功能安全中的安全分析

杨海生
TÜV南德大中华区交通服务部
邮箱: haisheng.yang@tuvsud.com

Add value.
Inspire trust.

TÜV南德意志集团概览

150+
年专注质量、安全和可持续发展

1,000+
遍布全球各地

€34亿
年销售额（欧元）

约30,000
全球员工数

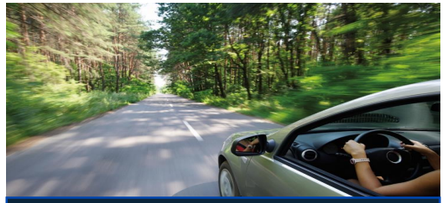
41%
德国境外销售额占比

574,000
张证书

100%
独立公正

1站式
解决方案提供商

汽车行业服务范围



整车服务

- 整车国际市场合规支持和准入服务
- 整车法规服务
- 整车排放、测试、评估以及认证服务
- 汽车禁限用物质管控以及ELV/RRR认证

零部件服务

- 零部件国际市场合规支持和准入服务
- 零部件测试
- 轮胎/轮毂测试认证
- 无线产品测试和全球市场准入
- 汽车动力电池测试和认证
- 充电系统部件测试和认证

自动驾驶

- 功能安全及预期功能安全

培训、评估和认证服务

- Auto-SPICE培训、评估和认证服务
- 汽车网络安全UN R155 & ISO21434 培训、评估和认证服务
- 汽车软件升级 UN R156培训、评估和认证服务
- 自动驾驶测试、评估以及技术支持服务

行业通用服务

- 管理体系评估和认证服务
- 汽车行业相关技术和质量工具培训
- 高压安全防护培训
- 二手车评估相关服务

功能安全和安全分析的定义

功能安全（functional safety）
absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems
(ISO 26262-1:2018)

功能安全（functional safety）
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.
(IEC 61508-4:2010)

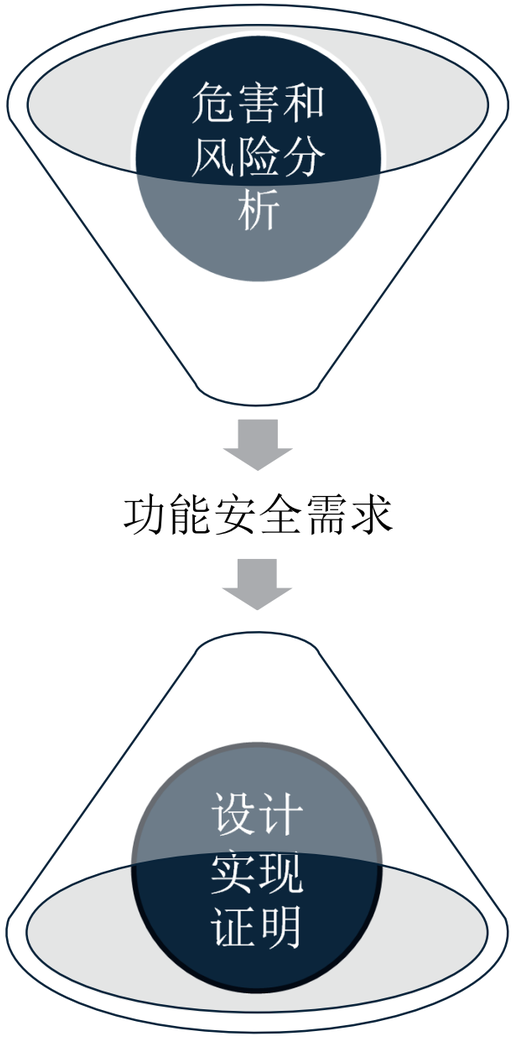
安全分析（Safety Analysis）
在功能安全领域，安全分析（Safety Analysis） 是通过系统化的方法识别、评估和控制由电子/电气/可编程系统（E/E/PE）失效引发的风险，以确保系统在发生故障时仍能维持或达到安全状态的结构化工程过程。

