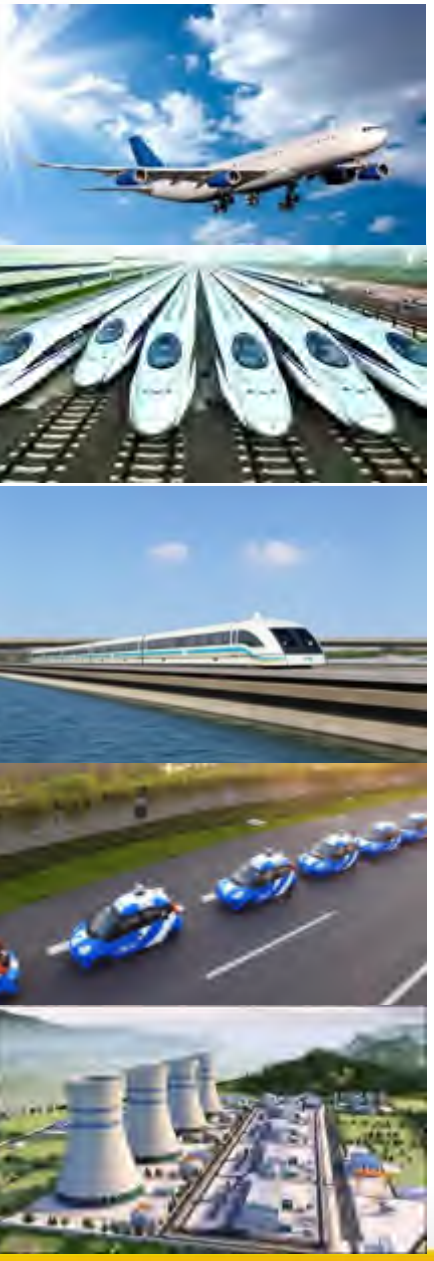
安全相关系统之安全分析及证明

方云根 / 评估与认证 总经理

上海轨道交通检测技术有限公司（SRCC）



主要内容

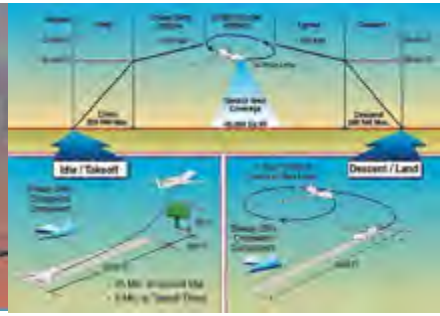
- 安全相关概念
- 安全分析方法
- 系统安全证明
- 系统安全评估

安全相关概念

- 安全相关系统(Safety-related System)是指其必须要实现要求的安全功能以达到或保持安全状态，它们与外部风险降低设施一道达到必要的风险降低量，以满足所要求的允许风险。

