功能安全基础培训

——产品工程部

二〇二一年四月

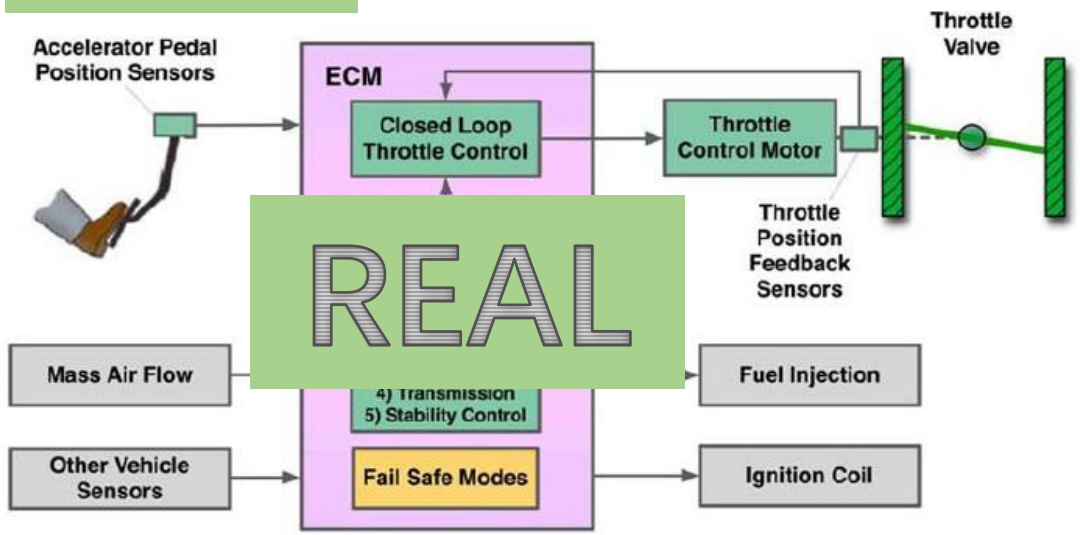
课程大纲

- 第一单元：基本概念
- 第二单元：功能安全管理
- 第三单元：概念阶段
- 第四单元：功能安全开发(ECU层级)
- 第五单元：支持流程和安全分析

功能安全定义(Functional Safety)

没有由电子/电气系统故障行为导致的危害所引起的不合理的风险(ISO26262-1)
Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems (ISO26262-1)

Is it FuSa case?



89 deaths/57 injuries/52 suspected/6200 complaints in decade

Is it FuSa case?

11 deaths

基本概念

Safety functions

- To add more function to reduce risk.
- To reduce the risk from higher level to lower level.

e.g. Airbag exploding to protect driver and passenger is (passive) safety function

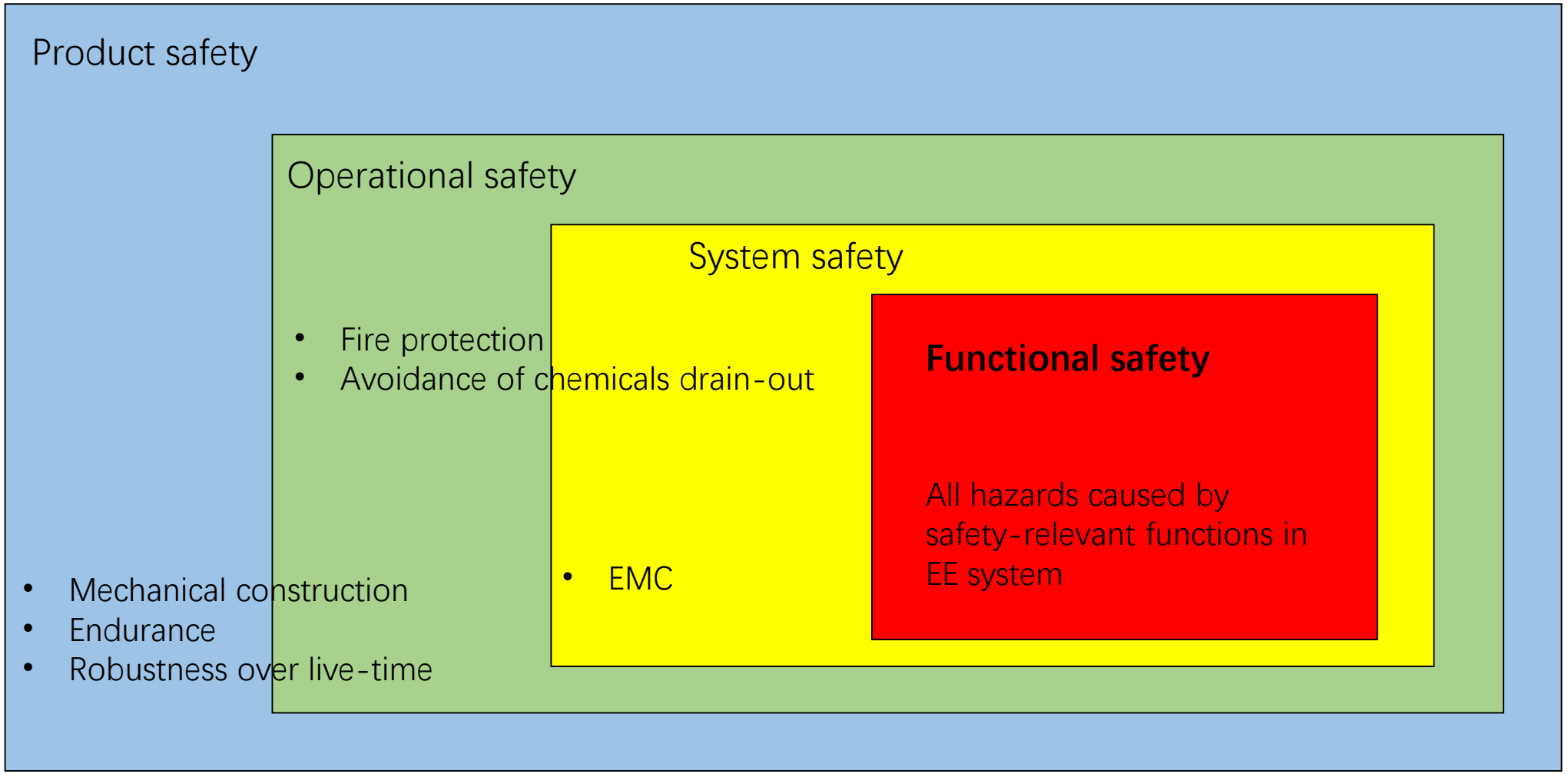
VS

Functional safety

- To absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems
- To reduce the risk from higher level to accepted risk.

e.g. “No unintended exploding” is functional safety

功能安全的范围


Product safety
Operational safety
System safety
Functional safety
All hazards caused by safety-relevant functions in EE system
• Fire protection
• Avoidance of chemicals drain-out
• EMC
• Mechanical construction
• Endurance
• Robustness over live-time

为什么需要功能安全

社会、客户和政府

- 防止事故和人身伤害的高期望
- 期望将风险降低到可接受的范围

OEM和供应商

- 期望满足客户和社会的需求
- 避免事故带来的名誉损失
- 倾向于避免投诉和损失

  E.g. 丰田油门踏板事件和波音737 Max事件

Boeing 737
l Preliminary Inve

法律和法规

1.德国产品责任法 German Product Liability Act

Compensation obligation of the manufacture is **only exclude if the fault could not be detected based on the states of science and technology which existed at the time** when the manufacture put the product into circulation. --*Section1, Para2, Number5, German Product Liability Act*

2. EU Regulation(E.g. ECE R13H; ECE R79; GTR 20)

ECE R13H **Annex8** / ECE R79 **Annex6:**

SPECIAL REQUIREMENTS TO BE APPLIED TO THE **SAFETY ASPECTS** OF **COMPLEX ELECTRONIC VEHICLE CONTROL SYSTEMS.**

3. 中国国标(SAC/TC114/SC29)

GB/T 34590《道路车辆 功能安全》

GB《电动汽车安全要求》

GB《电动客车安全要求》

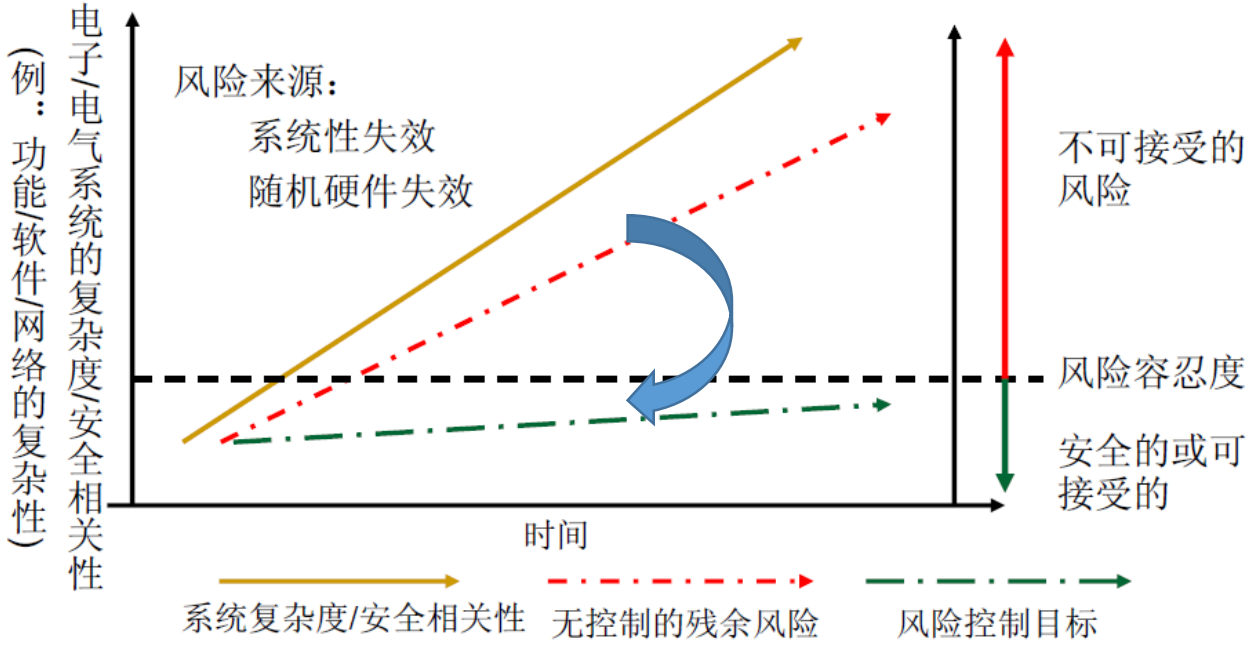
GB《电动汽车用锂离子动力蓄电池安全要求》

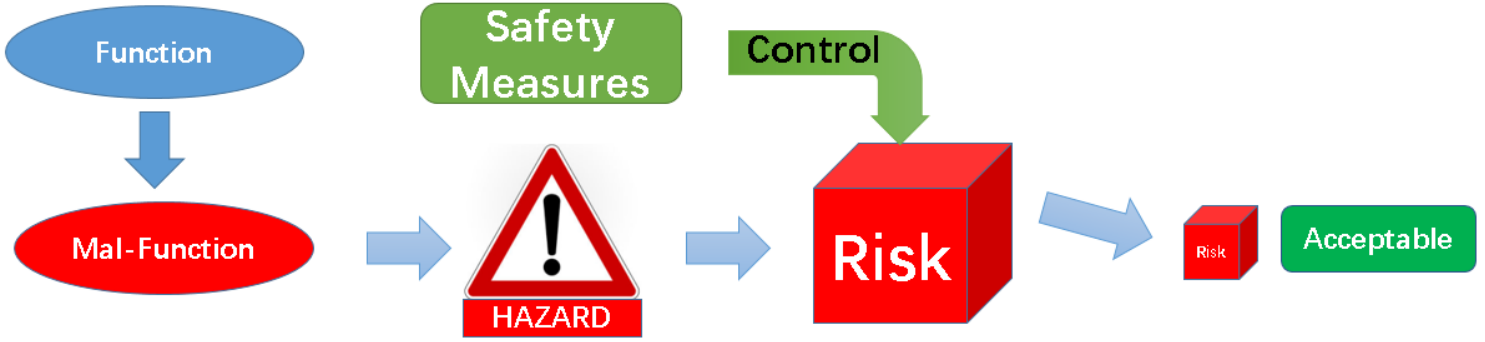
GB 17675 《汽车转向系 基本要求》附录D功能安全内容

GB 21670《乘用车制动系统技术要求及试验方法》附录D功能安全内容

功能安全的开发目标

针对汽车电子/电气系统复杂度和安全相关性的增长，风险越来越难以识别和控制，ISO 26262提供了解决功能安全的系统性方法。





功能失效的风险来源

系统性故障	随机硬件失效
1. 确定性，可重复性 2. 可避免，可控制 3. 一般无法量化 …	1. 不确定性，不可重复 2. 无法避免，可以控制 3. 可量化 …
E.g. 1. 设计错误 2. Bugs 3. 制造错误 4. 操作错误 …	E.g. 1. MCU故障: 位翻转，软错误 2. 线路故障：开路/短路 3. 卡滞 …

安全措施

用以避免或控制系统性失效，检测或控制随机硬件失效，或减轻它们影响的**活动**或**技术方案**

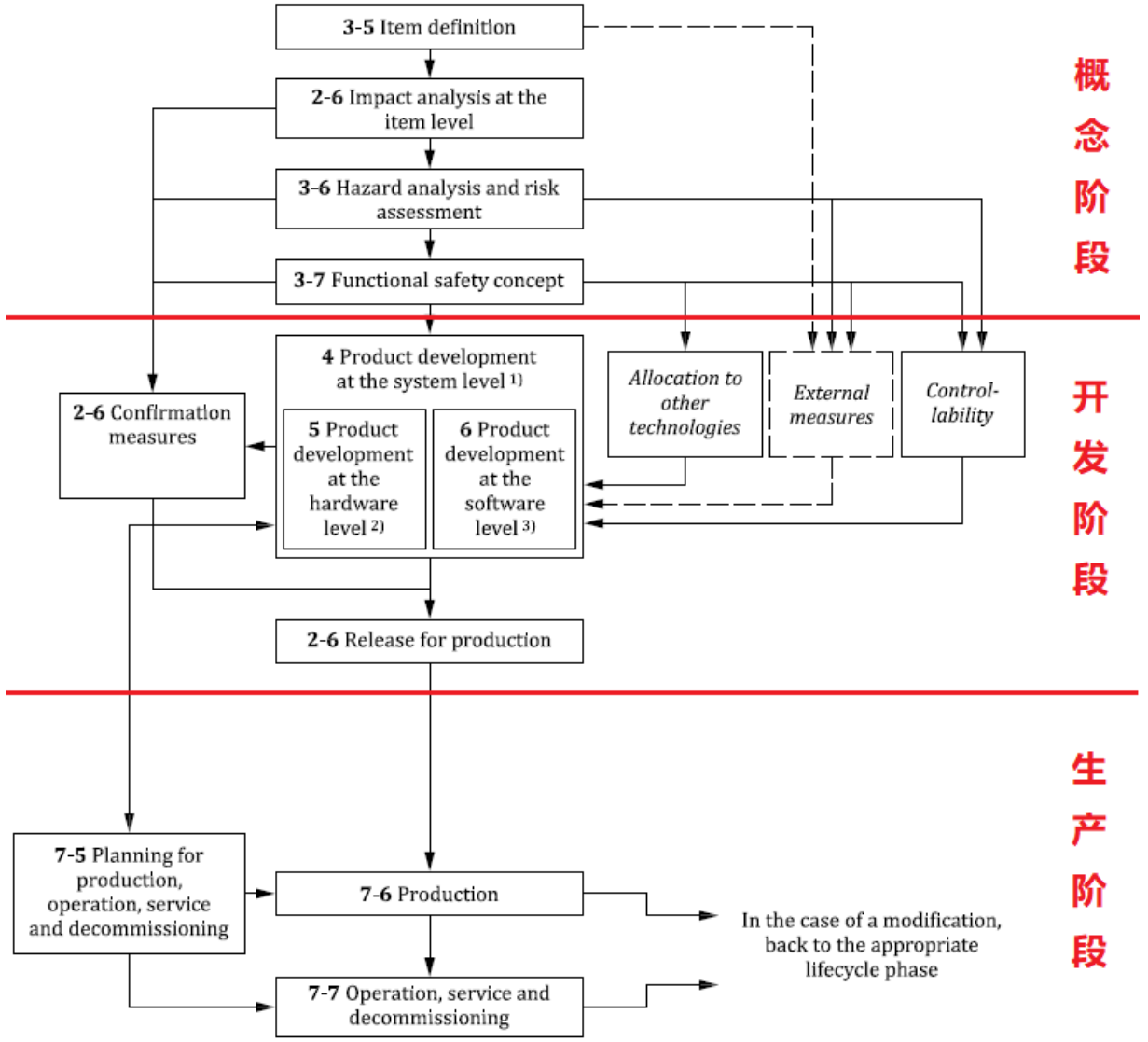
活动：
- ✓ V&V
- ✓ Confirmation measures
- ✓ Safety Case Compiling
- …

技术方案:
- ✓ Safety mechanism
- ✓ HARA
- ✓ Safety Analysis
- ✓ Fault Injection Test
- …

安全机制

为维持预期功能，实现或维持安全状态，由E/E 元素/功能或其他技术执行的**技术解决方案**，用以检测，减轻或者容忍故障，控制或避免失效。

安全生命周期


3-5 Item definition
2-6 Impact analysis at the item level
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
4 Product development at the system level 1)
2-6 Confirmation measures
5 Product development at the hardware level 2)
6 Product development at the software level 3)
Allocation to other technologies
External measures
Control-lability
2-6 Release for production
7-5 Planning for production, operation, service and decommissioning
7-6 Production
7-7 Operation, service and decommissioning
In the case of a modification, back to the appropriate lifecycle phase
概念阶段
开发阶段
生产阶段

