

ISO 26262

道路车辆 功能安全

Road vehicles—Functional safety



2020

课件使用及说明

- 本作品使用微软2016版PPT制作，也建议您使用相应软件打开及使用；
- 本作品的内容皆可根据您的需求**进行修改**，包括文字、图表、图片等；
- 本PPT背景可以修改，**增加PPT背景是因为防止盗图！**
- 为了节省空间和提高设计的效率，部分内容放置在母版中，当您需要修改时，请通过“视图”→“幻灯片母版”打开后修改；
- 如果有相关问题，可以在**本站内私信**；
- 严禁任何企业或个人**盗用或转卖**。



CONTENTS

- 1.什么是 ISO 26262
- 2.安全生命周期
- 3.系统开发
- 4.安全确认
- 5.认证流程
- 6.总结



/ 01

什么是 ISO26262

- 车辆行业功能安全应用目的
- 法律法规背景介绍
- ISO 26262 介绍
- 基本定义
- 如何根据ISO26262开发安全产品



车辆行业功能安全应用目的

安全，法规，产品责任，...

汽车电子的安全问题可能会导致高额的召回费用！

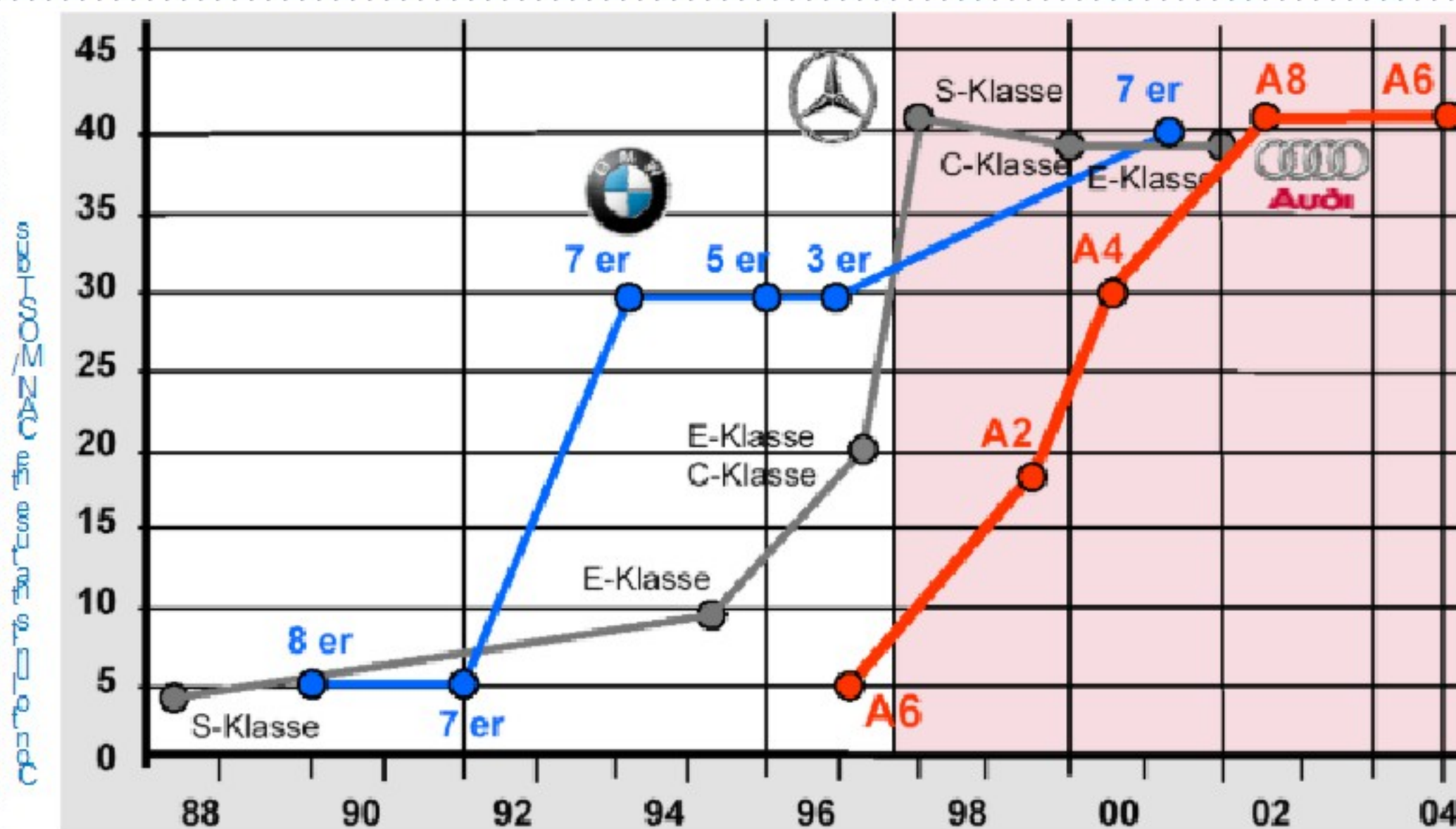
- 2013年10月日产SUV由于制动控制软件问题，召回15.2万辆！
- 2014年2月丰田第三代普锐斯由于混合系统中控制升压转换器软件问题召回190万辆！
- 2014年国内汽车122次召回中由于软件问题造成的有8次(中国汽车质量网统计)！



车辆行业功能安全应用目的

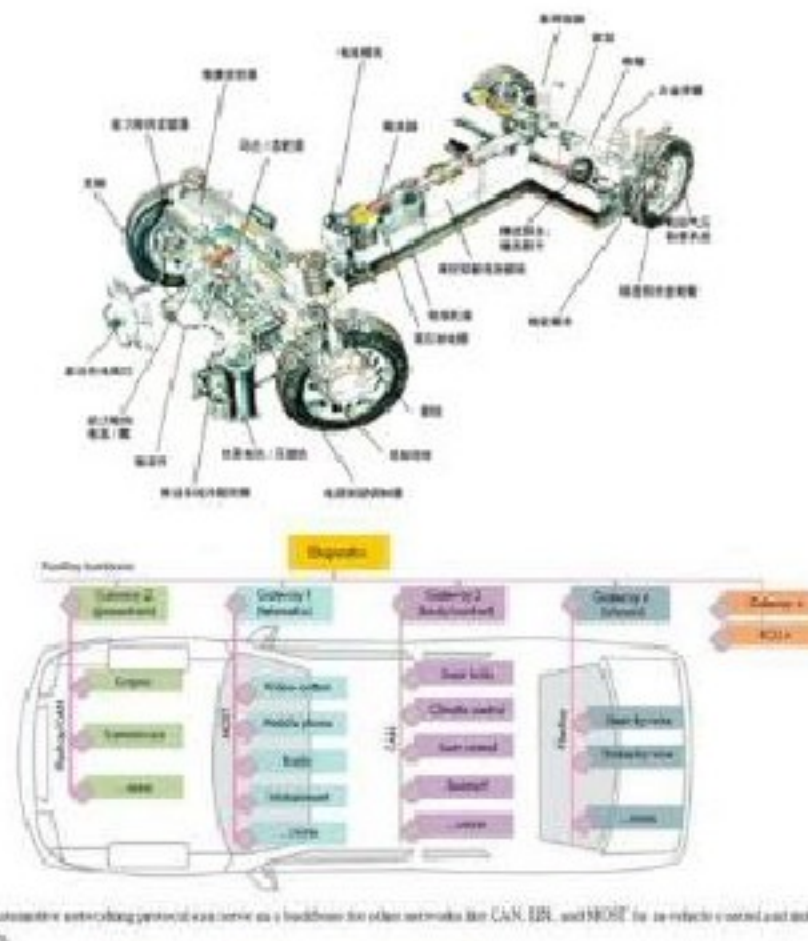
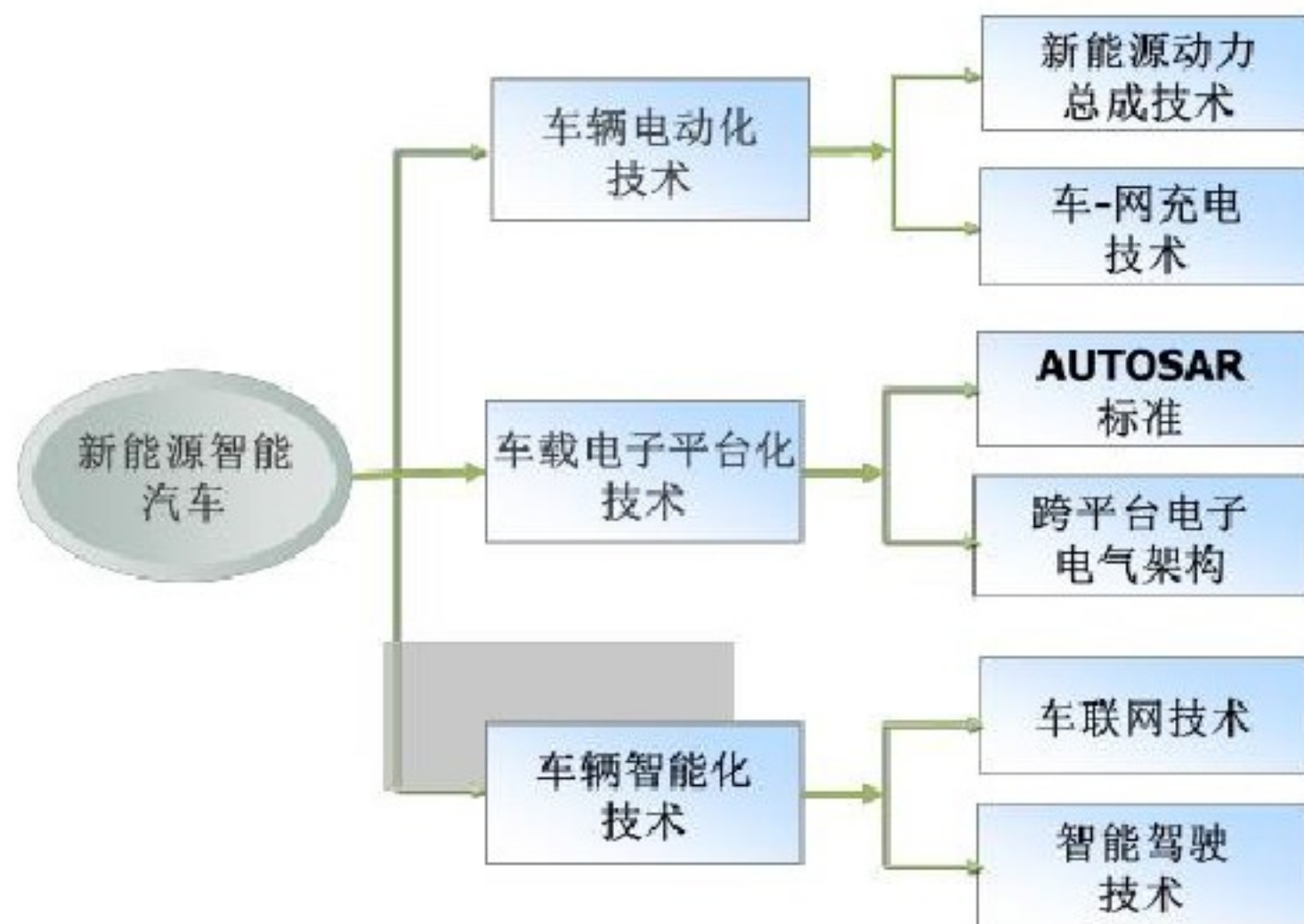
为什么产品要考虑功能安全？