- 安全相关系统可能包括：1）被用于防止危险事件的发生；或者2）被用来减轻危险事件的影响，即通过减轻后果的办法来降低风险。



安全相关概念

绝对安全观认为，安全是“不存在危险和风险”，“安全意味着系统没有引起事故的条件”，有时还将安全称为无事故。

相对安全观认为，“所谓安全系指判明的危险性不超过允许限度”；“安全意味着可以允许的风险程度，相对无受损害之忧和损害概率低的通用述语”。

安全(Safety):免除不可接受等级的伤害的风险。

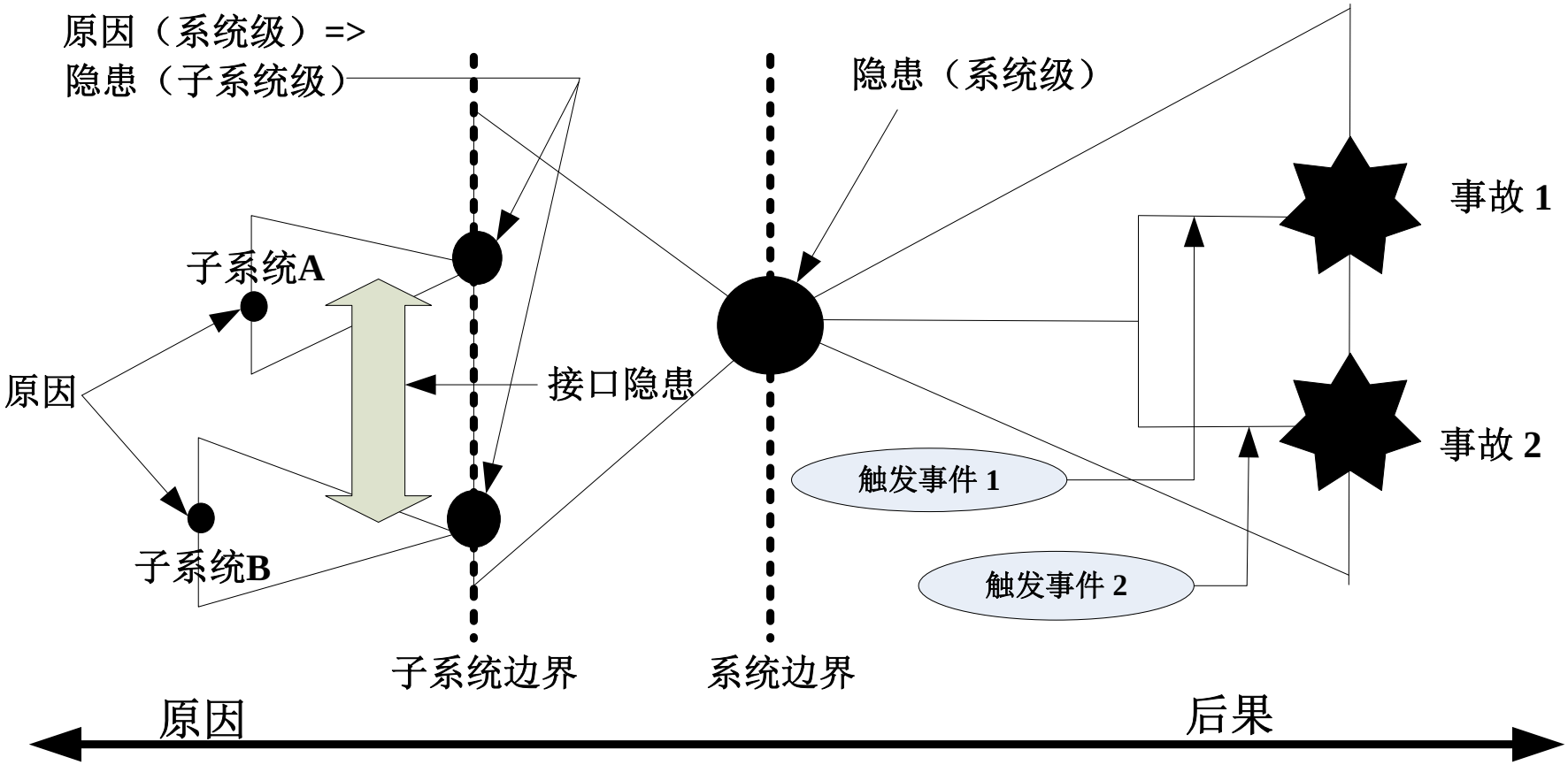
Freedom from unacceptable levels of risk of harm.