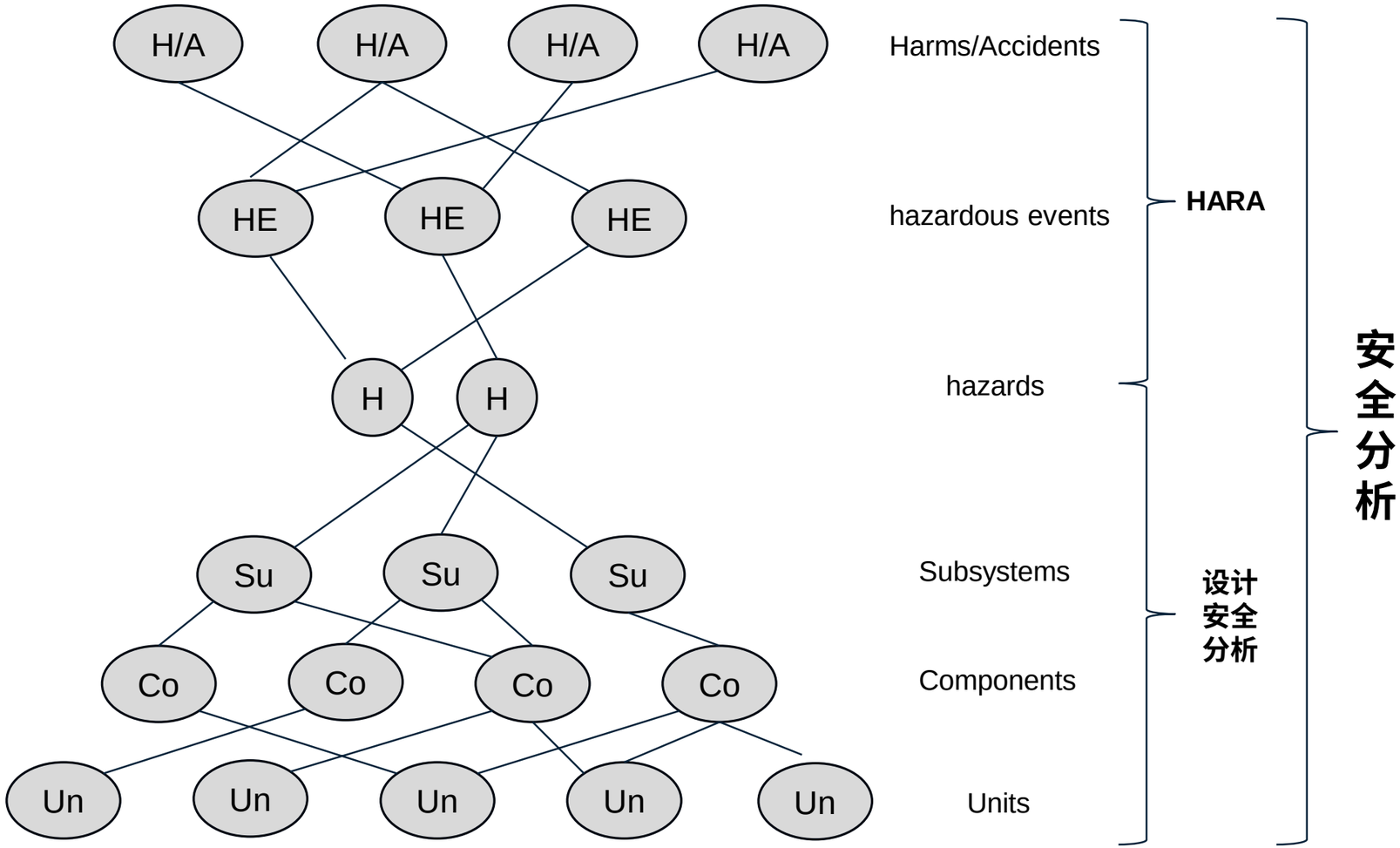
安全分析目的

安全分析的目的是确保由于系统性故障或随机硬件故障导致违反安全目标/安全需求的风险足够低。根据不同的应用，这是通过以下方式实现的：

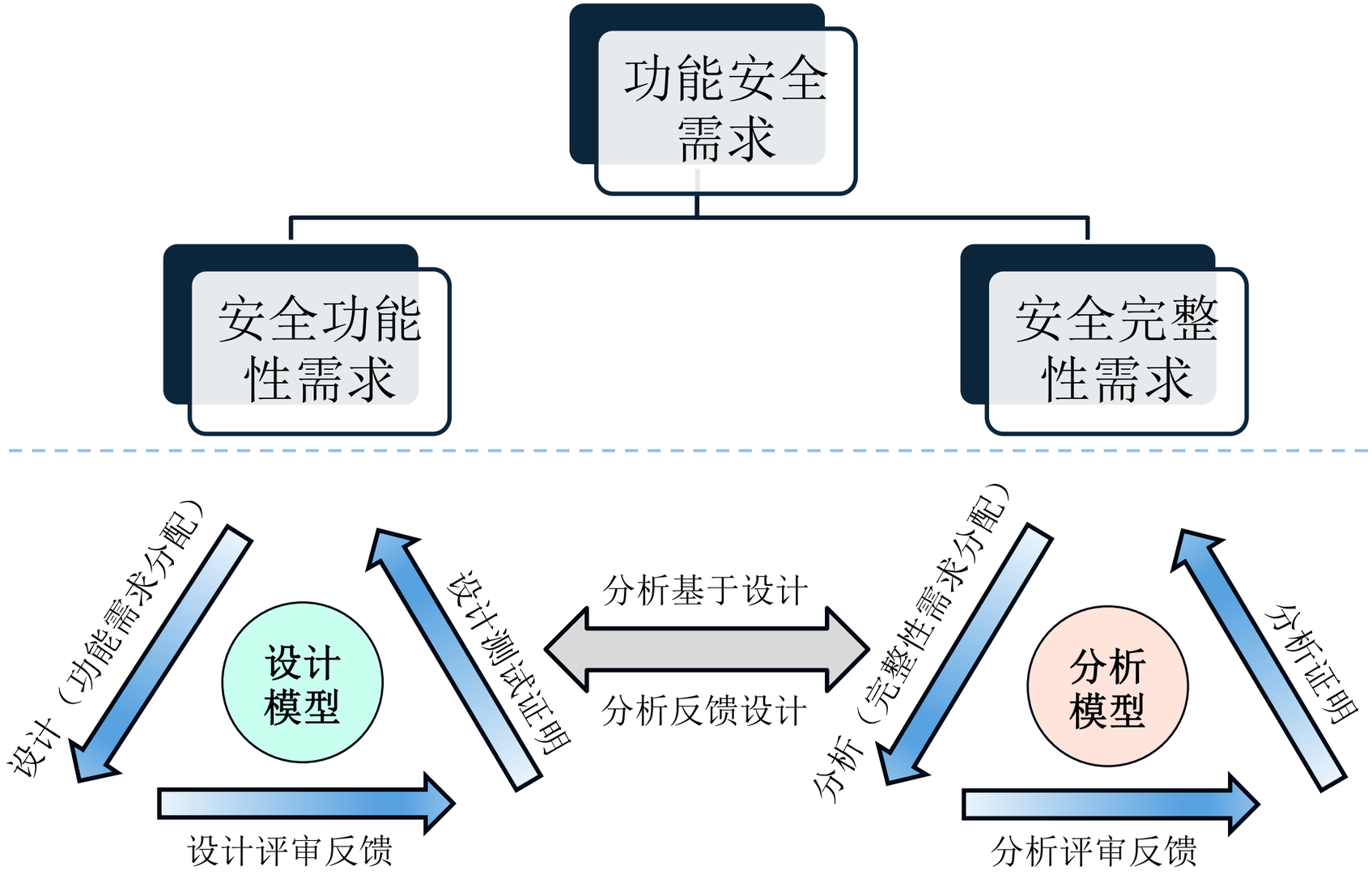
- Ø 识别在危害分析和风险评估期间未识别的新危害；
- Ø 识别可能导致违反安全目标或安全要求的故障或失效；
- Ø 识别故障和失效的潜在原因；
- Ø 支持定义用于故障预防或故障控制的安全措施；
- Ø 为安全概念的适用性提供证据；
- Ø 支持安全概念、安全要求的验证，以及设计要求和测试要求的识别。

