

ISO/DIS 26262

道路车辆—功能安全

赵斌

莱茵检测认证服务（中国）有限公司

电话: +86-10-65666660-104 传真: +86-10-6566 6667

电邮: bin.zhao@bj.chn.tuv.com 网址: www.chn.tuv.com



■ 议程

- 背景介绍
 - TUV莱茵集团及功能安全业务介绍
 - 车辆行业功能安全应用目的
 - 法律法规背景介绍
 - ISO 26262背景介绍
 - 基本定义
 - 如何根据ISO26262开发安全产品
- 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
- 系统开发
 - 系统级开发
 - 硬件开发
 - 软件开发
- 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
- 认证流程
- 总结



TUV莱茵集团及功能安全业务介绍



■ TÜV Rheinland Group – 全球服务



做为国际知名的跨国集团，我们提供质量、安全评估认证服务

- 成立于 1872
- 62个国家360个地区
- 员工超过 14,000
- 销售额1.2亿欧元
- 6 大业务领域
- 38个业务分支，超过2.500种不同的服务。



■ 德国莱茵TÜV大中华区



1988
TÜV莱茵香港

1993
TÜV莱茵深圳



1994
TÜV莱茵广州

2001
TÜV莱茵青岛



2007
TÜV莱茵无锡



1986
TÜV莱茵台湾

1989
TÜV莱茵上海



1995
TÜV莱茵北京

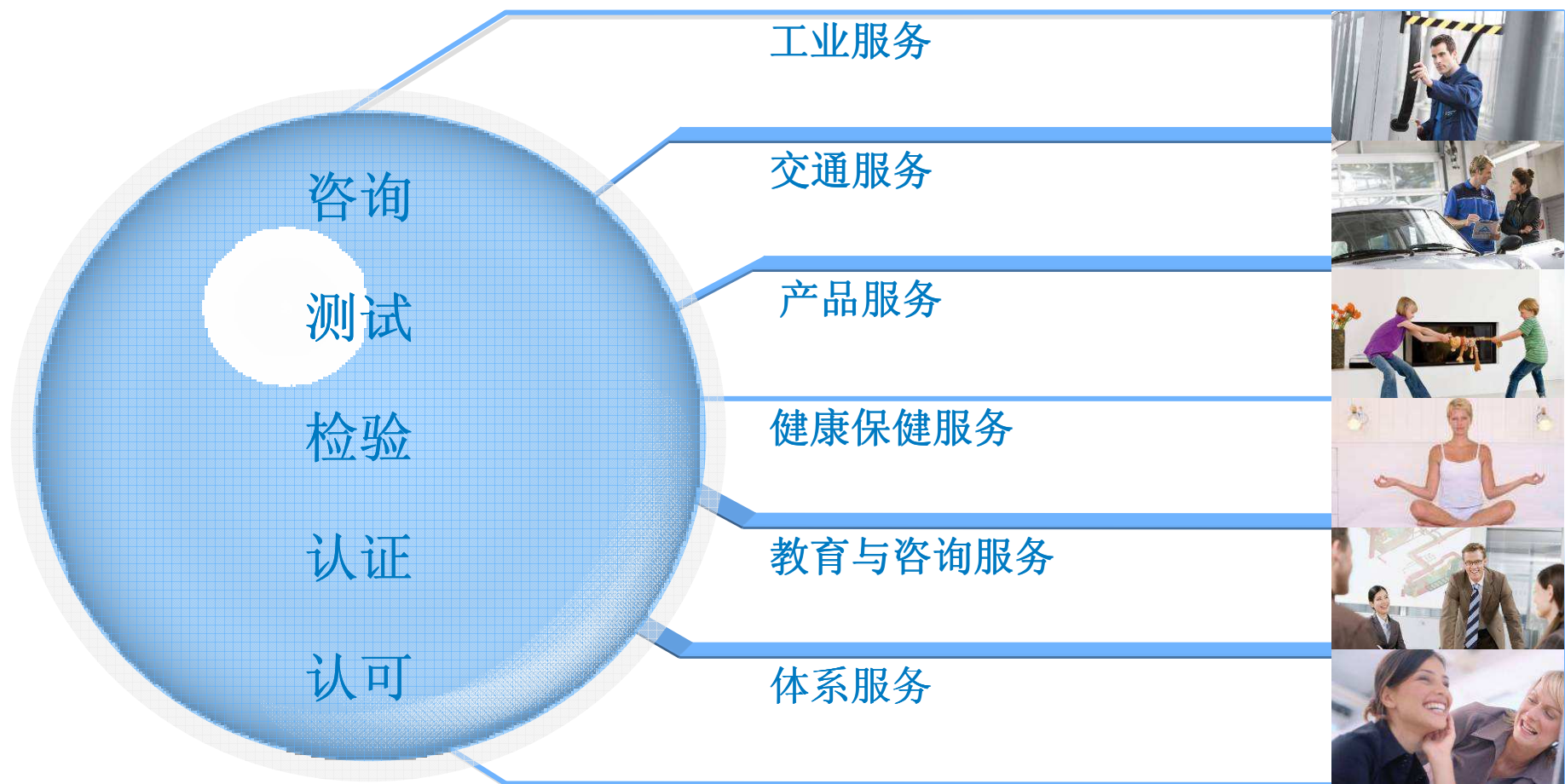
2002
TÜV莱茵宁波



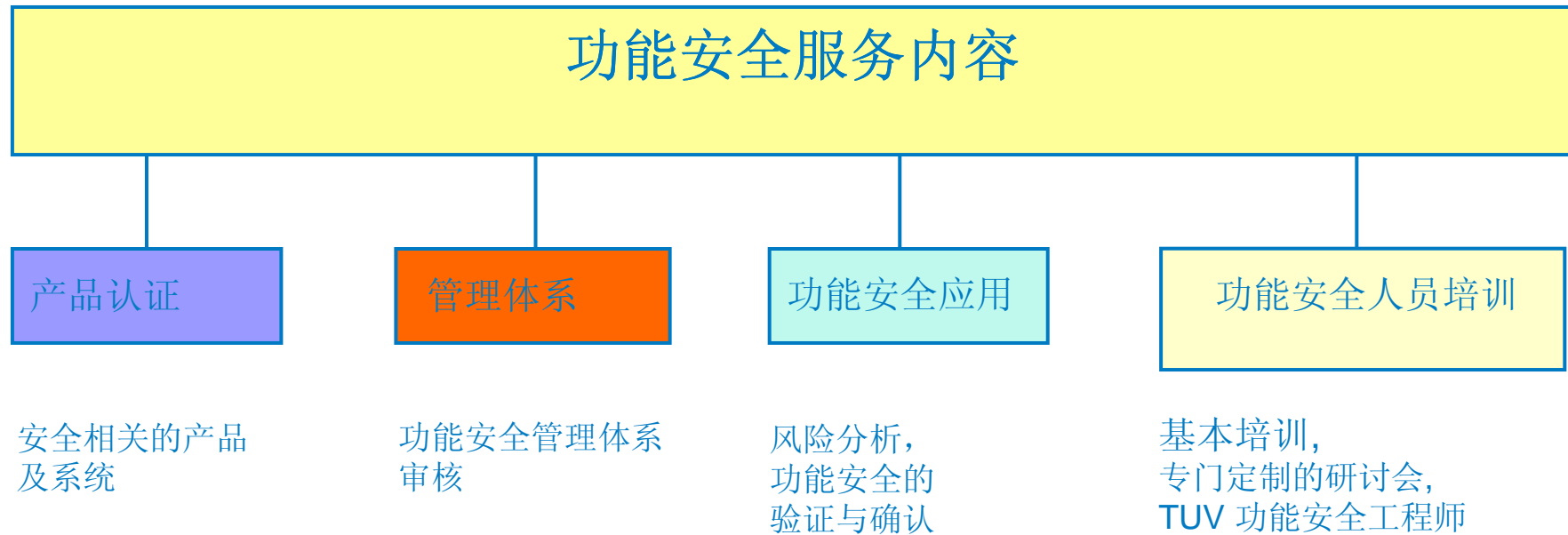
2007
台湾杜夫莱茵



■ 我们一直专注于安全和质量



■ 德国莱茵TÜV集团功能安全服务内容



■ 我们的服务

咨询

- 功能安全相关要求

测试 / 分析

- 形式认证
- 软件测试 (应用软件、编译器)
- 环境测试
(温度、气候、机械稳定性、电磁兼容等)
- 安全相关的可靠性数值计算
- 失效模式及有效性分析 (FMEA)

认证

- 产品认证并加贴标识
- 功能安全管理

培训 / 研讨会

- 企业内部培训
- TÜV 功能安全程序 (TÜV Functional Safety Program)
- 根据客户需要制定的研讨会 (针对产品、体系等)



■ TÜV 功能安全计划 (TÜV Functional Safety Program)

TÜV功能安全计划 是功能安全领域人员资格认证计划，课程由国际相关课程提供者组织，主要课程如下：

- 安全仪表系统(IEC61511)
- 软硬件设计(IEC61508)
- 机械功能安全 (IEC62061,ISO13849)
- 道路车辆功能安全 (ISO26262)
- 管理，销售，市场人员培训.