安全相关概念

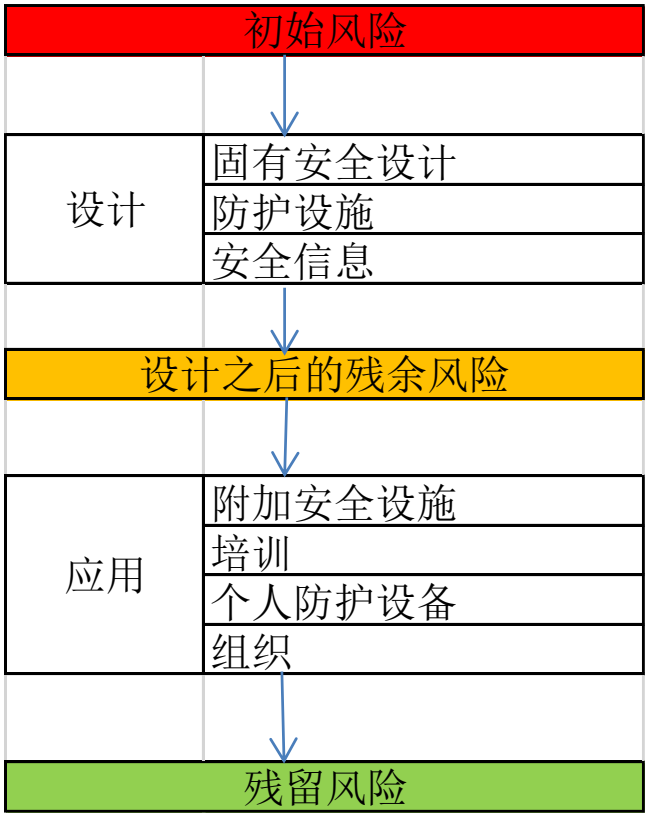
Hazard 危害/隐患

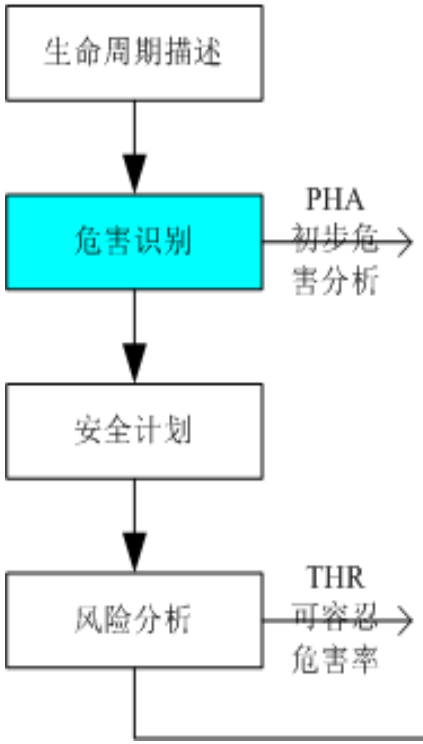
- 可能导致事故发生的物体、条件或者状态。在系统安全的背景下，隐患是系统的一种未受保护的状态，在一定的外部条件下，可能导致事故的发生。造成对人身伤害、财产损失或者环境破坏。

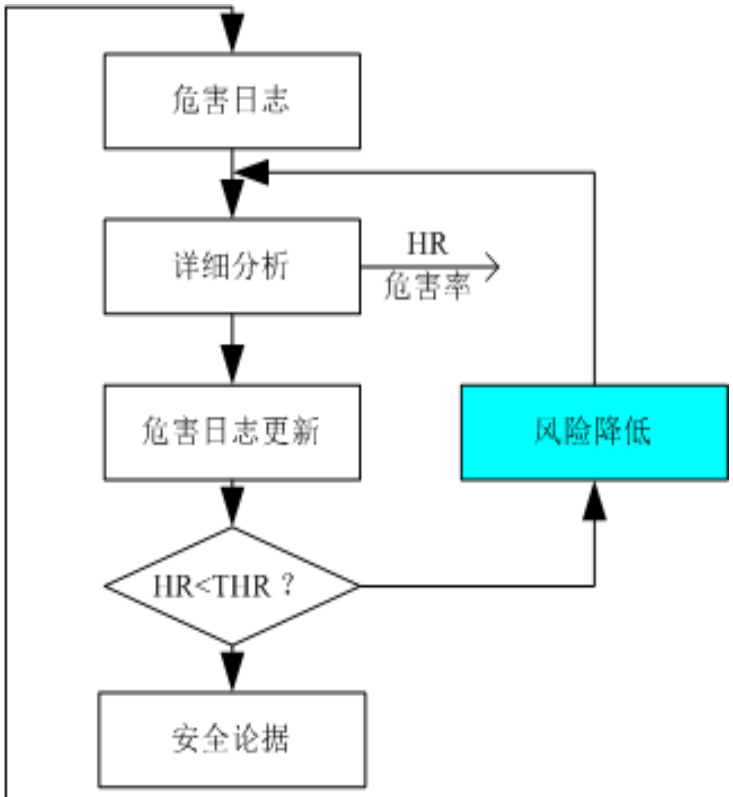
安全相关概念


原因（系统级）=>
隐患（子系统级）
隐患（系统级）
子系统A
原因
接口隐患
子系统B
事故 1
事故 2
触发事件 1
触发事件 2
子系统边界
系统边界
原因
后果