功能安全与安全分析的关系

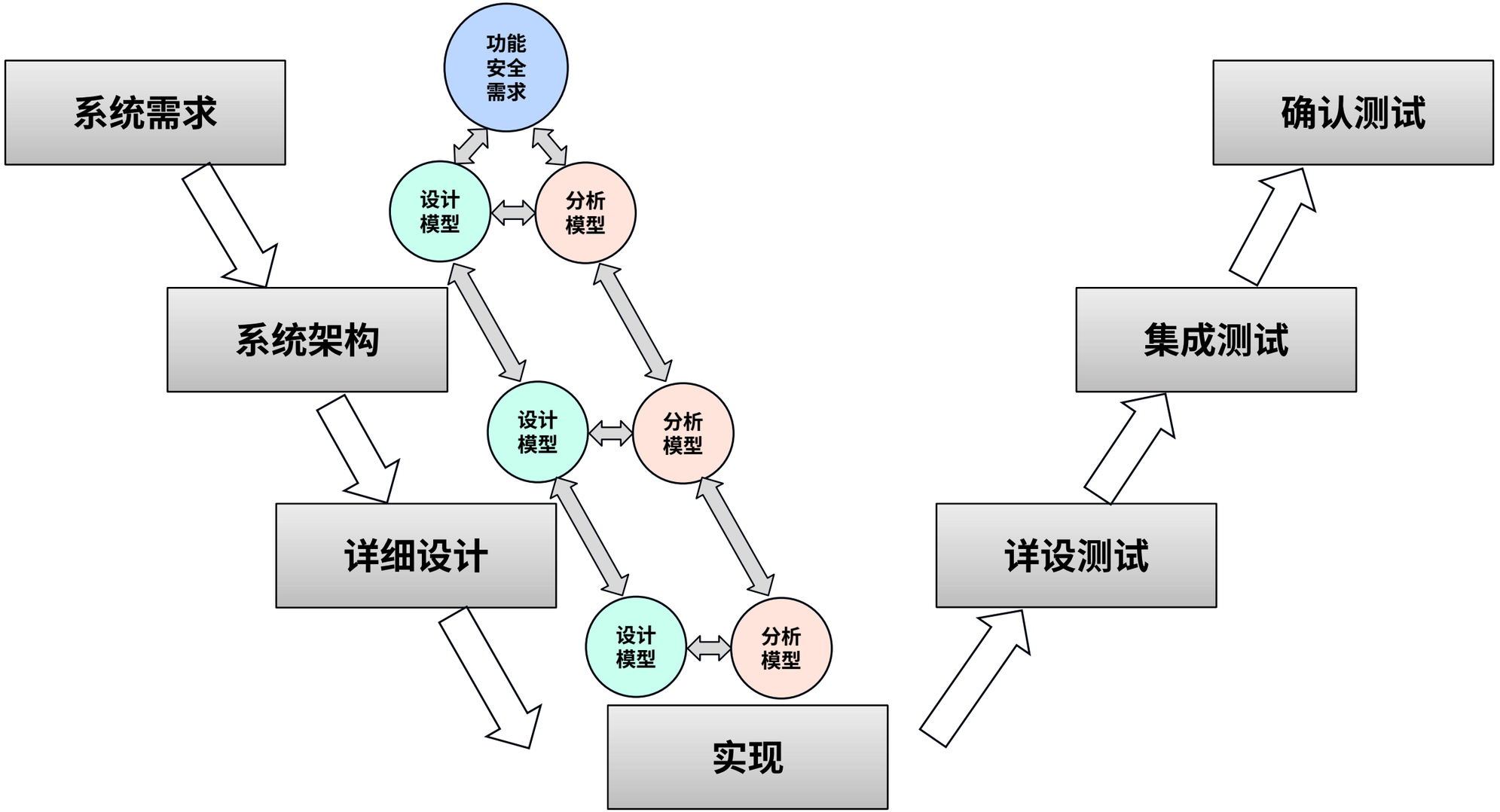




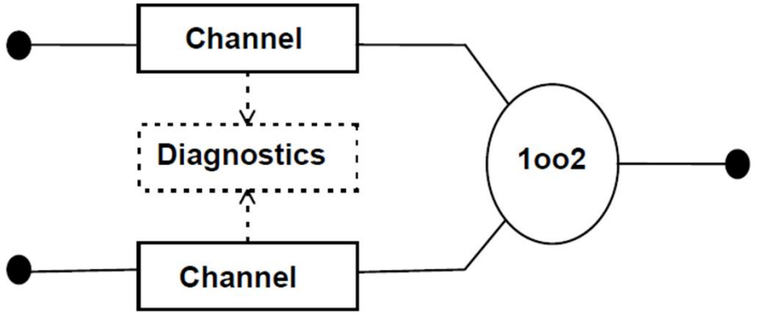
功能安全设计和安全分析的关系



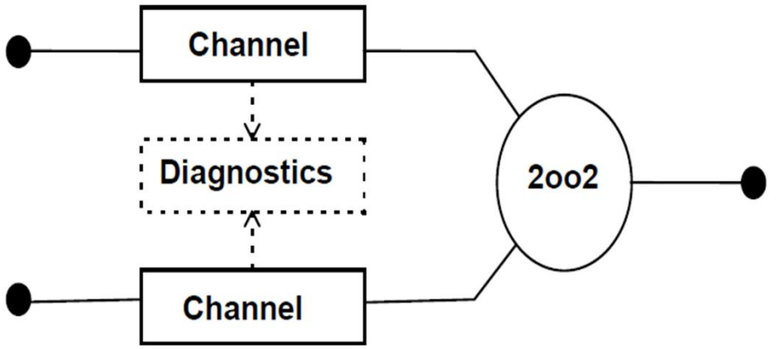
功能安全设计和安全分析在生命周期中的关系



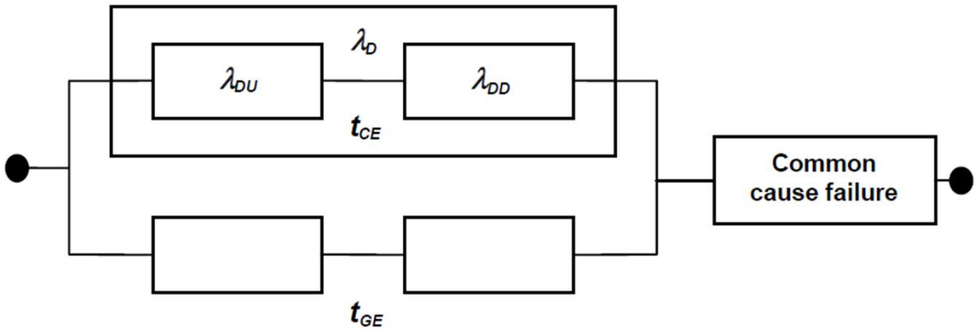
设计模型和分析模型举例



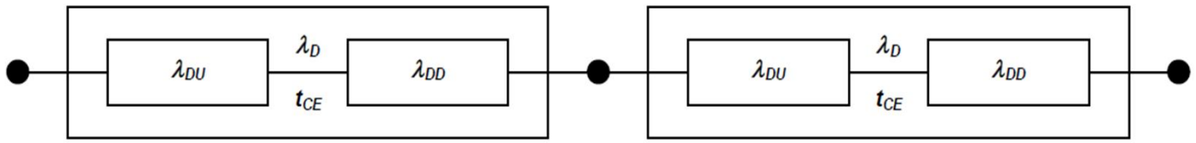
设计模型 – 1oo2 physical block diagram



设计模型 – 2oo2 physical block diagram



分析模型 – 1oo2 reliability block diagram



分析模型 – 2oo2 reliability block diagram

安全分析的关键特征

关键特征	说明
系统性	贯穿覆盖所有生命周期阶段
结构化分析方法	遵循标准规范的分析方法标准和逻辑链条准则
双维度评判	定性（逻辑关系）+ 定量（逻辑概率）
可追溯性	分析与应用/需求/设计之间追溯印证+分析之间的追溯
动态迭代性	分析与应用/需求/设计动态跟随更新迭代
分析不确定性控制*	系统安全冗余架构设计要求+保守分析原则

