准几乎为所有类型电子元器件提供了可靠性模型，是世界上应用最广泛的预计标准。现行版本为Notice 1,2。
Telcordia/Bellcore SR-332	可靠性预计程序文件	贝尔通讯实验室	该标准最初来源于MIL-HDBK-217,后经修改用于非军事领域。现行版本为SR-332。除了几乎适用于全部的电子元件外，Bellcore还可以利用实验数据、现场数据和老化数据对预计结果进行修正
CNET 93	可靠性预计程序文件	英国电信	该标准为大范围的元器件提供了可靠性模型。与MIL-HDBK-217相似，它是个综合性模型，可用来进行详尽的应力分析。
HRD5	可靠性预计程序文件	法国电信	该标准为大范围的元器件提供可靠性模型。与CNET 93相似，但它提供相对简单的模型，需要较少量的数据参数进行分析。

Demonstration

演示

4.3 维修性预计

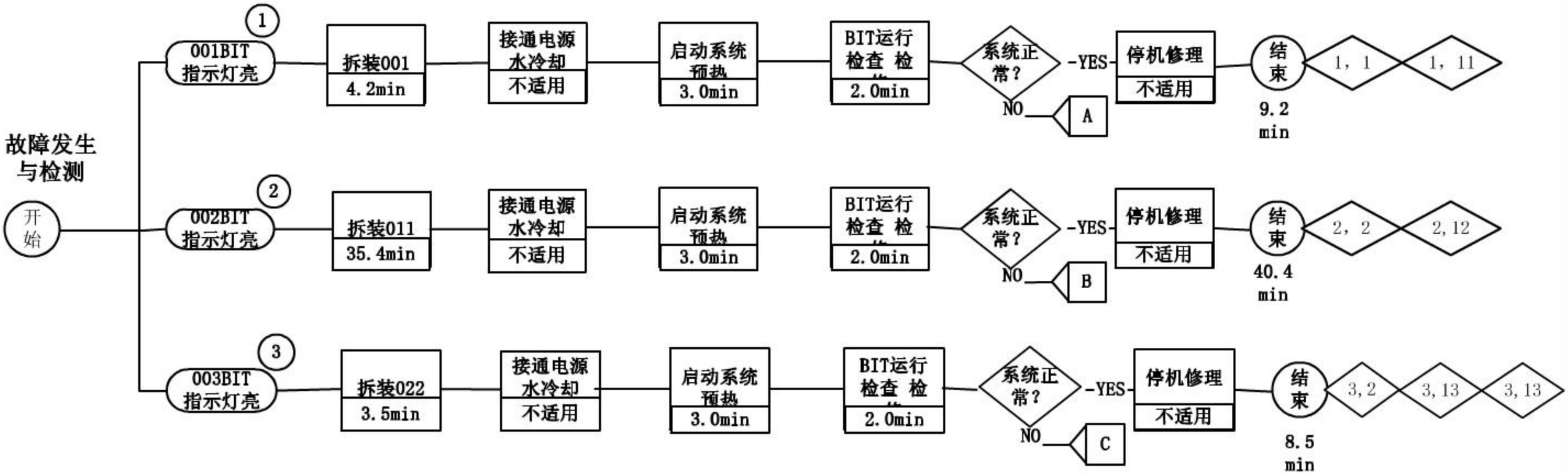
- 预计——预先估计产品的维修性参数，了解其是否满足规定的维修性指标。
- 定义：

  根据历史经验和类似产品的数据等估计、测算新产品在给定工作条件下的维修性参数，以了解产品设计满足维修性要求的程度。

- 预计的对象：
  - 参数：与合同规定的指标相一致，MTTR
  - 层次：通常是系统或设备级，以便与合同要求规定和使用需要相比较。

返回

维修流程图


故障发生
与检测
开始
1
001BIT
指示灯亮
拆装001
4.2min
接通电源
水冷却
不适用
启动系统
预热
3.0min
BIT运行
检查 检
2.0min
系统正
常？
-YES
停机修理
不适用
结
束
9.2
min
1，1
1，11
NO
A
2
002BIT
指示灯亮
拆装011
35.4min
接通电源
水冷却
不适用
启动系统
预热
3.0min
BIT运行
检查 检
2.0min
系统正
常？
-YES
停机修理
不适用
结
束
40.4
min
2，2
2，12
NO
B
3
003BIT
指示灯亮
拆装022
3.5min
接通电源
水冷却
不适用
启动系统
预热
3.0min
BIT运行
检查 检
2.0min
系统正
常？
-YES
停机修理
不适用
结
束
8.5
min
3，2
3，13
3，13
NO
C