根据参与者的工作领域及经验，可以获得以下两种资格

TÜV 功能安全工程师

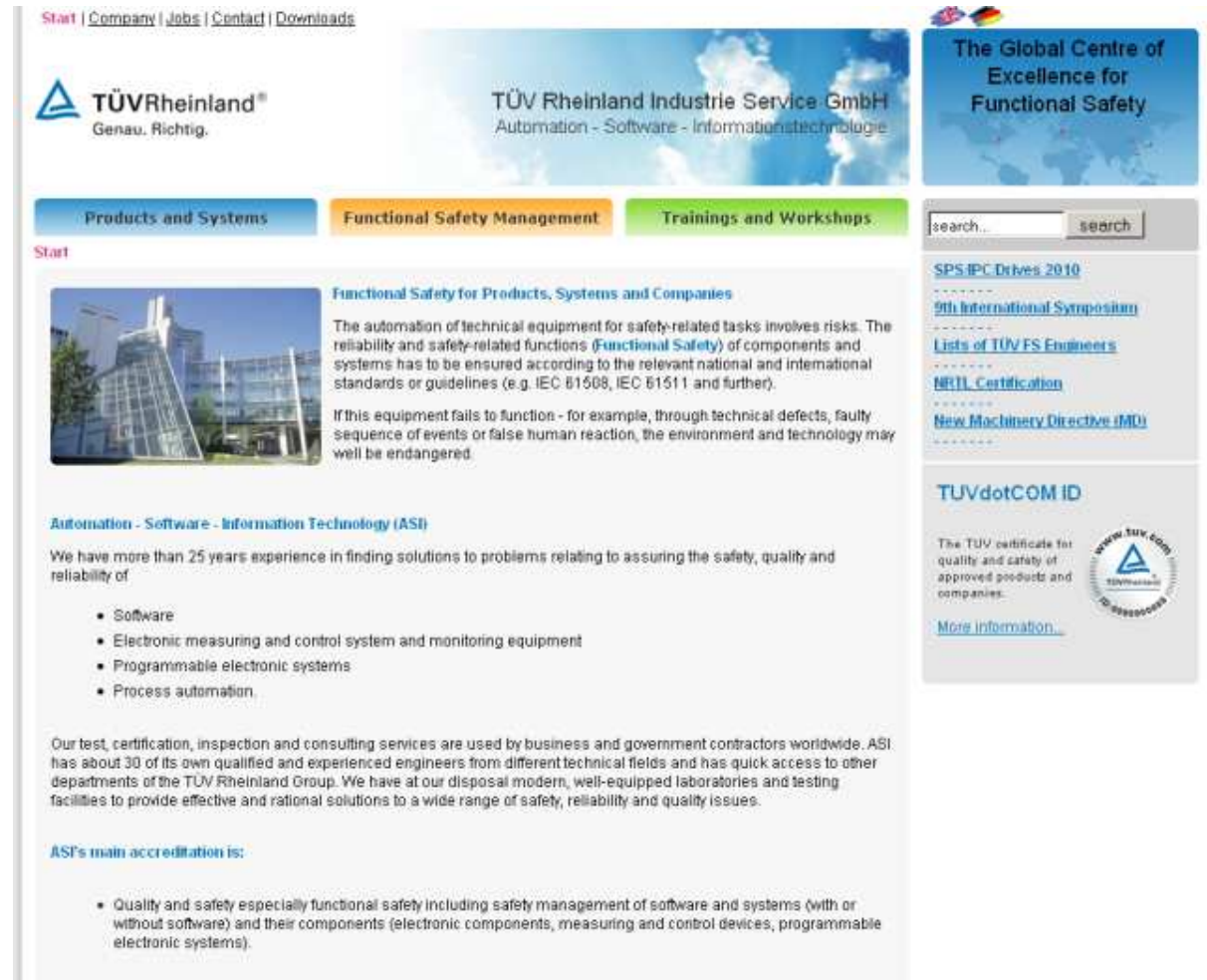


TÜV 功能安全专家



了解进一步信息

www.tuvasi.com



The screenshot displays the TÜV Rheinland website's Functional Safety section. The header includes navigation links (Start, Company, Jobs, Contact, Downloads) and the company logo with the tagline 'Genau. Richtig.'. The main navigation bar highlights 'Functional Safety Management'. The content area features a section titled 'Functional Safety for Products, Systems and Companies' with a photograph of a modern building. Text describes the risks of automation and the importance of functional safety, citing standards like IEC 61508 and IEC 61511. Below this, the 'Automation - Software - Information Technology (ASI)' section states the company's 25+ years of experience and lists services: Software, Electronic measuring and control system and monitoring equipment, Programmable electronic systems, and Process automation. It also mentions global test, certification, inspection, and consulting services. A sidebar on the right contains a search bar, links to 'SPS IPC Drives 2010', '9th International Symposium', 'Lists of TÜV FS Engineers', 'NFIL Certification', and 'New Machinery Directive (MD)', as well as 'TUVdotCOM ID' information and a circular logo.