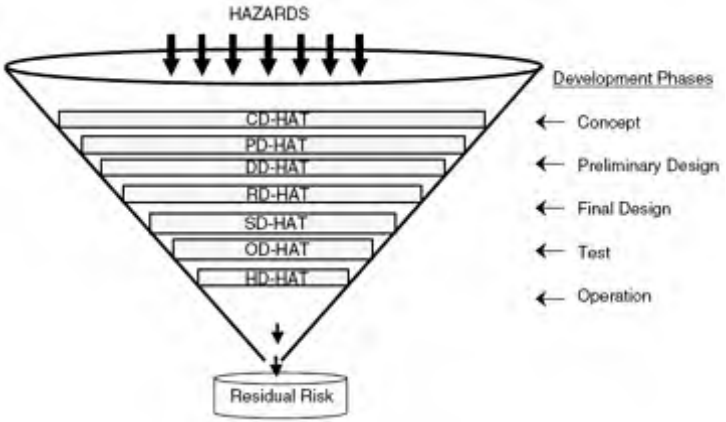
安全相关概念


初始风险
设计
固有安全设计
防护设施
安全信息
设计之后的残余风险
应用
附加安全设施
培训
个人防护设备
组织
残留风险


生命周期描述
危害识别
PHA
初步危害分析
安全计划
风险分析
THR
可容忍危害率


危害日志
详细分析
HR
危害率
危害日志更新
风险降低
HR<THR ?
安全论据

安全分析方法



概念
初步设计
详细设计
系统集成
测试
制造
运行
报废

概念设计危害分析技术
初步设计危害分析技术
详细设计危害分析技术
系统设计危害分析技术
运行设计危害分析技术
健康设计危害分析技术
需求设计危害分析技术

初步危害清单PHL
初步危害分析PHA
安全分析准则分析SRCA
系统危害分析SHA
操作和支持危害分析O&SHA
故障树分析FTA
失效模式影响分析FMECA
接口危害分析IHA
功能危害分析FHA
可靠性框图RBD
共因失效分析CCFA
危害和可操作性研究HAZOP
软件危害分析SWHA
马尔可夫分析MA

安全分析方法

《IEC 61508 电气/电子/可编程电子安全相关系统的功能安全 》对安全分析的要求

- 原因-后果分析Cause consequence analysis
- 故障树分析Fault tree analysis
- 马尔科夫模型Markov models
- 失效模式和影响分析Failure mode and effect analysis
- 可靠性框图Reliability block diagrams
- 供应失效分析Common cause failure analysis of
- Petri网Petri nets
- 事件树分析Event tree analysis
- 软件功能失效分析Software functional failure analysis

安全分析方法

《IEC 62425 轨道交通 通信、信号和处理系统-信号用安全相关电子系统 》对安全分析的要求

	Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4
1	Preliminary hazard analysis [a]	HR	HR	HR	HR
2	Fault tree analysis	R	R	HR	HR
3	Markov diagrams	R	R	HR	HR
4	FMECA	R	R	HR	HR
5	HAZOP	R	R	HR	HR
6	Cause-consequence diagrams	R	R	HR	HR
7	Event tree	R	R	R	R
8	Reliability block diagram	R	R	R	R
9	Zonal analysis	R	R	R	R
10	Interface hazard analysis	R	R	HR	HR
11	Common cause failure analysis	R	R	HR	HR
12	Historical event analysis	R	R	R	R