返回

- 计算

$$MTTRs = \sum_{i=0}^{n} \frac{MTTR_i * \lambda_i}{\lambda_s}$$

$MTTR_S$ 为系统的平均修复时间；

$MTTR_i$ 为针对系统组成单元i的平均修复时间；

λ_i 为系统组成单元i的失效率；

n 为设定了维修时间的全部系统组成单元数量；

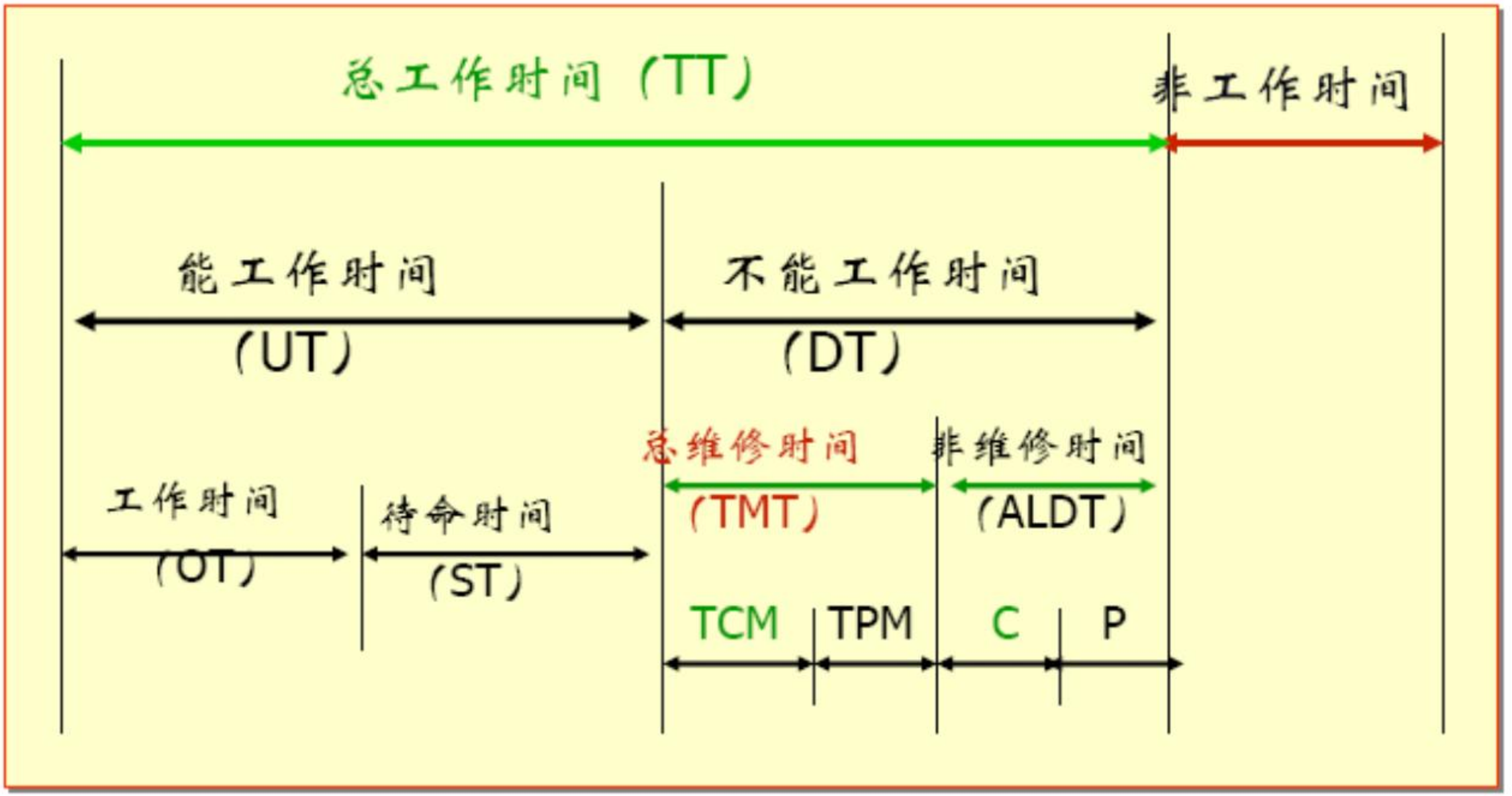
λ_S 为系统失效率。

4.4 可用性分析

- 可用性分析目的是分析产品的固有、运行等可用性参数指标，用于评价其是否符合要求，并针对其符合性结果进行设计或保障、维护策略的调整。

- 要点：
  - 考虑全面的影响因素，包括维修、等待、延迟等；
  - 针对可用性的不同指标进行分别分析。