安全分析的关键特征

分析不确定性控制 - 系统安全冗余架构设计要求+保守分析原则

IEC 61508:2010

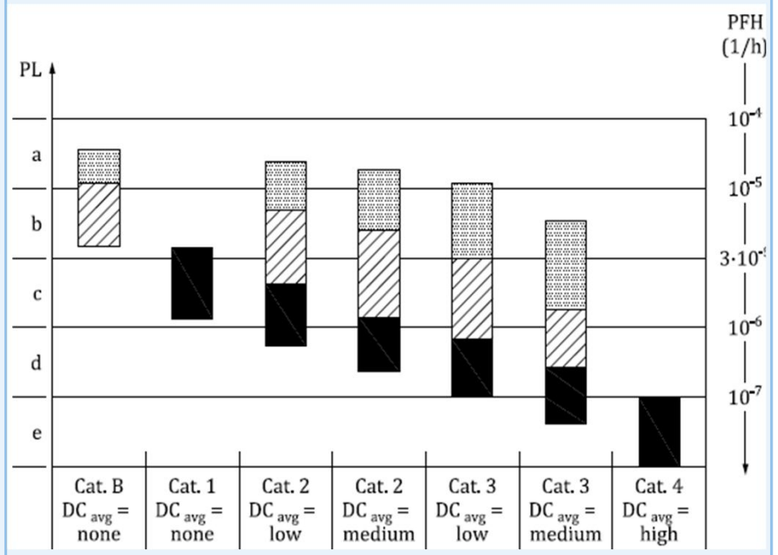
Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

ISO 26262:2018

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

ISO 13849:2023



常用分析方法

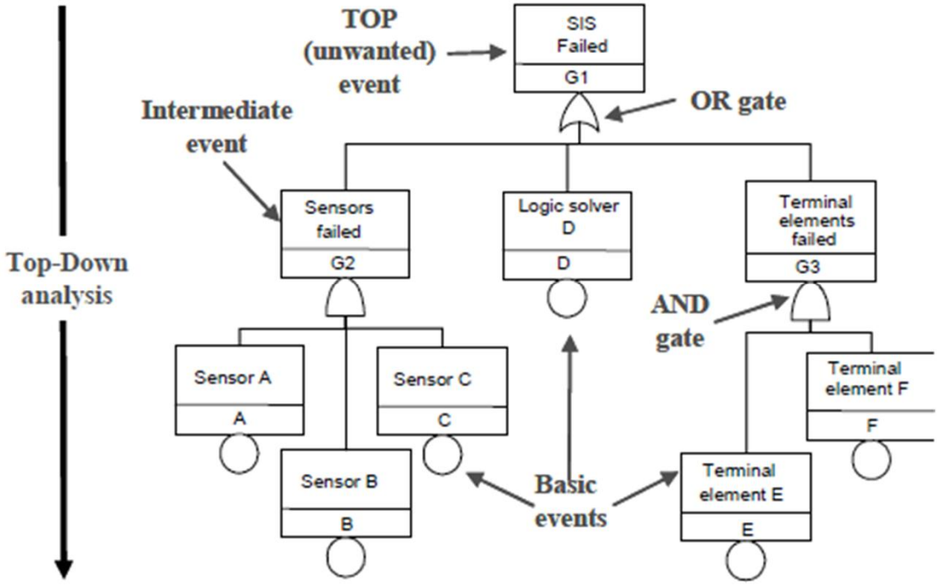
可靠性/失效率预计（failure rate prediction）
– 部件计数法分析（parts count analysis）；
– 部件压力法分析（parts stress analysis）；

危险与可操作性分析（Hazard and Operability Study, HAZOP）

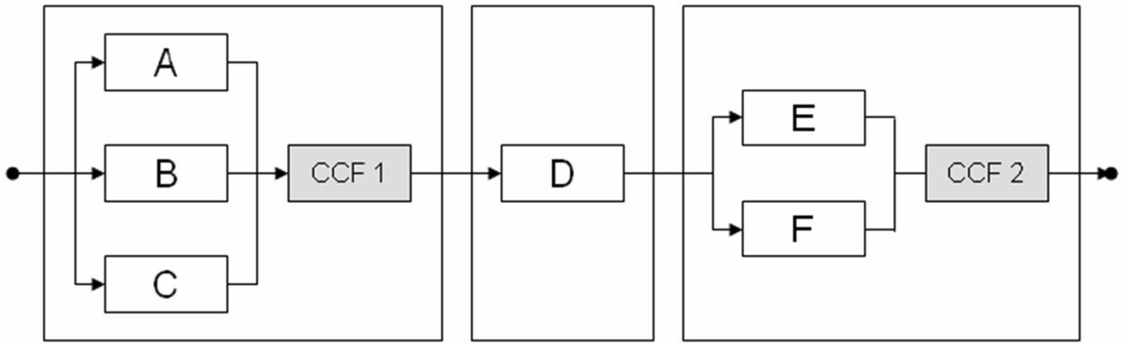
Guide word	Meaning
No or Not	Complete negation of the design intent
More	Quantitative increase
Less	Quantitative decrease
As well as	Qualitative modification/increase
Part of	Qualitative modification/decrease
Reverse	Logical opposite of the design intent
Other than	Complete substitution

