ISO 26262 Training

功能安全简介

SGS TÜV SAAR

WHEN YOU NEED TO BE SURE

SGS

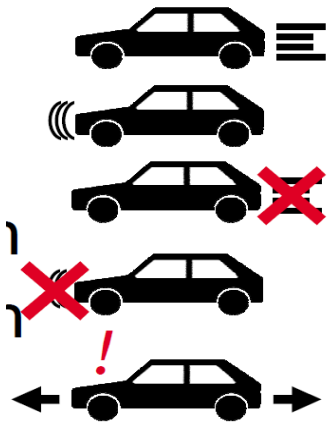
议程

1. **在汽车电子发展过程中导入功能安全**
2. **ISO 26262的简要概述**
3. **功能安全的现状与法律后果**

功能安全的定义

- 功能安全的定义
  - Absence of **unreasonable risk** due to **hazards** caused by **malfunctioning behaviour** of E/E systems
  - 不存在由E/E系统的失效行为导致的危害所引起的不合理风险
- “不合理”的定义
  - 不可接受
  - 过度的
- “风险”的定义
  - 危害几率和危害程度的组合

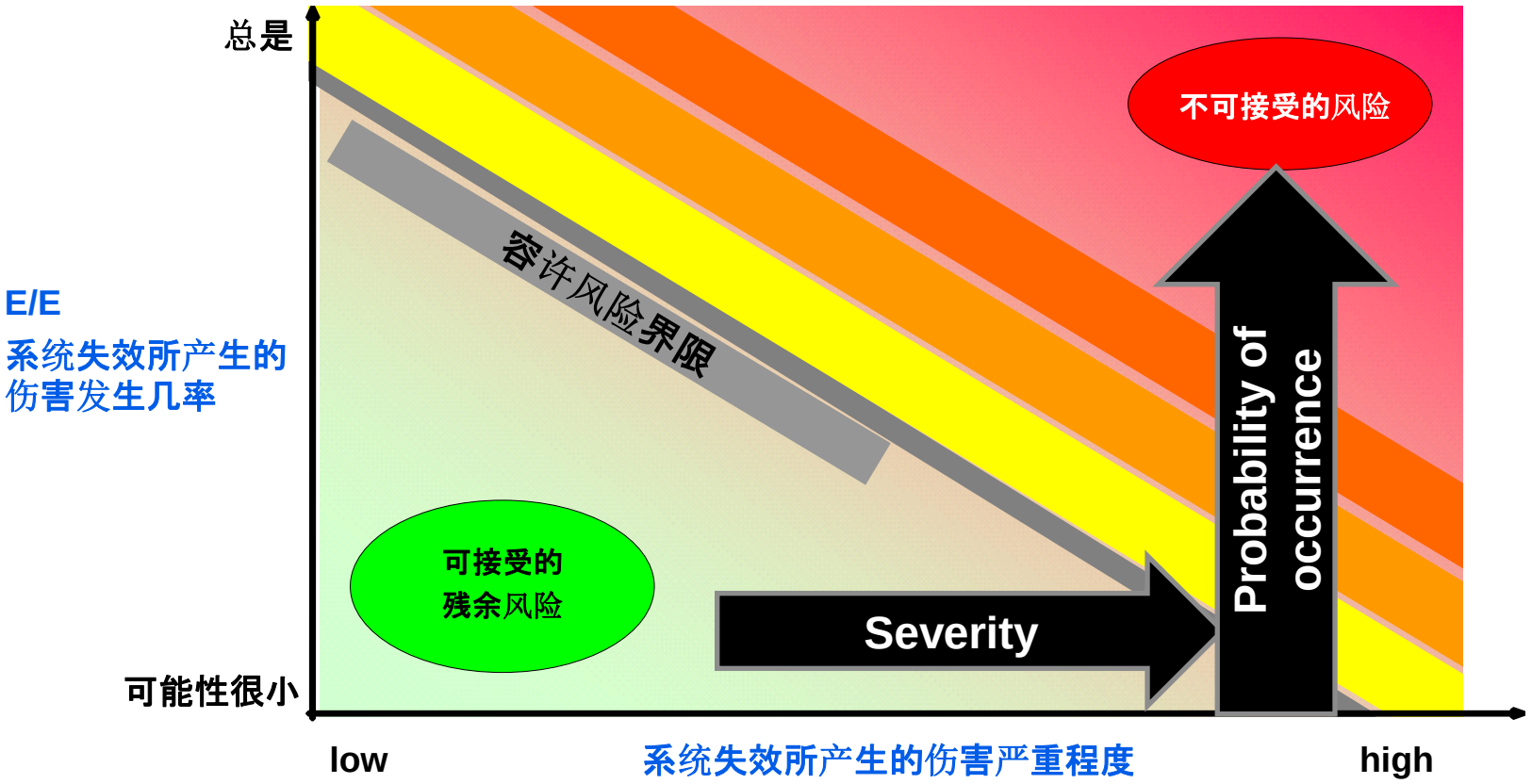
由道路车辆功能失效引起的风险



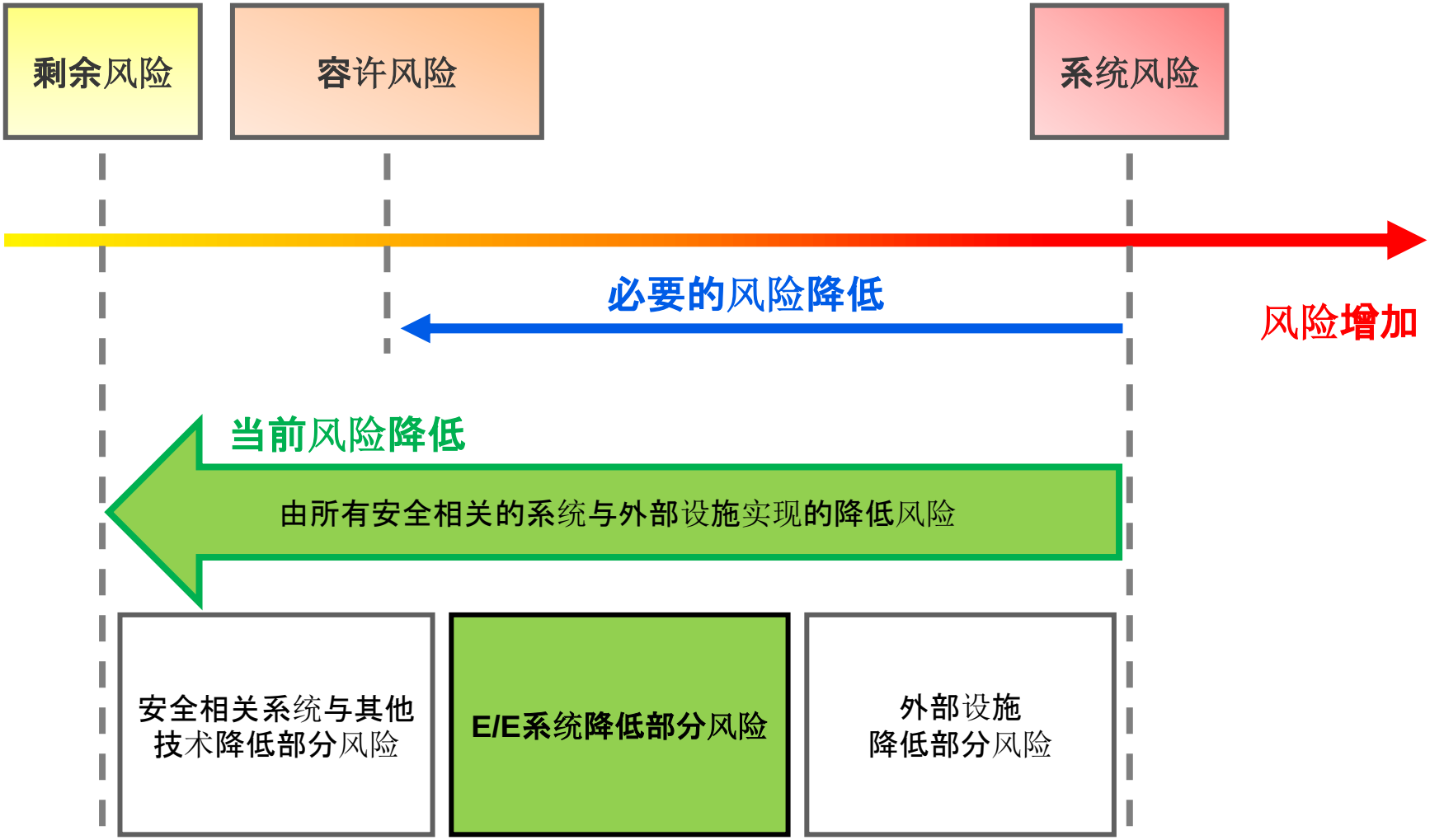
- 由E/E功能故障引起的主要风险
  - 非预期的加速
  - 非预期的减速
  - 非预期的失去加速
  - 非预期的失去减速
  - 非预期的车辆运动

- 由E/E功能故障导致的派生风险
  - 高压电击
  - 起火 / 爆炸

潜在风险的组成



降低风险的概念



议程

1. Introduction into Functional Safety in automotive electronics development
2. **ISO 26262 简要概述**
3. The current state of the art in Functional Safety and its legal consequences

历史

IEC 61508 Ed. 2.0	**针对电气/电子系统功能安全的基础标准**
ISO 26262	**基于IEC 61508，面向汽车工业的应用标准**

2011年11月14日，ISO 26262正式发布

范围

商用车与摩托车，目前不在第一版的要求之内，但会在第二版加入

- 有关安全的系统
  - 包括一个或多个E/E 子系统
  - 量产乘用车 (3.5吨以内)
  - 不包括残疾人专用车
- 应对可能存在的风险
  - 由E/E 系统的故障行为产生
  - 由E/E 系统自己产生