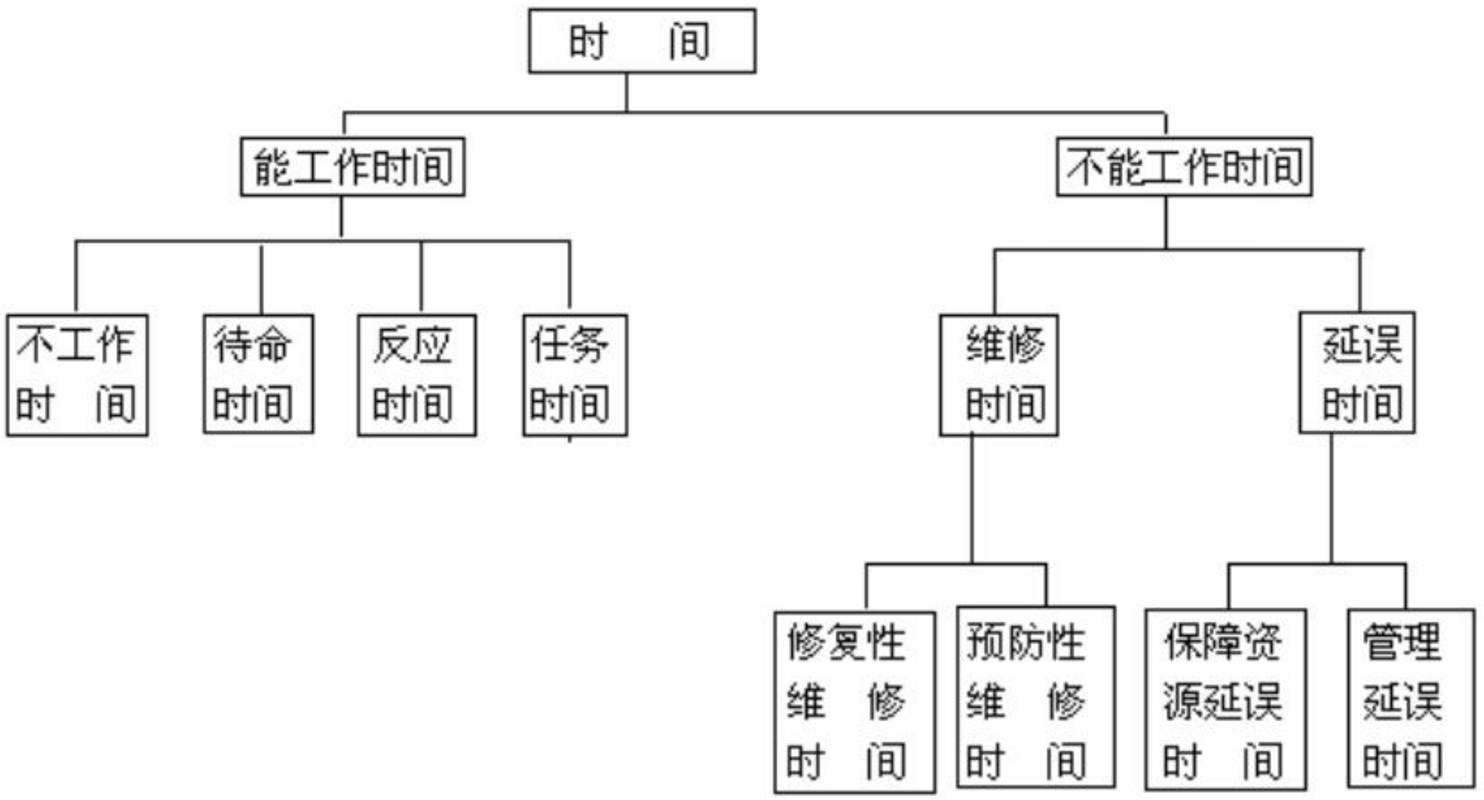
系统总工作时间分解


总工作时间（TT）
非工作时间
能工作时间
（UT）
不能工作时间
（DT）
工作时间
（OT）
待命时间
（ST）
总维修时间
（TMT）
非维修时间
（ALDT）
TCM
TPM
C
P

- 可用度 - A

可用度为在任意随机时刻，产品处于可运行状态的概率。用以下公式计算：

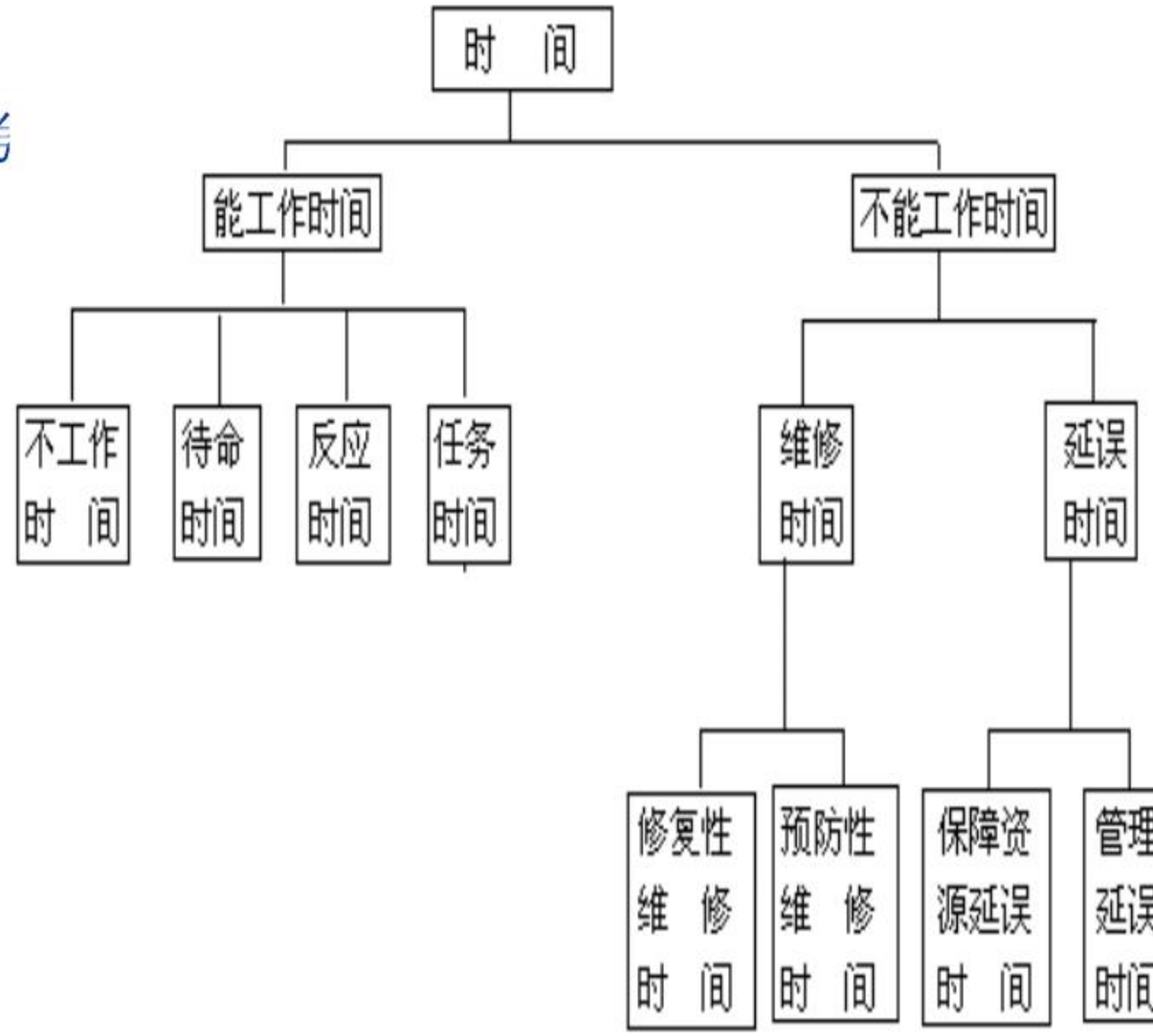
$$A=\frac{\text{可工作时间（MUT）}}{\text{可工作时间（MUT）}+\text{不可工作时间（MDT）}}=1-\frac{\text{MDT}}{\text{MUT}+\text{MDT}}$$