功能安全开发流程

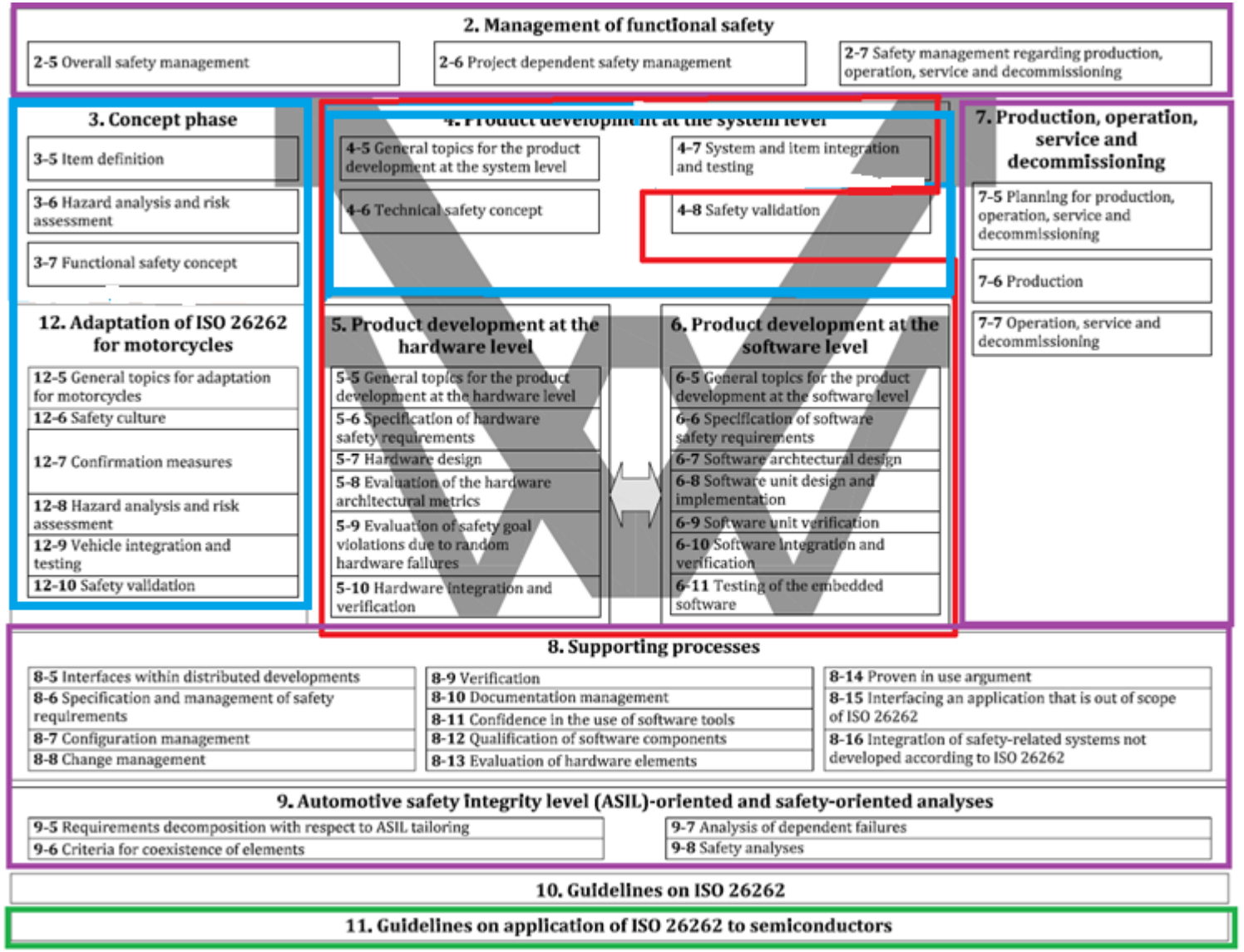
ISO26262-2018 功能安全开发全流程及相应的责任分工如右图所示：

OEM

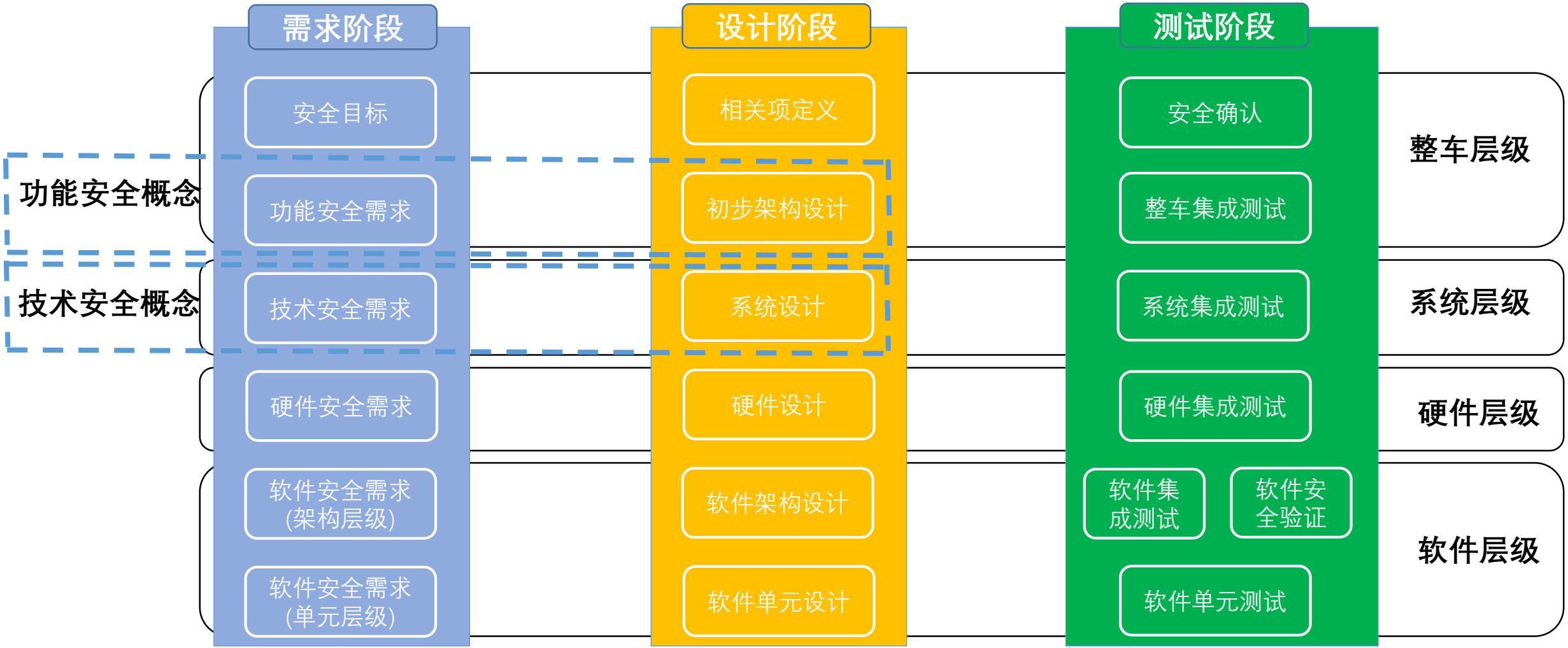
Supplier

OEM/Supplier

MCU/ASIC Supplier



功能安全概念到系统开发流程



课程大纲

- 第一单元：基本概念
- 第二单元：功能安全管理
- 第三单元：概念阶段
- 第四单元：功能安全开发(ECU层级)
- 第五单元：支持流程和安全分析

总体功能安全管理

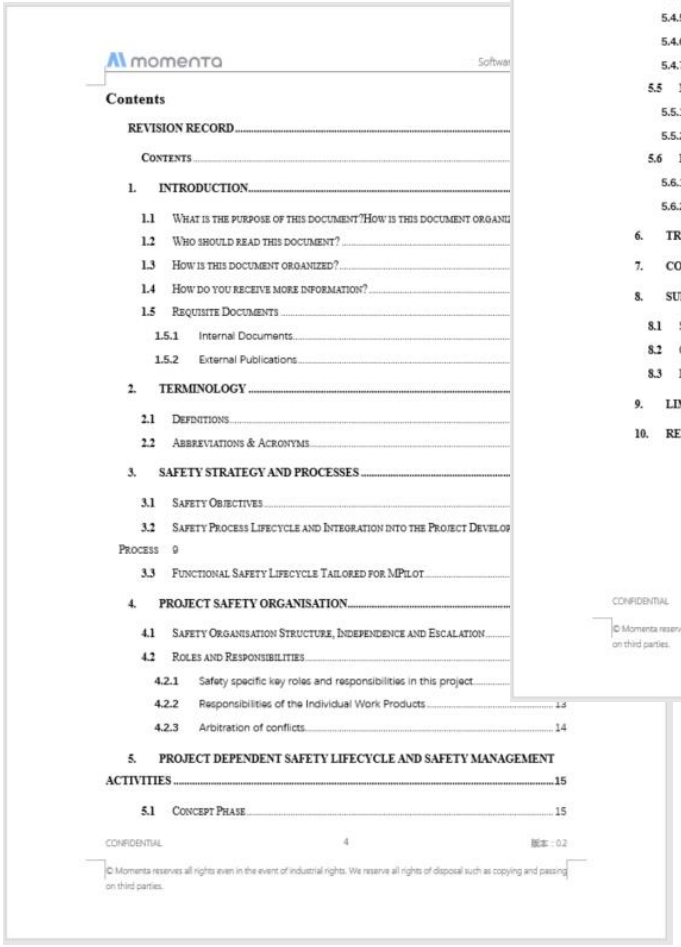
- 建立和促进“安全文化”
- 安全异常管理和问题升级机制
- 人员能力管理
- 质量管理
- 定义安全生命周期

项目相关的安全管理

- 定义安全活动人员的角色和职责
- 计划和协调安全活动
- 规定认可措施
- 安全档案收集和管理

项目相关的安全管理

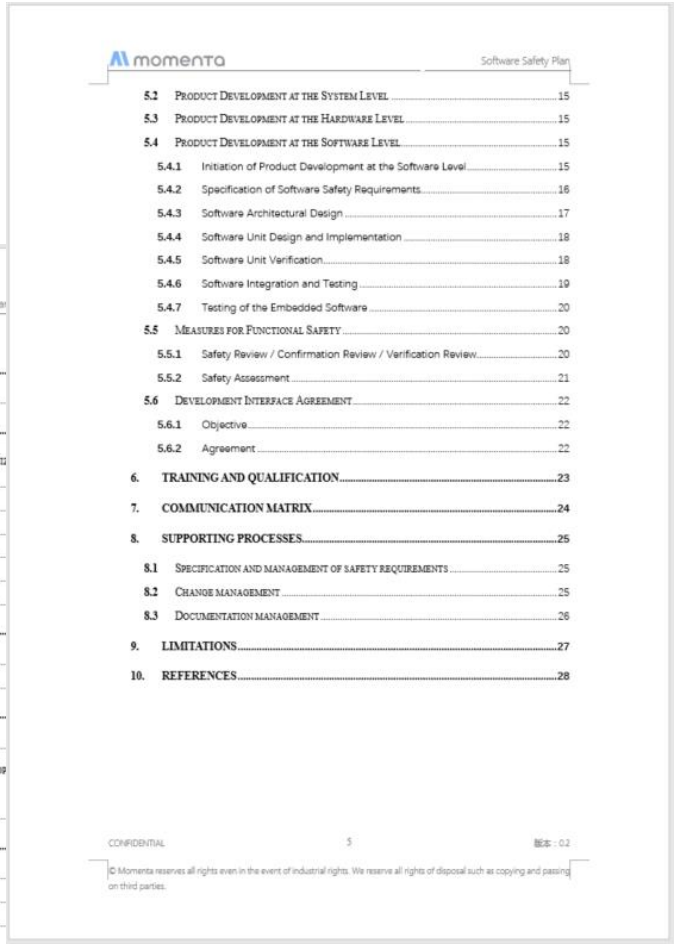
- **安全计划**
  - ✓ 功能安全要求的活动和流程
  - ✓ **开发接口协议(DIA)**
  - ✓ 支持流程
  - ✓ 危险分析与风险评估(H&R)
  - ✓ 安全需求的开发与应用
  - ✓ 相关失效分析和安全分析
  - ✓ 验证和确认活动(Verification & Validation)
  - ✓ 功能安全认可方法
  - ✓ 提供候选产品的在用证明(如需要)
  - ✓ 提供软件工具的置信度证明


momenta

Contents

REVISION RECORD
CONTENTS
1. INTRODUCTION
1.1 WHAT IS THE PURPOSE OF THIS DOCUMENT?HOW IS THIS DOCUMENT ORGANI
1.2 WHO SHOULD READ THIS DOCUMENT?
1.3 HOW IS THIS DOCUMENT ORGANIZED?
1.4 HOW DO YOU RECEIVE MORE INFORMATION?
1.5 REQUISITE DOCUMENTS
1.5.1 Internal Documents
1.5.2 External Publications
2. TERMINOLOGY
2.1 DEFINITIONS
2.2 ABBREVIATIONS & ACRONYMS
3. SAFETY STRATEGY AND PROCESSES
3.1 SAFETY OBJECTIVES
3.2 SAFETY PROCESS LIFECYCLE AND INTEGRATION INTO THE PROJECT DEVELOP
PROCESS 9
3.3 FUNCTIONAL SAFETY LIFECYCLE TAILORED FOR MPILOT
4. PROJECT SAFETY ORGANISATION
4.1 SAFETY ORGANISATION STRUCTURE, INDEPENDENCE AND ESCALATION
4.2 ROLES AND RESPONSIBILITIES
4.2.1 Safety specific key roles and responsibilities in this project
4.2.2 Responsibilities of the Individual Work Products
4.2.3 Arbitration of conflicts 14
5. PROJECT DEPENDENT SAFETY LIFECYCLE AND SAFETY MANAGEMENT ACTIVITIES 15
5.1 CONCEPT PHASE 15

CONFIDENTIAL 4


momenta Software Safety Plan

5.2 PRODUCT DEVELOPMENT AT THE SYSTEM LEVEL 15
5.3 PRODUCT DEVELOPMENT AT THE HARDWARE LEVEL 15
5.4 PRODUCT DEVELOPMENT AT THE SOFTWARE LEVEL 15
5.4.1 Initiation of Product Development at the Software Level 15
5.4.2 Specification of Software Safety Requirements 16
5.4.3 Software Architectural Design 17
5.4.4 Software Unit Design and Implementation 18
5.4.5 Software Unit Verification 18
5.4.6 Software Integration and Testing 19
5.4.7 Testing of the Embedded Software 20
5.5 MEASURES FOR FUNCTIONAL SAFETY 20
5.5.1 Safety Review / Confirmation Review / Verification Review 20
5.5.2 Safety Assessment 21
5.6 DEVELOPMENT INTERFACE AGREEMENT 22
5.6.1 Objective 22
5.6.2 Agreement 22
6. TRAINING AND QUALIFICATION 23
7. COMMUNICATION MATRIX 24
8. SUPPORTING PROCESSES 25
8.1 SPECIFICATION AND MANAGEMENT OF SAFETY REQUIREMENTS 25
8.2 CHANGE MANAGEMENT 25
8.3 DOCUMENTATION MANAGEMENT 26
9. LIMITATIONS 27
10. REFERENCES 28

CONFIDENTIAL 5

项目相关的安全管理

- **确认措施**
  - ✓ 确认评审： 评判关键工作产品能否提供充分和令人信服的证据证明它们对功能安全实现的贡献
  - ✓ 功能安全审核：评判功能安全所要求的开发流程的执行情况
  - ✓ 功能安全评估：通过开发的元素来评判已实现的相关项功能安全，或者对功能安全实现的贡献

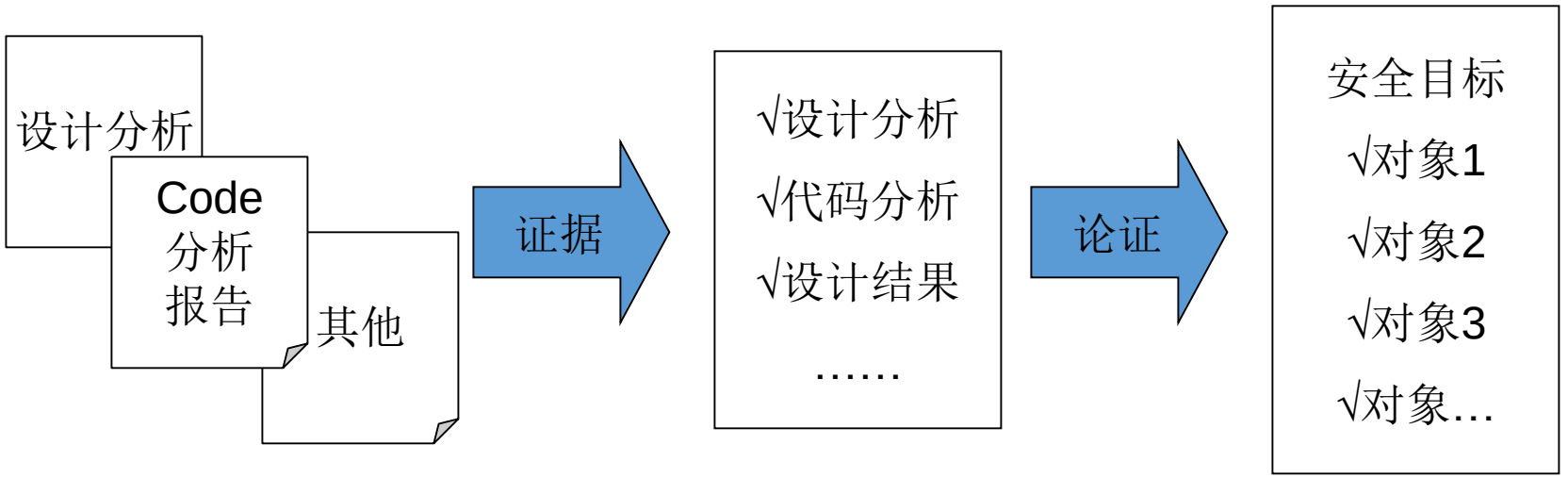
Table 1 *(continued)*

Confirmation measures	Level of independence[a] applies to					Scope
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
Confirmation review of the safety analyses and the dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262- 9:2018, Clause 7, respectively) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety requirements
Confirmation review of the safety case (see 6.5.4) Independence with regard to the authors of the safety case	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety requirements
Functional safety audit in accordance with 6.4.11 Independence with regard to the developers of the item and project management	—	—	I0	I2	I3	Applies to the highest ASIL among the safety requirements
Functional safety assessment in accordance with 6.4.12 Independence with regard to the developers of the item and project management	—	—	I0	I2	I3	Applies to the highest ASIL among the safety requirements

项目相关的安全管理

➢ 安全档案 Safety Case

Safety Case要求传递一个清晰的、可理解的和可信的(defensible)论证（由证据支撑），说明系统在特定环境下运行时没有不合理的风险。



批产后的安全管理

- **目标**

  定义在批产后的生命周期活动中，个人和组织为保证功能安全实现的职责

- **批产后的安全活动计划**
  - ✓定义相关角色、责任和活动
  - ✓定义批产后的安全流程，如现场监控流程(问题报告和记录，纠正措施)