标准的内容

此标准划分为10个部分并且反映了汽车行业标准产品开发流程需要满足的要求

Normative

Part 1: 词汇 – 术语与缩写

Part 2: 功能安全管理 – 组织方面

Part 3: 概念阶段 – 风险评估与安全概念设计

Part 4: 系统级开发 – 系统开发中的安全方面

Part 5: 硬件级开发 – 硬件开发中的安全方面

Part 6: 软件级开发 – 软件开发中的安全方面

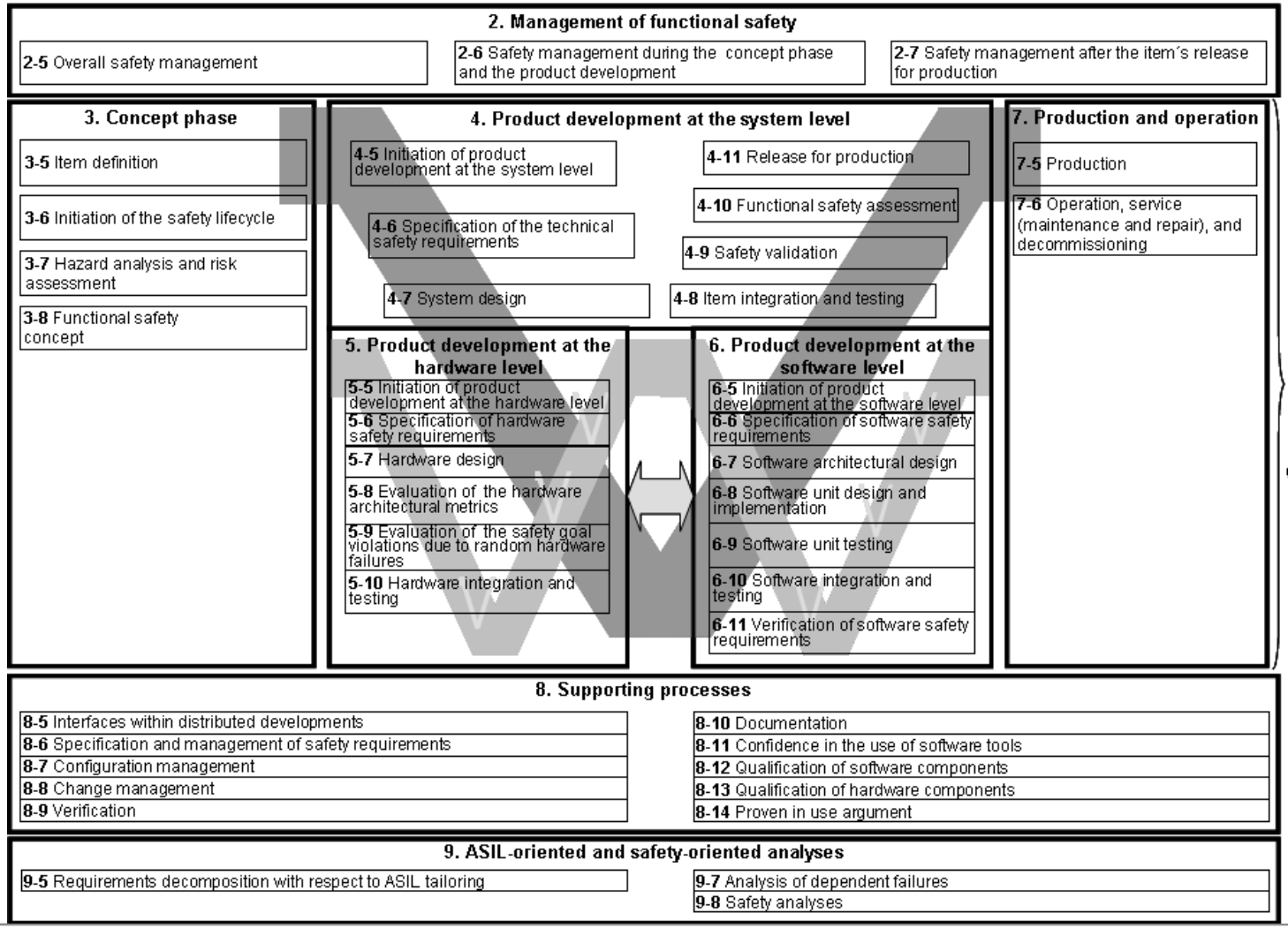
Part 7: 生产与运营 – SOP之后的安全方面

Part 8: 支持过程 – 质量保证过程

Part 9: ASIL导向与安全导向分析 – 安全分析

Part 10: ISO 26262指导 – 应用指南

结构



1. 术语

2. 功能安全管理

- 2-5整体安全管理
- 2-6概念阶段和产品开发阶段的安全管理
- 2-7生产发布后的安全管理

3. 概念阶段

- 3-5相关项定义
- 3-6安全生命周期启动
- 3-7危害分析和风险评估
- 3-8功能安全概念

4. 产品开发：系统层面

- 4-5系统层面产品开发启动
- 4-6技术安全要求规范
- 4-7系统设计
- 4-8相关项集成和测试
- 4-9安全确认
- 4-10功能安全评估
- 4-11生产发布

5. 产品开发：硬件层面

- 5-5硬件层面产品开发启动
- 5-6硬件安全要求规范
- 5-7硬件设计
- 5-8硬件架构指标
- 5-9由硬件随机失效而违反安全目标的评估
- 5-10硬件集成和测试

6. 产品开发：软件层面

- 6-5软件层面产品开发启动
- 6-7软件架构设计
- 6-8软件单元设计和实现
- 6-9软件单元测试
- 6-10软件集成和测试
- 6-11软件安全要求验证