- 产品越来越复杂
- 很多控制单元包括安全相关功能

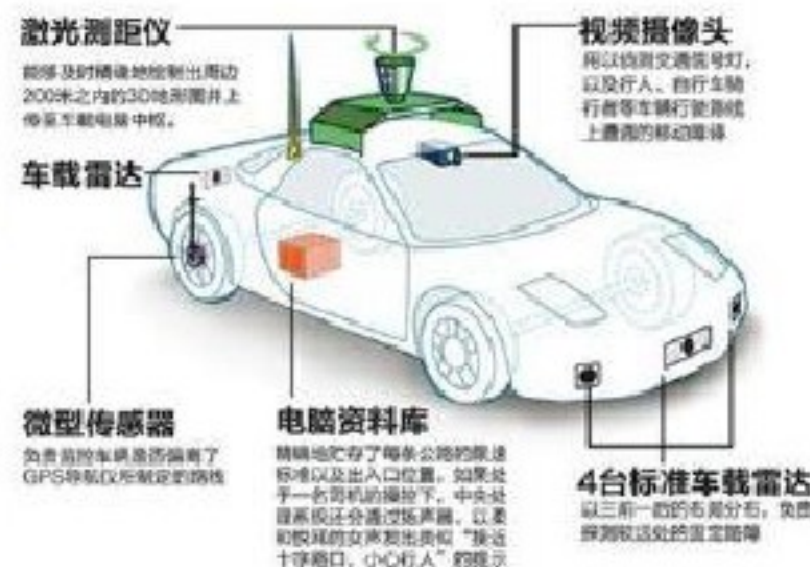
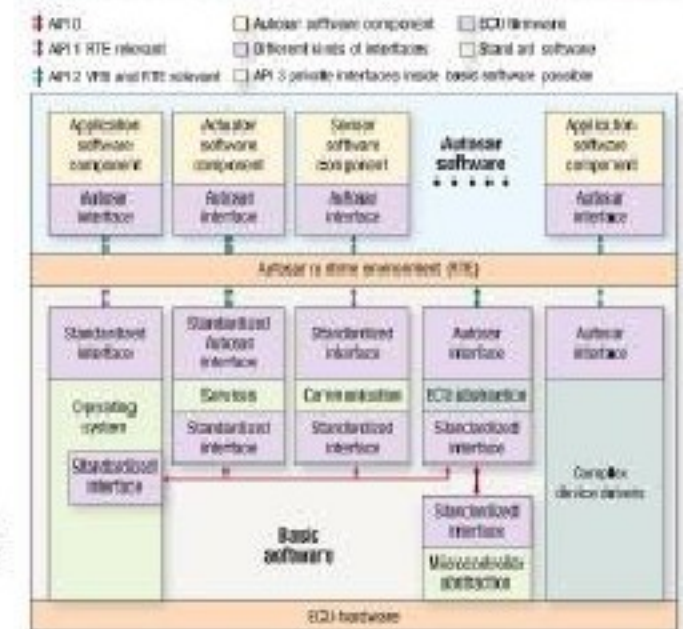


Reference:
Audi
Euroforum 2004

汽车行业技术发展趋势



The Autosar software architecture



安全功能举例

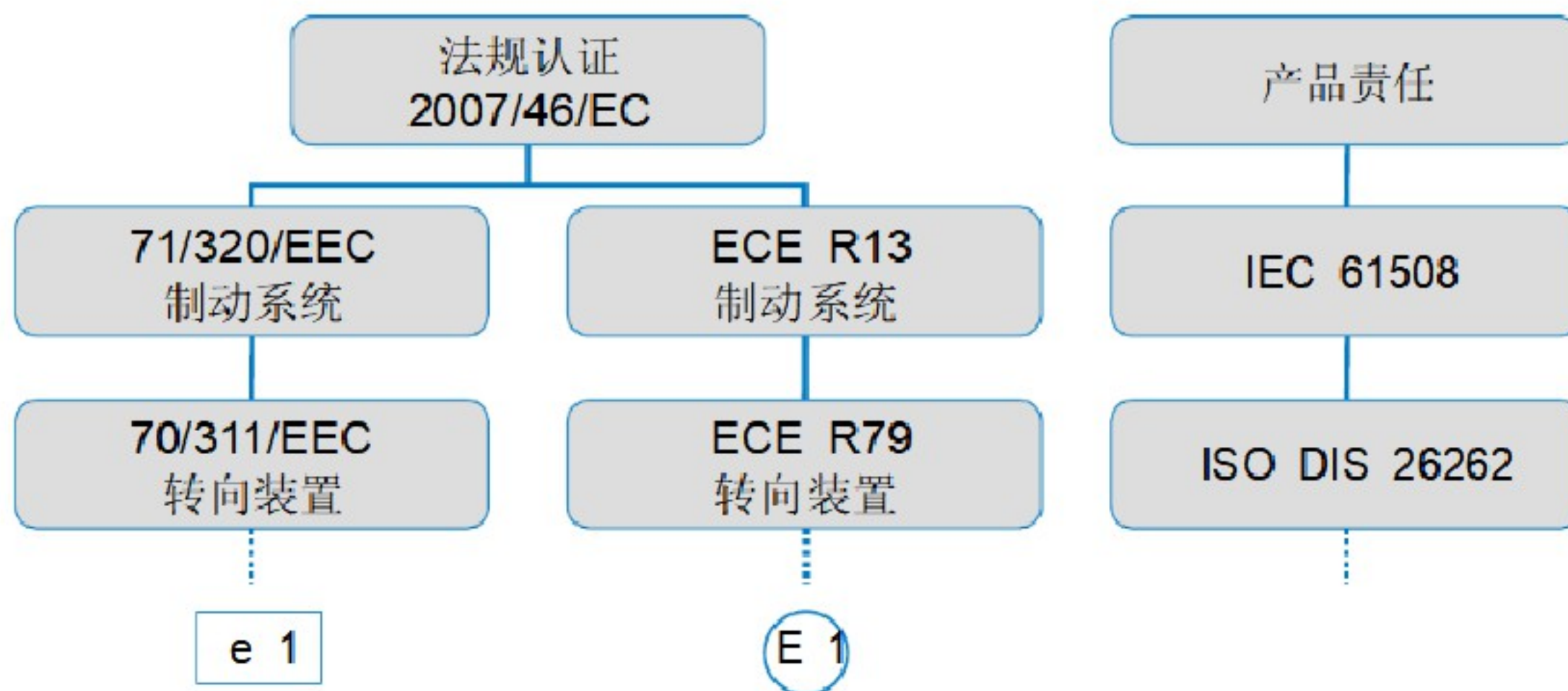
· 车辆系统越来越多的软件使用

· 软件包括安全相关部分

- 自适应前照明系统
- 汽车防抱死制动系统
- 车身稳定控制系统
- 牵引力控制
- 电子刹车力分配系统
- 紧急制动辅助系统
- 防撞系统
- 车道偏离警报系统
- 自适应助力转向
- 主动停车辅助系统
- 自适应悬架控制
- 电子制动系统
- 安全带预紧
- 安全气囊
- 司机瞌睡警示系统
- 司机监控系统
- 自适应远光灯辅助系统
- 自适应巡航系统
- 自动巡航系统
- 胎压监控系统
- 自适应前灯高度调节