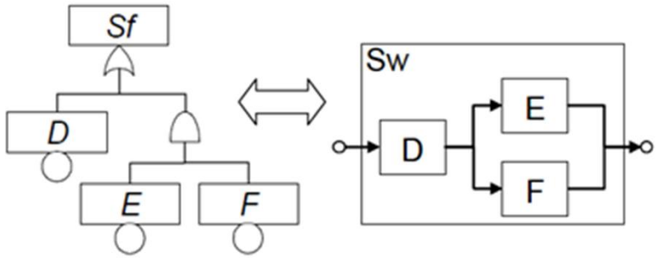
常用分析方法

故障树分析
（Fault Tree Analysis, FTA）



可靠性框图分析
（Reliability block diagram analysis, RBD）





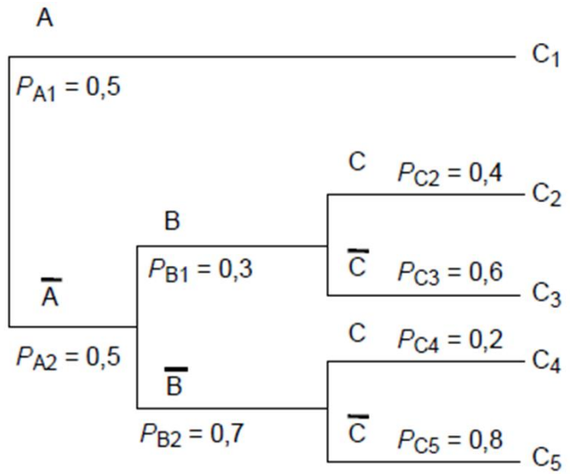
Equivalence fault tree / reliability block diagram

常用分析方法

失效模式和影响分析（Failure modes and effects analysis , FMEA）

Indenture level: Sheet No.: Mission phase					Design by: Item: Issue:				Prepared by: Approved by: Date:			
Item ref.	Item description / function	Failure entry code	Failure mode	Possible failure causes	Symptom detected by	Local effect	Effect on unit output	Compensating provision against failure	Severity class	Failure rate	Data source	Recommendations and actions taken
1.1.1	Motor stator	1111	Open circuit	Winding fracture	Low speed roughness	Low power	Trip	Single phase protection temperature trip	4			
		1112	Open circuit	Connection fracture	Low speed roughness	Low power	Trip	Single phase protection temperature trip	3			

事件树分析（Event tree analysis, ETA ）



Car came to a slow stop, no damage to the car, other property or injuries $P_{C1} = 0,5$

Car came to a slow stop, damaged wheel, $P_{C2} = 0,5 \times 0,3 \times 0,4 = 0,06$

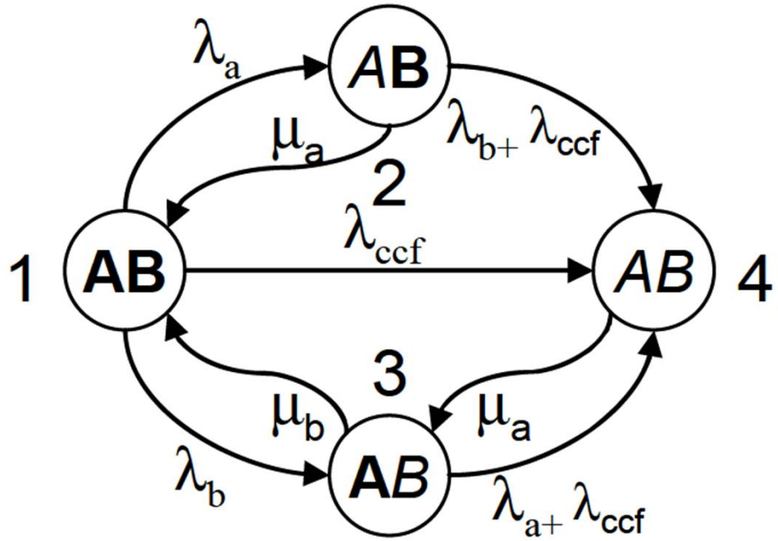
Car collided with the centre divider, damage to the car and divider: $P_{C3} = 0,5 \times 0,3 \times 0,6 = 0,09$

Car ran off the road, damage to the car, driver injured: $P_{C4} = 0,5 \times 0,7 \times 0,2 = 0,07$

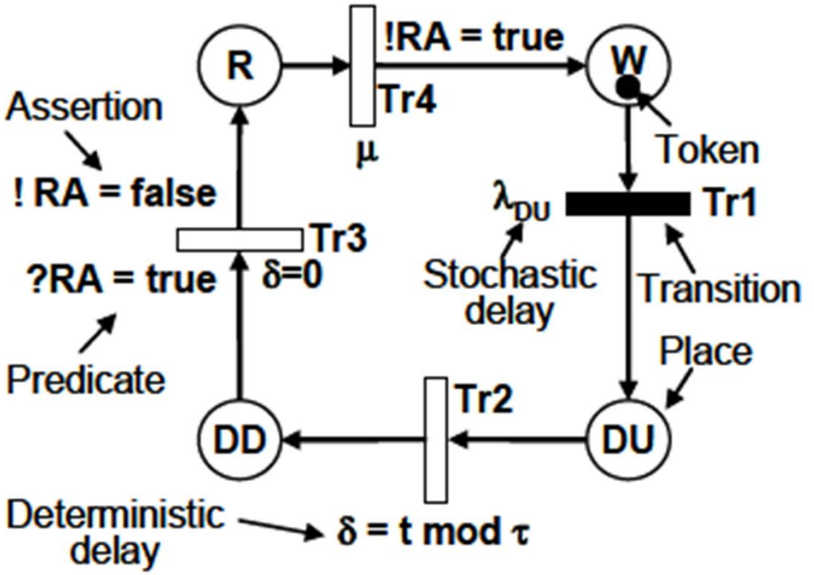
Collision with another vehicle, damage to both, both drivers injured: $P_{C5} = 0,5 \times 0,7 \times 0,8 = 0,28$

常用分析方法

马尔可夫分析（Markov analysis）



Petri网分析（Petri net analysis）



分析方法分类

根据分析中对逻辑链条的梳理方向和相应的系统层次结构分析方向，可以将分析方法如下分类：

1) **自下而上分析方法**（**归纳分析方法**，通常针对单一失效的影响进行分析）
   自下而上分析方法的起点是在下层部件/组件所识别的失效和失效模式。对于每种失效模式，向上归纳推导出对相关更高层面系统级别的应用影响。基于部件清单和检查清单，自下而上的分析方法将尽可能覆盖分析起点层次的所有单一失效的向上影响。

2) **自上而下分析方法**（**演绎分析方法**，能支持对多故障组合的影响进行分析）
   自上而下分析方法的起点是上层系统的失效模式或危害，依次逐层向下级部件/组件演绎分析导致上层失效的原因，自上而下分析方法可以分析评估多个故障组合而共同作用的影响，还可以考虑它们发生的顺序和共因的影响，能针对复杂结构系统的进行分析。