固有可用度 - Ai

Ai（inherent Availability）指只考虑到故障修复情况，不进行预防性维修（保养），没有资源延迟，也没有管理延迟。

Ai的计算方法为：

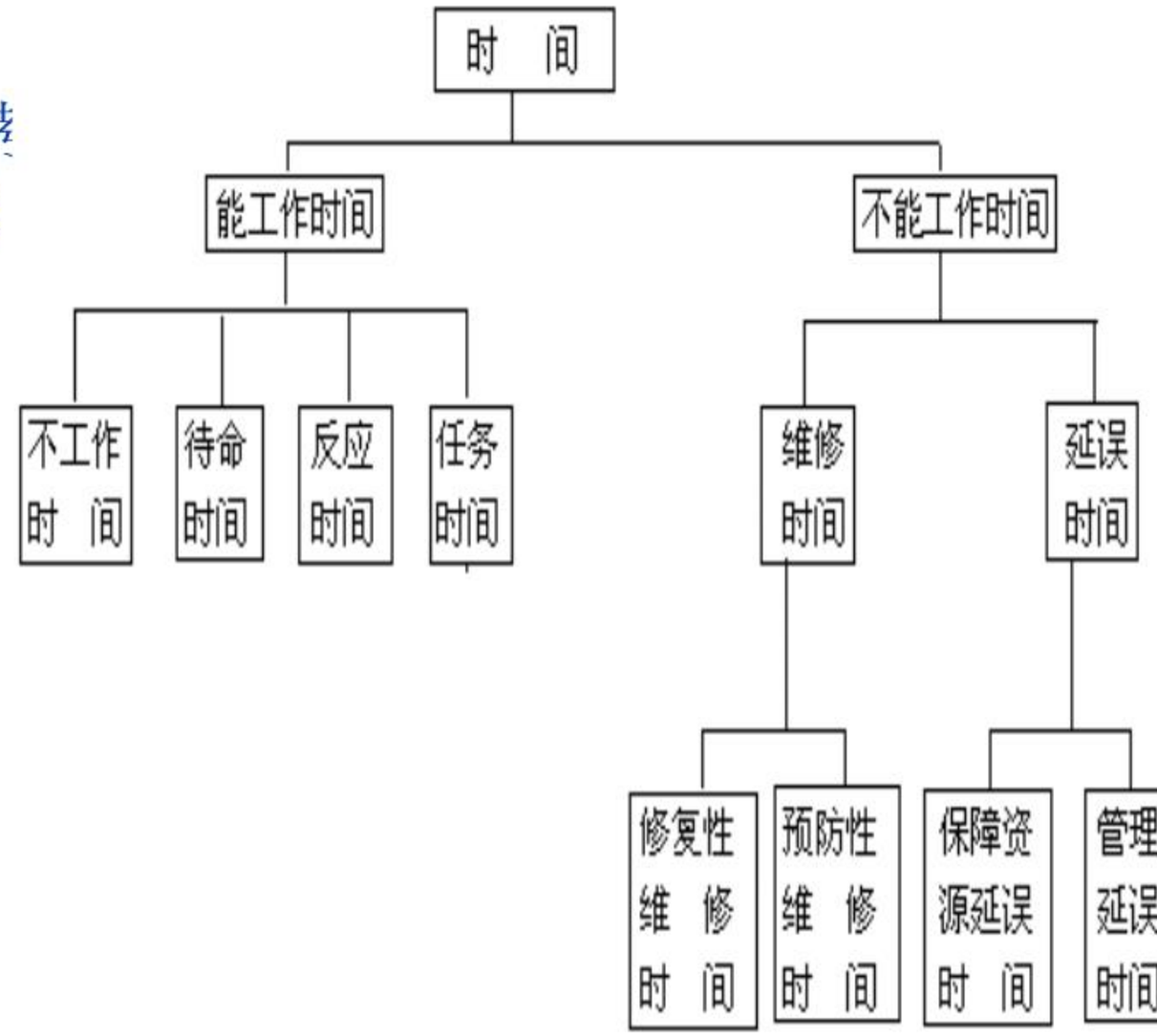


$$A_i = \frac{MTBF}{MTBF + MTTR}$$

可达可用度 - Aa

Aa（achieved Availability）考虑到故障修复和预防性情况，没有考虑备件和管理延迟。Aa的计算方法为：

$$A_a = \frac{MTBM}{MTBM + MTTM}$$

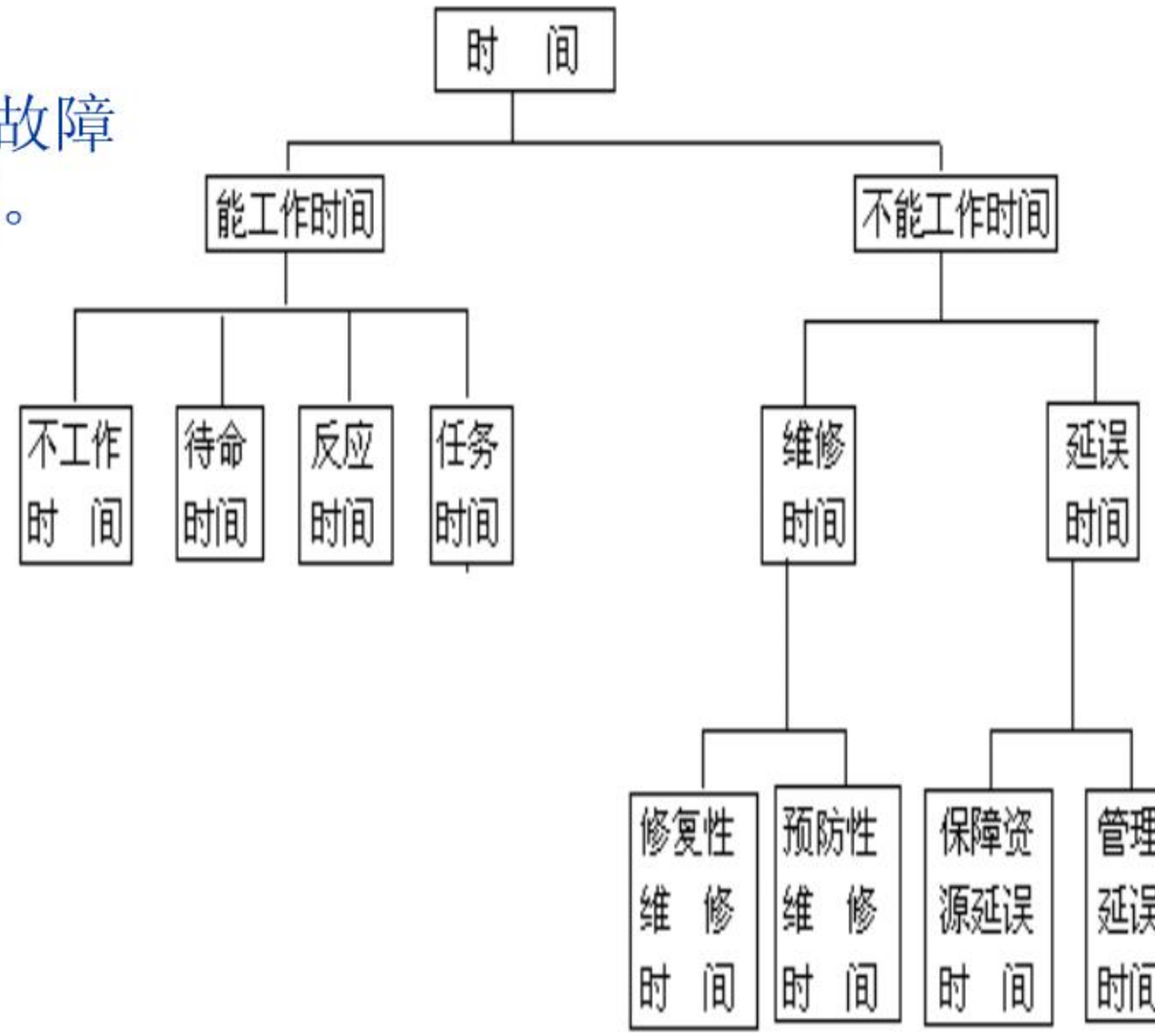


主要参数_运行可用度Ao

- 运行可用度 - Ao

Ao（operational Availability）考虑到故障修复和预防性情况，并考虑到保障延迟。

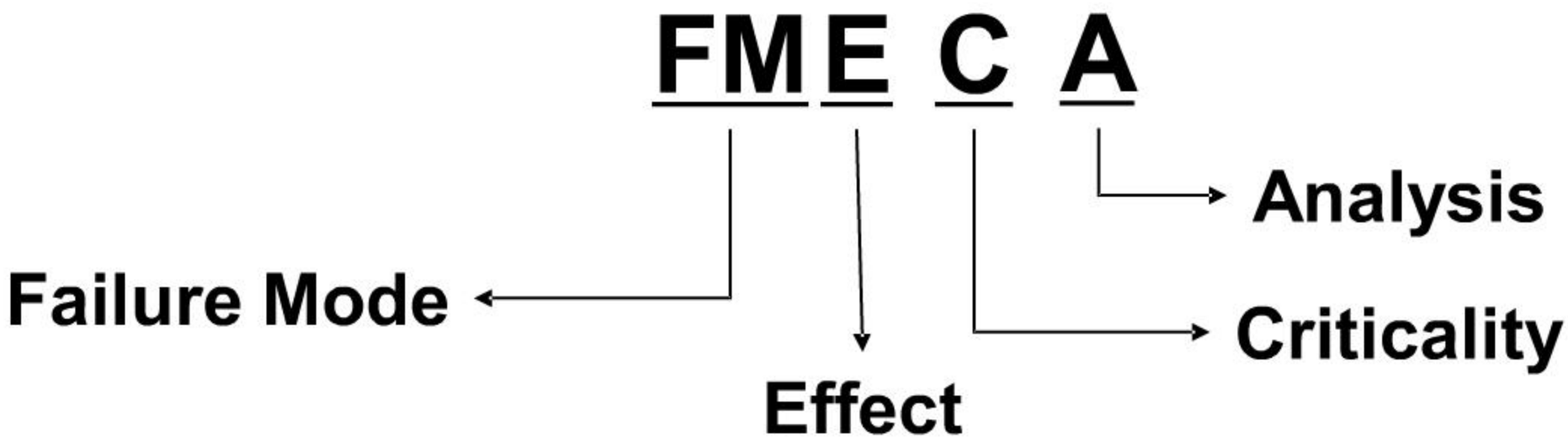
- Ao的计算方法为：



$$A_o = \frac{MTBM}{MTBM + MDT}$$

Demonstration

演示



- 故障模式影响及危害性分析
- 是分析系统中每一产品所有可能产生的故障模式及其对系统造成的所有可能影响，并按每一个故障模式的严重程度、检测难易程度以及发生频度予以分类的一种归纳分析方法。
- 通过FMECA 寻找导致危险的故障，并将其风险进行量化描述

FMECA

FMECA Sheet (CLC/TR 50126-3)

Items FMECA Sheets

Rolling Stock
Code L1
L1 Assy

Code L2
L2 Assy
Drwg or Diagr Ref

Doc. N.
Version Number
Date of version
Drawn up by
Page n/N

File name

Code LRU	LRU Description	Part Number	Qty	Function	Failure Mode	Failure Cause	Failure Rate (F/Mh)	Effects			Criticality	Failure Category	Diagnosis	Corrective Actions	Notes
								Local	Assy	Rolling Stock					

Demonstration

演示

4.6 初步危险分析（PHA）

- 确定危险源 - 根据系统的组成和功能单元的划分，确定各个部位是否存在以下类别的危险：