功能安全法律法规背景介绍



2007/46/EC给出了EC指令和ECE法规的适用完整列表

功能安全法律法规背景介绍

法规认证vs.产品责任（2）

法规认证

- 只能由被认可的“技术服务机构”进行评估如：
ECE R13 Annex 18 or ECE R79 Annex 6



产品责任

- 独立的评估根据：
- （车辆）安全完整性等级（A）SIL
- 应用标准



为什么使用这IEC 61508、ISO 26262标准？

ISO26262背景介绍

道路车辆-功能安全

IEC61508-电子电气可编程电子安全相关系统的功能安全

- 80年代末期开始研究，应用于越来越复杂的安全相关系统。
- 来源于过程工业
- 1998年发布第一版·2010年发布第二版

ISO 26262的目的

- 汽车行业的一些要求与机械行业和过程行业不同。
- 汽车安全相关系统的复杂性越来越高
- 电子稳定性控制
- 紧急制动辅助系统
- 等

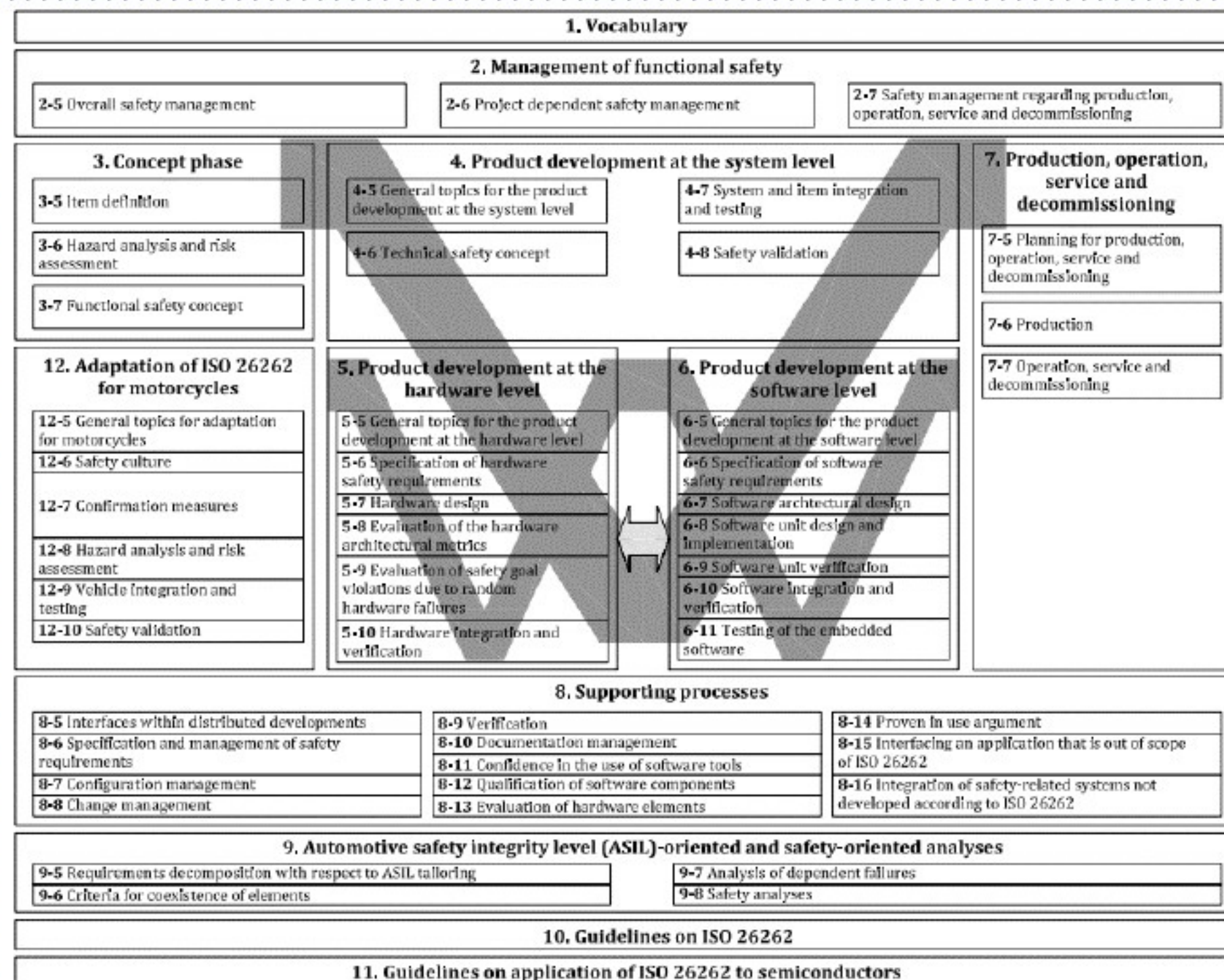
ISO26262 标准

ISO26262 : 11版介绍



ISO26262 标准

ISO26262 : 18版介绍



ISO26262背景介绍

ISO26262范围

应用于安全相关系统

- 包括一个或多个电子电气系统并且
- 安装于不超过3.5吨的乘用车

ISO 26262不应用于

- 安装在特殊目的的的车辆上的电子电气系统。如：残疾人车辆
- 非安全相关的电子电气系统。

Q?