自下而上的分析方法（归纳分析方法）和自上而下的分析方法（演绎分析方法）作用互补，通常需要结合一起使用。

分析方法分类

根据分析中对能否考虑时间顺序或动态演变的逻辑链条，可以将分析方法如下分类：

1) **静态分析方法**（“快照式”分析，与时序和状态变迁无关的分析）
   静态分析方法基于基于布尔静态逻辑因果关系，分析过程中系统状态不发生变化，分析中的逻辑时序变化不影响分析的结果。适用于具备时间无关性和逻辑确定性的应用场景。

2) **动态分析方法**（“电影式”分析，能分析时序和状态变迁的作用和影响）
   动态分析方法基于状态和状态变迁的动态状态空间演变，分析中可以覆盖系统的多个状态，以及在这些状态间迁移的逻辑关系。适用于有时间依赖性和状态连续性的应用场景。

通常动态分析方法能覆盖静态分析方法的应用场景，但反之不能成立。通常动态分析方法的应用和计算比静态分析方法复杂，在工程应用中通常优先使用静态分析方法，当分析中涉及到时序和状态变迁时结合使用动态分析方法。

常用分析方法的分类

	自下而上分析方法	自上而下分析方法
静态分析方法	FMEA HAZOP 可靠性/失效率预计	FTA RBD
动态分析方法	ETA	马尔可夫分析 Petri网分析

常用分析方法的特点和应用对比

分析方法	需求分配支持性	定性分析	定量分析	支持设计评审和证明
可靠性/失效率预计	可用于没有冗余结构的串行系统的需求分配	-	可定量计算串行无冗余组件/系统的失效率和MTTF	支持
故障树（FTA）	可用于没有显著时序和状态变迁的系统需求分配	考虑故障场景，可以考虑冗余系统结构（多故障影响）	可定量计算系统PMHF/PFH/PFD等，并能体现相关子系统/组件对计算结果的贡献程度	适用
可靠性框图（RBD）	可用于系统模块具备独立性的场合，同FTA情况	考虑可靠场景，同FTA情况	可定量计算系统PMHF/PFH/PFD等，并能体现相关子系统/组件对计算结果的贡献程度	适用
失效模式和影响分析（FMEA/FMECA/FMEDA）	可用于主要为单一独立失效的分析场合，通常针对串行无冗余的情况	失效的影响及传递	可定量计算串行无冗余组件/系统的失效率和MTTF	适用
HAZOP分析	支持	偏离的识别和因果分析	不支持	不适用
事件树（ETA）	可能支持	失效的结果分析	可计算失效结果的概率	适用
马尔可夫分析（Markov）	支持	分析时序和状态的关系和作用	可定量计算系统PMHF/PFH/PFD等，并能体现时序和状态变迁的过程和最终稳态结果	适用
Petri网分析	支持	分析时序和状态的关系和作用，控制状态空间爆炸	可定量计算系统PMHF/PFH/PFD等，并能体现时序和状态变迁的过程和最终稳态结果	适用
蒙特卡罗方法*	可能支持	可能支持	通过概率模拟统计得到定量概率，非解析计算方式，适用于复杂结构系统	支持

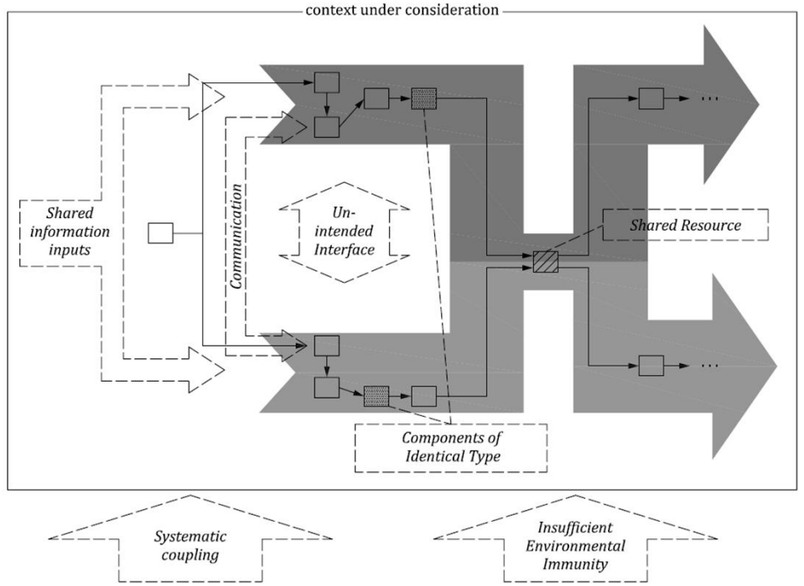
安全分析中共因失效的考量

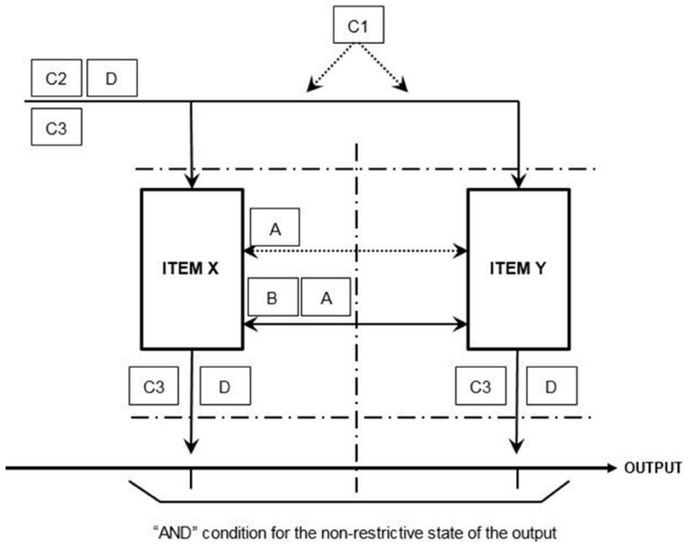
在安全分析中要求各个分析对象的失效是独立的，无论对于单通道串行结构还是多通道冗余结构都是如此，独立性要求对于冗余结构尤其重要。当失效无法独立即意味着这存在共因失效。因此，在安全分析中需要对共因失效进行分析并采取有效的保障措施。

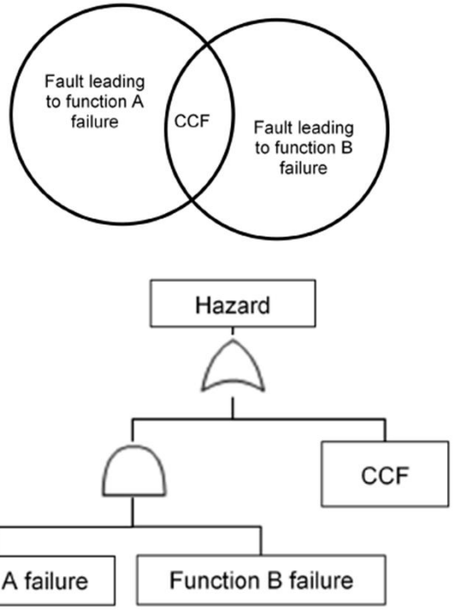
共因失效分析（CCF）的本质是识别导致相关失效的所有原因，对于其中有干涉影响的共有原因（即共因）采取措施：