7. 生产和运行

- 7-5生产
- 7-6运行、维护和报废

8. 支持过程

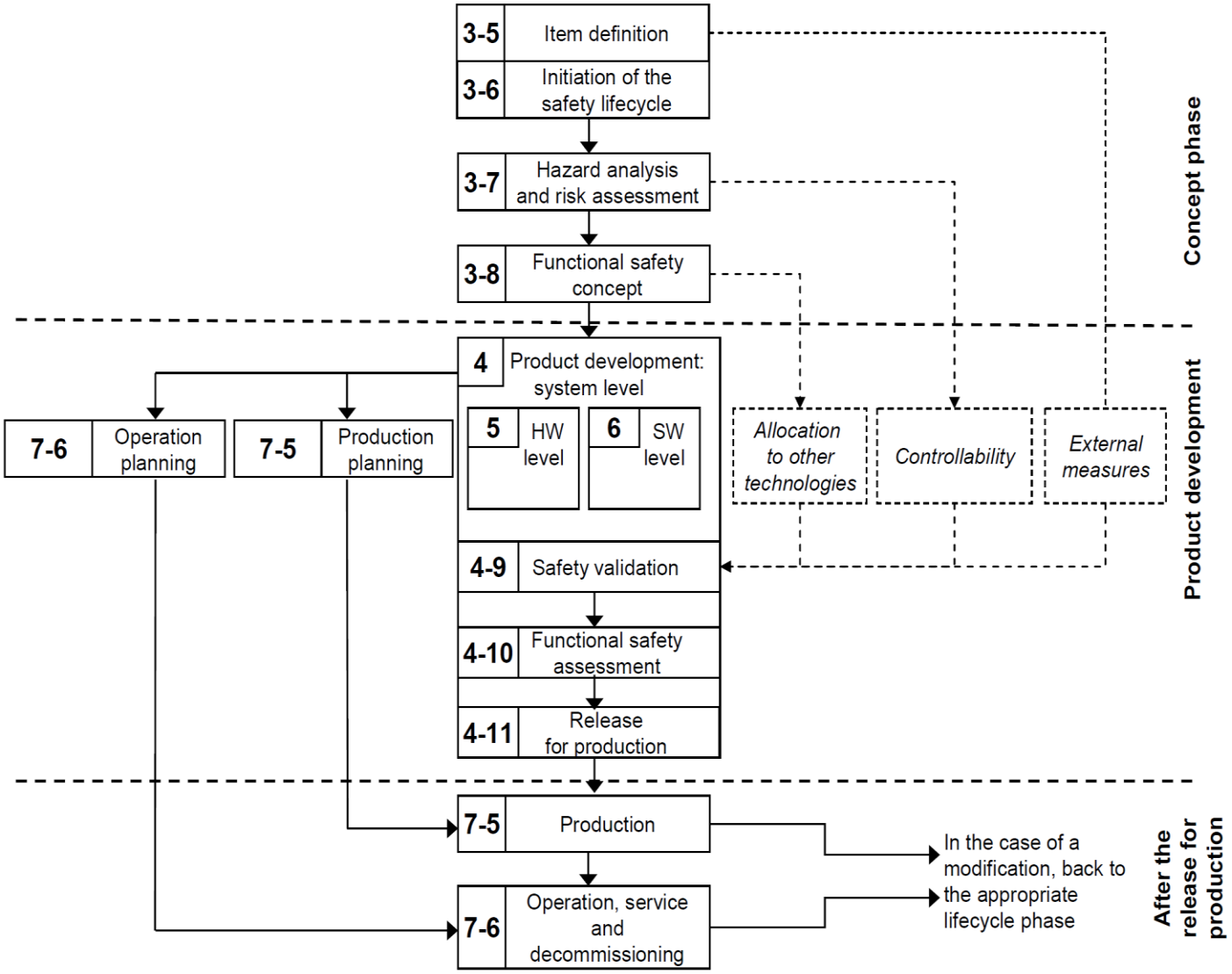
- 8-5分布式开发接口
- 8-6安全要求管理和规范
- 8-7配置管理
- 8-8变更管理
- 8-9验证
- 8-10文档
- 8-11软件工具资质
- 8-12软件组件资质
- 8-13硬件组件资质
- 8-14在用证明