什么是乘用车？

基本定义

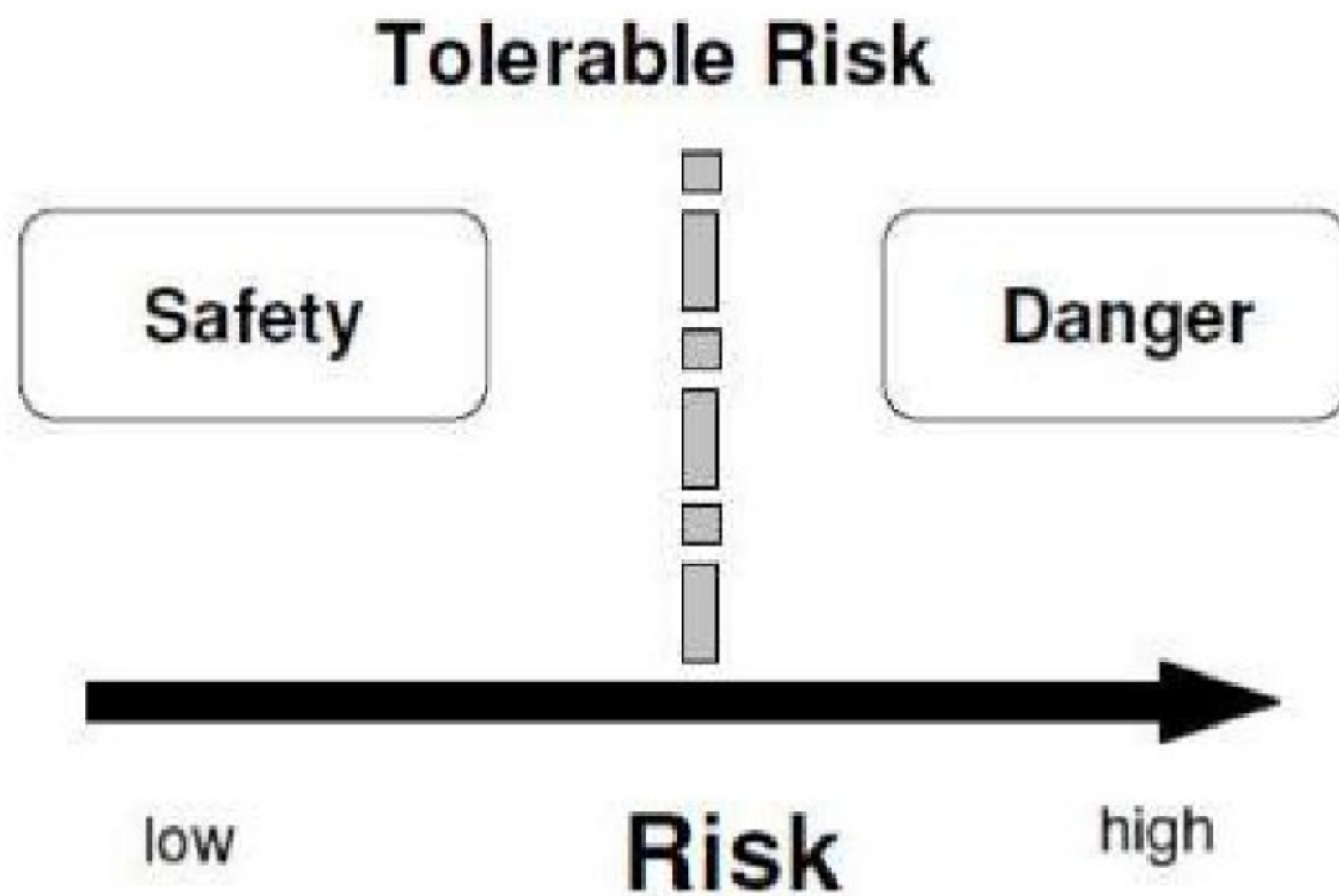
什么是安全？

安全？？？



基本定义

达到什么程度才算安全？



基本定义

功能安全

满足下列条件，安全系统是符合功能安全的：

- 随机、系统、共因失效不会导致安全系统的错误功能，从而导致：
- 人的伤害或死亡
- 环境的污染
- 设备或财产的损失

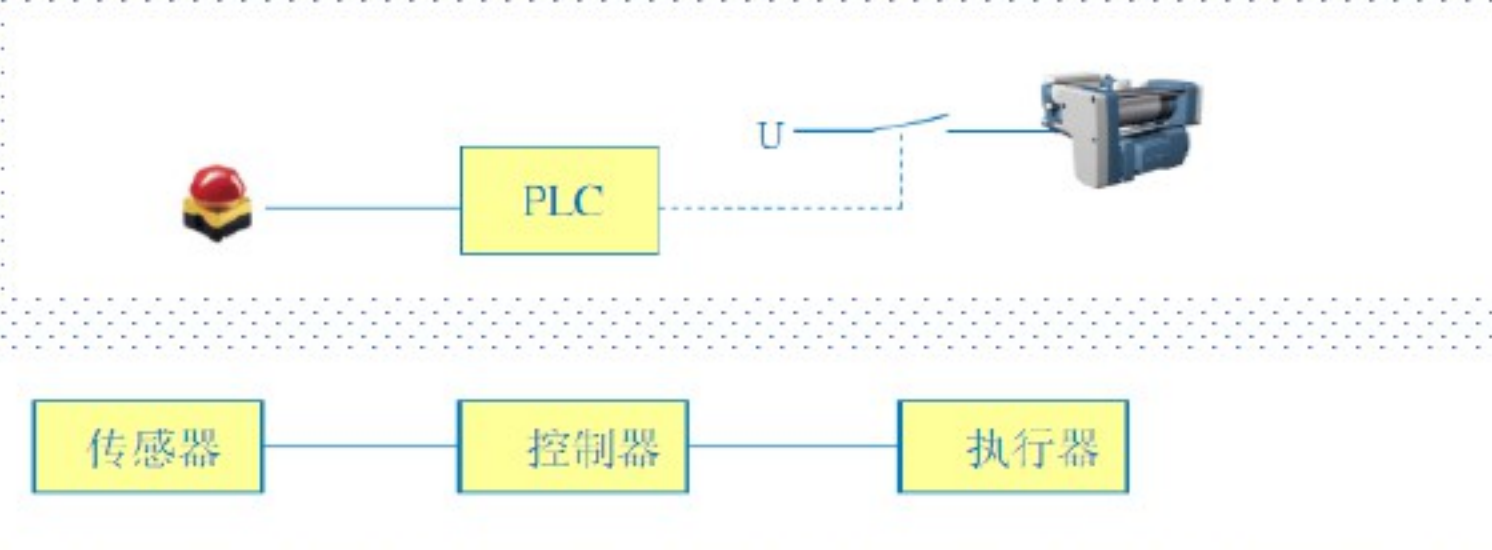


在正常条件及存在故障条件下，控制设备、系统的安全功能必须都能够保证！

基本定义

安全功能

安全相关系统的功能，用来减小风险并且达到/保持安全状态



PLC安全功能总是针对一个安全回路而言，不是针对一个设备或部件



基本定义

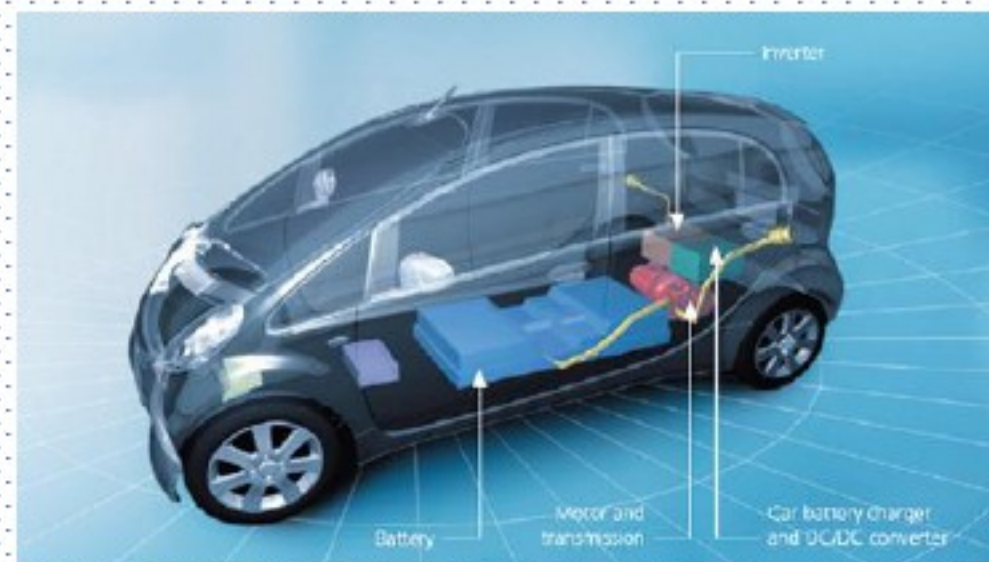
安全机制（ safety mechanism ）

由E/E功能或元素执行的措施，或者是其他技术，目的是达到安全状态或保持安全状态，或者两者同时考虑。

如：

能够达到，保持安全状态

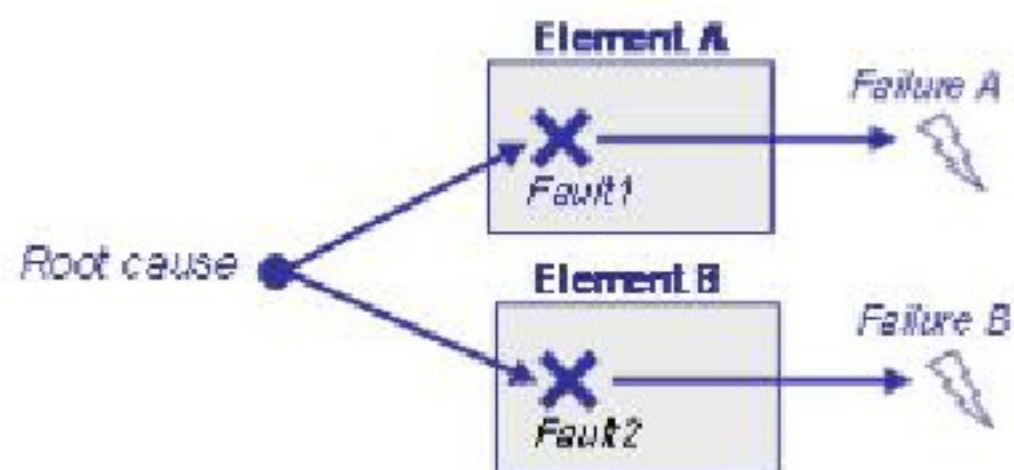
能够警告司机，以便于司机能够及时采取措施避免失效的影响



基本定义

级联失效和共因失效

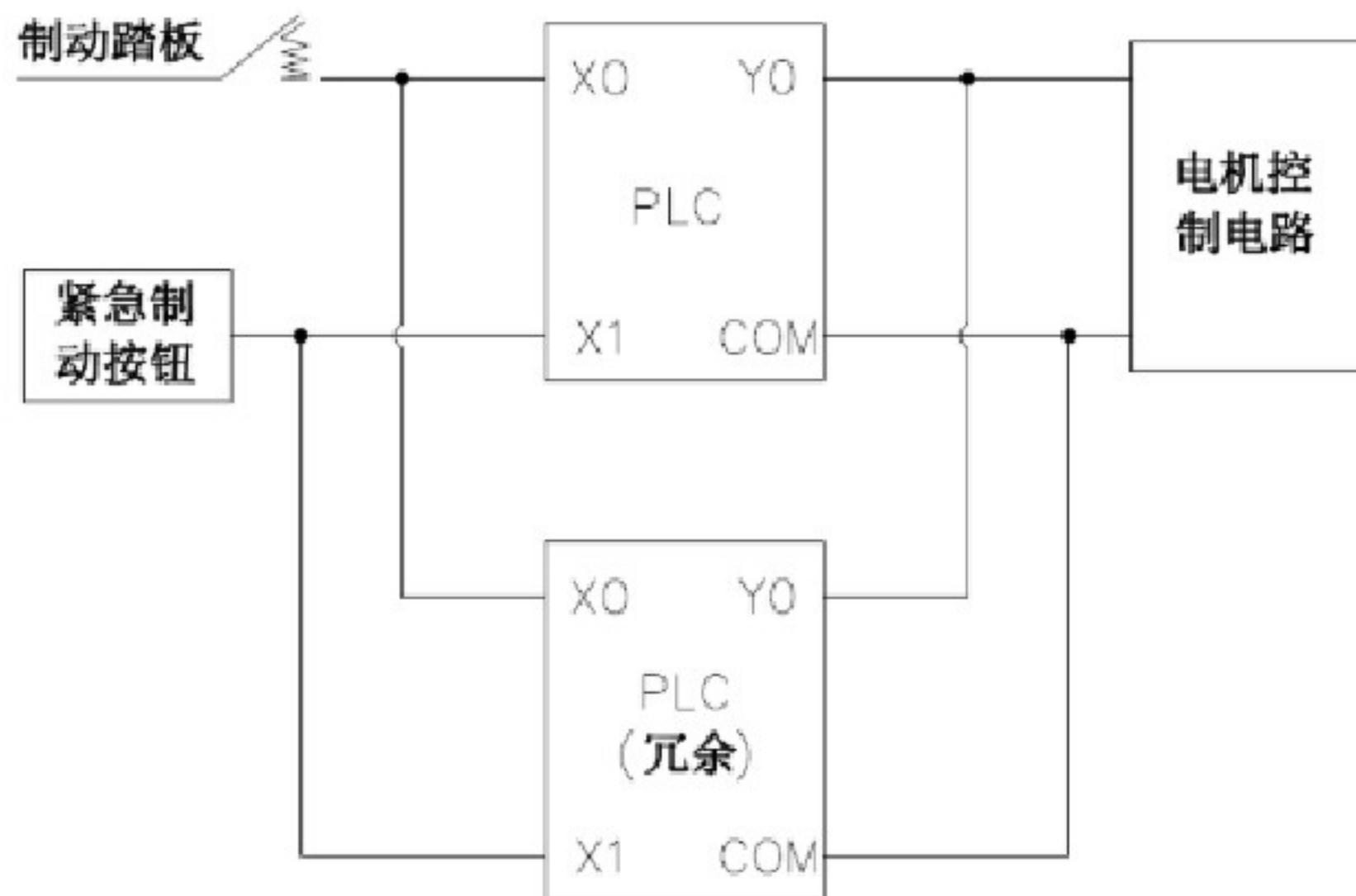
级联失效



基本定义

安全架构（safety architecture）

通过一组元素相互作用，来满足安全要求，包括冗余、独立概念



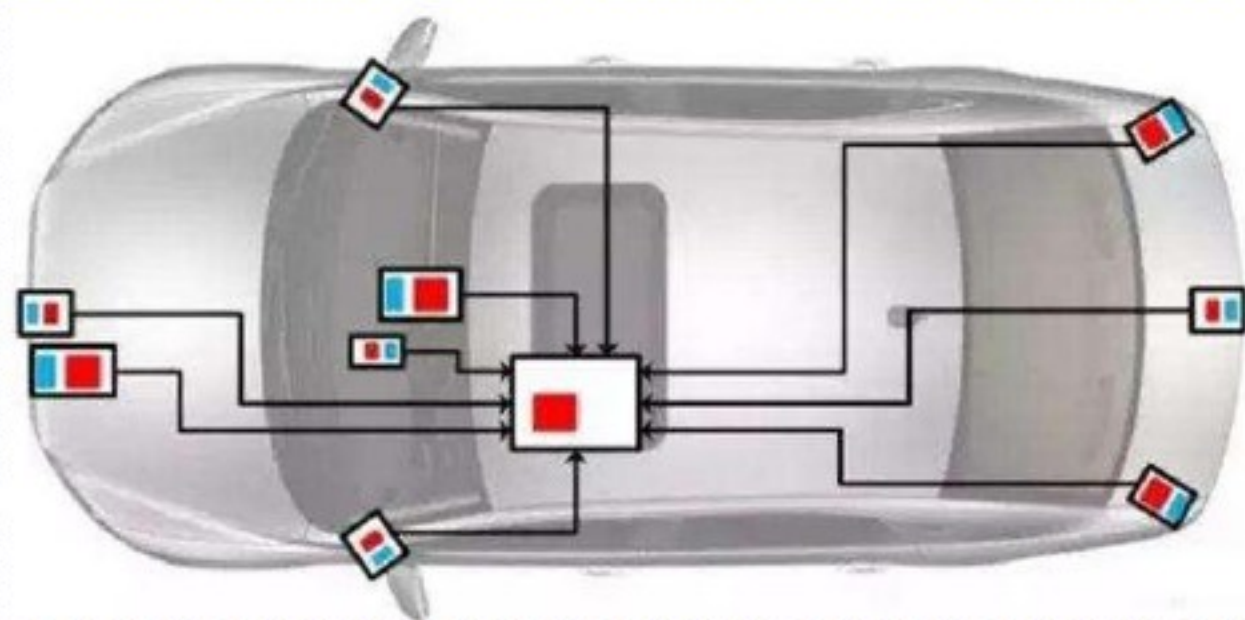
基本定义

充分信任的设计原则 (well-trusted design principle)

—预先使用经验证明没有安全问题的设计原则。

如：

- 隔离安全功能和非安全功能
- 67%降额使用



如何根据ISO26262开发安全产品？

功能安全：5个步骤实现 第一步

所有产品都来源于设想：

- 公司想开发一个更好的刹车系统。
- 航线偏离报警系统的更改
- 产品成本太高/制造难度大/可靠性低....