安全分析方法

《ISO 26262 道路车辆 功能安全》对安全分析的要求

安全分析的范围包括：

— 对安全目标和安全概念的确认；

— 对安全概念和安全要求的验证；

— 对可导致违背安全目标或安全要求的条件及包括故障和失效的原因的识别；

— 对关于故障探测或失效探测的额外要求的识别；

— 对探测故障或失效所需的响应行为/响应措施的制定；及

— 对关于验证安全目标和安全要求得到满足的额外要求的识别，包括安全相关的车辆测试。

定性分析方法包括：

— 系统、设计或过程层面的定性FMEA；

— 定性FTA；

— 危害与可操作性分析(HAZOP)；

— 定性ETA。

定量分析方法包括：

— 定量FMEA；

— 定量FTA；

— 定量ETA；

— 马尔科夫(Markov)模型；

— 可靠性框图。

安全分析方法

《SAE ARP 4761对民用机载系统和设备进行安全性评估过程的准则和方法》对安全分析的要求

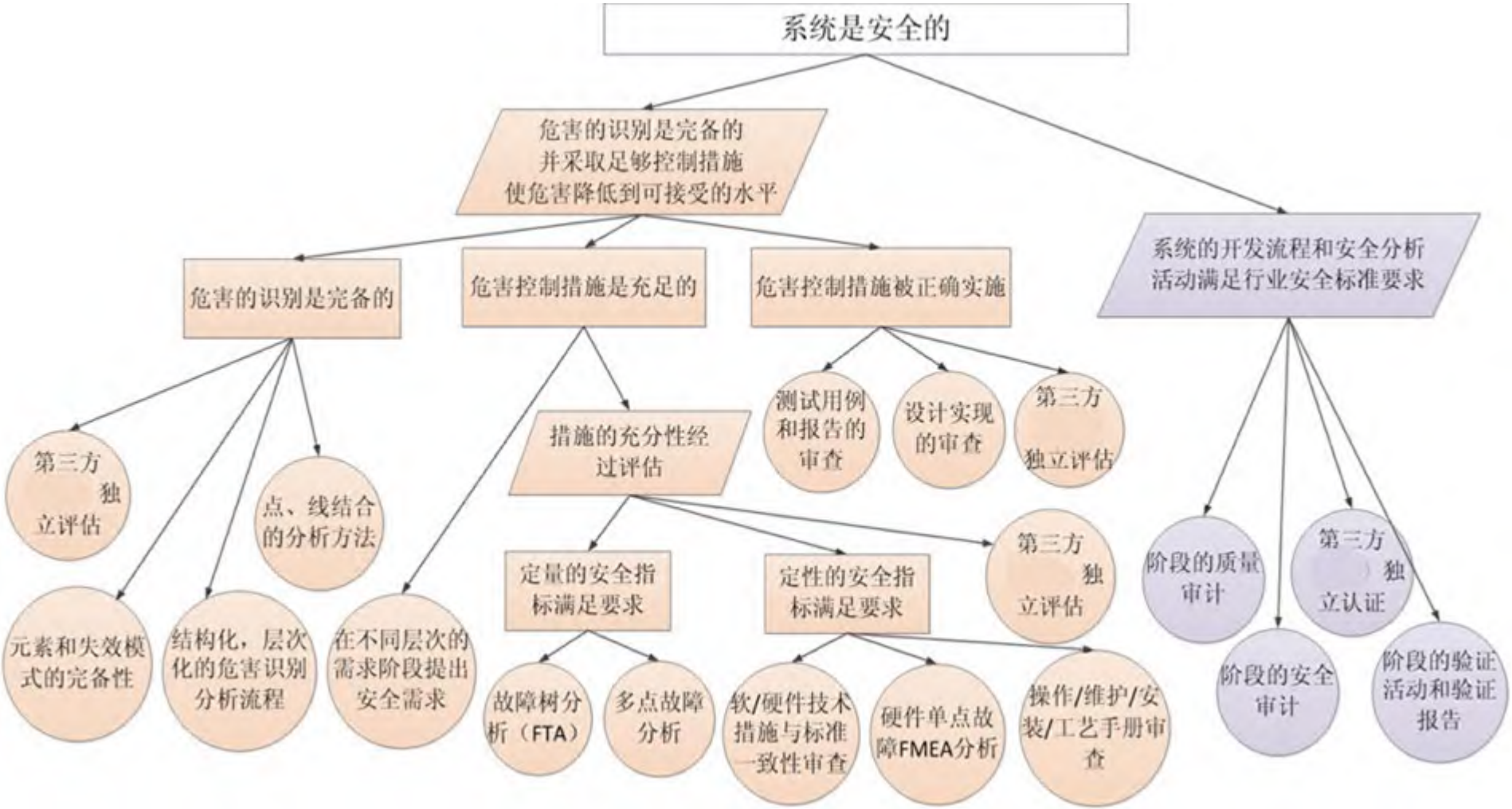
- 故障树分析 FTA
- 相依关系图 Dependence Diagram
- 马尔科夫分析 Makov Analysis
- 失效模式影响分析FMEA
- 失效模式影响总结FMES
- 共因失效分析CCA
- 区域安全分析ZSA
- 特殊风险分析PRA
- 共模分析CMA