- 识别危险事件 - 根据已识别的危险源，分析可能导致危险后果的危险事件。
- 危险风险评价 - 对各个危险事件进行风险评价
- 当前控制措施分析 - 针对每个危险事件分析当前已经采取的控制措施
- 安全性计划 - 根据初步危险分析的结果，得到需重点分析和控制的部位和危险事件，修订安全性计划。

危险识别

ID	Name
LA	Door System
LAA	Right drive screw ass'y
LAAA	Drive screw housing, right
LAAB	Spindle, right
LAAC	Center shaft
LAAD	Spindle nut, right
LAAE	Coupling Motor
LAB	Left drive screw ass'y
LABA	Spindle left
LABB	Spindle nut left
LABC	Coupling center

?

- 加速器或辐射器
- 放射性材料
- 爆炸物
- 激光
- 化学毒性材料
- 电
- 机械危险
- 非电离辐射
- 热危险
- 压力危险
- 噪音
- 环境危险
- 火灾
- 其它危险

确定危险事件

- 危险事件可能是：
  - 产品故障模式
  - 流程或操作错误
  - 特殊条件（外部、环境等）

危险日志（Hazard Log）

- 危险事件用危险日志记录
- 危险日志包括：
  - 系统、分系统、单元 - System, subsystem, unit
  - 危险事件描述 - Description
  - 原因 - Cause(s)
  - 影响 - Possible effects, effect on system
  - 分类 - Category(probability and severity)
  - 设计约束 - Design constraints
  - 纠正和预防 - Corrective or preventative measures
  - 安全措施 - possible safeguards
  - 建议措施 - recommended action
  - 危险发生时的运行阶段 - Operational phase
  - 责任 - group or person for ensuring safeguards provided.
  - 试验 - to be undertaken to demonstrate safety.
  - 处理状态 - Status of hazard resolution process