对于复杂性系统，功能安全很重要，如果：

- 功能失效会导致危险事件·功能丧失会导致危险事件
- 危险分析和风险评估结果证明需要ASIL

如何根据ISO26262开发安全产品？

功能安全：5个步骤实现 第2步

接下来建立功能安全管理制度

也就是为安全工作的协调和监控提供一个框架



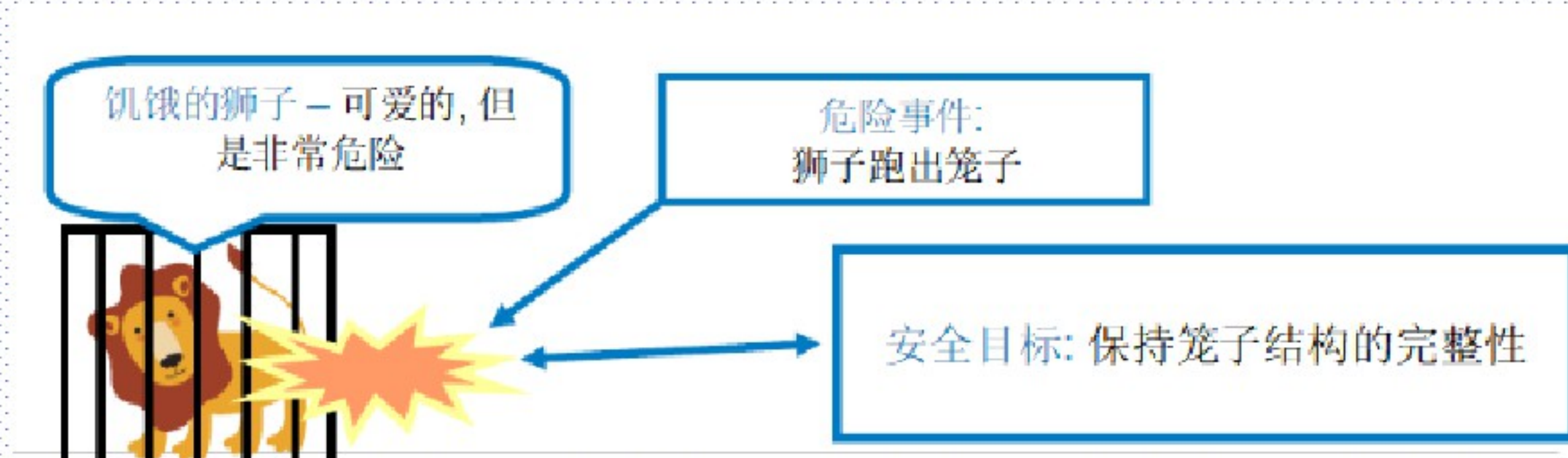
如何根据ISO26262开发安全产品？

功能安全：5个步骤实现 第3步

通过危险分析和风险评估来确认哪些危险事件应该考虑。

对每一个可识别的危险事件，都需要定义相应的安全目标（safety goal）

- 确认如何能够到达并且保持安全状态（safe state）
- 确认ASIL的级别



如何根据ISO26262开发安全产品？

功能安全：5个步骤实现 第4步

根据可识别的安全目标，做出安全概念
(safety concept) 包括以下内容

- 基本系统架构
- 达到并且保持安全的技术措施

- 系统级设计，软硬件设计和开发将依据安全概念。
- 在设计开发过程中，应采取必要的安全措施和验证活动。



如何根据ISO26262开发安全产品？

功能安全：5个步骤实现 第5步

安全确认用来确保开发项目能够满足分配给它的安全目标。

功能安全评估同时考虑到产品和过程，提高了项目的安全置信级别。



/ 02

什么是安全生命周期

- 功能安全管理
- 项目定义
- 风险分析，风险评估安全目标定义
- 功能安全要求



功能安全管理

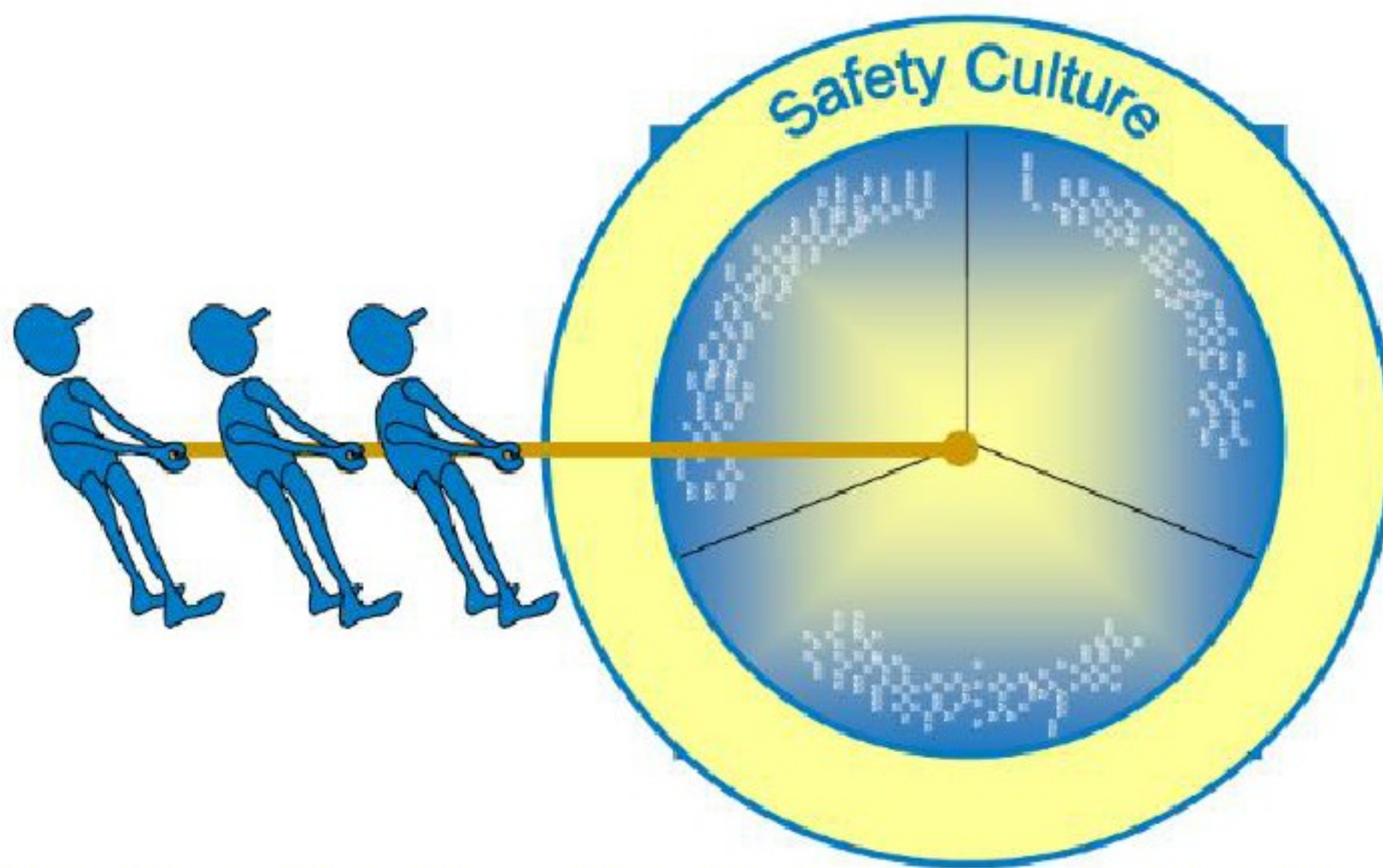
安全管理：

- 定义安全生命周期模型
- 需要创造培养公司的安全文化
- 定义相关部门、人员的职责
- 确保人员能力资质
- 确保足够的质量管理工作



功能安全管理

功能安全需要做什么



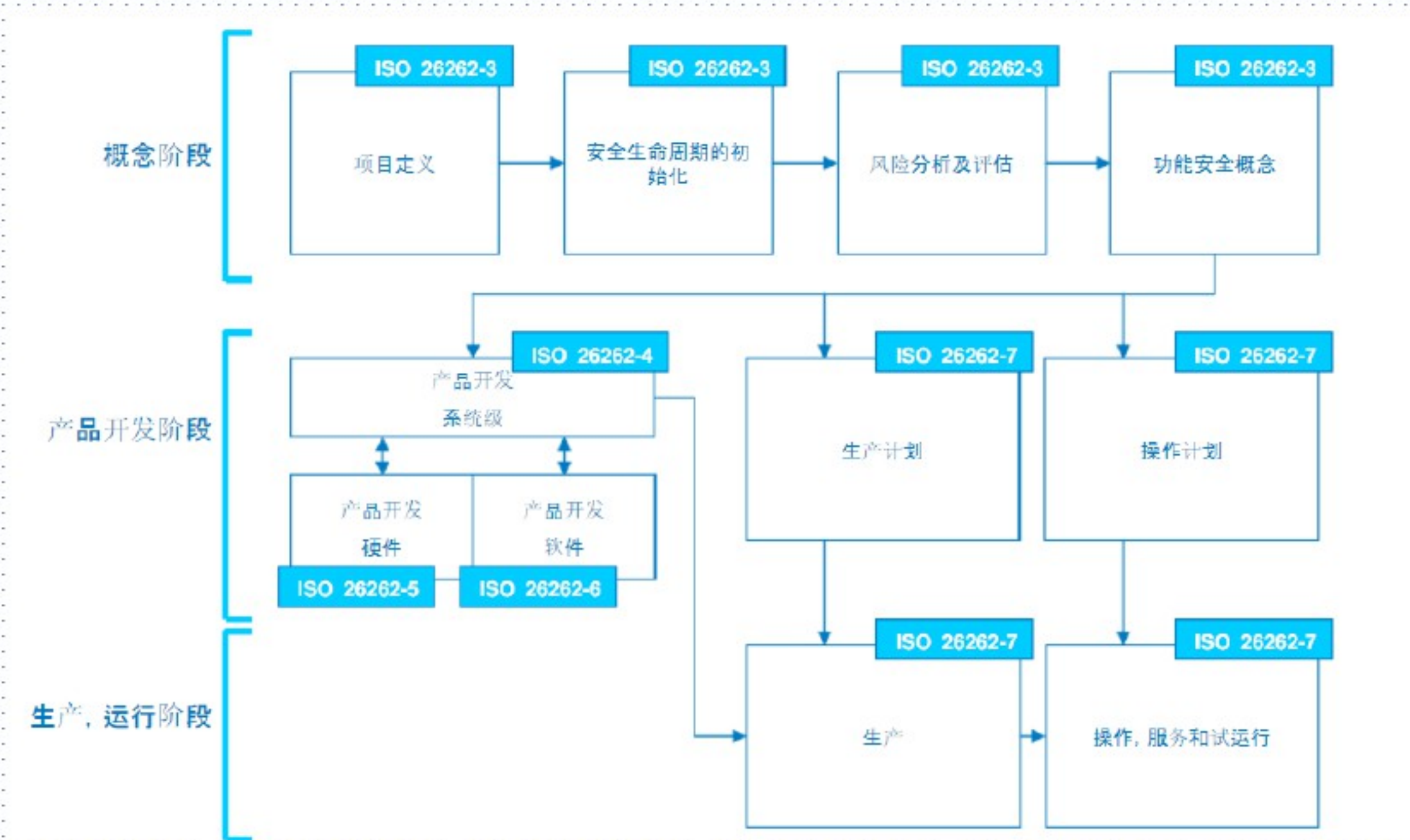
功能安全管理

开发阶段安全生命周期模型



功能安全管理

ISO26262-安全生命周期模型



项目和其他相关概念

项目和其他相关概念

ISO26262-10 Clause 4.2

在安全相关产品开发时，第一件事就是项目定义项目定义

关注以下开发内容：

- 确认相关功能
- 开发怎样进行
- 再使用存在的产品或更改？

不正确的项目定义可能会导致后继工作出现严重的问题!