Ø 避免共因（则可以在安全分析中按照独立失效进行分析）

Ø 控制共因（在安全分析中增加对共因失效作用的分析）







安全分析方法的选择

安全分析方法各有特点，没有通用的应用选择标准，需要根据实际情况判断选择合适的安全分析方法，可以通过以下项点支持分析方法的选择：

a) 系统复杂性

b) 系统新颖性

c) 定性分析vs定量分析

d) 单个故障vs多故障组合

e) 时间顺序依赖性

f) 系统状态依赖性

g) 自下而上vs自上而下

h) 安全完整性需求分配的适用性

i) 分析技术使用的能力要求

j) 分析技术通用性和可接受性

k) 工具需要性

l) 工具可用性

m) 合理性检查可行性

n) 分析方法的标准程度

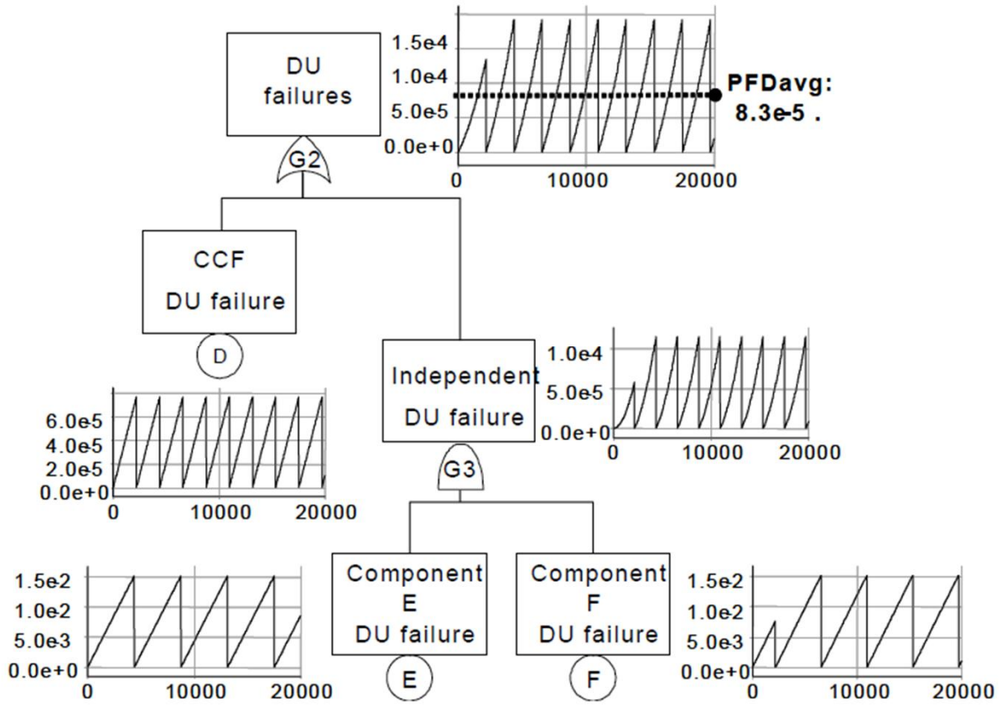
安全分析方法的选择

分析方法	复杂系统	新颖系统	定量分析	组合故障	时序相关	状态相关	分析方向	需求分配	能力要求	可接受性	需要工具	工具可用	合理性检查	标准
可靠性/失效率预计	否	是	是	否	否	否	向上	是	低	高	中	高	是	IEC 61709
故障树（FTA）	是	是	是	是	否	否	向下	是	中	高	中	高	是	IEC 61025
可靠性框图（RBD）	否	否	是	否	是	是	向上	否	高	中	中	中	是	IEC 61078
失效模式和影响分析（FMEA/FMECA/FMEDA）	否	否	是	否	否	否	向上	否	低	高	低	高	是	IEC 60812 SAE J1739
HAZOP分析	是	是	否	否	否	否	向上	否	低	中	低	中	是	IEC 61882
事件树（ETA）	否	否	是	否	是	是	向上	否	高	中	中	中	是	
马尔可夫分析（Markov）	是	是	是	是	是	是	向下	是	高	中	高	中	否	
Petri网分析	是	是	是	是	是	是	向下	是	高	低	高	低	否	

安全分析方法的融合应用

在对以上常用分析方法的实践应用中，为了消除分析方法的限制或结合不同分析方法的优点，在实际用于中会将不同的安全分析方法加以融合：在一种分析方法中体现其他分析方法的内容。这一方面增加了安全分析方法的灵活性和适用性，但另一方面也增加了安全分析方法使用的复杂程度。

通过融合应用马尔可夫模型
将静态FTA扩展为动态FTA



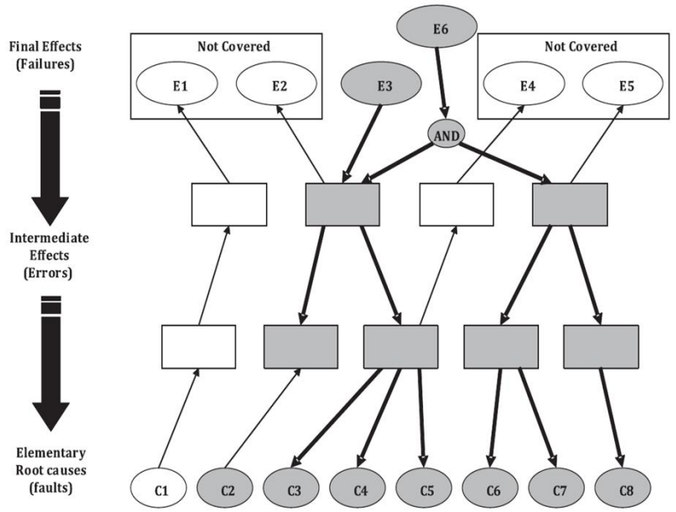
通过融合应用FTA模型将处理单一失效的
FMEA扩展为能够处理多失效组合的FMEDA