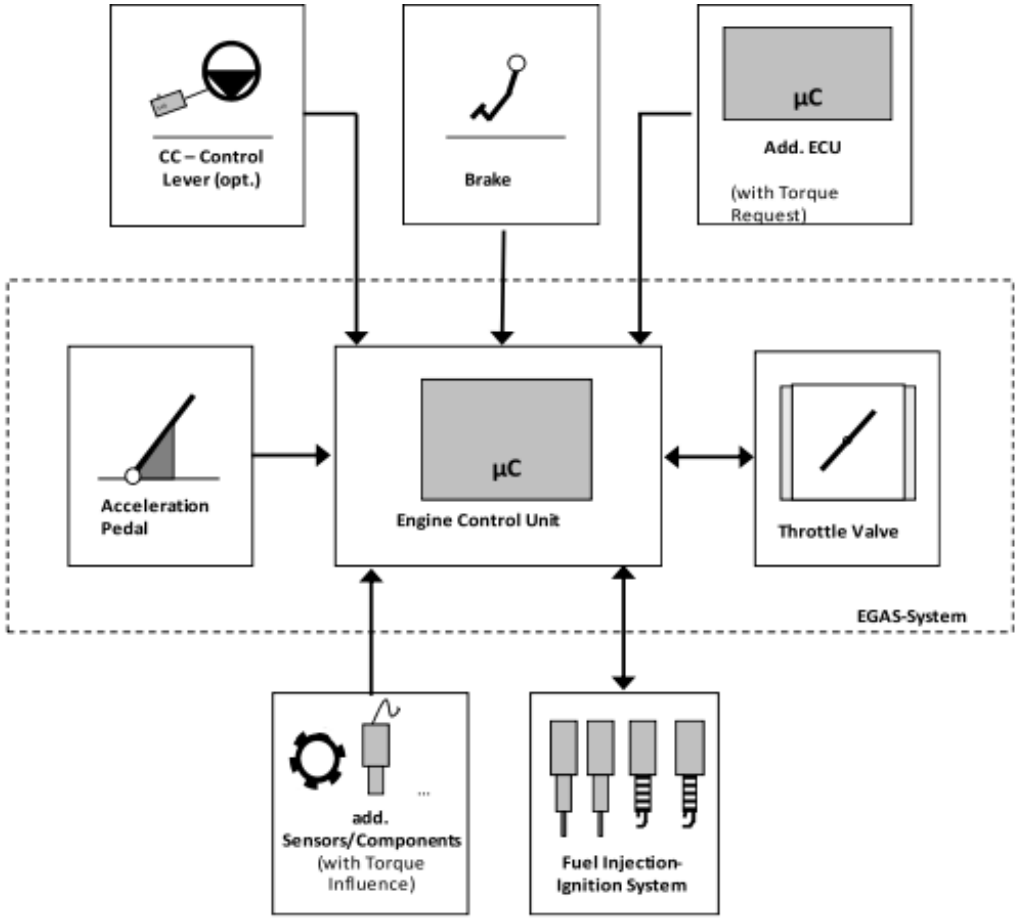
- **现场监控流程**
  - ✓报告和记录每个安全事故
  - ✓纠正措施和记录

课程大纲

- 第一单元：基本概念
- 第二单元：功能安全管理
- 第三单元：概念阶段
- 第四单元：功能安全开发(ECU层级)
- 第五单元：支持流程和安全分析

相关项定义

相关项：执行一个或部分整车功能的系统或系统的集合，相关项的定义其功能、接口、边界条件、环境条件、法规要求和危害等。



以ETC系统为例：

功能:

- 提供驱动扭矩
- 通过发动机拖拽，提供制动扭矩

结构：

- 发动机是单一驱动扭矩源
- 发动机通过传传动系直接耦合到车轮
- 发送机通过ECM控制

应用环境： 乘用车

ETC系统包括：

- 加速踏板
- ECU
- 节气门阀

危害识别

相关项的功能失效行为可通过**HAZOP**(Hazard and Operability Analysis，危险与可操作性分析）方法识别.

基于HAZOP，主要考虑Item(相关项)的如下功能失效：

- 功能丢失
- 功能执行错误
  - ✓ 功能错误－功能过大
  - ✓ 功能错误－功能过小
  - ✓ 功能错误－功能反向
- 功能非期望激活
- 输出卡滞－输出保持不变

然后，建立**相关项的功能失效**和**整车危害**的映射关系。

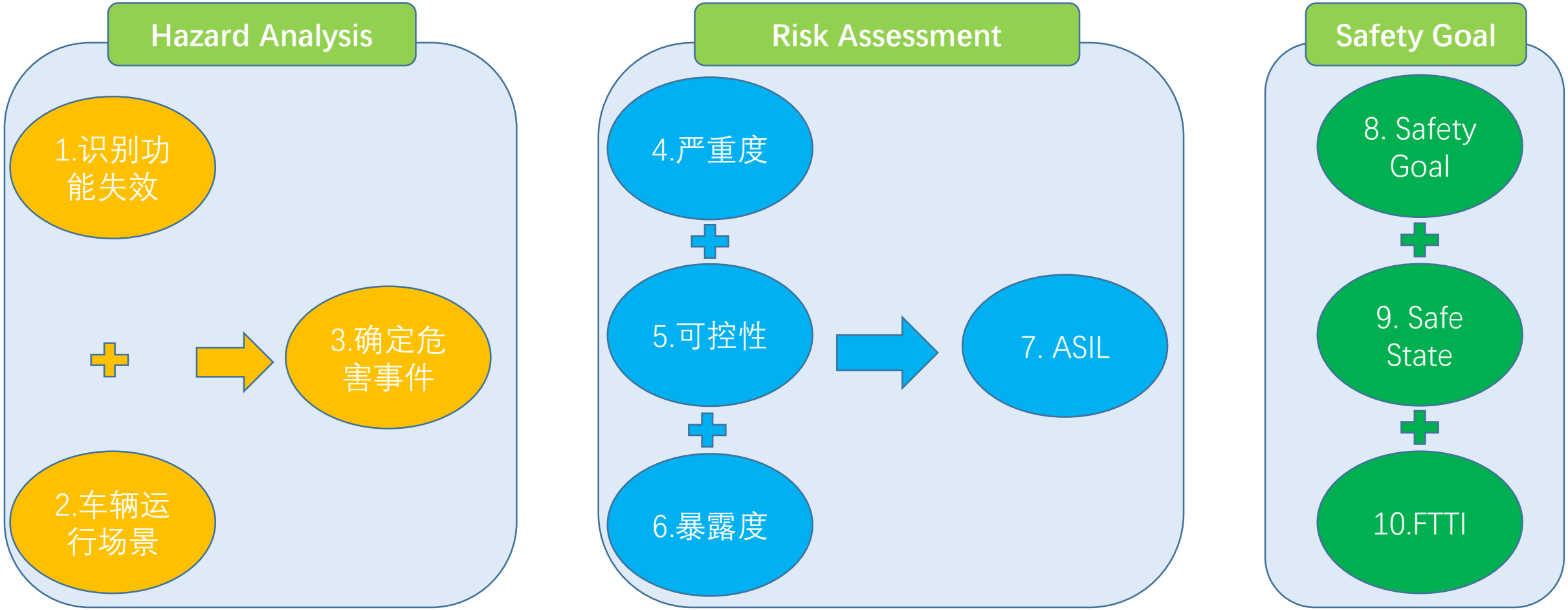
以转向助力系统(EPAS)功能为例：

表1　EPAS系统HAZOP分析

HAZOP	功能失效	整车危害
功能丢失	丢失助力转向	增加人的手动转向
功能过小	过小助力转向	
功能过大	过大助力转向	非期望的侧向运动/非期望的车辆横摆
功能反向	反向助力转向	
非期望的功能激活	非期望的助力转向激活	
输出卡滞	助力转向锁死	丢失车辆侧向运动控制

危害分析和风险评估(HARA)

- 识别系统中故障可能导致的风险，并将其分类
- 建立安全目标以避免不合理的风险

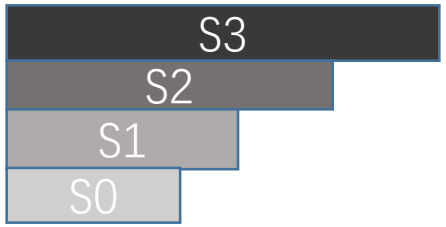


危害分析和风险评估(HARA)

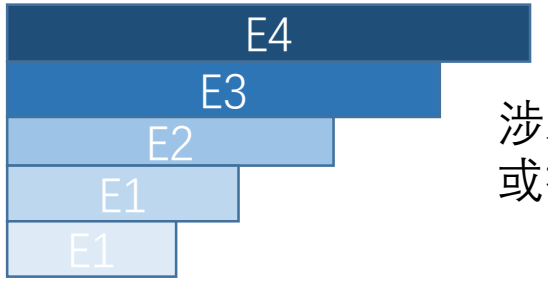
$$ASIL = f(S,E,C)$$

S: Severity
E: Exposure
C: Controllability

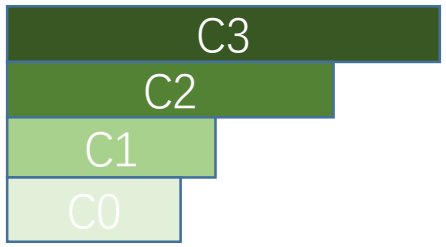
ASIL: Automotive Safety Integrity Level



对人员的物理性伤害



涉及场景的处出现频度，
或持续时间



面对潜在的危害，
相关人员的控制能力

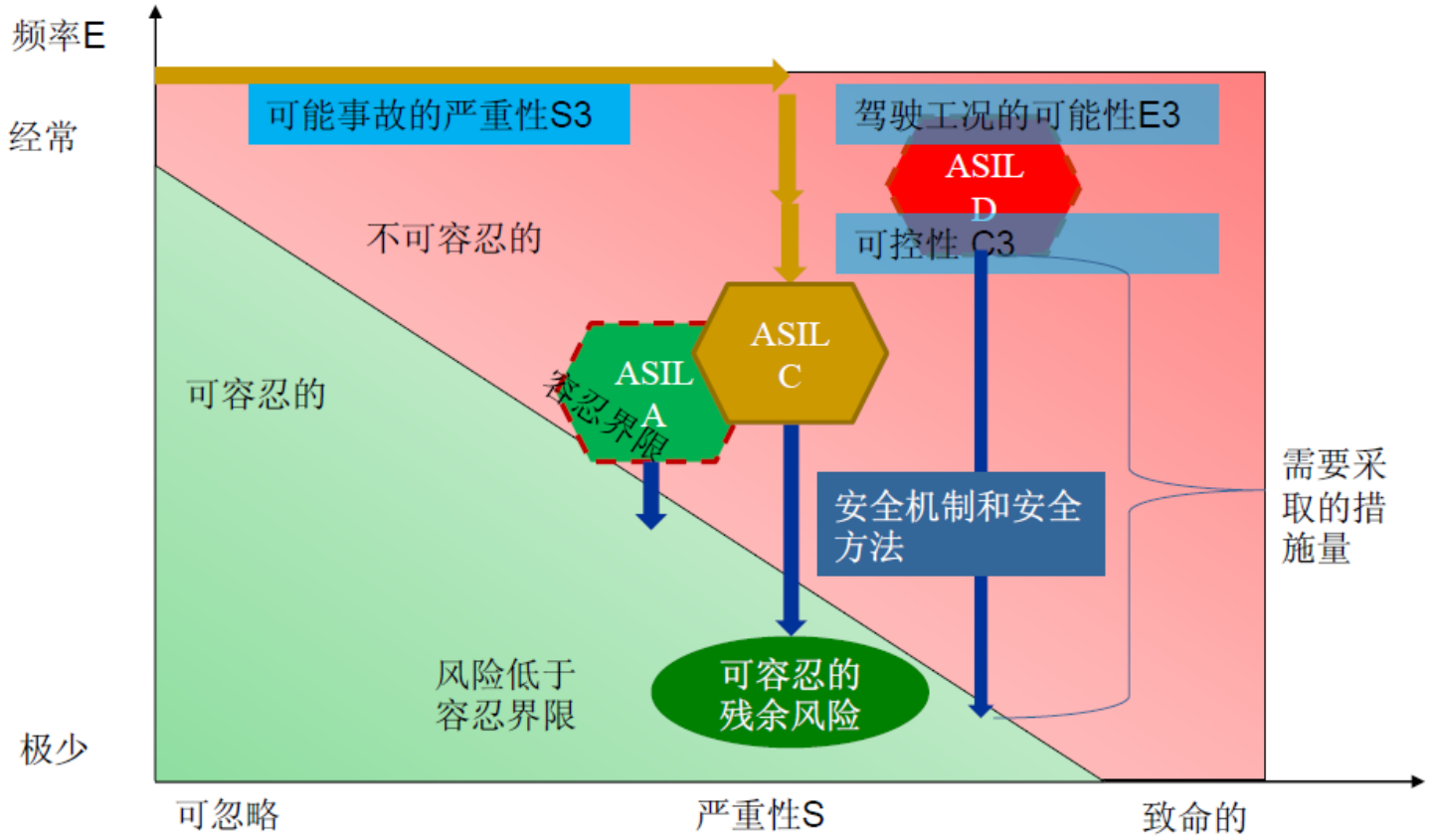
S	E	Controllability(C)		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	ASIL A	ASIL B
	E4	QM	ASIL B	ASIL C
S3	E1	QM	QM	QM
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

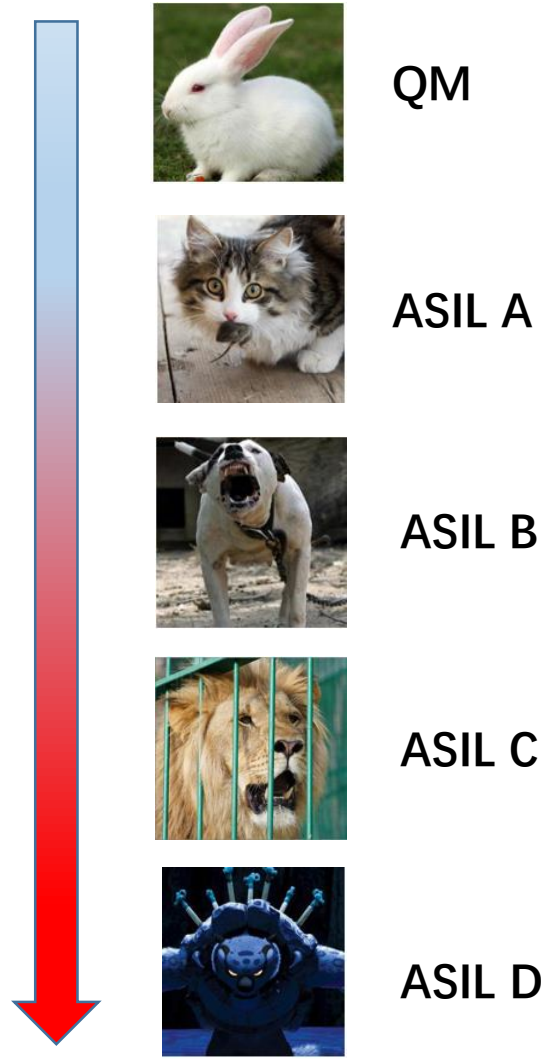
ASIL Rating 示例

Malfunction	Operational Scenario			E	C	S	ASIL
No Braking Effect	> 100 km/h	Highway	Wet road	E3	C3	S3	C
Unexpected Braking Effect	> 50 km/h < 100 km/h	Main Road	Dry road	E4	C2	S3	C
Asymmetric Braking Effect	Parking < 10 km/h	Side Road	Dry road	E4	C2	S1	A

- Exposure:
  - E3: 1-10% of average operating time
  - E4: >10% of average operation time
- Controllability (Average Driver):
  - C2: Hazardous situation is usually controllable
  - C3: Hazardous situation is usually not controllable
- Severity:
  - S1: Light to moderate injuries
  - S3: Critical injuries

ASIL及其意义


频率E
经常
极少
可能事故的严重性S3
驾驶工况的可能性E3
ASIL D
可控性 C3
不可容忍的
ASIL C
ASIL A
容忍界限
可容忍的
安全机制和安全方法
需要采取的措施量
风险低于容忍界限
可容忍的残余风险
可忽略
严重性S
致命的


风险升高
QM
ASIL A
ASIL B
ASIL C
ASIL D

功能安全目标

功能安全目标是相关项的顶层安全需求。需要由安全目标得出必需的功能安全需求，以避免危害事件的不合理的风险。

常见的控制器及所对应的安全目标如下：

表2　常见控制器安全目标及ASIL

控制器	安全目标实例	安全等级
约束系统控制器SRS	防止非期望的安全气囊开启	ASIL D
转向柱锁SCL	防止非期望的转向柱锁死	ASIL D
动态域控制器VDDM	防止非期望的制动	ASIL D
发动机控制器ECM	防止非期望加速	ASIL C
变速箱控制器TCM	防止非期望的输出轴锁死	ASIL C
电池管理系统BECM	防止电池热失效引起起火或有害气体释放	ASIL C

功能安全状态

发生故障时，**相关项**进入没有不合理风险等级的工作模式。例如：关闭输出级，跛行，故障指示，功能降级等。

常见2种安全状态属性：

- Fail Safe: Fail silent && Fail degradation
- Fail Operation:

右表以踏板传感器的安全状态定义为例：

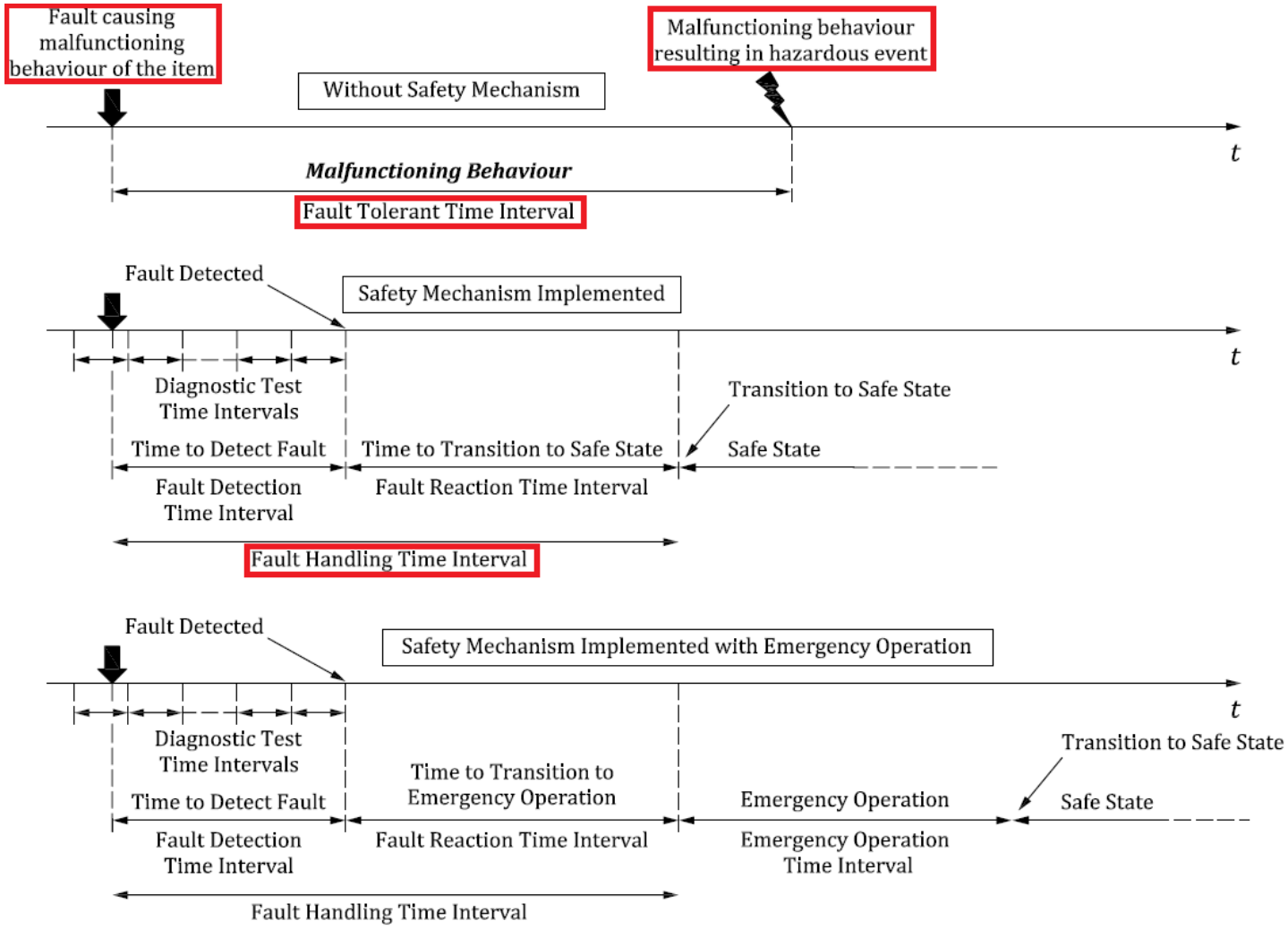
表3 踏板传感器失效的安全状态定义

What is the safe state for pedal? (Moving Stationary)	1 or 2 sensors	Shut down pedal (Fail -Silent)
	3 sensors	Use signals from remaining 2 sensors (Fail -Operational)
What are the measures to bring the pedal to the safe state? (Moving Stationary)	1 or 2 sensors	• Disable electronic to shut down pedal • Indicate fault to driver
	3 sensors	• Safety and availability: Continue operation using 2 sensors • Indicate fault to driver

FTTI

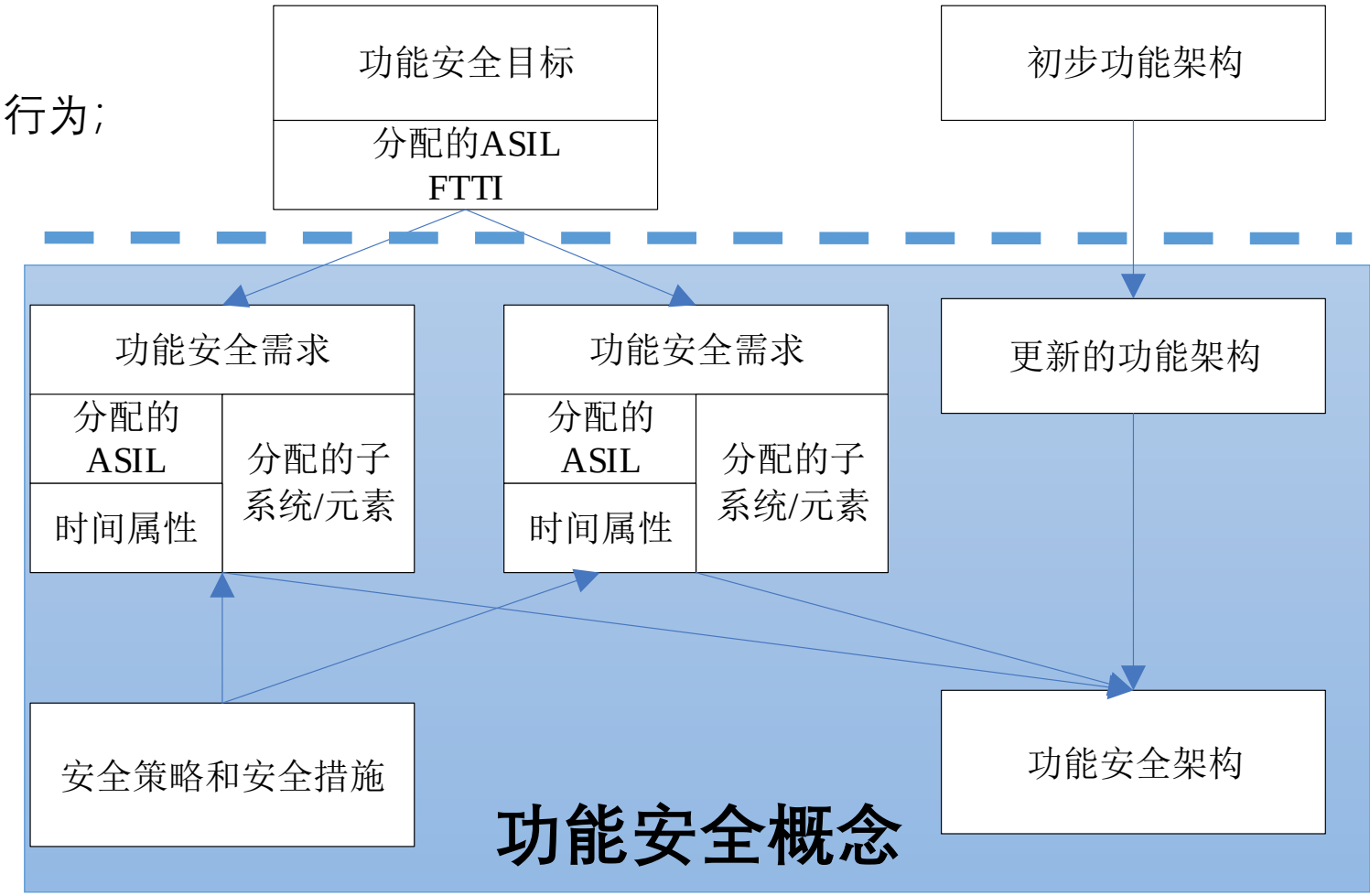
安全机制或安全措施**未工作**情况下，从**相关项故障发生**到可能的**危害事件产生**的**最小时间间隔**。

ISO26262-2018 安全时间间隔示意如图：



功能安全概念

- 由功能安全目标得出功能安全需求;
- 分配功能安全需求到基本架构元素;
- 规定安全策略或措施以容忍或减轻故障影响
- 规定相关项安全目标相关的功能或降级功能行为;
- 规定功能安全确认标准

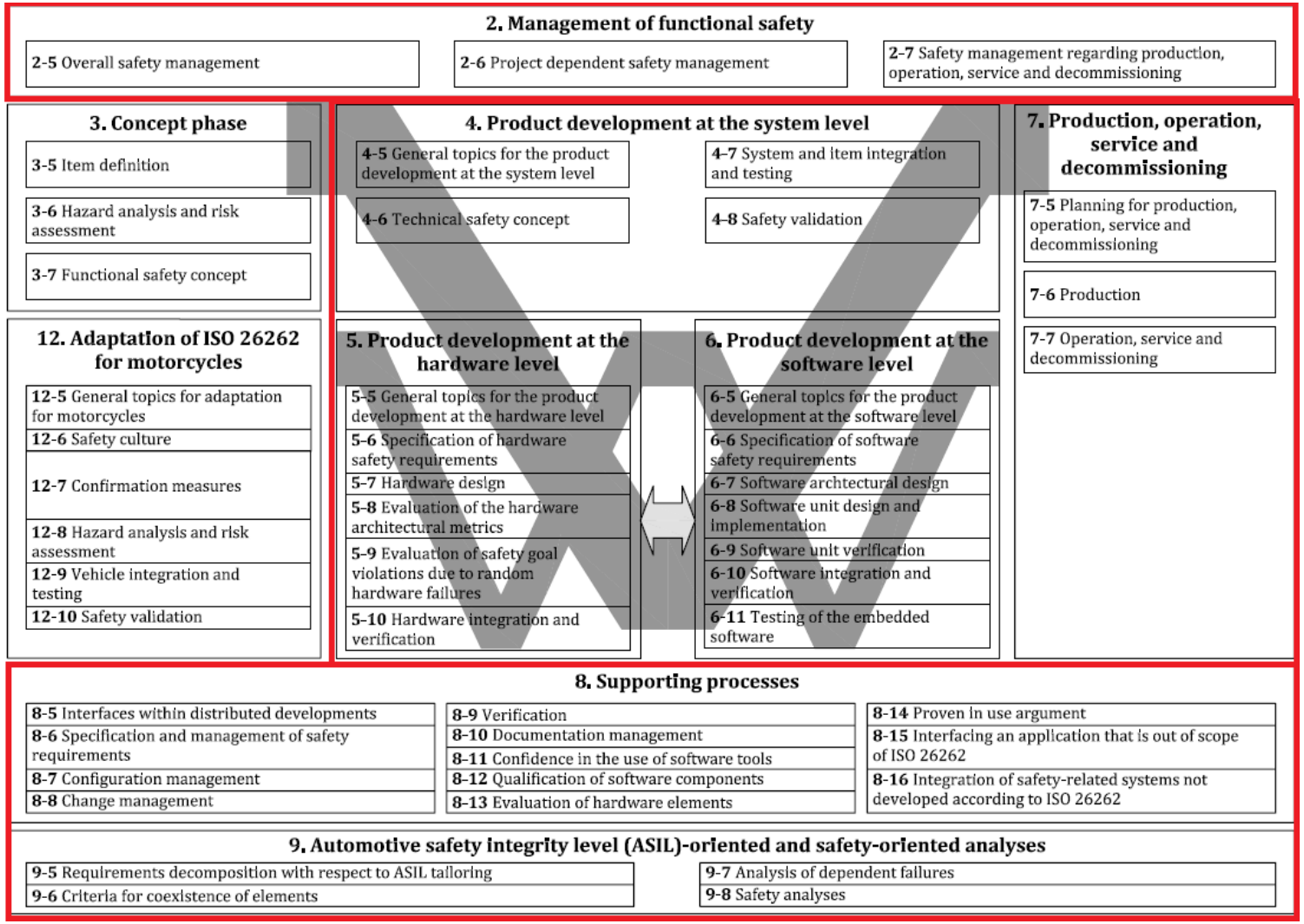


课程大纲

- 第一单元：基本概念
- 第二单元：功能安全管理
- 第三单元：概念阶段
- 第四单元：功能安全开发(ECU层级)
- 第五单元：支持流程和安全分析

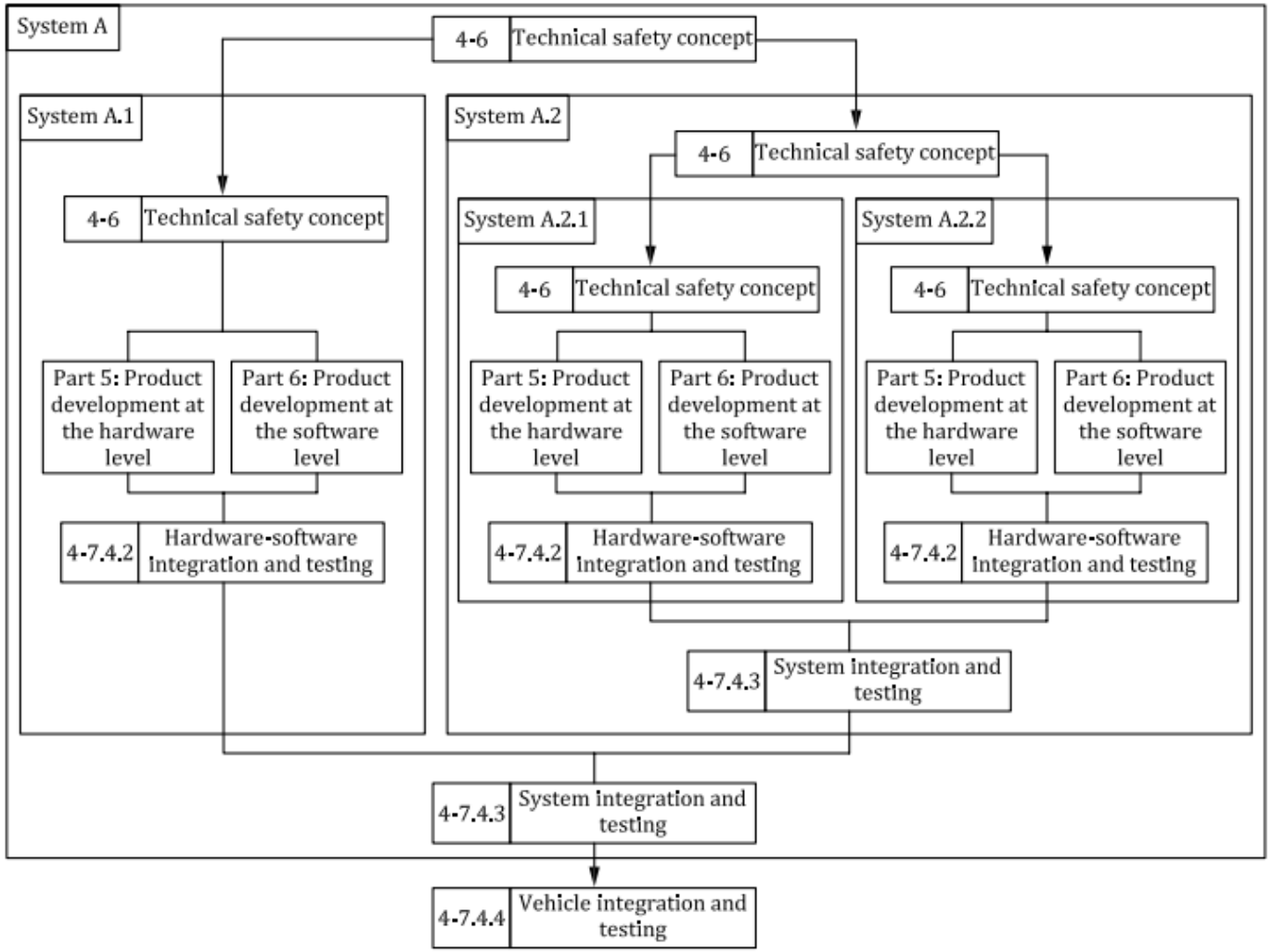
功能安全开发(ECU层级)

功能安全系统开发活动(ECU层级)



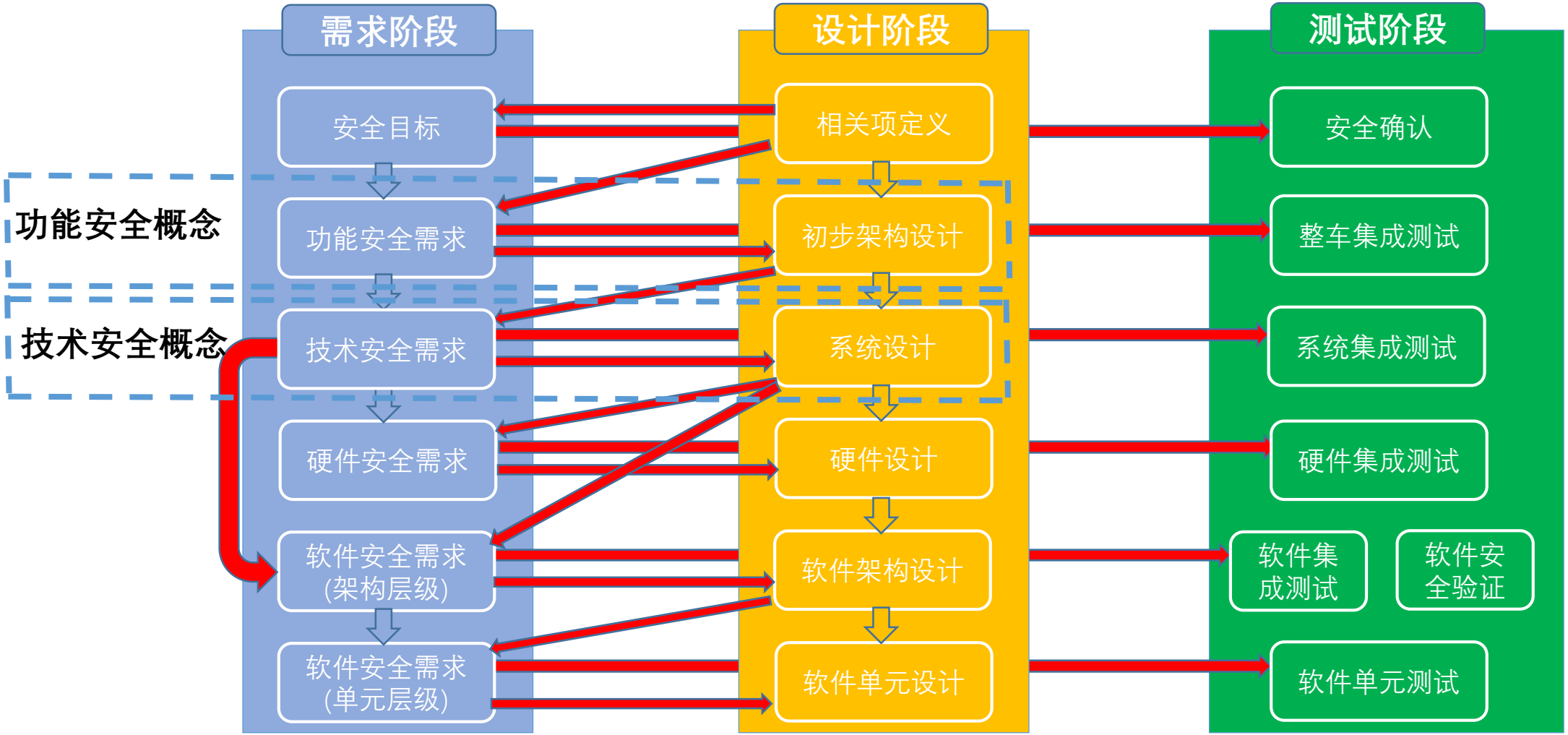
功能安全开发(ECU层级)

系统层级开发流程



功能安全开发(ECU层级)

功能安全概念到系统开发流程



技术安全概念

技术安全概念是**技术安全需求**和相应**系统架构设计**的的集合，并提供原理阐述为什么系统架构设计合适的满足概念阶段得出的功能安全需求和设计约束，主要包括以下内容：