项目定义

ISO26262-3 Clause 5在项目定义过程中，必须考虑所有相关需求

- 功能性的需求
- 非功能性需求（费用，尺寸，环境要求，ASIL.....）
- 法规要求
- 标准，导则

项目定义要考虑行业专家意见！

项目定义对于开发正确的系统起着关键作用。



编号:2015072502250000400 汇图网正版商业图库 (www.huitu.com) by:壹图

项目定义

ISO26262-3 Clause 5

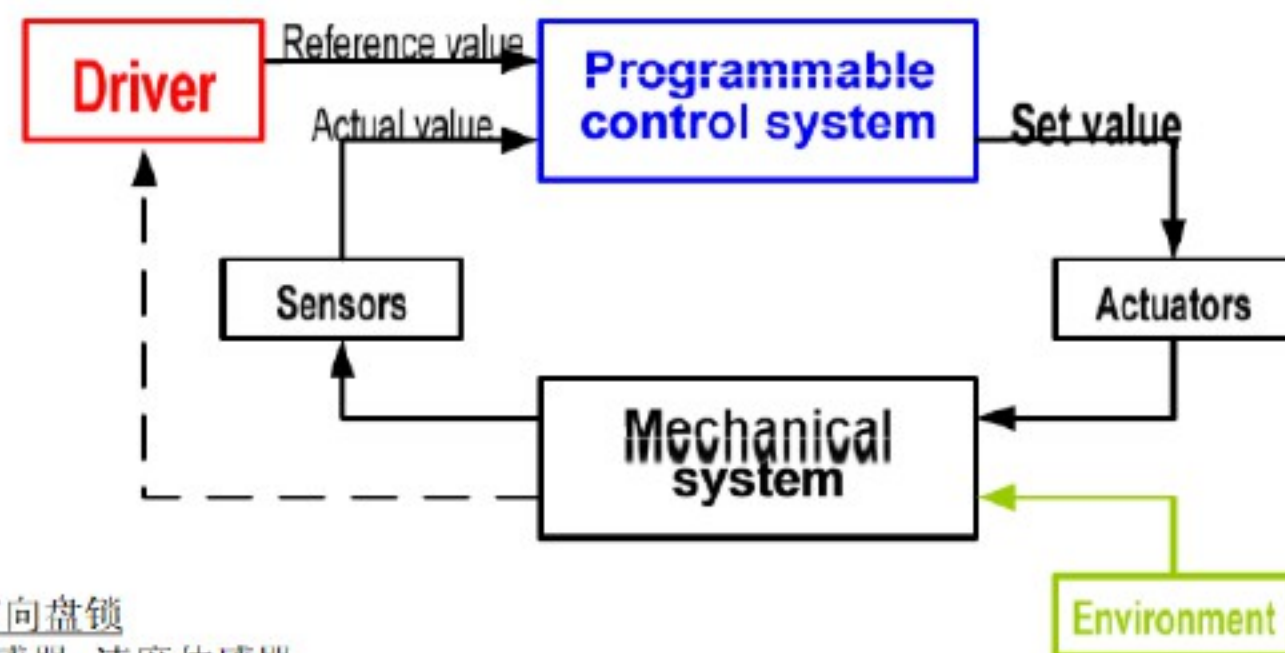
举例：方向盘锁

传感器：速度传感器

执行器：电机带动涡轮，涡轮控制锁定装置

机械系统：涡轮

司机：踩踏板控制速度的参考值



例：方向盘锁
传感器：速度传感器

危险分析、风险评估和安全目标

标执行危险分析和风险评估

ISO26262-3, clause 7

对于项目来说，理解相关功能必须：

- 对项目相关危险识别和分类
- 制定安全目标预防或减轻危险

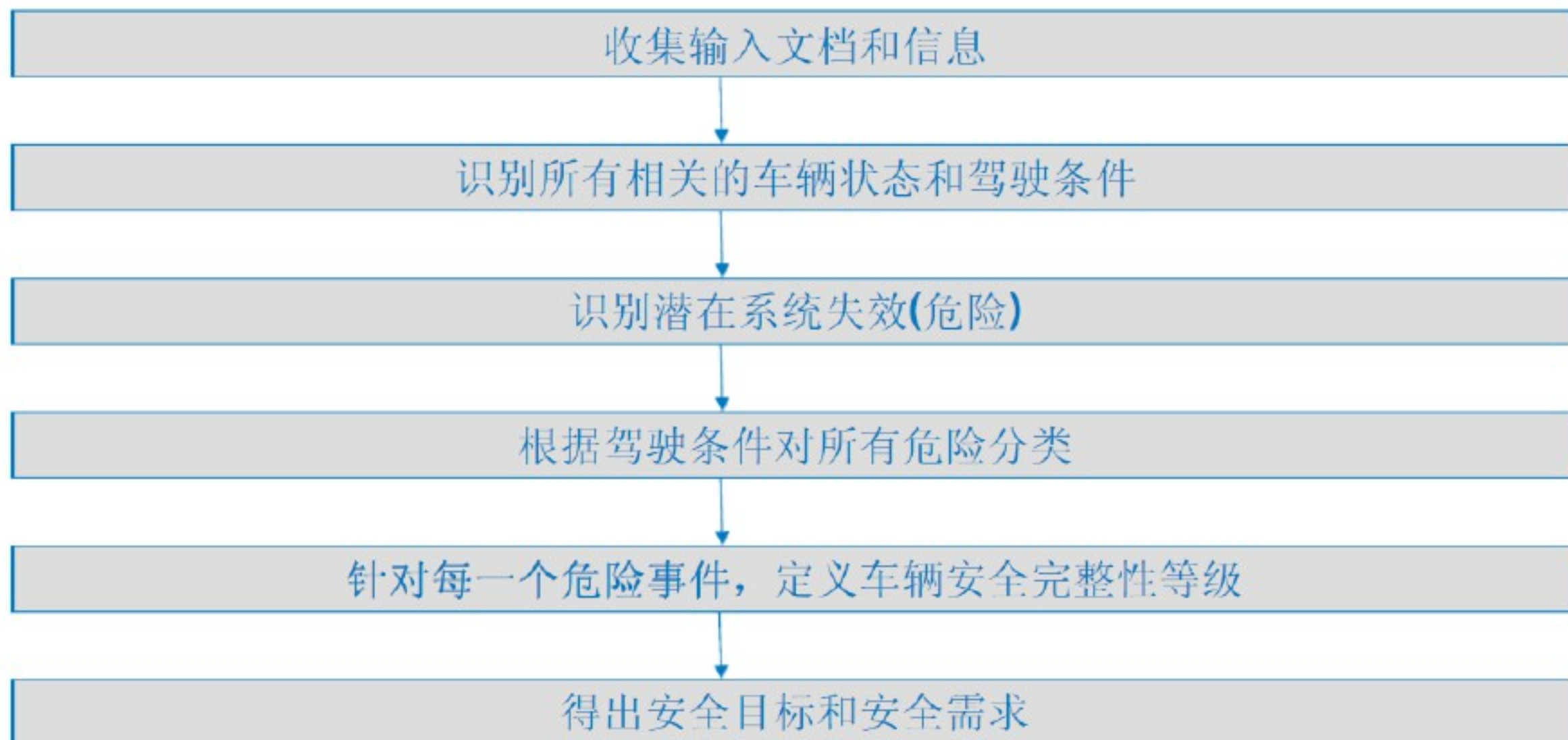
安全目标应保证项目的运行风险低至可以接受！



汽车领域项目基本流程

汽车领域项目基本流程

ISO26262-3, clause 7; ISO26262-3, annex B



危险分析、风险评估和安全目标

车辆安全完整性等级评估（4）

S：严重性

E：暴露的可能性

C：可控性

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

危险分析、风险评估和安全目标

车辆安全完整性等级



ASIL 0



ASIL A



ASIL B



ASIL C



ASIL D

危险分析、风险评估和安全目标

汽车安全完整性等级举例

TSR-交通标识识别

- 正确识别：QM or ASILA

电磁方向盘锁定系统

- 驾驶时防止锁定：ASILD

安全气囊

- 需要时打开安全气囊：ASIL A
- 不需要时不能打开气囊：ASILD

注：汽车安全完整性等级主要与安全需求和功能安全概念有关。

/ 03

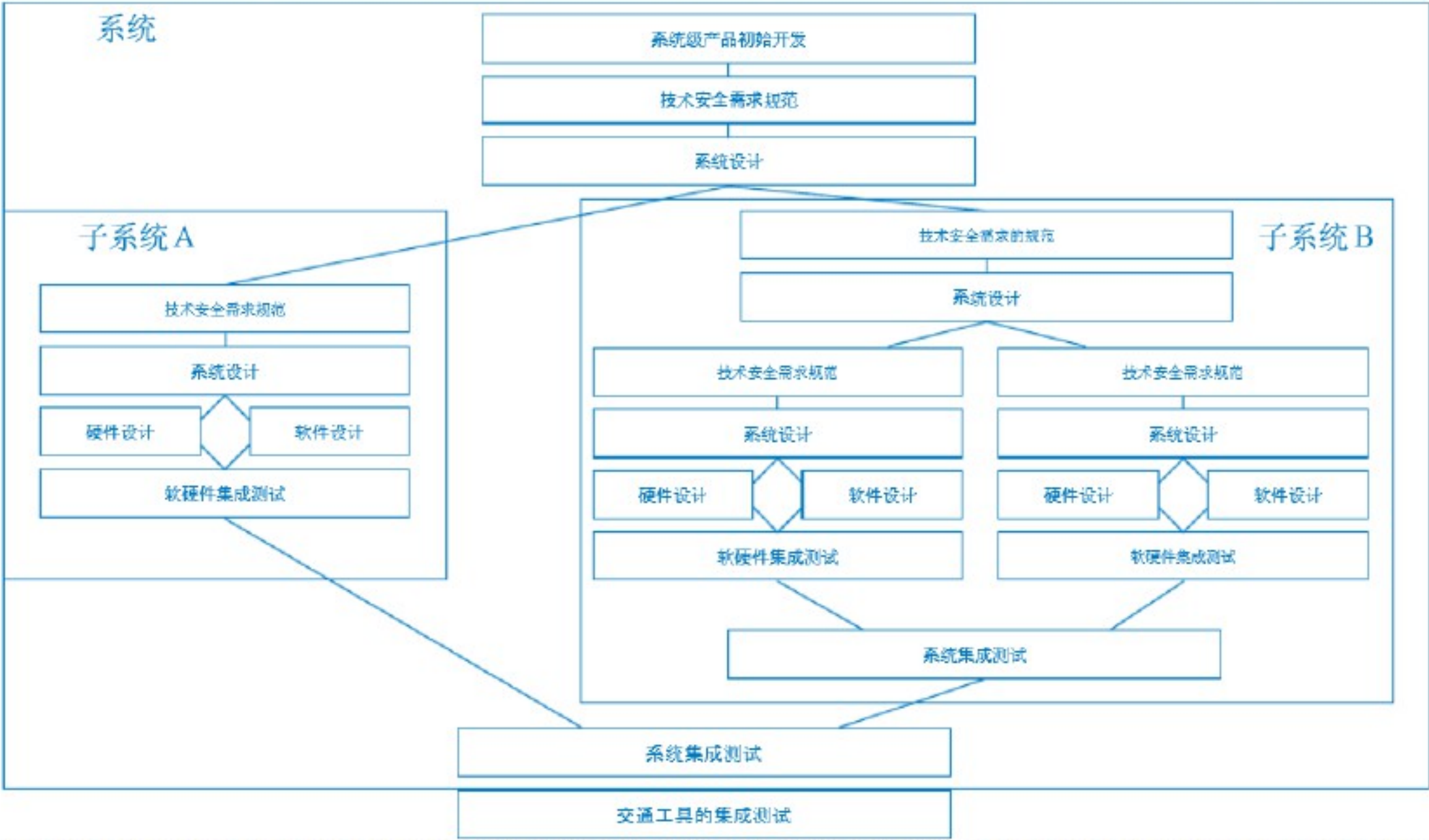
系统开发

- 系统级开发
- 硬件开发
- 软件开发



系统开发

生命周期



系统设计

技术安全概念和系统设计描述：

- 如何应用功能需求和技术安全需求功能安全系统设计应保证
- 充分信任的和实验证明良好的系统架构
- 可验证的、标准里描述的经验证使用的方法。

可能使用的功能安全验证方法包括

- 系统设计检查，走查
- 仿真
- 原型设计，车辆测试
- 安全分析（FTA，FMEA）



硬件开发

硬件安全需求规范

基于技术安全需求，对于硬件设计，以下各方面需要清晰定义：

1. 硬件安全需求规范包括

- 测试规则
- 质量规则

2. 硬件架构指标需求

- 单点故障指标 (SPFM)
- 潜在故障指标 (LFM)