9. 汽车安全完整性等级导向和安全导向分析

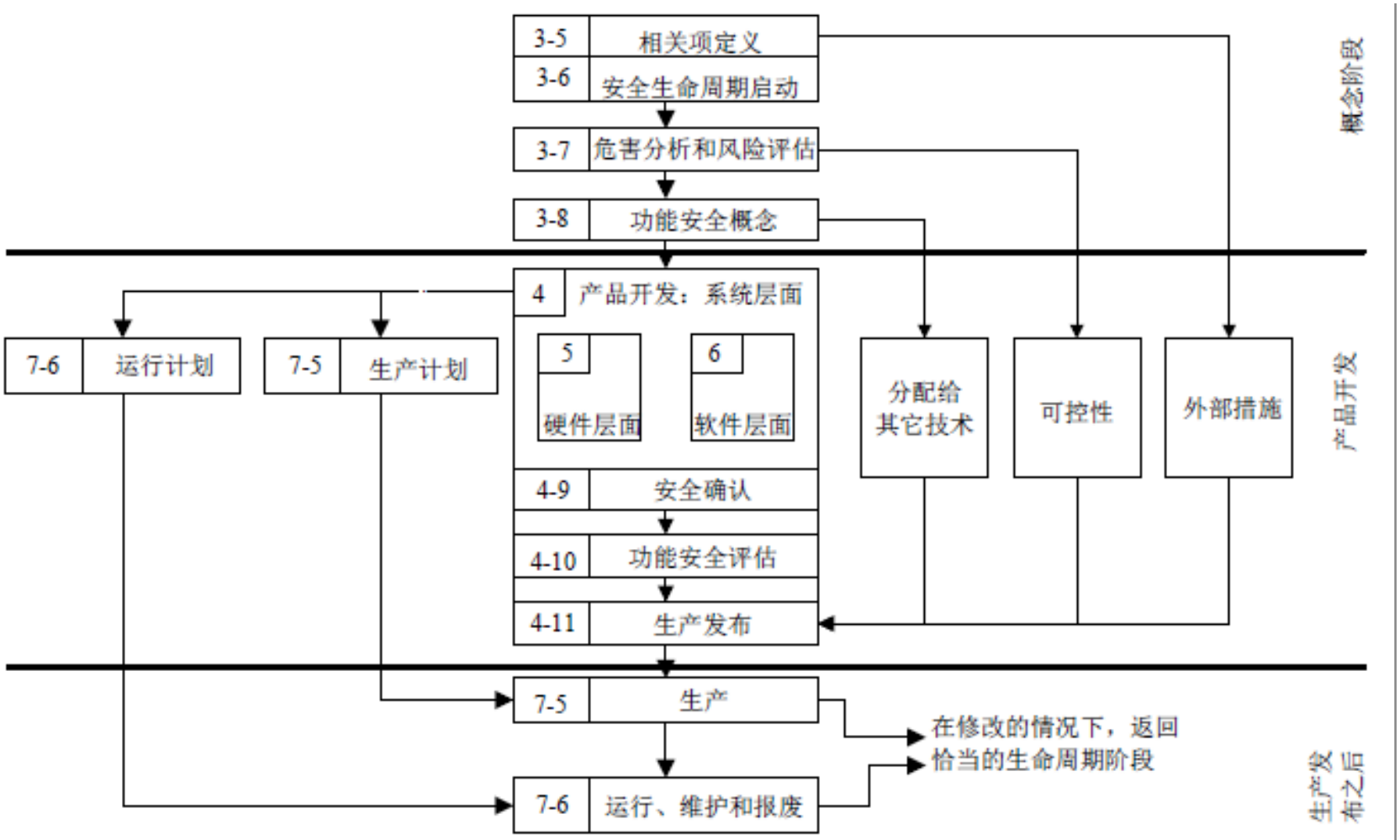
- 9-5关于ASIL剪裁的要求分解
- 9-6要素共存的标准
- 9-7相关失效分析
- 9-8安全分析