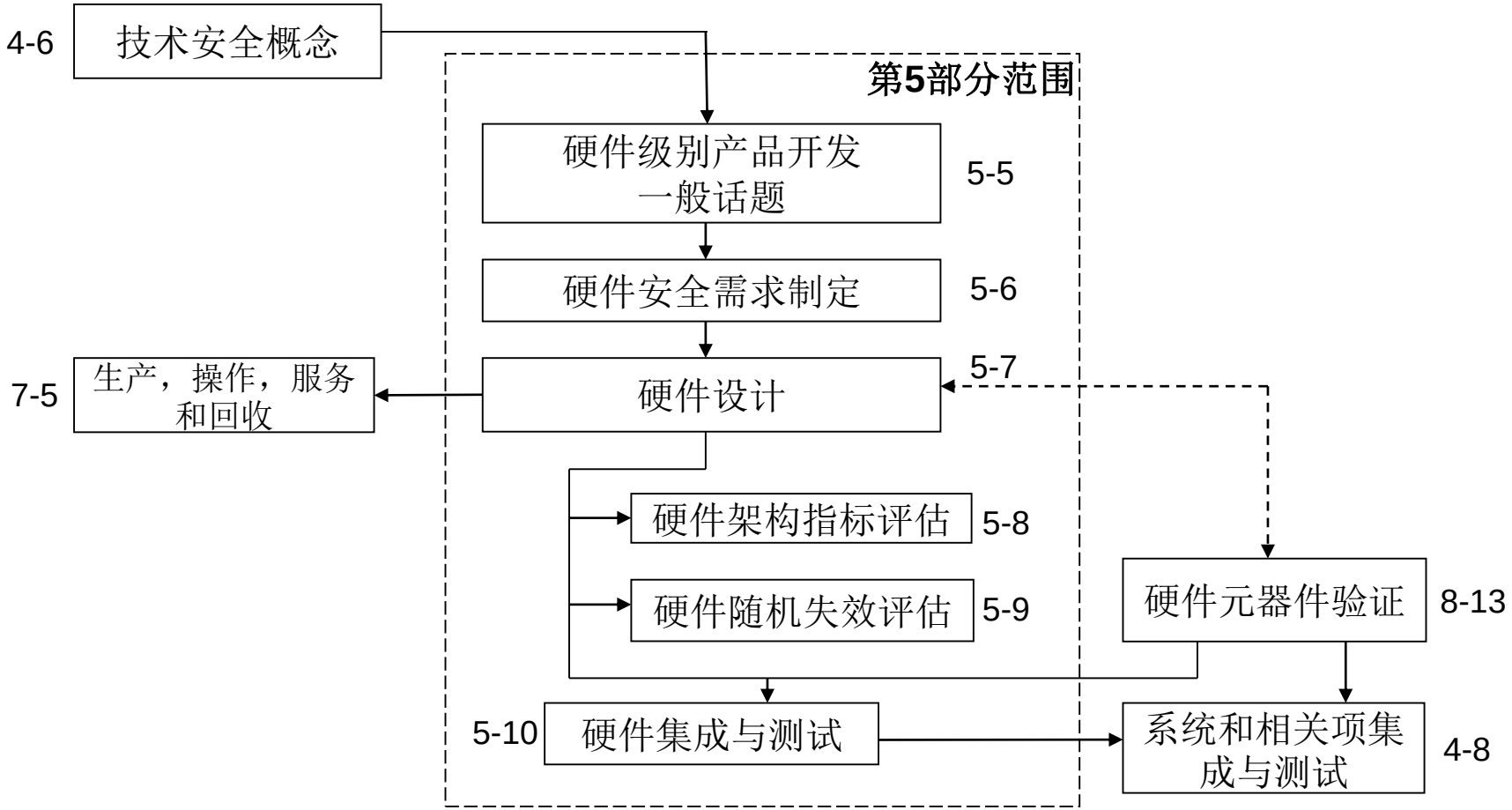
- 定义技术安全需求
- 系统架构设计
- 规定安全机制
- 系统安全分析
- 分配软件和硬件安全需求
- 软硬件接口规范定义
- 验证系统架构设计和技术安全需求

功能安全开发(ECU层级)

系统测试与验证

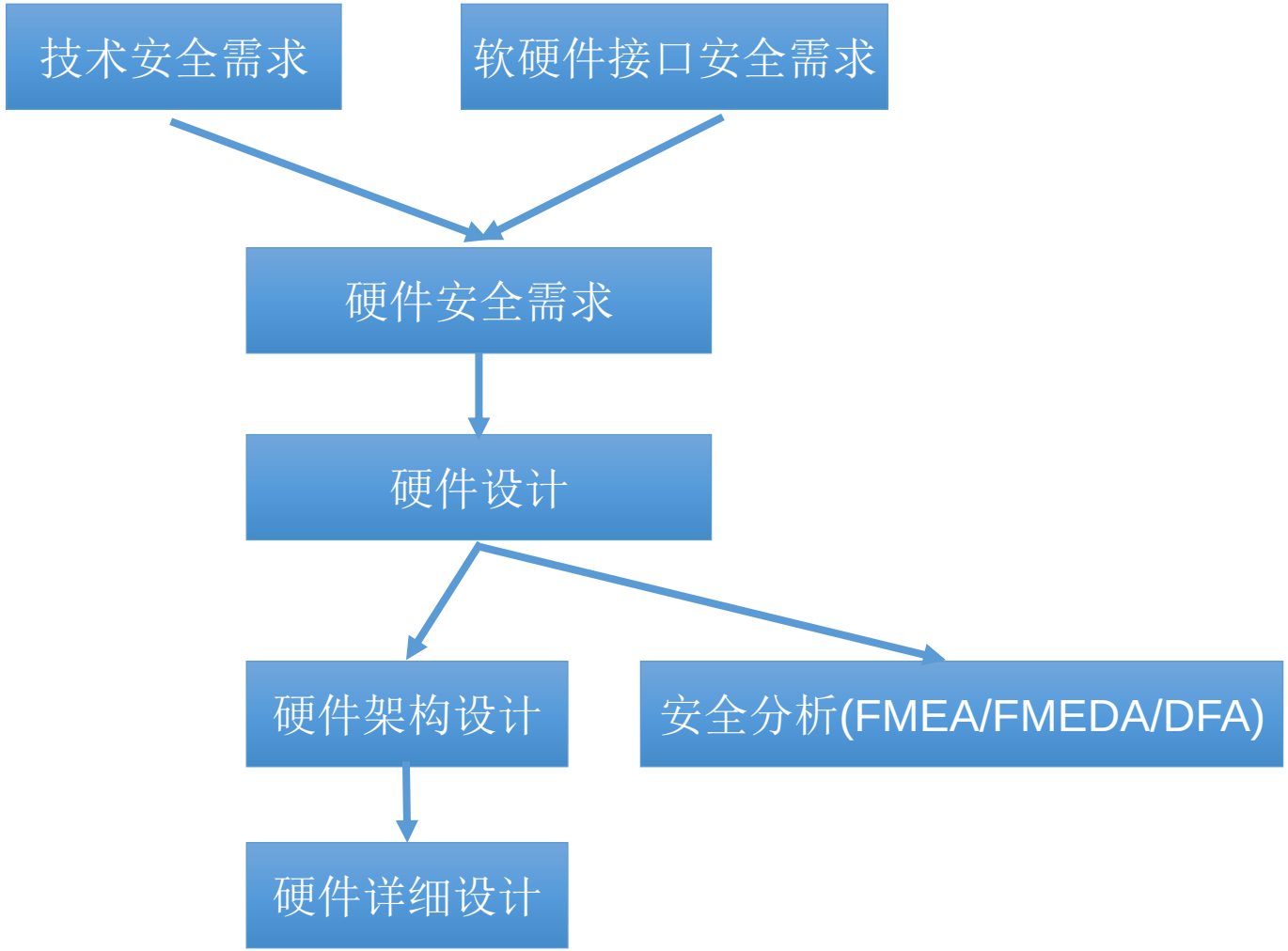
- 软硬件集成测试 → 软硬件接口(HSI)
- 系统和相关项集成测试 → 技术安全需求(TSR)
- 整车集成和测试 → 功能安全需求(FSR)
- 安全验证 → 安全目标(SG)

硬件开发流程


4-6
技术安全概念
第5部分范围
硬件级别产品开发
一般话题
5-5
硬件安全需求制定
5-6
7-5
生产，操作，服务
和回收
硬件设计
5-7
硬件架构指标评估
5-8
硬件随机失效评估
5-9
硬件元器件验证
8-13
5-10
硬件集成与测试
系统和相关项集
成与测试
4-8

功能安全开发(ECU层级)

硬件安全需求和设计



硬件失效分类

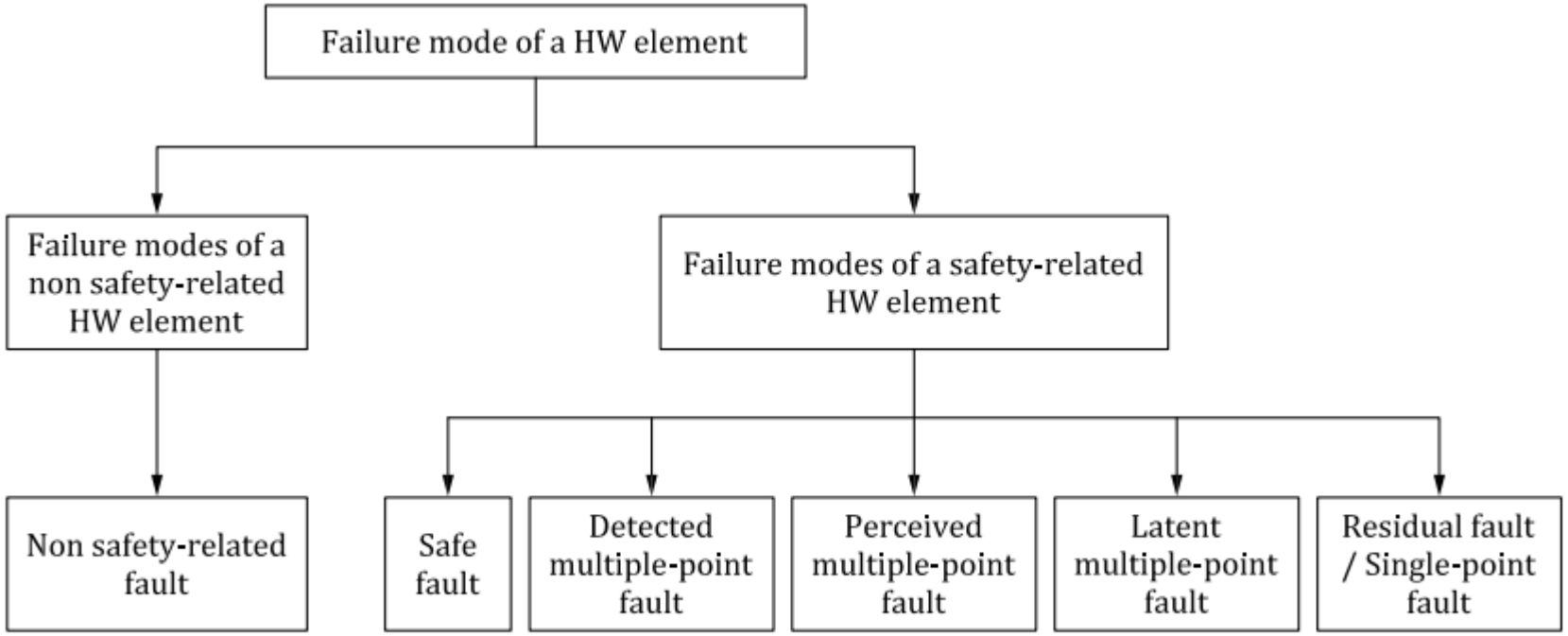


Figure B.1 — Failure mode classifications of a hardware element

硬件失效分类

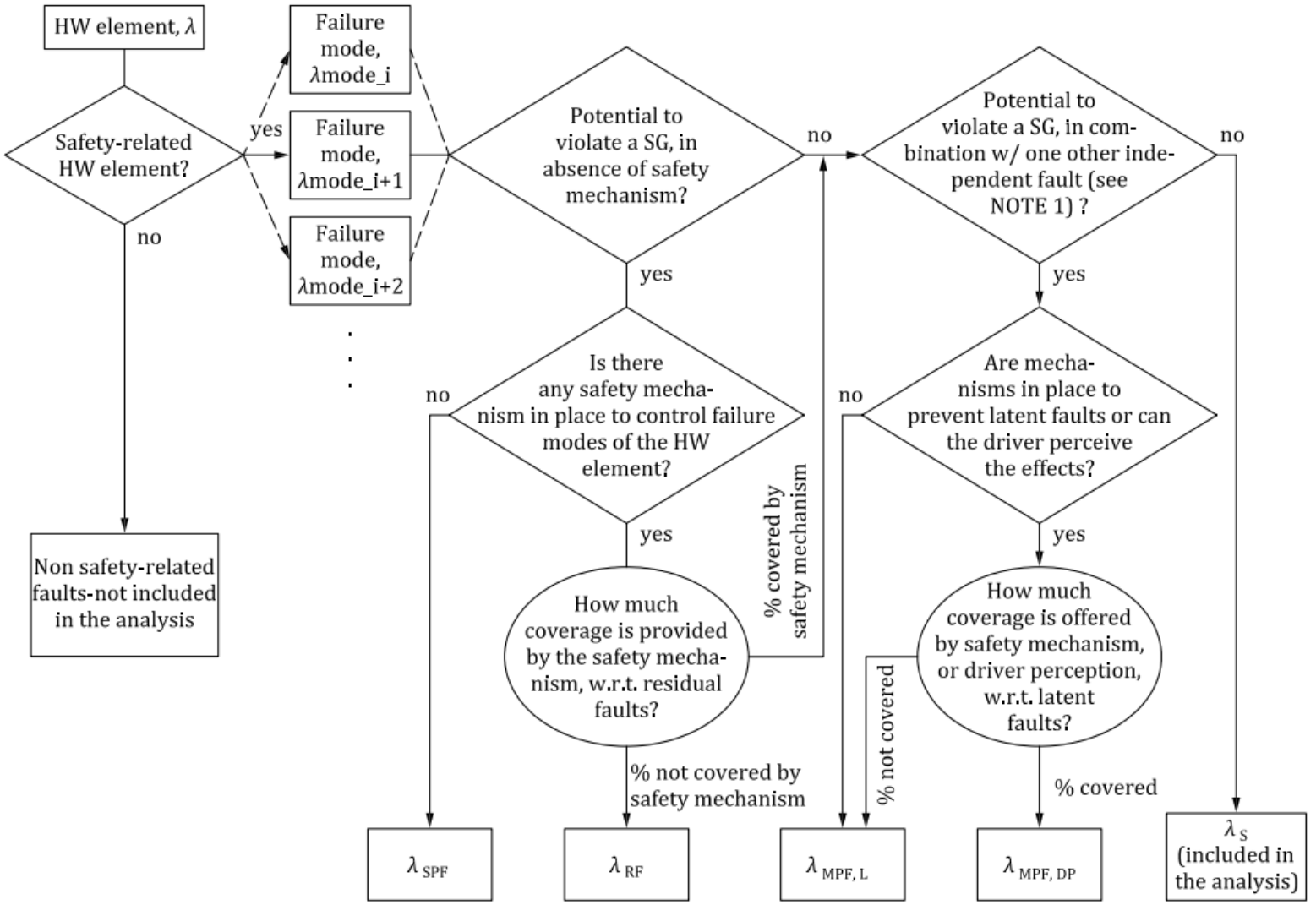


Figure B.2 — Example of flow diagram for failure mode classification

硬件架构指标

1. **硬件架构指标评估：**
   - 单点故障指标(SPFM)
   - 潜伏失效指标(LFM)

2. **随机硬件失效评估：**
   - 随机硬件失效可能指标的评估(PMHF)
   - 导致安全目标违反的每个因素评估(EEC)

表4　单点/潜伏故障指标目标值

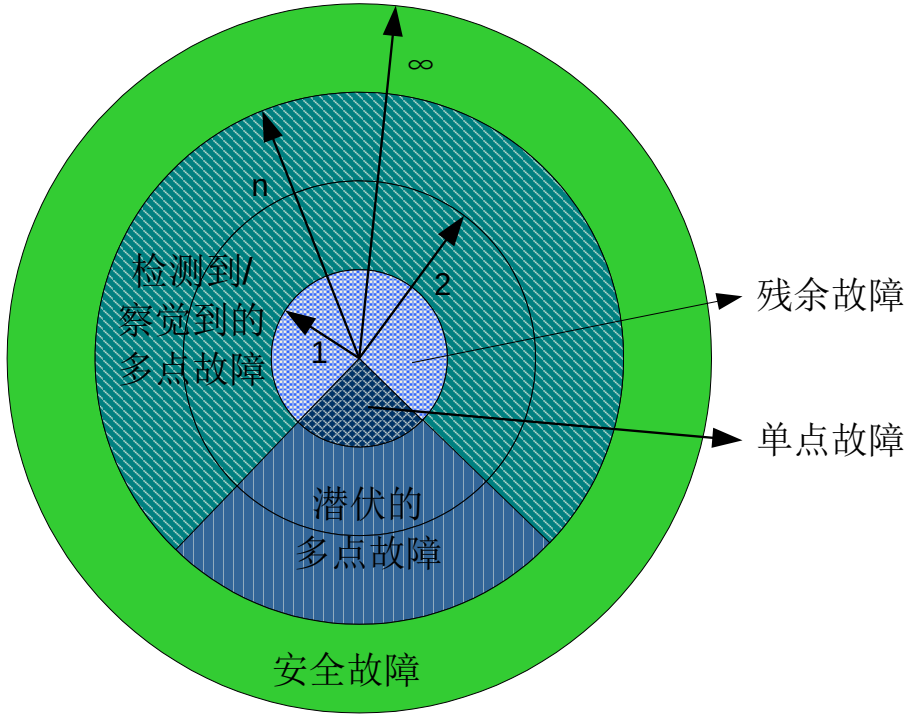
	ASIL B	ASIL C	ASIL D
单点故障指标	≥90%	≥97%	≥99%
潜伏故障指标	≥60%	≥80%	≥90%