■ 任重而道远



车辆行业功能安全应用目的



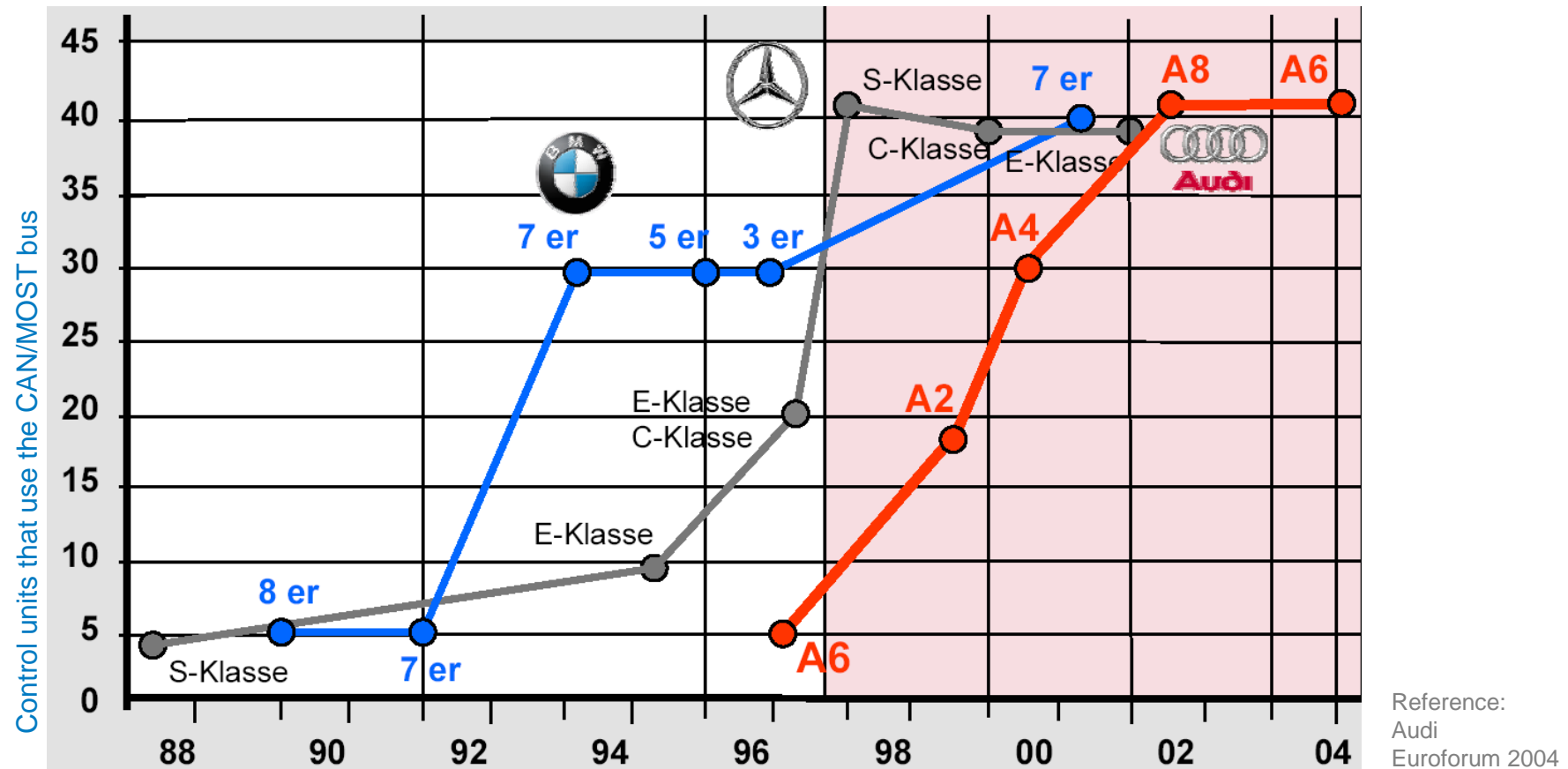
■ 安全, 法规, 产品责任, ...

汽车电子的安全问题可能会导致高额的召回费用

- 2010: 丰田召回几百万的车辆, 由于汽车油门踏板故障
- 2010: 丰田召回超过300, 000 普瑞斯, 由于潜在刹车问题
- 2010: 尼桑召回超过500, 000车辆, 用于刹车和油量表问题
- 2009: 奥迪召回超过10, 000 车辆, 由于传输控制问题

■ 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



■ 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

Adaptive front lights
Anti-locking braking system
Vehicle stability control
Traction control
Electronic brake force distribution
Emergency brake assist
Collision prevention
Lane departure warning system
Adaptive power steering
Parking assistant