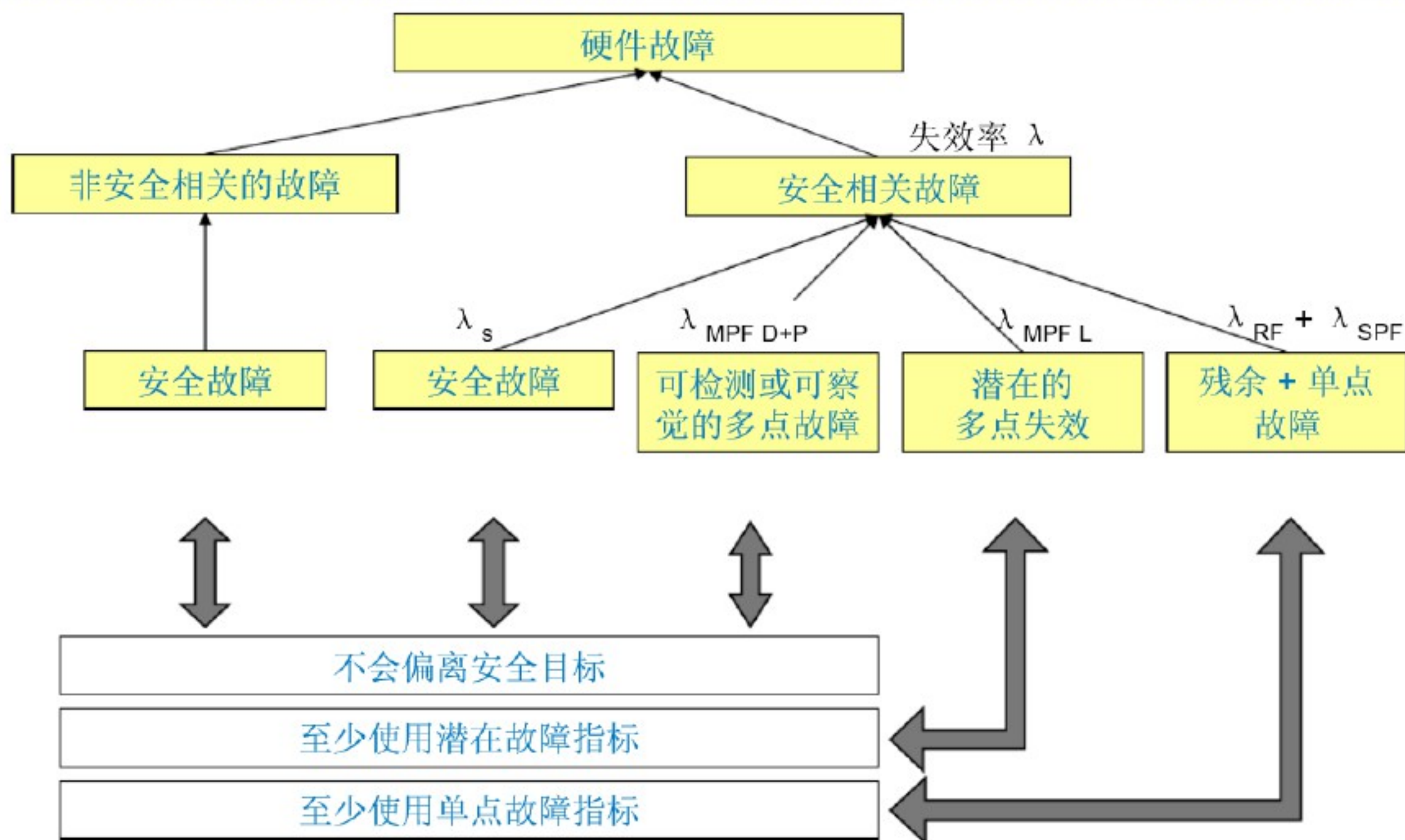
3. 随机硬件失效需求

- 偏离安全目标的概率

4. 软硬件接口 (HSI) 规范

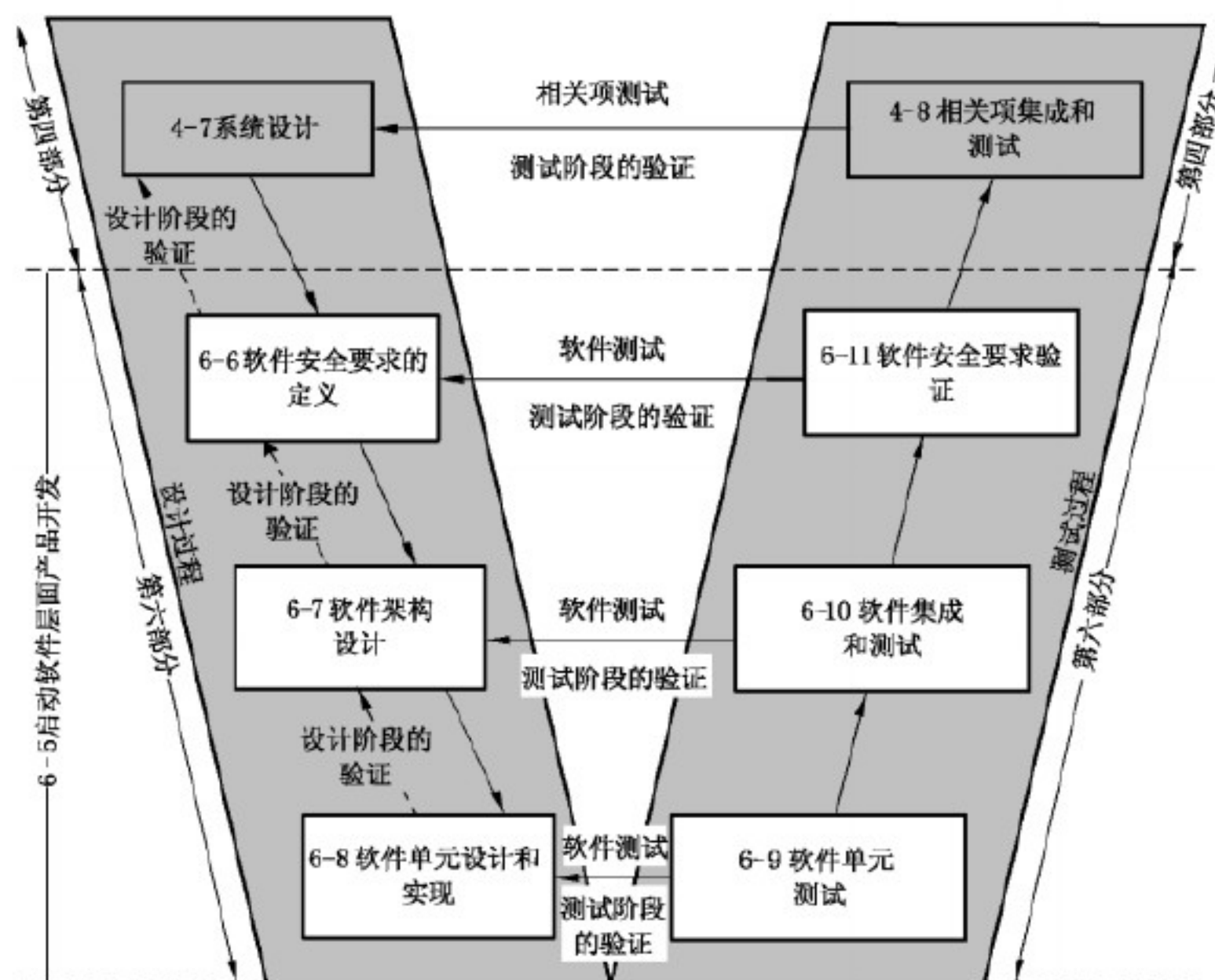


硬件失效模式的分类



软件开发

软件开发参考阶段模型



注：图中 GB/T 34590—2017 每部分的特定章用以下方式标示：“m-n”，“m”代表部分号，“n”代表章号，例如“4-7”代表 GB/T 34590.4—2017 第 7 章。