4.7 故障树分析（FTA）

- FTA = Fault Tree Analysis（故障树分析）

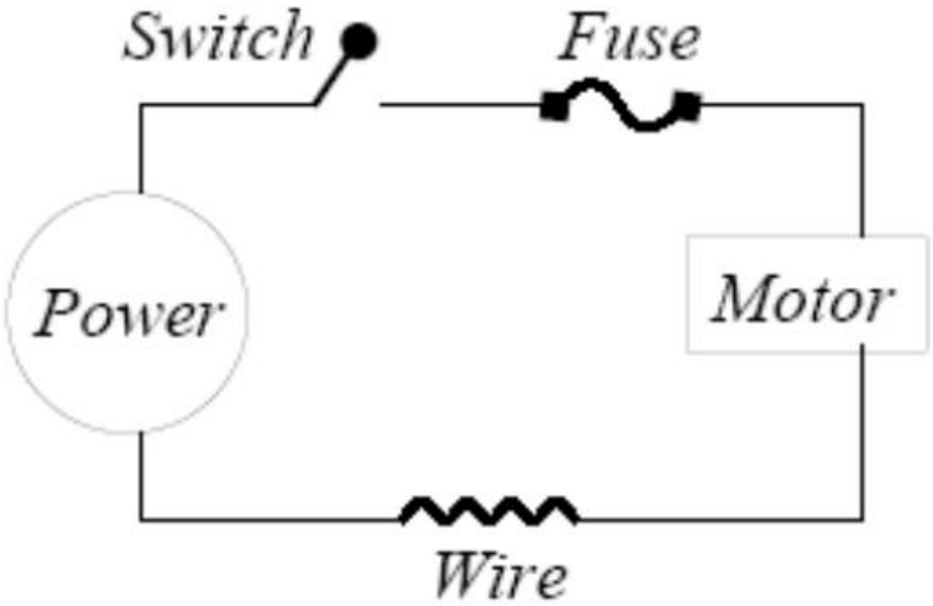
- 通过对可能造成产品故障的硬件、软件、环境、人为因素进行分析，确定产品故障原因的各种可能的组合方式及其发生概率，从而有效的确定系统发生故障的各种途径，并提高系统的可靠性和安全性。