10. 指南

SAFETY LIFE CYCLE



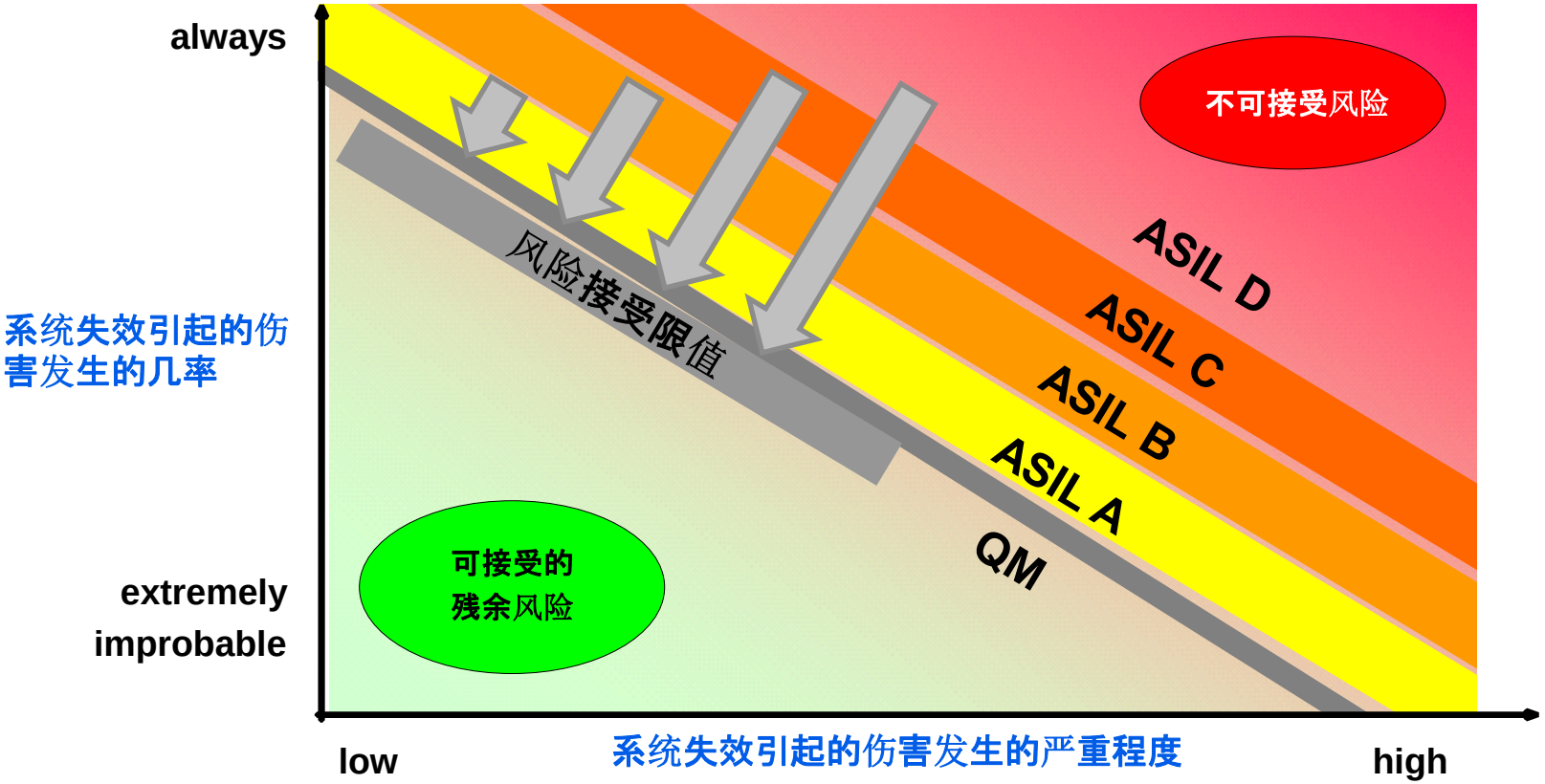
安全生命周期



衡量车辆系统/功能的潜在风险

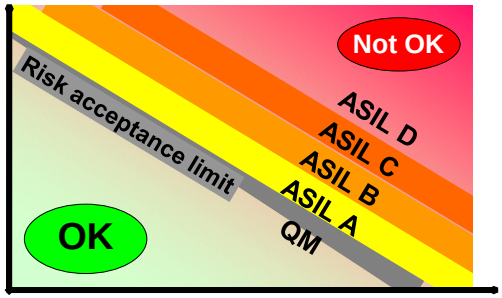
- Automotive Safety Integrity Level (ASIL) 车辆安全完整性等级
  - 5级标定 (QM, A, B, C, D)
  - QM 表示“质量保证是足够的”（源于ISO TS16949的应用）
  - 从ASIL A开始，必须采取额外的降低风险的措施
  - ASIL D 表示最高等级的潜在风险
  - ASIL等级会安置在对应的需求上：整车层级所定义的安全目标是最高阶的安全需求。

潜在风险的分类



何时应用标准

判断潜在风险的等级



ASIL ≥ A

No

标准流程
(EXIT)

Yes

采取额外措施，把风险降低至可接受的水平

避免系统性故障

避免随机故障

安全管理流程与支持流程

技术要求
(功能, 系统, 子系统, 硬件, 软件)

安全管理

- 公司安全管理
  - 安全文化
  - 资质管理
  - 质量管理
  - 安全生命周期
- 具体项目安全管理
  - 角色, 职责, 计划
  - 具体项目的安全生命周期裁剪
  - 安全案例
  - 安全确定措施
- 生产后的安全管理