/ 04

安全确认，功能安全评估

- 安全分析
- 安全确认
- 安全论证
- 证明措施



安全分析、安全确认与安全论证

安全分析

ISO 26262-9 Section 8安全分析主要目的：

- 检查故障和失效的后果。
- 考虑项目和元素的功能，运行状况和设计
- 提供有可能造成偏离安全目标的原因和条件的信息。

分析也考虑

- 识别新的功能性的和非功能性的危险。

安全分析支持安全系统的开发，通过另一个视角对系统和功能检查！

安全分析

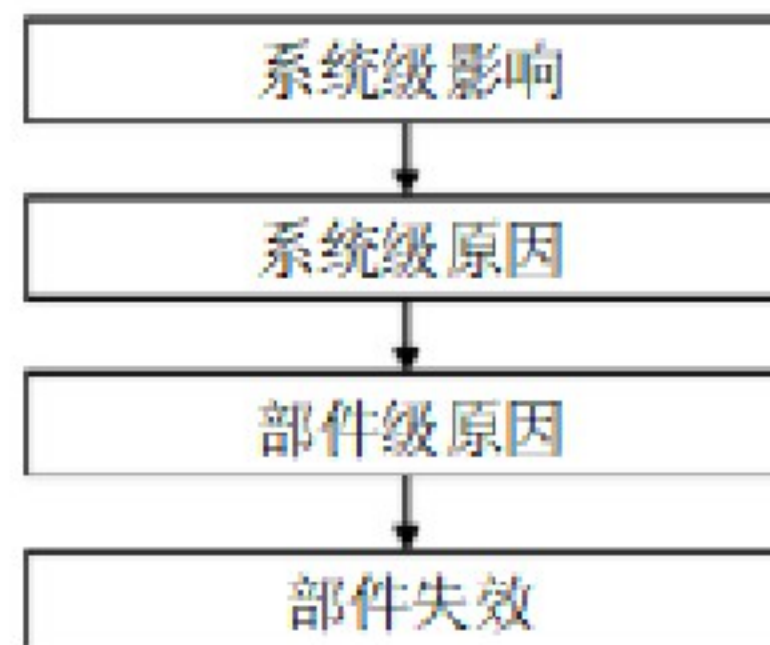
ISO28282-9 Secion 8

安全分析可以用不同的方法

- 归纳法，i.e.由下至上分析
- 演绎法，i.e.由上至下分析

安全分析方法举例

- 失效模式及潜在后果分析（FME
- 故障树分析（FTA）
- 马尔可夫模型
- 可靠性框图



安全确认

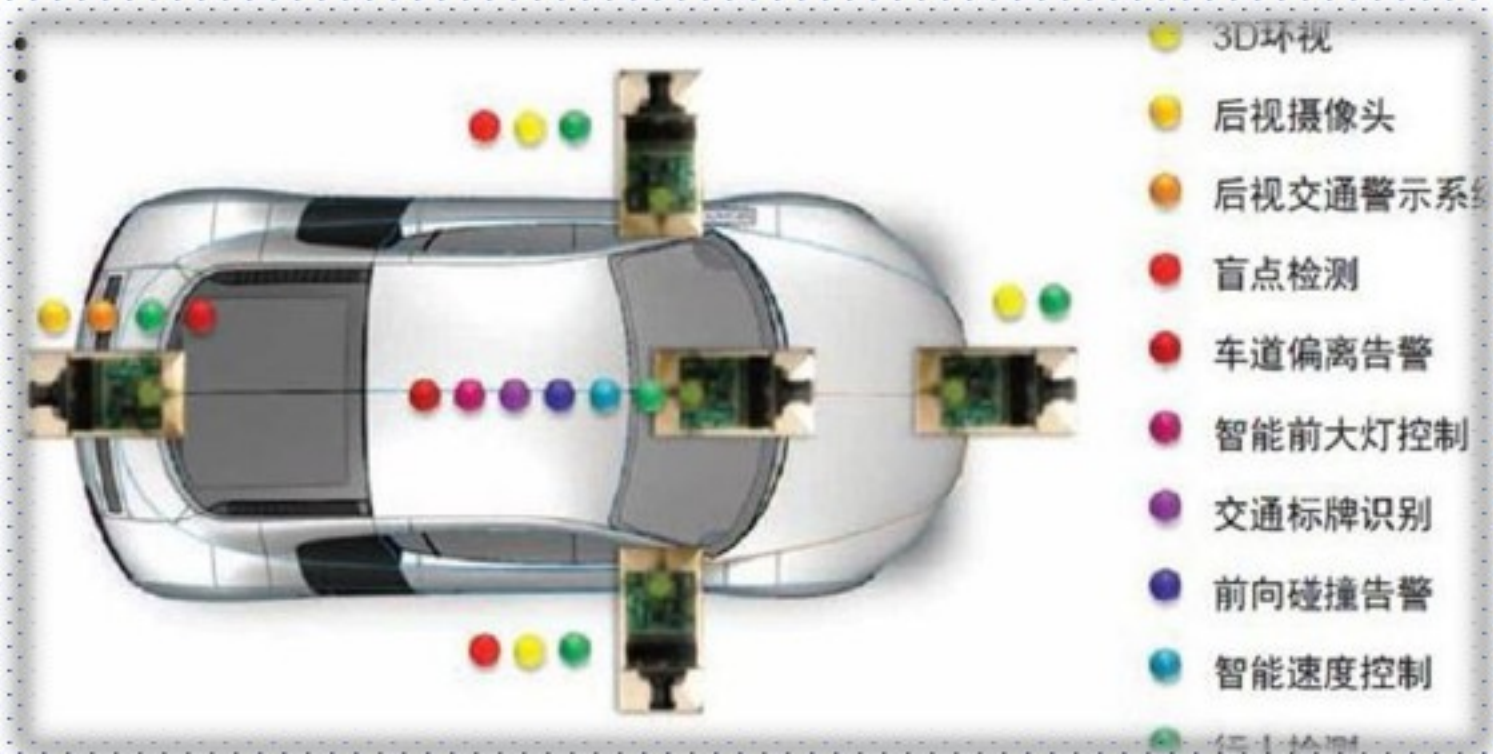
ISO28262-4Clause9

安全确认（车辆级别vehicle level）

- 电子电气系统
- 软件·硬件
- 其他技术相关的元素
- 外部措施

为研发的系统提供下列证据：

- 适合预期用途
- 安全措施是充分的



安全论证

什么是安全论证？

ISO 262622 , 64.5

通过分析开发阶段安全工作的产出，论证项目的安全目标是否达到并满足要求。

ISO 26262-1 , 1.103

安全论证定义为

·清晰的、易于理解的、可辩护的论证：对于具体环境来说，系统的安全是可以接受的。



[1] T. P. Kelly, Arguing Safety A Systematic Approach to Safety Case Management, DPhil Thesis, Department of Computer Science, University of York, UK, 1998

证明措施的独立性要求

ISO26262-2 Table 1

证明措施		ASIL			
Type	Target	A	B	C	D
复核	危险分析和风险评估	l3	l3	l3	l3
复核	安全计划	—	l1	l2	l3
复核	集成和测试计划	l0	l1	l2	l2
复核	确认计划	l0	l1	l2	l2
复核	安全分析 (FMEA, FTA, ...)	l1	l1	l2	l3
复核	软件工具的考核	—	l0	l1	l1
复核	预先使用的论证	l0	l1	l2	l3
复核	安全论证的完成	l0	l1	l2	l3
审核	功能安全过程	—	l0	l2	l3
评估	功能安全评估	—	l0	l2	l3

第三方功能安全评估

为了增加项目符合ISO26262的可信度，可以由第三方评审人员做功能安全评估。

对ASILC和ASILD需要满足独立性要求

- 标准没有正式提到第三方评估

第三方评估的好处：

- 另一种角度
- 功能安全评估专业知识
- 公司外的人力资源



/ 05

认证流程

■ 认证过程介绍



认证流程

认证流程



第一阶段的主要任务：

概念评估：

- 检查并评审产品需求规范和安全设计概念
- 在产品各个生命周期阶段，尤其在开发过程中（质量管理），检查并评估故障避免措施的计划。
- 评估检测和控制故障需采取的措施（诊断）FMEDA，评价是否安全完整等级能够达到预期的目的。
- 文件系统的审核（设计和质量管理）
- 电磁兼容，环境测试需求的定义。
- 为主检阶段出具项目计划
- 根据概念评估的结果出具报告。

第二阶段的主要任务：

主检：

- 测试所有的安全相关的功能，最坏情况分析（软硬件）
- 检测和控制故障的验证（故障插入测试），FMEDA的验证与执行。
- 软件验证测试的评审（模块，集成测试，系统测试）
- 对开发过程中创建的产品文档评审（设计文档，测试、验证、审核记录）
- 安全相关的可靠性数据的定义及计算
- 环境测试（incl. EMC）
- 用户文档的检查（安装，操作手册，安全手册）
- 提供测试报告

第三阶段

发证：

·基于测试报告，认证机构颁发证书

	
ZERTIFIKAT CERTIFICATE	
Nr./No. 955 EZ 887.09/05	
Produktname Product name	Programmierbare Sicherheitssteuerung Programmable Safety Controller
Lizenznehmer License holder	ZPOK Corp. Post code 315-0895 1-7 Wts-Herweg, Polinop Nordero-Grp, 100110 China
Typbezeichnung Type designation	S-PLC-PCS-H Version 3.5.3
Nennanwendungszweck Intended application	Maschinensicherheit Anwendungen, in denen der energie- lose Zustand der sichere Zustand ist Safety of machines, applications, where the de-energized state is the safe state
Bezugsnormen Covers and standards forming the basis of testing	IEC 61508:1998 4: 2000 EN 954-1:1996 EN 60204-1:2006 NFPA 79:2007 (chapters 4.4, 5, 5.4, 3) UL 1998:2004 (Revision 4:6:2004)
Prüfungsergebnis Test results	Die programmierbare Sicherheitssteuerung erfüllt die normativen Anforderungen und kann bis maximal SIL 3 nach IEC 61508, bis Kategorie 4, PL e nach EN ISO 13849-1 und bis Kategorie 4 nach EN 954-1 eingeordnet werden. The programmable safety controller fulfills the normative requirements and can be used in applications up to SIL 3 acc. to IEC 61508, up to Cat. 4, PL e acc. to EN ISO 13849-1 and Cat. 4 acc. to EN 954-1.
Besondere Bedingungen Special requirements	Die Hinweise in der Bedienungsanleitung sind zu beachten. The information provided in the instruction manual must be considered.
 Functional Safety Type Approved FS	
Der Prüfbescheid... 955 EZ 887.09/05 vom 25.08.2008 ist Bestandteil des Zertifikats. Der Hersteller muss für das Produkt gültige Genehmigungs- Anweisungen in Betracht, die mit dem Prüfbescheid übereinstimmen. The test report... 955 EZ 887.09/05 dated 2008-08-25 is an integral part of this certificate. The holder of a valid license certificate for the product tested is authorized to affix the test mark shown opposite to products when they are tested with the product tested.	
TÜV Rheinland Industrie Service GmbH Geschäftsfeld AGI Autobahn, Gefälle der Industriestadt 4th, Gussan Str., 51 135 H2 in Postfach 91 00 05, 51 101 H2 in	
20.08.2008 Datum/Date	Firmensiegel/Company seal
Dipl.-Ing. Stephan Hüb	

/ 06

总结&答疑

■ 课程总结



总结

ISO26262 在2017年中正式发布

- 描述汽车系统功能安全当前发展水平

ISO26262日前没有指令和法规的强制要求

- 不符合标准可能导致产品责任相关的问题

早期准备符合ISO26262是非常必要的

- 对于产品设计、开发、生产所有方面有大量的

ISO 26262-总结

功能安全管理

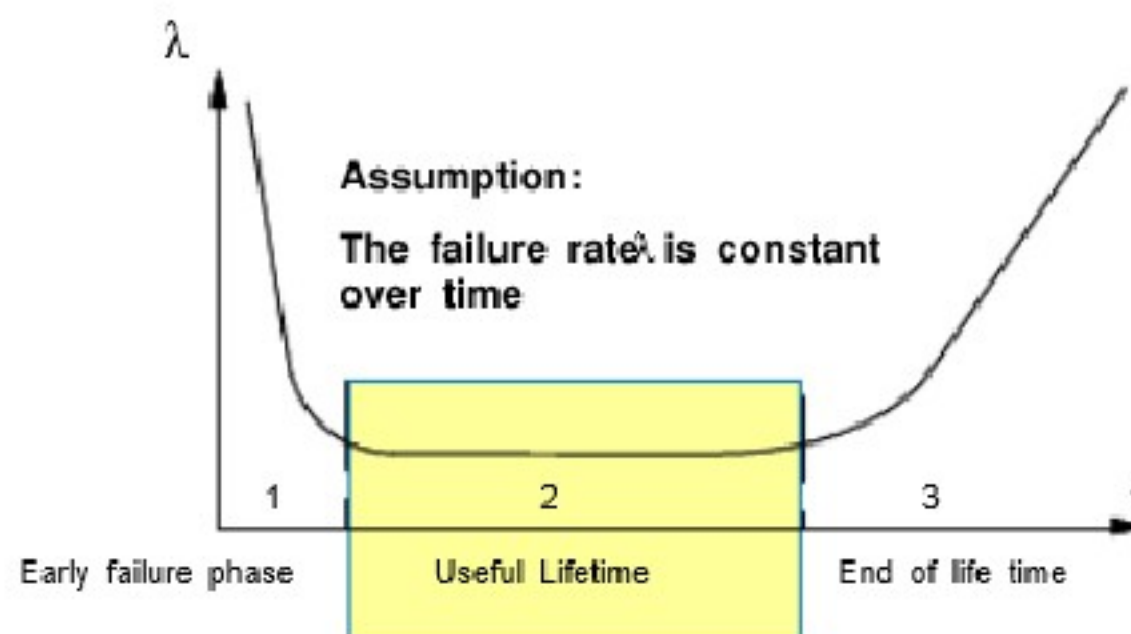
- 安全组织机构的管理
- 人员资质的要求
- 安全文化是必要的

技术要求

- 随机硬件失效，架构指标
- 系统失效
- 软件开发需求

生产和操作要求

- 生产控制、质量确保
- 现场反馈监控、持续改进



Thanks



2020.3.14