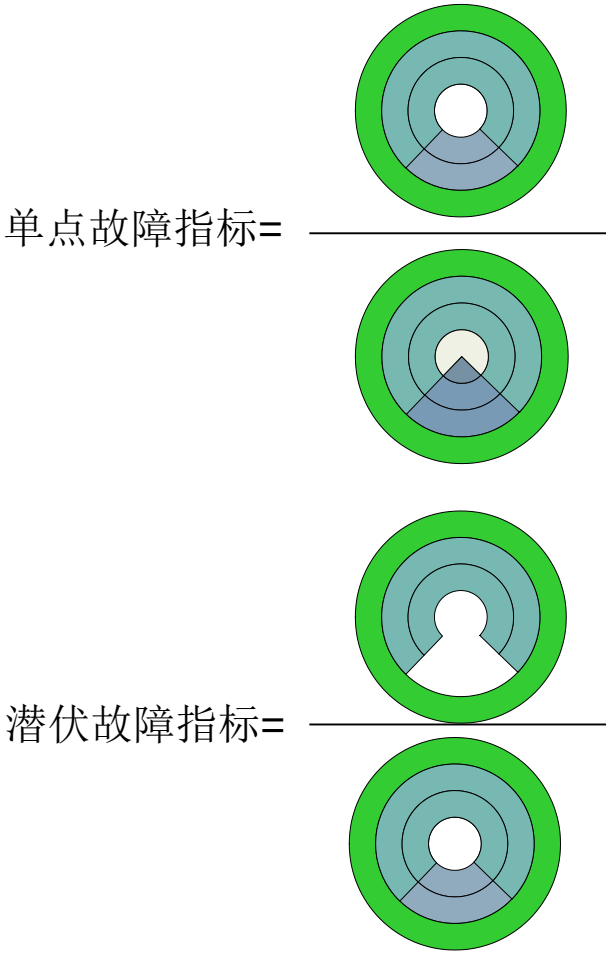
表5　随机硬件失效目标值

ASIL	随机硬件失效目标值
D	$< 10^{-8}\ h^{-1}$(10FIT)
C	$< 10^{-7}\ h^{-1}$(100FIT)
B	$< 10^{-7}\ h^{-1}$(100FIT)

Note: 1FIT = $10^{-9}\ h^{-1}$
FIT: Failure In Time

硬件架构度量





残余故障=所有故障*(1-残余故障的诊断覆盖率)

潜伏故障=所有故障*(1-潜伏故障的诊断覆盖率)

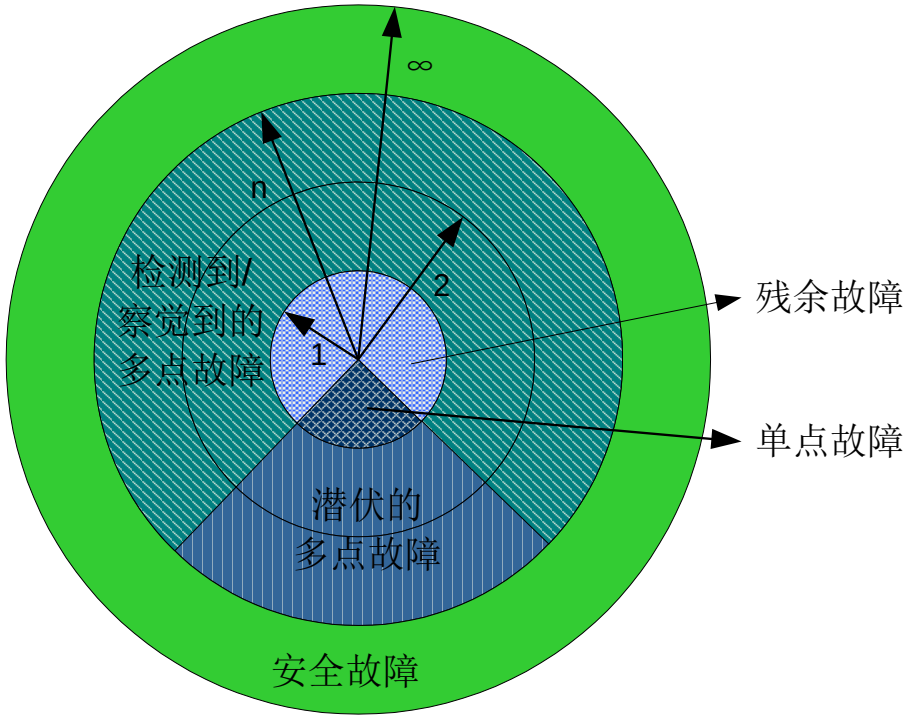
硬件随机失效度量

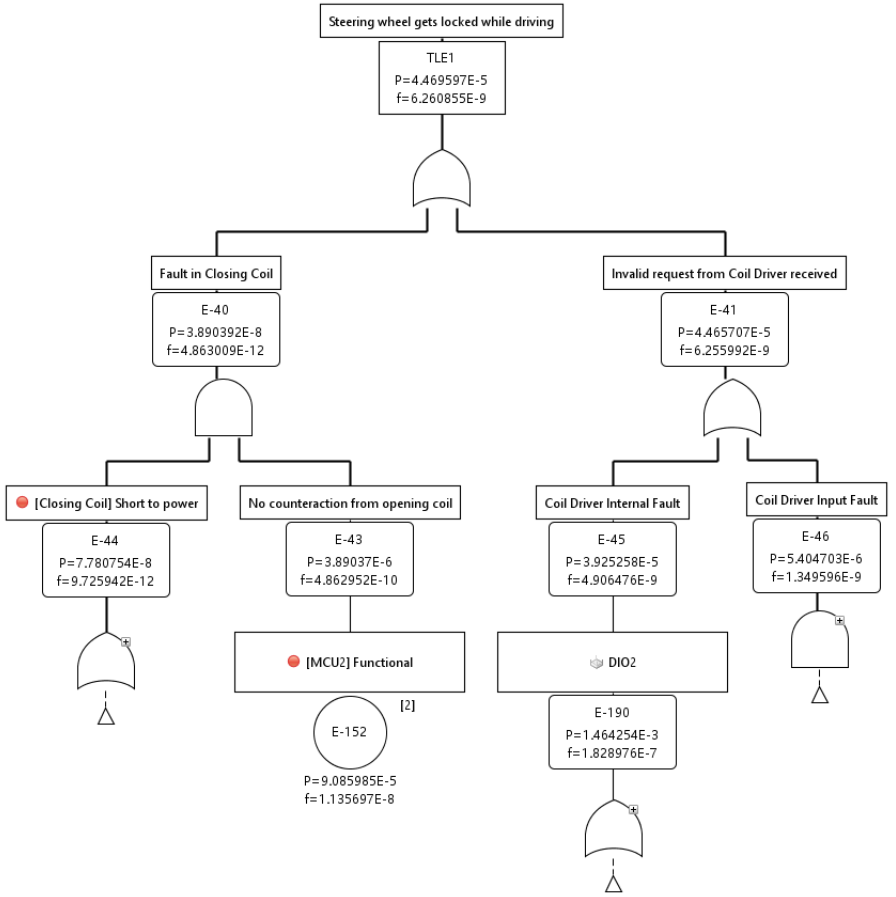
随机硬件失效可能指标 (PMHF)评估方法如下：

- **PMHF计算公式**

  PMHF = 单点故障+残余故障+ 检测到的多点故障 × 潜伏的多点故障 × 产品的生命周期

- **定量FTA**

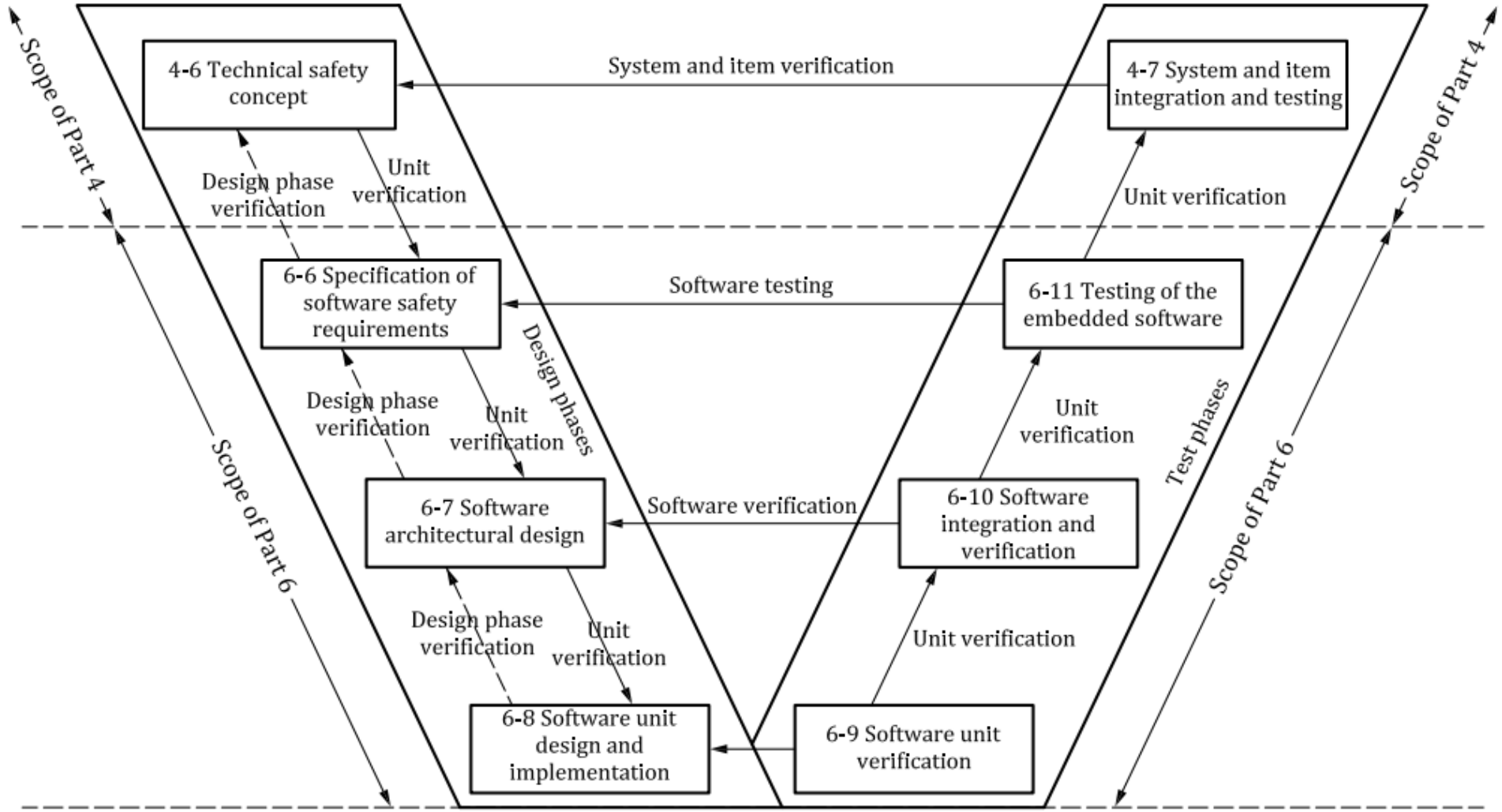




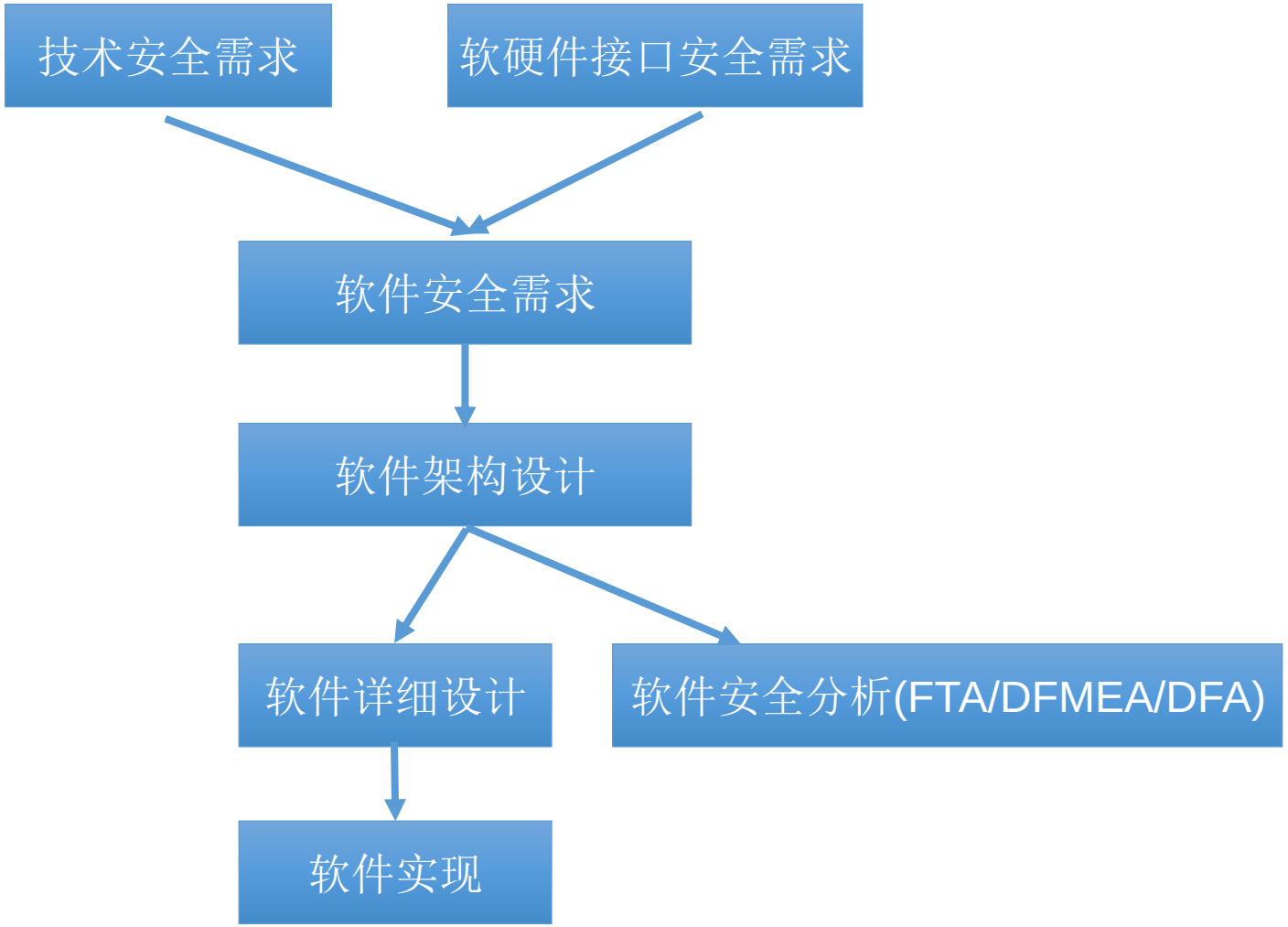
硬件验证与测试

- **集成测试案例选取**
  - ✓需求分析
  - ✓内外部接口分析
  - ✓环境条件和工况分析
  - ✓基于经验或知识的错误猜想
  - ✓重要变量分析
  - …
- **安全机制的完整性与测试**
  - ✓功能性测试
  - ✓错误注入测试(验证安全机制)
  - ✓电测试(验证电气特性）
- **设计鲁棒性和应对外部压力的测试**
  - ✓功能环境工况测试
  - ✓最坏情况测试
  - ✓加速寿命测试
  - ✓EMC和ESD测试
  - …

软件开发流程

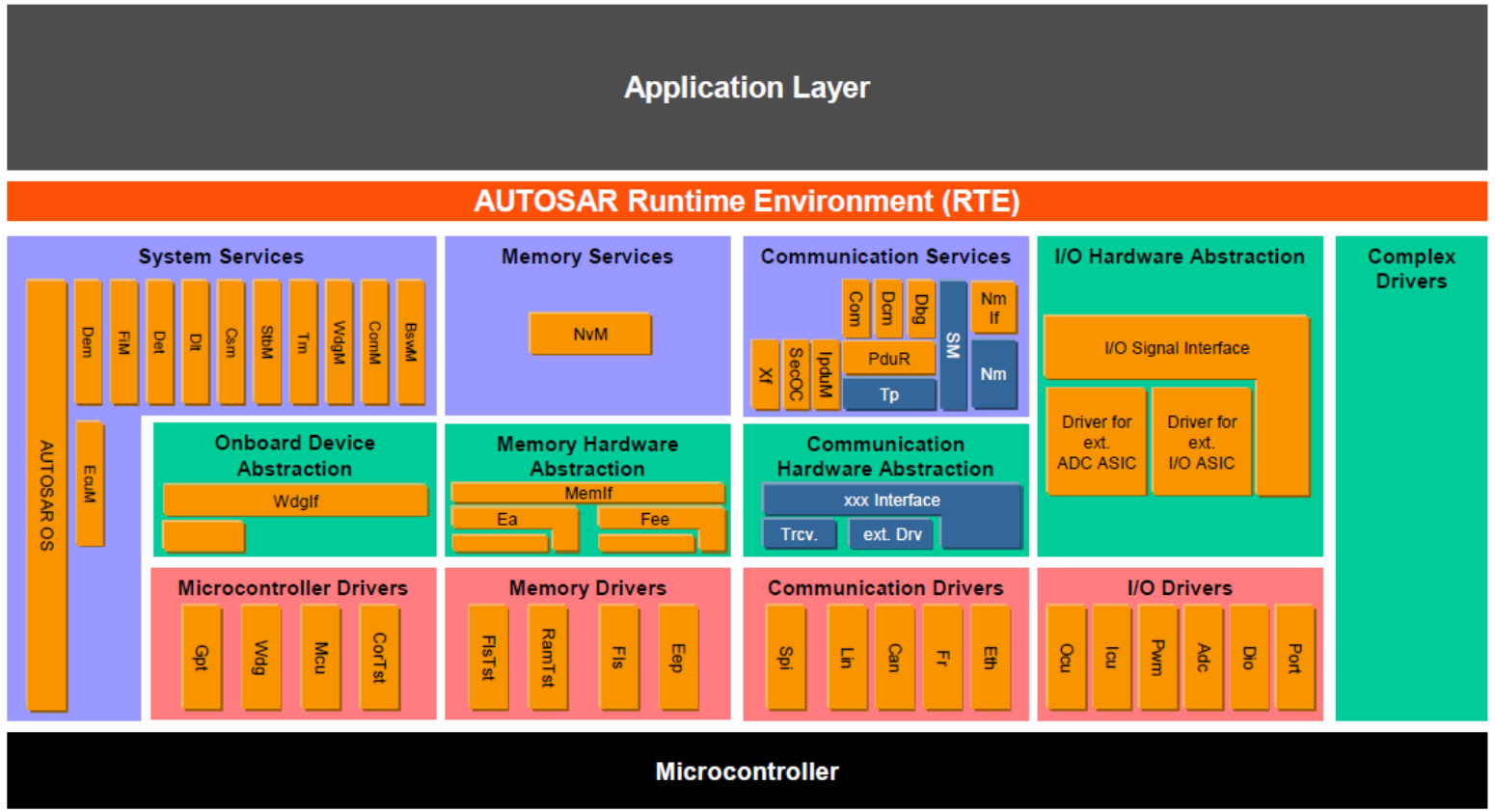

Scope of Part 4
4-6 Technical safety concept
System and item verification
4-7 System and item integration and testing
Scope of Part 4
Design phase verification
Unit verification
Unit verification
6-6 Specification of software safety requirements
Software testing
6-11 Testing of the embedded software
Design phase verification
Unit verification
Design phases
Unit verification
Test phases
Scope of Part 6
6-7 Software architectural design
Software verification
6-10 Software integration and verification
Scope of Part 6
Design phase verification
Unit verification
Unit verification
6-8 Software unit design and implementation
6-9 Software unit verification