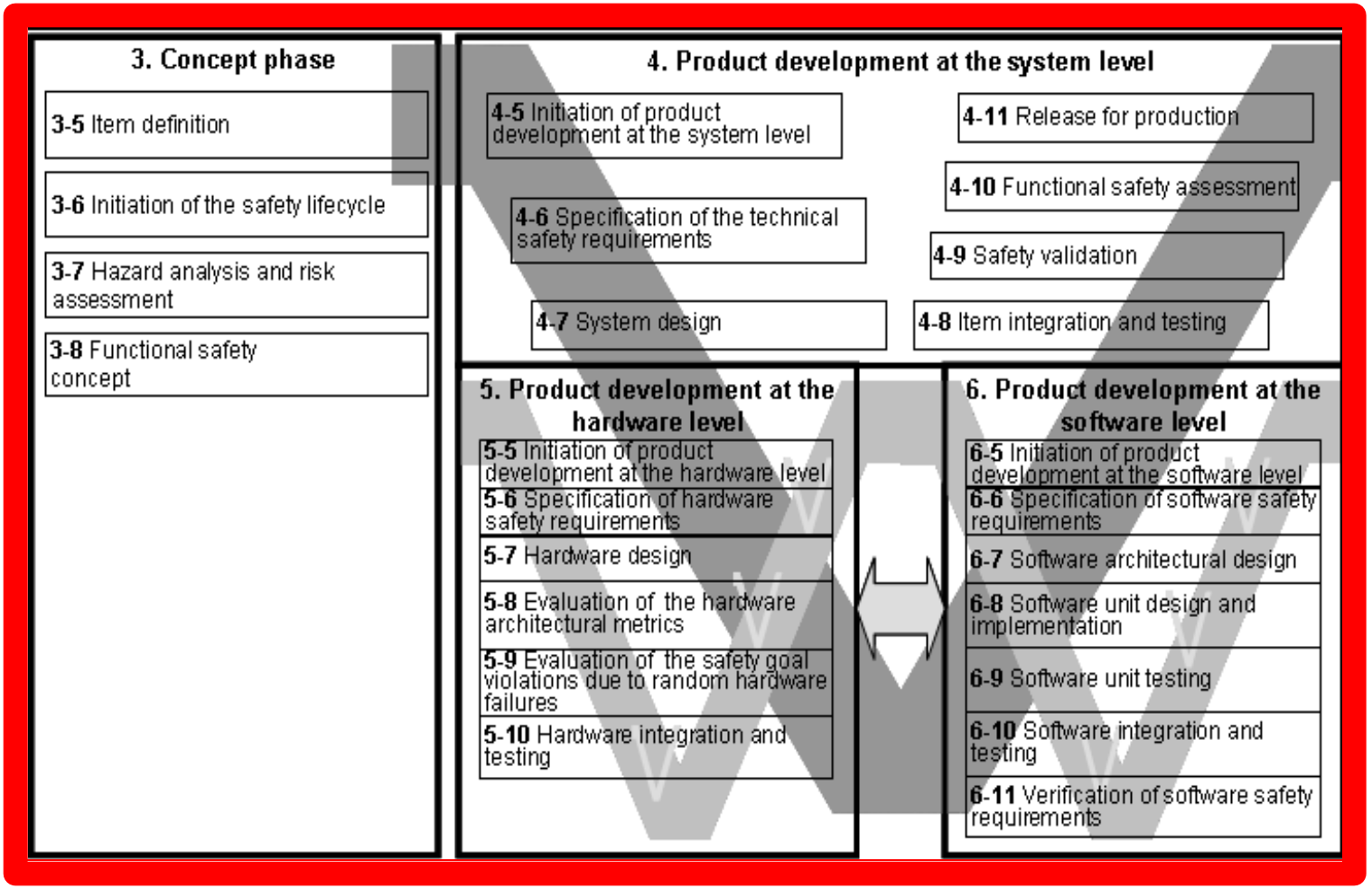
安全管理的定义

- EN 50129:2003（用于轨道交通的通讯、信号与处理系统）

  管理架构必须确保安全流程被正确执行

- 或者换句话说
  - 通过培训的并有经验的专业人士执行安全管理。
  - 安全管理包括预防性的安全措施与防御危险的措施

FUNCTIONAL SAFETY PROCESS MODEL



概念阶段的安全活动

- 相关项的定义
  - 范围是整车级别
  - 功能要求，法律要求，操作条件， 根据其他项添加的要求
- 安全生命周期初始化
  - 决定开发的类型
    (新开发, 修改, 重复使用)
  - 安全生命周期的影响分析与裁剪
- 危害分析与风险评估
  - 运用标准的方法识别可能的风险与确定潜在的风险
  - 确定ASIL与相关安全目标
- 功能安全概念
  - 导出功能安全需求与相关参数 （安全条件，容错时间等）
  - 完成已设立安全目标的功能概念

系统级产品开发中的安全活动

- 系统级产品开发的启动
  - 系统开发中安全活动的计划
  - 验证行动的计划
  - 安全评估活动的计划
- 技术安全要求规范
  - 为达到安全目标的技术安全要求规范，功能安全要求与功能安全概念
  - 环境要求规范
  - 其他系统与接口的要求规范
- 系统设计
  - 从功能安全概念和技术安全要求导出的系统设计（迭代过程）
  - 技术安全概念的创立

系统级产品开发中的安全活动

- 相关项的集成与测试
  - 验证功能与技术安全需求的集成测试
  - 根据ASIL，选择测试方法
- 安全确认
  - 整车级安全目标的确认
  - 测试是基于安全目标，功能安全的要求及预期用途
- 功能安全评估
  - 功能安全的独立评估
  - 形式和内容相关性检查（安全案例）
- 生产发布
  - 判定生产发布的条件
    (提供功能安全信任的批准流程)

硬件级产品开发中的安全活动

- 硬件级产品开发的初始化
  - 硬件开发过程的安全活动计划
  - 安全计划的细节
- 硬件安全要求规范
  - 从技术安全概念与系统设计说明导出硬件安全要求
  - 硬件需要满足的可靠性要求规范
  - 硬件-软件接口规范的细节
- 硬件设计
  - 根据系统设计规范和硬件安全要求设计硬件
  - 对照系统设计规范和硬件安全要求验证硬件设计

硬件级产品开发中的安全活动

- 硬件架构矩阵的评估
  - 根据故障处理的要求评估相关项的硬件架构
  - 单点故障度量 (SPFM)
  - 潜伏故障度量 (LFM)
- 评估由于硬件随机故障引起的违反安全目标
  - 证明由于随机硬件故障导致相关项违反安全目标的剩余风险足够低
  - Option A: Probabilistic Metric for Random Hardware Failures = PMHF 随机硬件失效概率度量
  - Option B: 评估违反安全目标的每种原因
- 硬件集成与测试
  - 通过测试验证硬件开发和硬件规范的一致性