系统安全证明

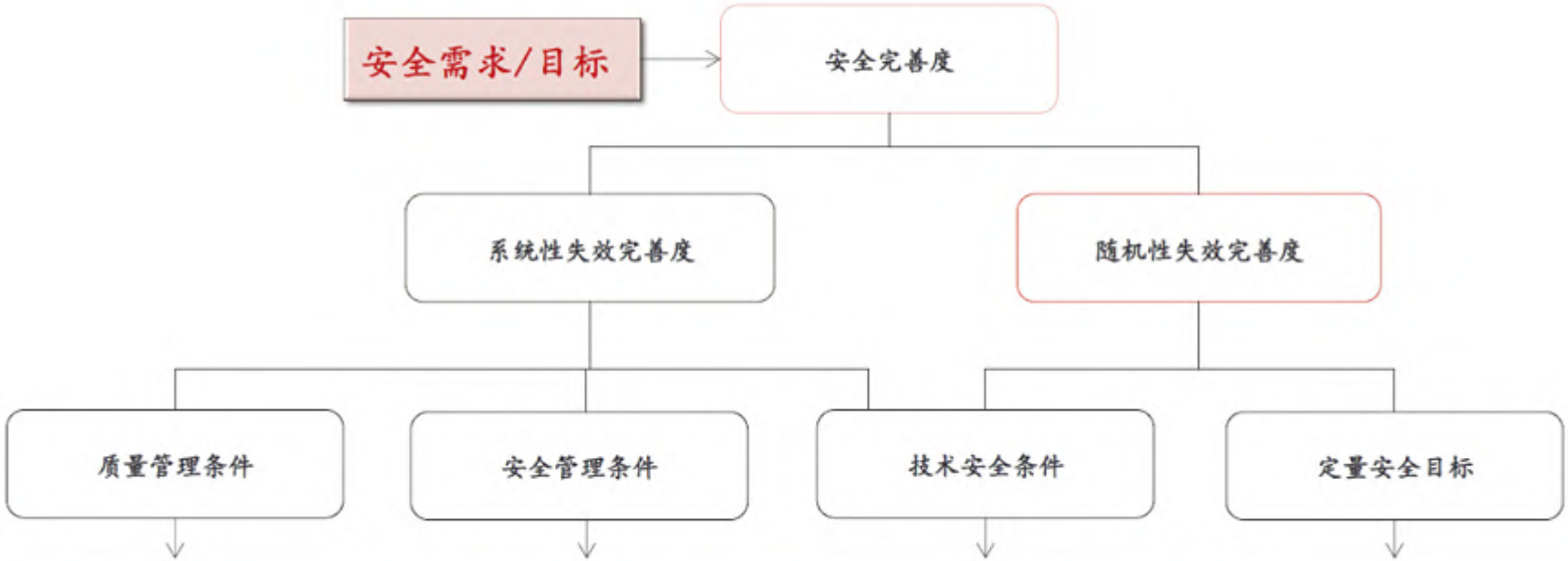
系统是否安全？

- 系统在正常运行的条件下
- 系统在发生故障的条件下
- 系统在紧急救援的条件下运行
- 系统在发生误操作的情况下
- 系统外部接口不良的条件下
- 系统在维修和保障的过程中
- 在不同的人为因素条件下
- 在不同的自然环境下，雷电、暴雪、洪水、地震等
- 在不同的电气、机械环境下