软件安全需求和设计


技术安全需求
软硬件接口安全需求
软件安全需求
软件架构设计
软件详细设计
软件安全分析(FTA/DFMEA/DFA)
软件实现

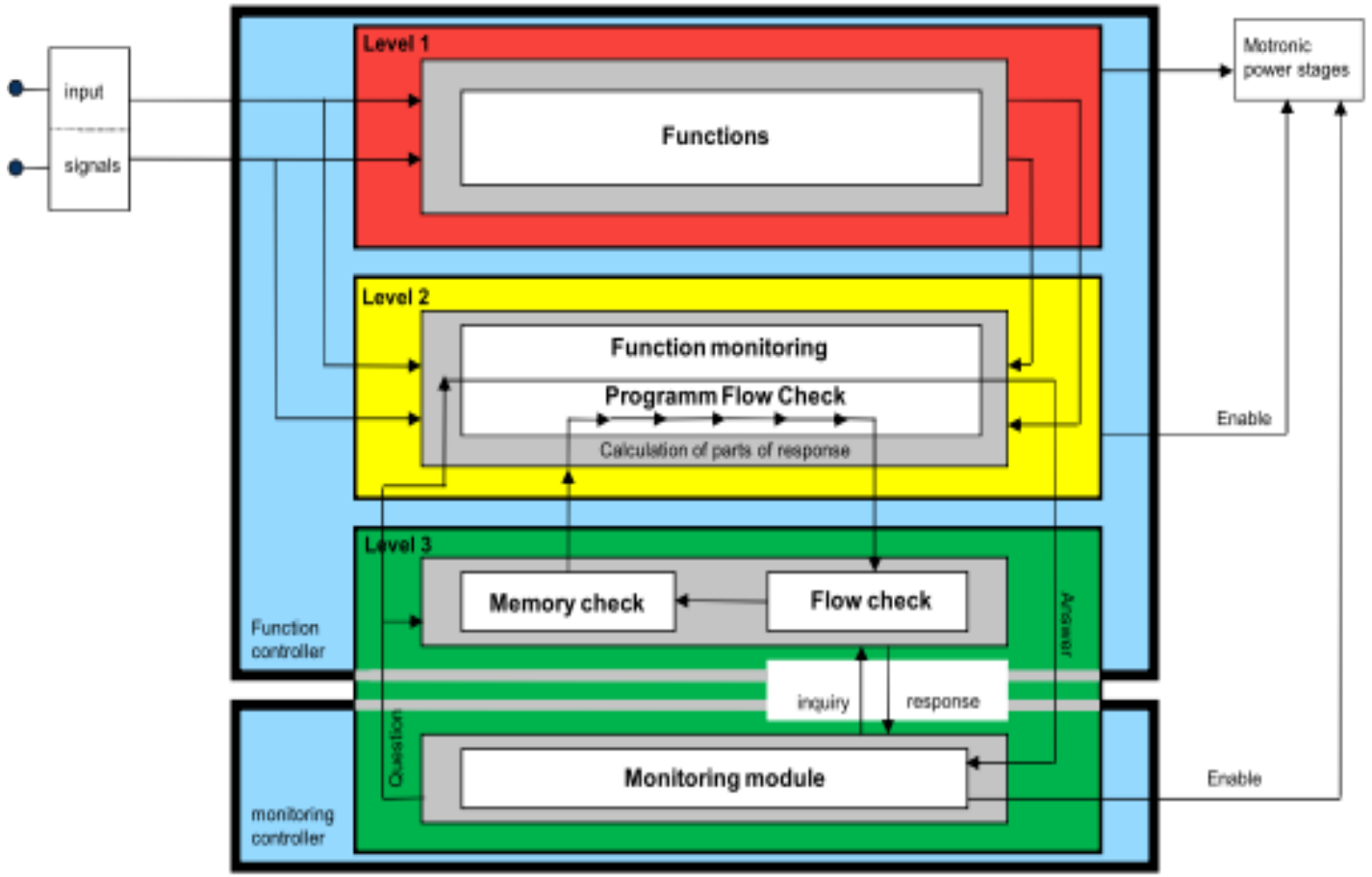
功能安全开发(ECU层级)

软件层级架构(AutoSAR)



- **MCU抽象层**：主要包括MCU内部驱动模块，可直接访问MCU内核以及外设寄存器，以及通过总线扩展的外部设备，使上层软件与MCU设备不相关。
- **ECU抽象层**：主要包括MCU外部IC设备的驱动程序模块，使上层软件不关心MCU设备或外部IC设备在ECU内的硬件分布。
- **服务层**：主要包括操作系统功能、网络通讯和管理服务、存储服务、诊断服务等。
- **RTE层**：底层软件与应用层软件之间的接口层。
- **应用层**：主要包括ECU应用功能模块。
- **复杂驱动**:主要包括与ECU应用相关的专用驱动程序，可直接访问MCU以及外部IC设备，并直接向应用层提供服务。

功能安全软件架构(E-GAS 3-Level结构)



特点：

- 硬件—双芯片架构
  - 功能芯片
  - 监控芯片
- 软件—三层结构
  - Level 1：应用功能层
  - Level 2 ：功能监控层
  - Level 3 ：控制器监控层

常见功能安全机制

表6　Level 3常用软件安全机制

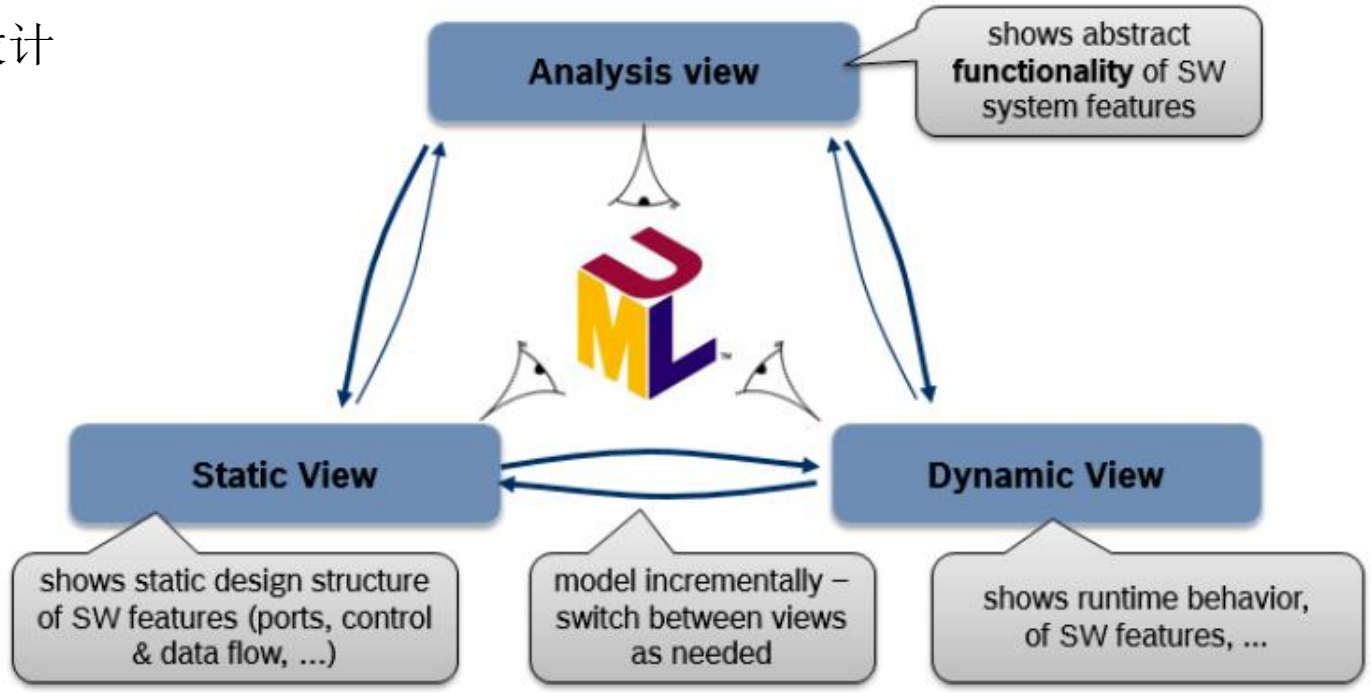
No	Defect	Safety Mechanism
1	Process/Scheduling	Program Flow Check
2	RAM defect in driving cycle	Cyclic RAM test
3	RAM override	Complement Data Storage
4	ROM defect in driving cycle	Cyclic ROM test
5	ADC defect	ADC Monitoring
6	MM defect	MM Monitoring
7	Runtime problem	MM Monitoring
8	Instruction failure	Instruction Test
9	Register failure	Instruction Test
10	SOP defect	SOP test
11	GPTO defect	GPTO test
12	Stack Failure	Stack over/under flow monitor
13	RAM defect	Complete RAM Test
14	ROM defect	Complete ROM Test

软件单元设计和实现

软件单元设计规范包含如下内容：

- 软件单元设计要满足相应的软件安全需求
- 软件单元设计应与软件架构设计规范和软硬件接口规范一致
- 软件单元设计应避免系统性故障
- 软件单元规范应描述单元功能行为，内部设计
- 软件单元设计和代码实现应遵顼原则：
  - ✓ 接口一致性
  - ✓ 正确的数据流和控制流
  - ✓ 简单，可读，易于理解
  - ✓ 鲁棒性
  - ✓ 可验证性

UML软件单元设计如右图所示：



软件验证与测试

➢ 单元验证和测试

✓Walk-through/Inspection
✓静态代码分析
✓数据流和控制流分析
✓故障注入测试
…

✓需求测试
✓等价类测试
✓边界值测试
✓基于经验或知识的错误猜想测试

✓分支覆盖度测试
✓MC/DC覆盖度测试

➢ 软件集成验证和测试

✓需求测试
✓接口测试
✓故障注入测试
✓数据流和控制流验证
…

✓等价类测试
✓边界值测试
✓基于经验或知识的错误猜想测试
✓资源评估

✓功能覆盖度评估
✓函数调用覆盖度评估

…

➢ 嵌入式软件测试

✓HIL测试
✓整车测试

✓需求测试
✓故障注入测试

✓等价类测试
✓边界值测试
✓基于经验或知识的错误猜想测试
…

生产/操作/服务/报废流程

- 制定生产/操作/服务/报废计划时应考虑安全相关的特性，相关失效对功能安全的影响，以及识别安全需求并反馈给开发人员；
- 生产流程/设备/工具的能力应满足安全相关特殊特性，若造成安全特性偏离，应识别相应的失效，及其对功能安全的潜在影响，并采取合适的措施避免或降低影响
- 针对潜在的安全相关事件，定义现场监控流程，以提供并分析现场数据以检测存在的安全功能问题，并触发响应(如事件上报，决策流程，抑制和纠正措施等)

课程大纲

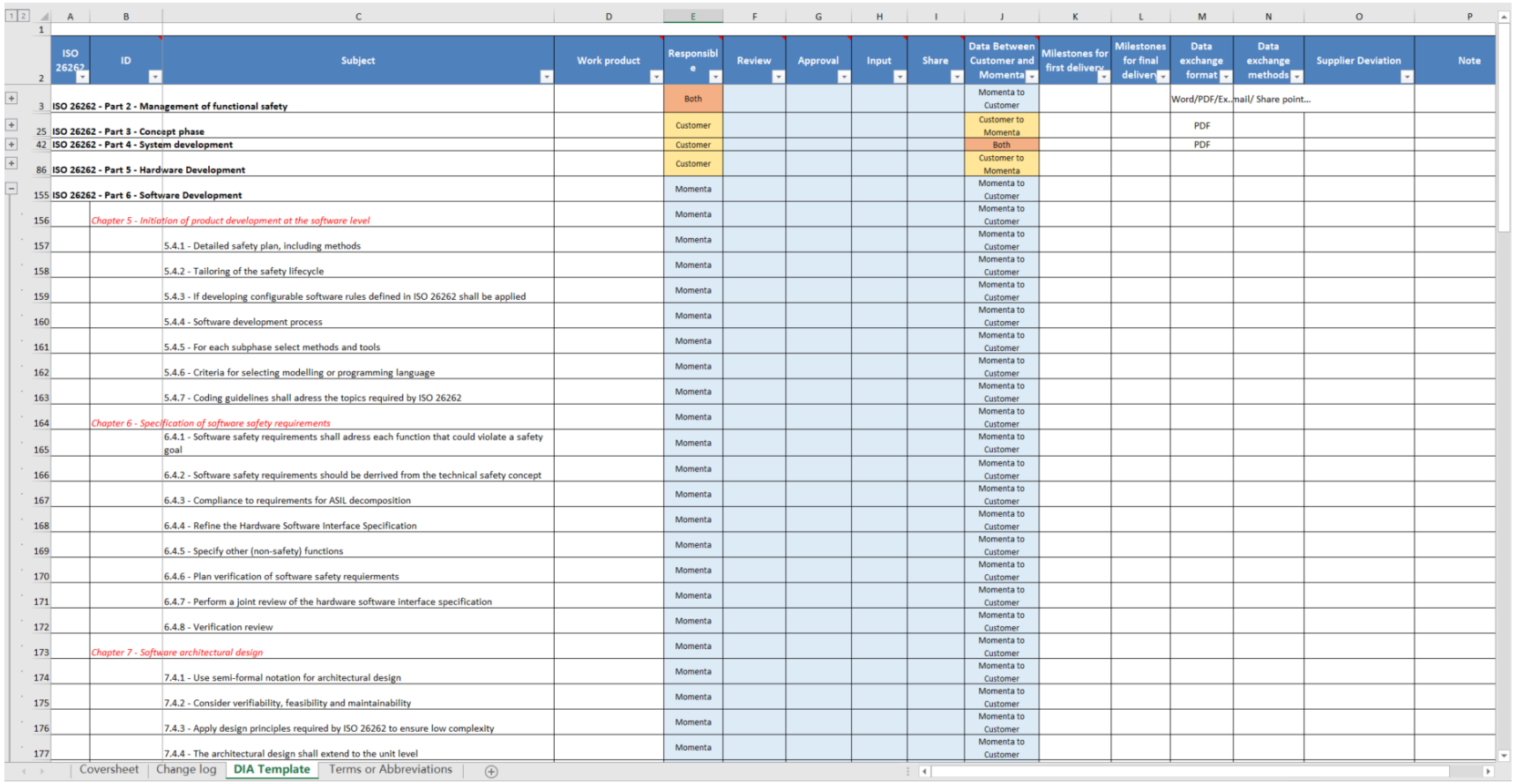
- 第一单元：基本概念
- 第二单元：功能安全管理
- 第三单元：概念阶段
- 第四单元：功能安全开发(ECU层级)
- 第五单元：支持流程和安全分析

支持流程

- 开发接口协议DIA
- 安全需求管理
- 配置管理
- 变更管理
- 验证流程
- 文档管理
- 软件工具置信度
- 软件组件证明
- 硬件元素评估
- 在用证明
- 与非ISO26262的应用接口
- 集成非ISO26262流程开发的安全相关系统

开发接口协议

明确客户和供应商的功能安全开发活动范围和相关职责

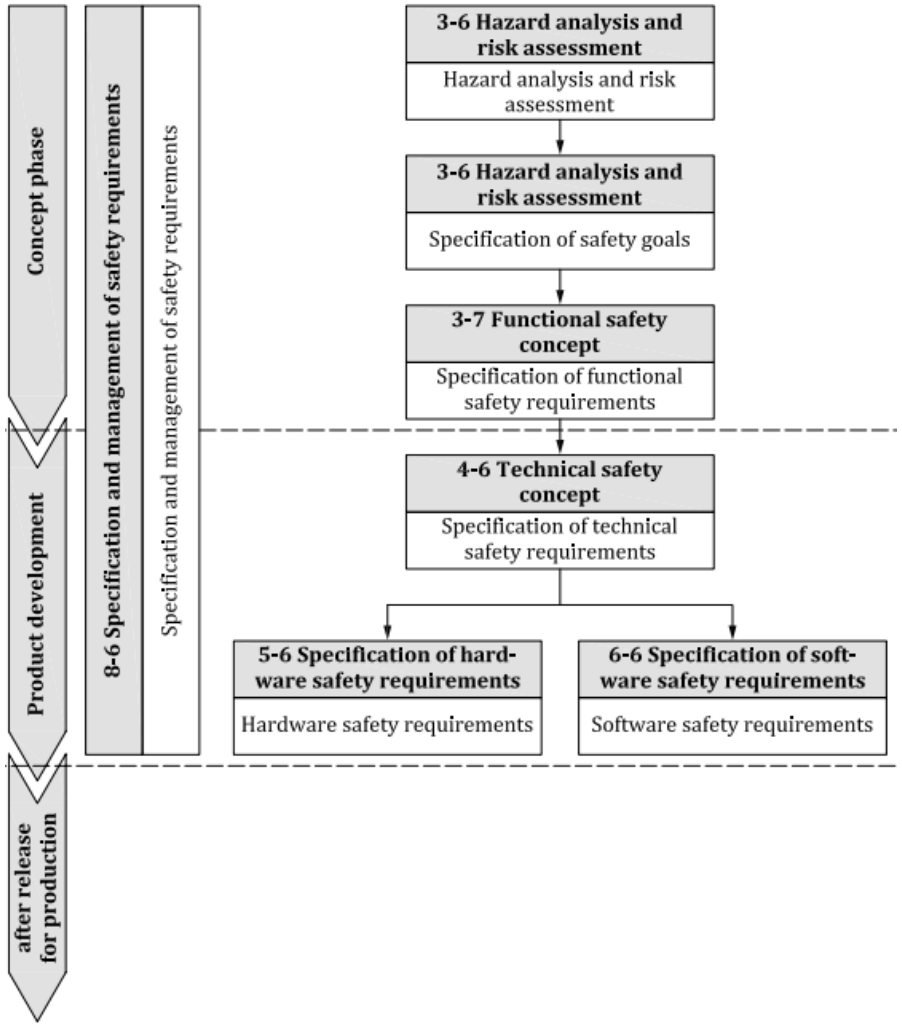


	ISO 26262	ID	Subject	Work product	Responsible	Review	Approval	Input	Share	Data Between Customer and Momenta	Milestones for first delivery	Milestones for final delivery	Data exchange format	Data exchange methods	Supplier Deviation	Note
3	ISO 26262 - Part 2 - Management of functional safety				Both					Momenta to Customer			Word/PDF/Ex...	mail/ Share point...		
25	ISO 26262 - Part 3 - Concept phase				Customer					Customer to Momenta			PDF			
42	ISO 26262 - Part 4 - System development				Customer					Both			PDF			
86	ISO 26262 - Part 5 - Hardware Development				Customer					Customer to Momenta						
155	ISO 26262 - Part 6 - Software Development				Momenta					Momenta to Customer						
156		Chapter 5 - Initiation of product development at the software level			Momenta					Momenta to Customer						
157			5.4.1 - Detailed safety plan, including methods		Momenta					Momenta to Customer						
158			5.4.2 - Tailoring of the safety lifecycle		Momenta					Momenta to Customer						
159			5.4.3 - If developing configurable software rules defined in ISO 26262 shall be applied		Momenta					Momenta to Customer						
160			5.4.4 - Software development process		Momenta					Momenta to Customer						
161			5.4.5 - For each subphase select methods and tools		Momenta					Momenta to Customer						
162			5.4.6 - Criteria for selecting modelling or programming language		Momenta					Momenta to Customer						
163			5.4.7 - Coding guidelines shall adress the topics required by ISO 26262		Momenta					Momenta to Customer						
164		Chapter 6 - Specification of software safety requirements			Momenta					Momenta to Customer						
165			6.4.1 - Software safety requirements shall adress each function that could violate a safety goal		Momenta					Momenta to Customer						
166			6.4.2 - Software safety requirements should be derrived from the technical safety concept		Momenta					Momenta to Customer						
167			6.4.3 - Compliance to requirements for ASIL decomposition		Momenta					Momenta to Customer						
168			6.4.4 - Refine the Hardware Software Interface Specification		Momenta					Momenta to Customer						
169			6.4.5 - Specify other (non-safety) functions		Momenta					Momenta to Customer						
170			6.4.6 - Plan verification of software safety requierments		Momenta					Momenta to Customer						
171			6.4.7 - Perform a joint review of the hardware software interface specification		Momenta					Momenta to Customer						
172			6.4.8 - Verification review		Momenta					Momenta to Customer						
173		Chapter 7 - Software architectural design			Momenta					Momenta to Customer						
174			7.4.1 - Use semi-formal notation for architectural design		Momenta					Momenta to Customer						
175			7.4.2 - Consider verifiability, feasibility and maintainability		Momenta					Momenta to Customer						
176			7.4.3 - Apply design principles required by ISO 26262 to ensure low complexity		Momenta					Momenta to Customer						
177			7.4.4 - The architectural design shall extend to the unit level		Momenta					Momenta to Customer						