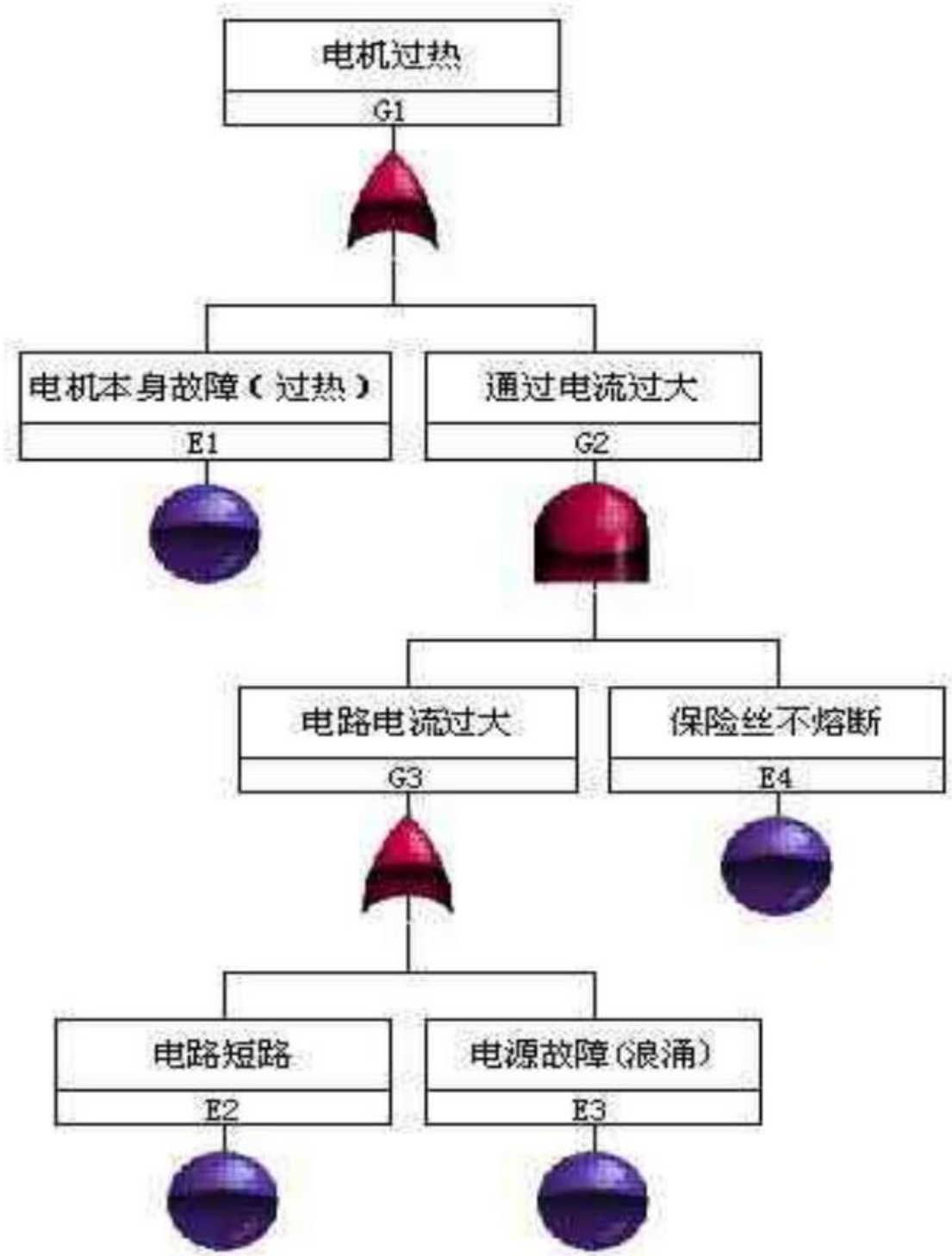
- 是自顶向下的分析方法。

FTA 的概念解释

- 事件（Event）
- 逻辑门（Gate）
- 割集（Cut Set）
- 重要度（Important）

一个例子


Switch
Fuse
Power
Motor
Wire


电机过热
G1
电机本身故障（过热）
E1
通过电流过大
G2
电路电流过大
G3
保险丝不熔断
E4
电路短路
E2
电源故障(浪涌)
E3

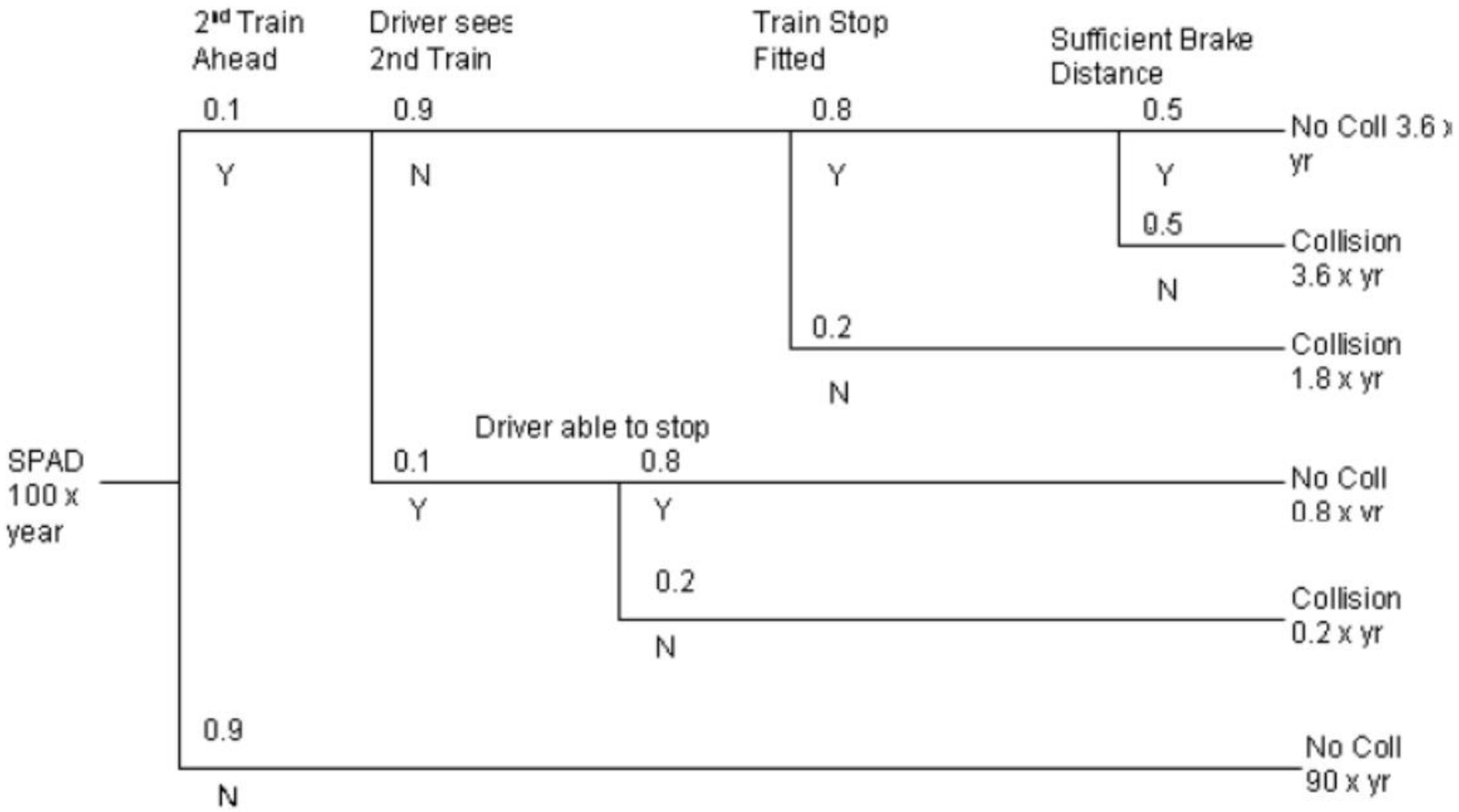
Demonstration

演示

4.8 事件树分析（ETA）

- ETA=Event Tree Analysis
- ETA 方法是一种逻辑演绎法，它在给定的一个初因事件的前提下，分析此初因事件可能导致的各种序列事件的结果，从而可以评价系统的可靠性与安全性。
- 事件树分析可用于描述系统中可能出现的事件序列，在分析复杂系统的重大故障和事故时，是一种有效的方法，对于铁路产品，尤其适用于具有冗余设计、故障监测与保护设计的复杂系统的安全性和可靠性分析。同时，对于人为失误引起的系统故障，ETA也是一种较好的分析方法。

一个ETA的例子


2nd Train Ahead
Driver sees 2nd Train
Train Stop Fitted
Sufficient Brake Distance
0.1
0.9
0.8
0.5
Y
N
Y
Y
No Coll 3.6 x yr
0.5
Collision 3.6 x yr
N
0.2
Collision 1.8 x yr
N
Driver able to stop
SPAD 100 x year
0.1
0.8
Y
Y
No Coll 0.8 x yr
0.2
Collision 0.2 x yr
N
0.9
No Coll 90 x yr
N