系统安全证明

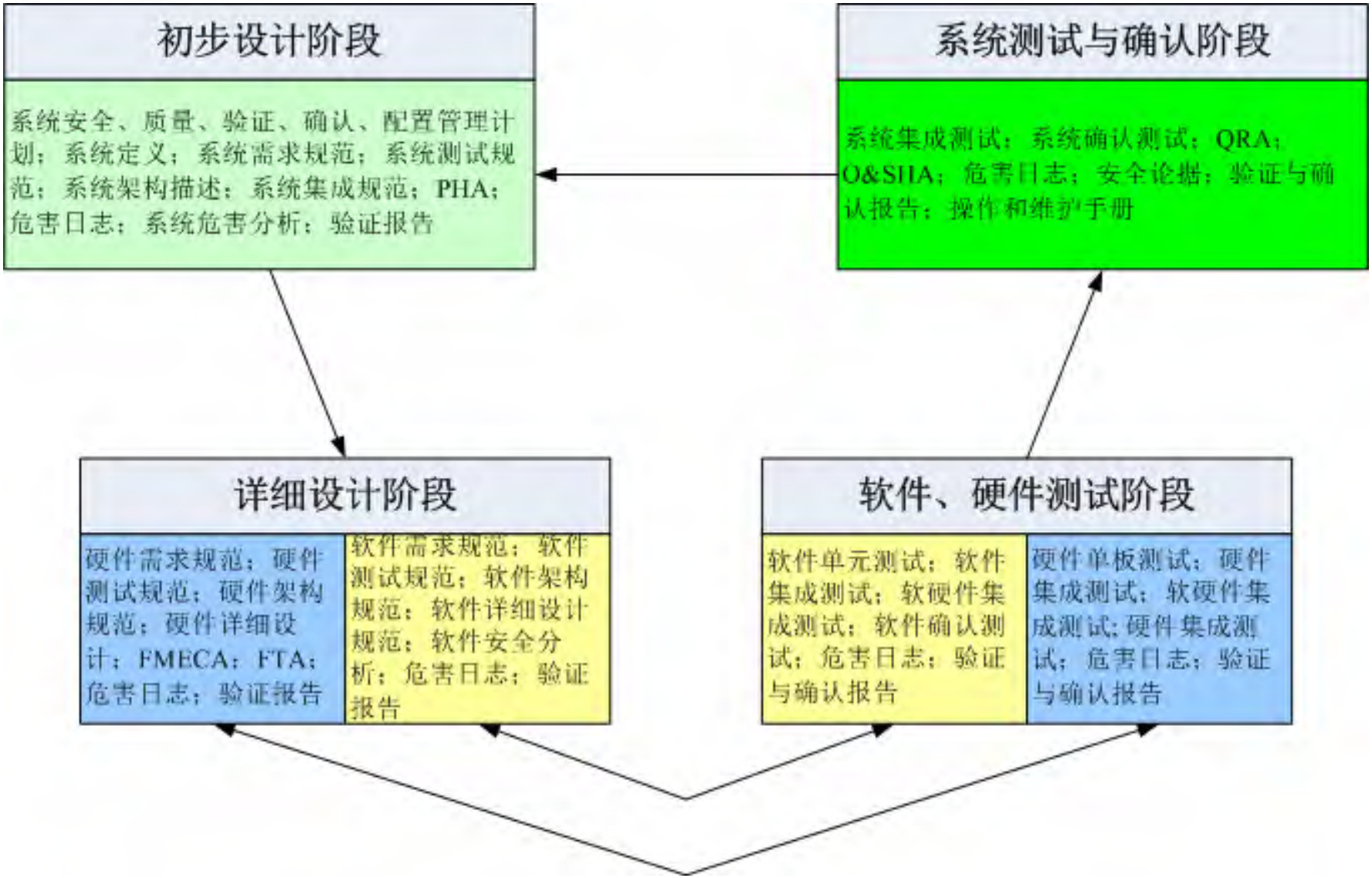

系统是安全的
危害的识别是完备的并采取足够控制措施使危害降低到可接受的水平
系统的开发流程和安全分析活动满足行业安全标准要求
危害的识别是完备的
危害控制措施是充足的
危害控制措施被正确实施
第三方独立评估
点、线结合的分析方法
元素和失效模式的完备性
结构化，层次化的危害识别分析流程
措施的充分性经过评估
测试用例和报告的审查
设计实现的审查
第三方独立评估
在不同层次的需求阶段提出安全需求
定量的安全指标满足要求
定性的安全指标满足要求
第三方独立评估
故障树分析（FTA）
多点故障分析
软/硬件技术措施与标准一致性审查
硬件单点故障FMEA分析
操作/维护/安装/工艺手册审查
阶段的质量审计
第三方独立认证
阶段的安全审计
阶段的验证活动和验证报告