软件级产品开发的安全活动

- 软件级产品开发的初始化
  - 软件开发过程的安全活动计划
  - 安全计划的细节
  - 方法，工具，模型和编程语言的选择和验证
- 软件安全需求规范
  - 从技术安全概念和系统设计规范导出软件安全要求
  - 硬件-软件接口规范（HSI）的细节
- 软件架构设计
  - 开发一个软件的架构设计，以实现软件安全要求
  - 验证软件架构设计

软件级产品开发的安全活动

- 软件单元的设计与执行
  - 根据软件架构设计与软件安全要求详细说明软件单元
  - 按照说明执行软件单元
  - 静态验证软件单元的设计与执行
- 软件单元测试
  - 证明软件单元满足软件单元设计规范，同时不包含无用功能
- 软件集成与测试
  - 软件元素集成
  - 证明嵌入式软件实现软件架构设计
- 软件安全需求的验证
  - 证明嵌入式软件实现软件安全需求

系统设计分析方法

Method	ASIL			
	A	B	C	D
演绎分析 ▪ FTA ▪ Reliability Block diagrams可靠性框图 ▪ Ishikawa diagram 鱼骨图	O	+	++	++
归纳分析 ▪ FMEA 失效模式分析 ▪ ETA 事件树分析 ▪ Markov modelling 马尔可夫模型	++	++	++	++

”++” Deviations must be conclusively justified

“+“ Method is recommended for this ASIL

“o“ Method is neither recommended nor not recommended.

Reference: ISO 26262-4, § 7.4.3.1 Table 1

职责与信息流

Abstraction level	Vehicle 整车	E/E 总系统	E/E 子系统	HW 硬件	SW 软件
发展阶段	Concept (part 3)	System (part 4)	System (part 4)	Hardware (part 5)	Software (part 6)
信息流	•安全目标 •ASIL •功能安全需求 •功能安全概念	•技术安全需求 •技术安全概念	•技术安全需求 •技术安全概念	•硬件安全要求 •硬件设计	•软件安全要求 •软件设计
责任人	OEM	OEM or Tier1	Tier1 or Tier 2..n	HW supplier (complex function, e.g. µC or ECU)	SW supplier (application)

分步式开发的接口

- 供应商的选择
  - 检查供应商是否能够按照ISO26262进行开发
  - 在RFQ列出规范的要求
  - 把项目定义、安全目标与功能安全需求发给供应商
  - 功能安全评价是前提条件
- 项目处理
  - 开发接口（DIA）协议包括：
    - 所有参与方的安全经理
    - 安全生命周期的裁剪
    - 活动与职责的分配
    - 信息交换

项目管理规则

- 配置管理
  - 与如下流程一致
    - ISO TS 16949 or
    - ISO 10007 or/and
    - ISO 12207, 6.2 (Software)
  - 适用于全部安全生命周期的产出物，并且归档在配置管理计划中
  - 在整个安全生命周期中运行

项目管理规则

- 变更管理
  - 变更请求
  - 变更请求的分析
  - 关于变更请求的决定
  - 变更请求的执行与文档编制
- 文档编制
  - Standard QM requirements标准质量管理要求
  - 文件必须参考产出物
  - 对于保留方式与保留期限没有要求

验证

- 验证的方法
  - Review 检查
  - Simulation 模拟
  - Test 测试
- 测试环境
- “通过/不通过”的标准
- 对安全要求的明确参考
- 使用的工具

软件工具的资格认可

	TD1	TD2	TD3
TI1	TCL1	TCL1	TCL1
TI2	TCL1	TCL2	TCL3

- 软件工具必须根据其具体应用进行资格认可，才可以认为是安全使用
- 当软件工具达到所需要的工具置信等级（TCL），则通过资格认可

Reference: ISO 26262-8

实施ISO 26262的安全活动小结

议程

1. Introduction into Functional Safety in automotive electronics development
2. Quick overview of ISO 26262 requirements
3. **功能安全的现状与法律后果**

法律后果

- 适用标准与行业特定标准
  - 反映技术的通用规则
  - 定义最低标准
- 目前发展水平
  - 标准 + 竞争 + 成果
  - 在世界某个地方已经被发布
  - 最新的技术
  - 在经营中被证明
  - 普遍使用的技术成果（未必是新技术）

技术建议的法律后果

标准的主要法律意义是：在各个产品领域设立最低的标准

- Liability for defects缺陷责任
  - 典型设计/工艺
- Product liability 产品责任
  - 商业安全义务
- Public Law 公共法
  - 保护公众防范可避免的安全风险
- Criminal Law 刑法
  - 生命与健康的保护

实施ISO 26262的法律后果

- 已经发布的ISO 26262 描述了目前发展水平
- 自标准发布之日起，所有投入生产的E/E系统必须遵守ISO 26262的推荐
- 既然没有过渡期，ISO26262的推荐必须百分之百执行。

现有设计的法律后果

- ISO 26262 允许豁免标准发布之前开发的E/E系统
- 假设随后发生变更，需要做delta评估，也就是说只有实际变更的部分必须依据ISO 26262进行评估。
- 上述内容与产品责任条款有冲突，后者是基于目前发展现状

评估的法律后果

- 一旦需要举证，需要提交符合性证明
- ISO 26262本身不排除内部组织单元执行评估的可能性
- 律师意见是内部评估缺乏中立性，可能不被认可为“目前发展现状”
- 推荐由ISO/IEC 17025认可机构进行评估