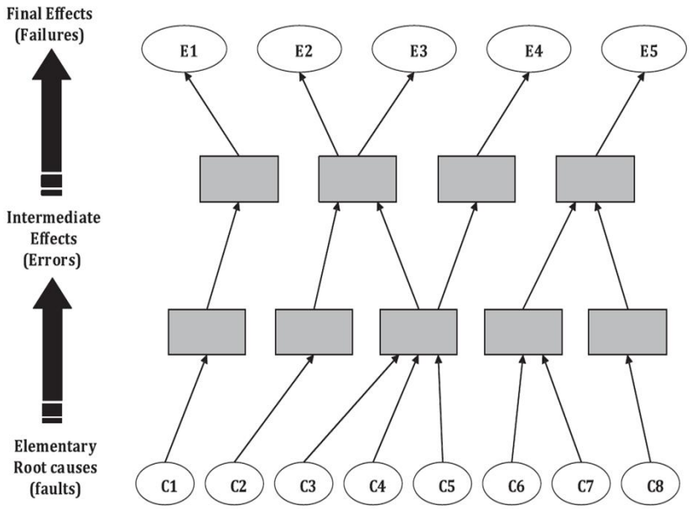
Component Name	Failure rate (e-9/h)	Failure Mode	Failure Mode Distribution	Failure mode has the potential to violate the safety goal in absence of safety mechanisms	Safety mechanism(s) preventing the failure mode from violating the safety goal	Failure mode coverage wrt. violation of safety goal	Residual or Single-Point Fault failure rate (e-9/h)	Dual Point Fault failure rate (e-9/h)	Description	Detection means or Safety mechanism(s) preventing the failure mode from being latent	Failure mode coverage with respect to latent failures	Latent Multiple-Point Fault failure rate (e-9/h)	Description	Detected Dual Point Fault failure rate (e-9/h)	Description
IF	100	Safe	0,5												
		FM A	0,2	X	SM1	0,9	2,0	18,0	$\lambda_{IF,DPF,secondary}$	SM1	0,8	3,6	$\lambda_{IF,DPF,latent,secondary}$	14,4	$\lambda_{IF,DPF,detected,secondary}$
		FM B	0,15	X	none	0	15,0								
		FM C	0,15					15,0	$\lambda_{IF,DPF,primary}$	SM1	0,7	4,5	$\lambda_{IF,DPF,latent,primary}$	10,5	$\lambda_{IF,DPF,detected,primary}$
SM1	50	Safe	0,5												
		FM D	0,15	X	SM2	0,8	1,5	6,0	$\lambda_{SM1,DPF,primary}$	SM2	0,6	2,4	$\lambda_{SM1,DPF,latent,secondary}$	3,6	$\lambda_{SM1,DPF,detected,secondary}$
		FM E	0,2					10,0	$\lambda_{SM1,DPF,primary}$	SM2	0,4	6,0	$\lambda_{SM1,DPF,latent,primary}$	4,0	$\lambda_{SM1,DPF,detected,primary}$
		FM F	0,15					7,5	$\lambda_{SM1,DPF,primary}$	none	—	7,5	$\lambda_{SM1,DPF,latent,primary}$		$\lambda_{SM1,DPF,detected,primary}$

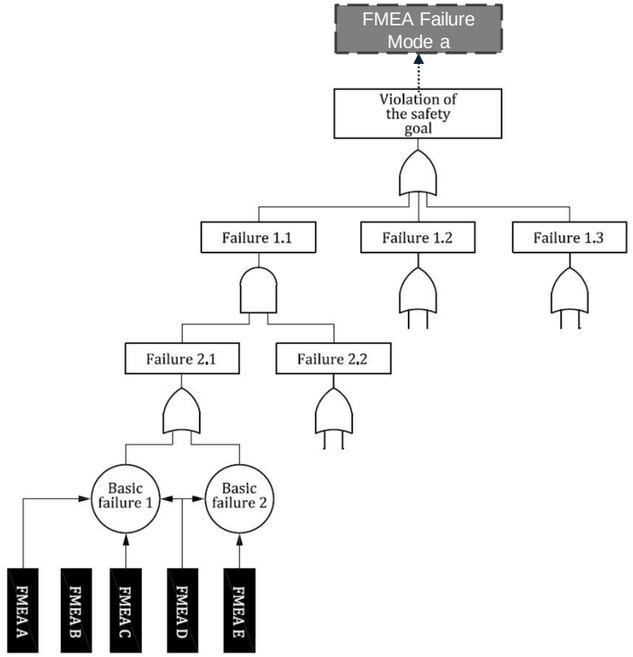
$$M_{\mathrm{PMHF}} = \lambda_{\mathrm{SPF}} + \lambda_{\mathrm{RF}} + \lambda_{\mathrm{SM1,DPF,detected}} \times \lambda_{\mathrm{IF,DPF}} \times T_{\mathrm{service}} + \lambda_{\mathrm{IF,DPF,detected}} \times \lambda_{\mathrm{SM1,DPF}} \times T_{\mathrm{service}}$$

安全分析方法的组合应用

到目前为止的工程项目实际应用经验表明没有一种安全分析方法能够单独实现对有一定复杂程度的系统或设计的充分分析，因此在实践应用中通常需要根据实际情况结合使用多种安全分析方法以达到分析的充分性。
同时，对于复杂系统的设计通常都基于多层次的设计模型和生命周期模型，层次间有着密切的逻辑追溯关联，每个层次的安全分析相应的需要建立与上下游层次的逻辑链条，这也涉及到不同安全分析方法之间的衔接和追溯。







安全分析方法应用中的核心要素 – 人

除了各种安全分析方法本身的特点会影响对它们的选择和应用之外，**安全分析方法的使用者的能力**是非常重要的，**这可能比实际使用的技术更重要**。分析人员有责任验证任何特定方法的基础假设是否得到满足，或者是否需要进行任何调整以获得充分的现实保守结果。

安全分析方法的使用者的能力包括但不限于：

- **对分析方法的熟悉程度、**
- **对分析方法的应用能力、**
- **对分析方法限制约束的把握控制、**
- **对分析工具的应用能力等**

全球TÜV SÜD交通服务团队——您在国际项目中的行业合作伙伴

400+ 汽车专家

170+ 授权的认证工程师

25+ ISO资质的实验室

电池实验室 | 环境实验室 | 后视镜实验室 | 被动/主动安全实验室 | 轮胎/轮毂实验室

EMC实验室 | 内饰燃烧实验室 | 排放实验室 | 汽车实验室 (其它)

携手TÜV南德
驶向智慧未来

杨海生
TÜV南德大中华区交通服务部
邮箱: haisheng.yang@tuvsud.com
手机：18918568595

关注我们:

tuvsud.com
mobility@tuvsud.com