系统安全证明

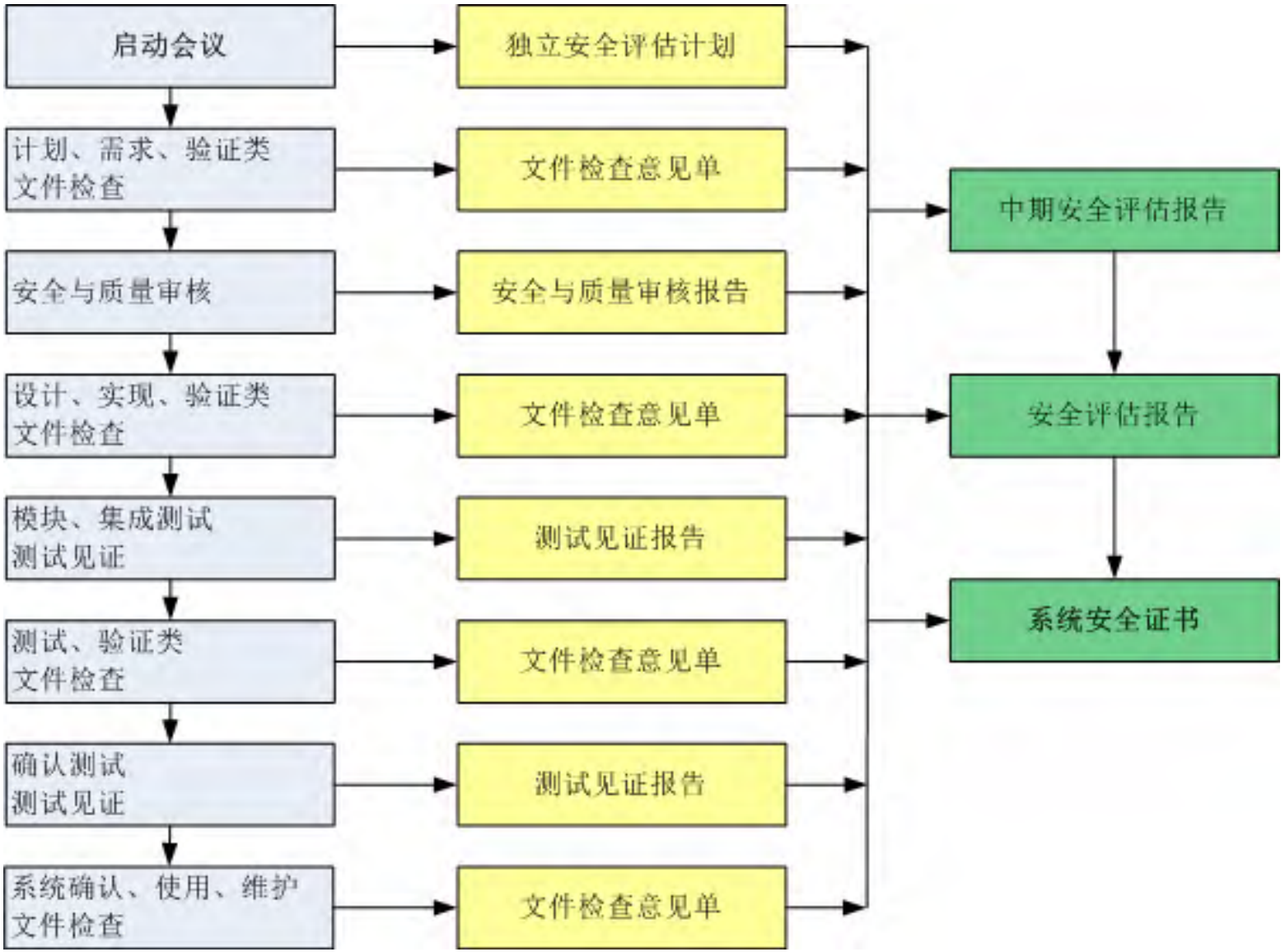


SIL4	根据SIL等级划分的一系列方法和工具（EN 50128、EN 50129、EN50159等）
SIL3	
SIL2	
SIL1	
SIL0	无特殊的要求

系统安全评估


初步设计阶段
系统安全、质量、验证、确认、配置管理计划；系统定义；系统需求规范；系统测试规范；系统架构描述；系统集成规范；PHA；危害日志；系统危害分析；验证报告
系统测试与确认阶段
系统集成测试；系统确认测试；QRA；O&SHA；危害日志；安全论据；验证与确认报告；操作和维护手册
详细设计阶段
硬件需求规范；硬件测试规范；硬件架构规范；硬件详细设计；FMECA；FTA；危害日志；验证报告
软件需求规范；软件测试规范；软件架构规范；软件详细设计规范；软件安全分析；危害日志；验证报告
软件、硬件测试阶段
软件单元测试；软件集成测试；软硬件集成测试；软件确认测试；危害日志；验证与确认报告
硬件单板测试；硬件集成测试；软硬件集成测试；硬件集成测试；危害日志；验证与确认报告

系统安全评估


启动会议
计划、需求、验证类文件检查
安全与质量审核
设计、实现、验证类文件检查
模块、集成测试测试见证
测试、验证类文件检查
确认测试测试见证
系统确认、使用、维护文件检查
独立安全评估计划
文件检查意见单
安全与质量审核报告
文件检查意见单
测试见证报告
文件检查意见单
测试见证报告
文件检查意见单
中期安全评估报告
安全评估报告
系统安全证书

- 方云根 Felix Fang
- 总经理 General Manager
- 评估与认证 Assessment& Certification
- 上海轨道交通检测技术有限公司Shanghai Railway Certification Co.,Ltd
- 电话：13817644197
- 邮箱：felix.fang@chinasrcc.com

感谢聆听