Coversheet | Change log | DIA Template | Terms or Abbreviations

安全需求管理

- 保证安全需求及其属性/特性的正确规范
- 保证全生命周期安全需求的一致管理，以及需求的追溯性



配置管理

目标:

- 确保工作产物及其生成条件能独一地识别，并可控制再现
- 确保当前和早期版本的关系和差异能被追溯

要求:

制定配置管理计划;

配置管理流程应符合质量管理系统和软件开发的相关要求；

安全计划要求的工作产物及需要在线的元素应放在配置管理下，并打基线；

配置管理策略应定义需独一识别的工作产物的条件和目的；

配置管理应在全安全生命周期内维护；

变更管理

目标：分析和控制安全相关工作产物的变更

要求：

制定变更管理流程和计划;

定义变更请求规范和格式

变更请求分析和评估；

执行变更请求并归档

验证流程

验证活动用以保证工作产物符合相应的需求，涉及概念阶段，产品开发阶段(设计/测试)和生产/操作阶段。

常用验证方法： Review，Analysis， Simulation和Test

要求:

制定验证计划;

编写相应验证规范

执行验证并评估验证结果

文档管理

定义全生命周期的文档管理策略，以促进有效和可重复的文档管理流程

要求:

制定文档管理计划;

定义文档管理Guideline, 如整体文档结构和文档格式等

软件工具置信度

软件工具置信度评估：

用于系统/软件/硬件开发的软件工具需要对其置信度(TCL)进行评估，以避免软件工具失效导致的错误输出影响安全相关元素(TI)，同时评估对上述错误的预防和检测能力(TD)；

Table 3 — Determination of the Tool Confidence Level (TCL)

		Tool error detection		
		TD1	TD2	TD3
Tool impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

软件工具质量：

针对TCL不为TCL1的软件工具，根据不同ASIL等级要求，需要采用合适的质量评估方法，以证明软件工具用于功能安全开发活动是合适的。

Table 4 — Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard[a]	+	+	++	++

Table 5 — Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance with a safety standard[a]	+	+	+	+

ASIL分解

目的:

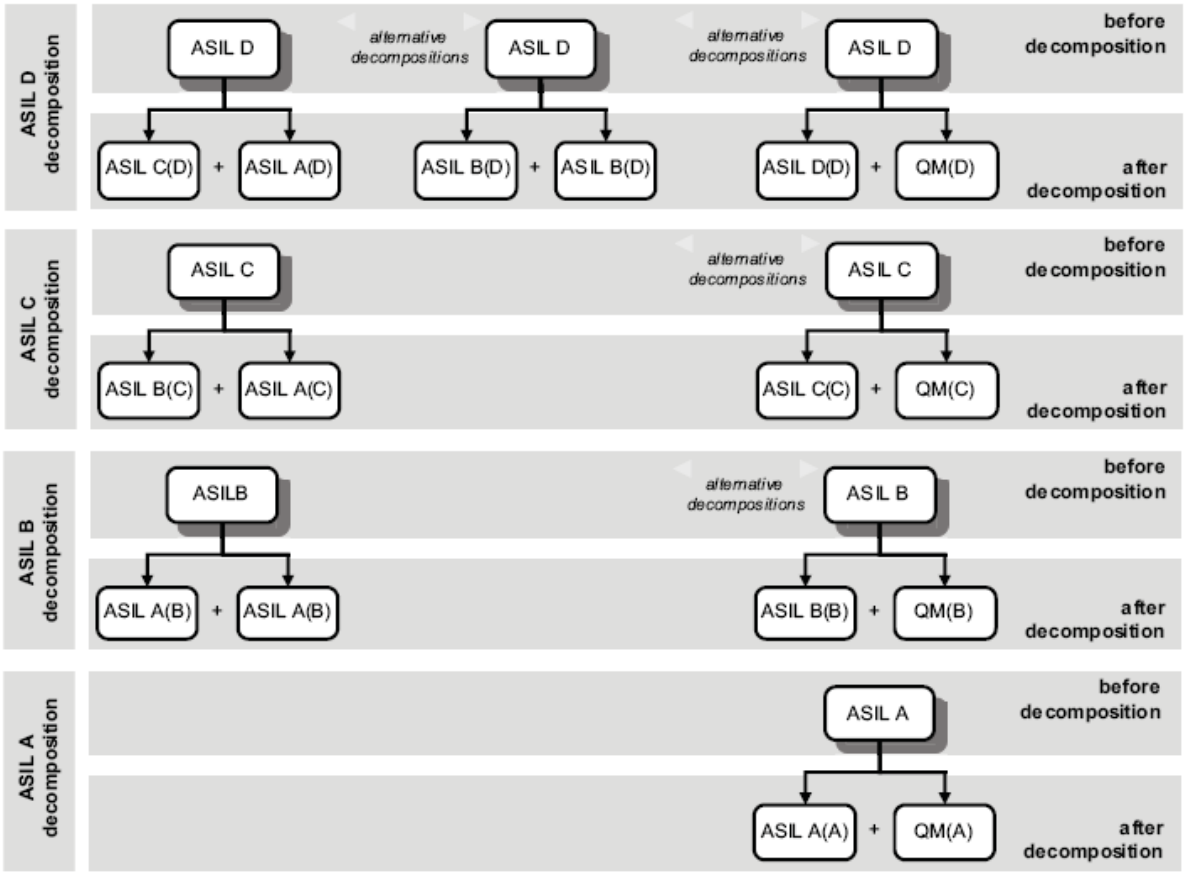
- 结构优化
- 安全功能组合
- 降低开发负荷

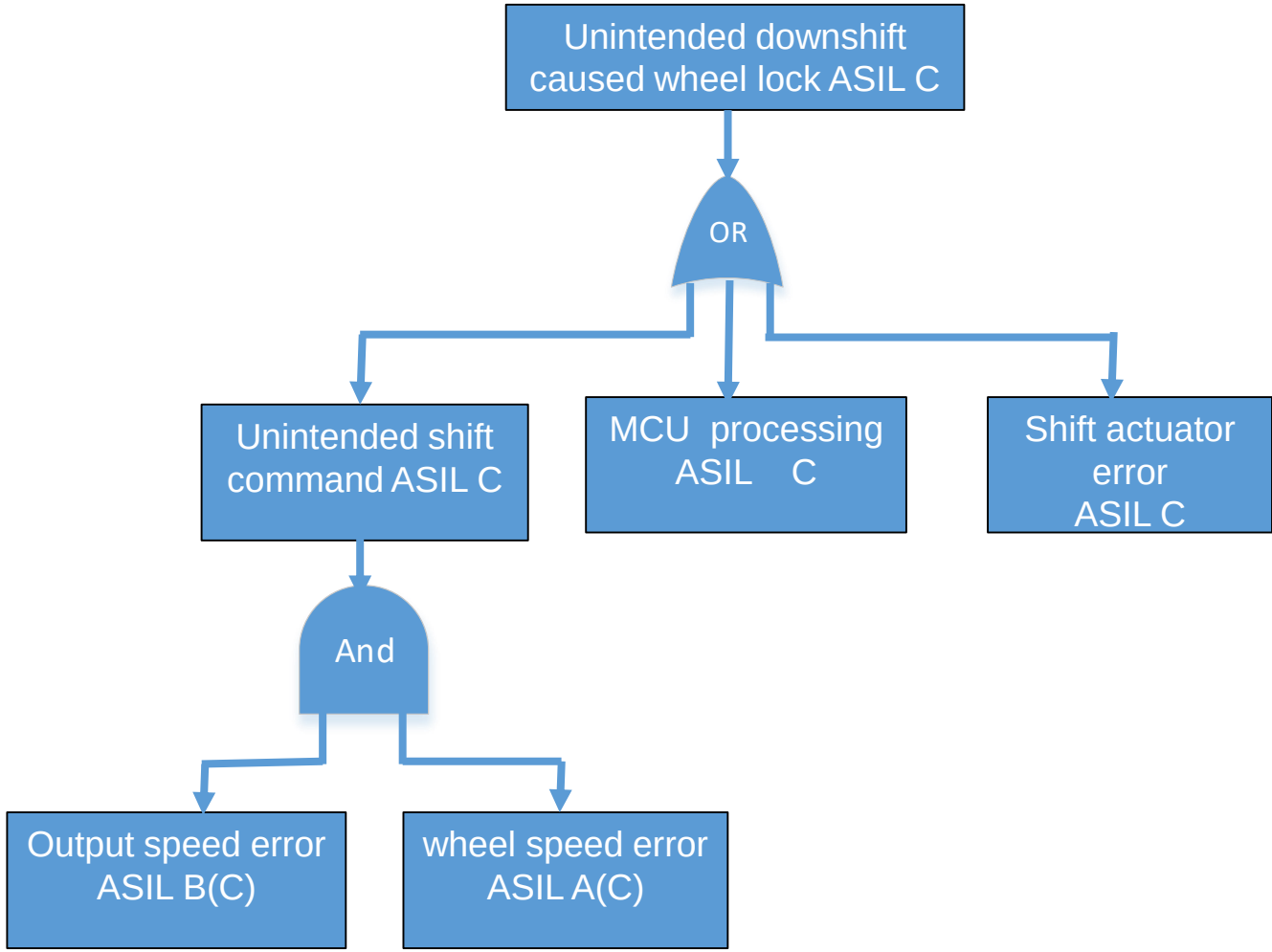
原则:

- 保证分解安全需求的冗余性
- 保证分解后模块的独立性(共因失效和级联失效分析)
- ASIL分解后硬件评估指标不变
- 验证和“认可”采用分解前ASIL级别流程和需求

ASIL 分解方案及示例

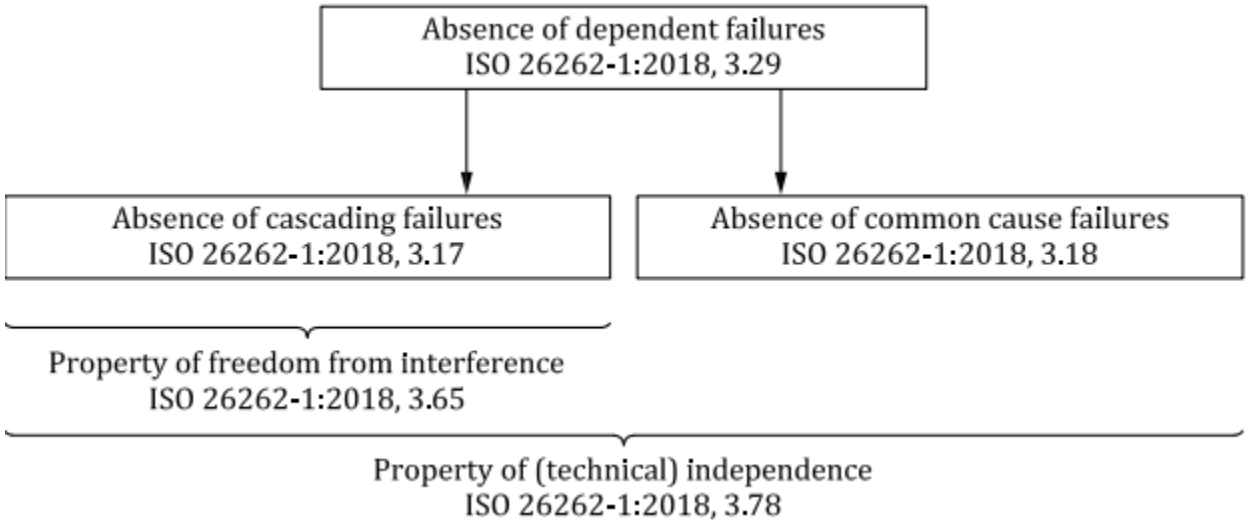
ASIL分解的意义：通常低ASIL开发成本更低（人力、时间、物料）





相关失效分析DFA

关联分析主要考虑系统/软件/硬件间可能存在的共因失效和级联失效，并安全措施以减轻关联失效，以满足独立性要求。



安全分析

安全分析用以确保由于系统失效和随机硬件失效导致安全目标违反的风险充分低。如危害识别，故障/失效及其潜在原因识别，支持安全措施定义和安全概念验证等。

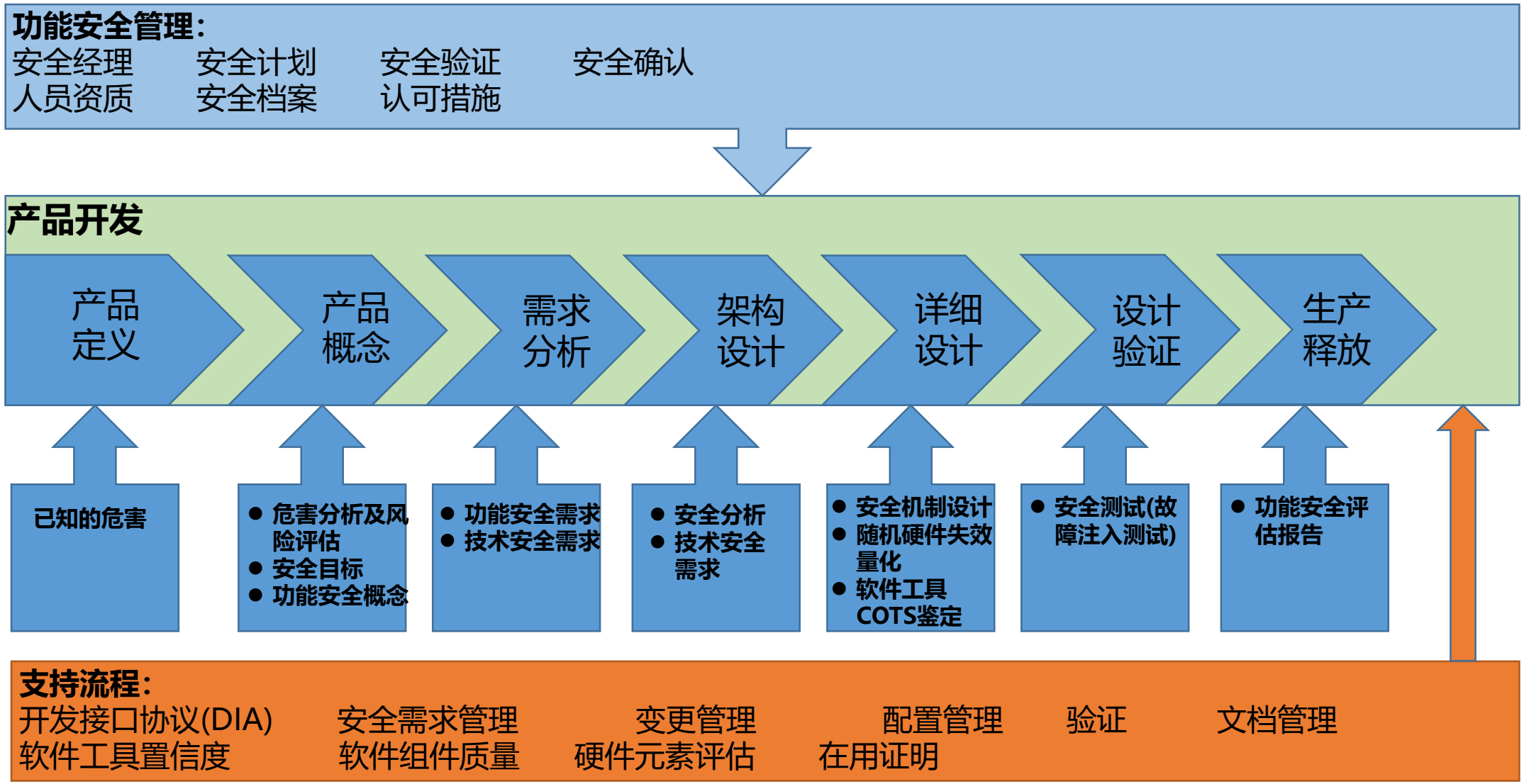
定性分析：

- HAZOP
- 定性FMEA(design & process)
- 定性FTA
- 定性ETA

定量分析：

- FMEDA
- 定量FMEA
- 定量FTA
- 定量ETA
- Markov模型
- 可靠性模块图

总结


功能安全管理：
安全经理
安全计划
安全验证
安全确认
人员资质
安全档案
认可措施
产品开发
产品定义
产品概念
需求分析
架构设计
详细设计
设计验证
生产释放
已知的危害
危害分析及风险评估
安全目标
功能安全概念
功能安全需求
技术安全需求
安全分析
技术安全需求
安全机制设计
随机硬件失效量化
软件工具COTS鉴定
安全测试(故障注入测试)
功能安全评估报告
支持流程：
开发接口协议(DIA)
安全需求管理
变更管理
配置管理
验证
文档管理
软件工具置信度
软件组件质量
硬件元素评估
在用证明

Functional Safety

What & Why?

Functional Safety Management

Organization, Role & Responsibility , Activity

Functional Safety Development

OEM & Supplier Level

Functional Safety supporting process

Q & A

THANKS

功能安全安全机制设计常用状态机