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

■ 安全功能举例

Adaptive suspension control

Electronic brake system

Seat-belt pre-tensioning

Airbags

Driver drowsiness detection

Driver monitoring system

Adaptive high beam (lights) assistant

Adaptive cruise control

Autonomous cruise control

Tire pressure monitoring system

Automatic front light height adjustment

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

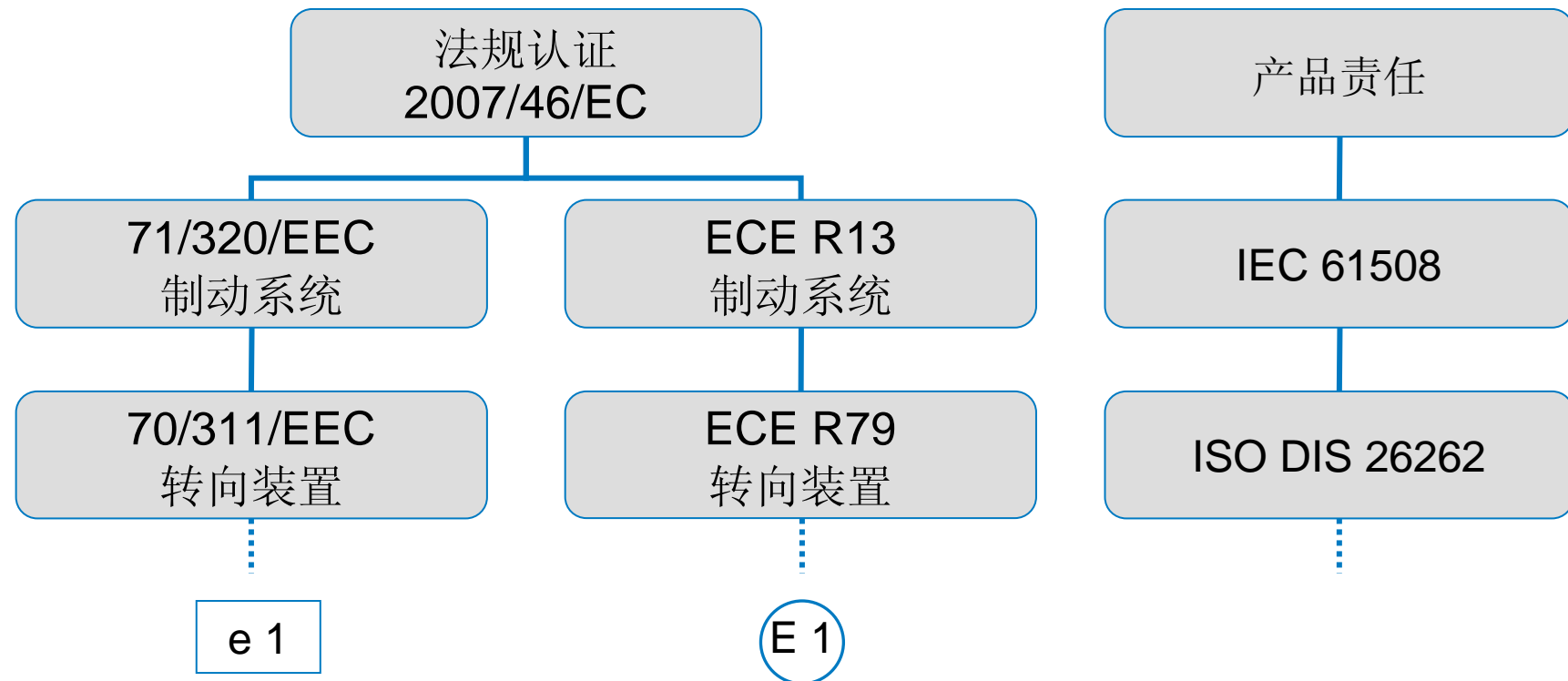
胎压监控系统

自适应前灯高度调节

功能安全法律法规背景介绍



■ 法规认证 vs. 产品责任 (1)



■ 法规认证 vs. 产品责任 (2)

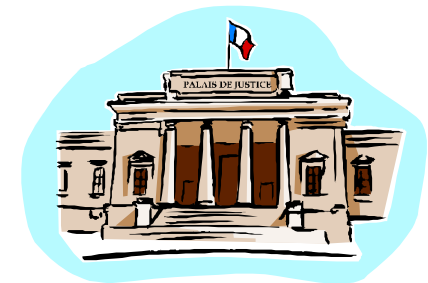
法规认证

- 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
 - **IEC 61508**
 - **ISO DIS 26262**



为什么使用这两个标准？

ISO26262背景介绍



■ ISO/DIS 26262 – 道路车辆 – 功能安全

IEC 61508 – 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/DIS 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
 - ...

■ ISO/DIS 26262范围

ISO/DIS 26262 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/DIS 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

ISO/DIS 26262 不应用于非安全相关的电子电气系统。

Q?

什么是乘用车？

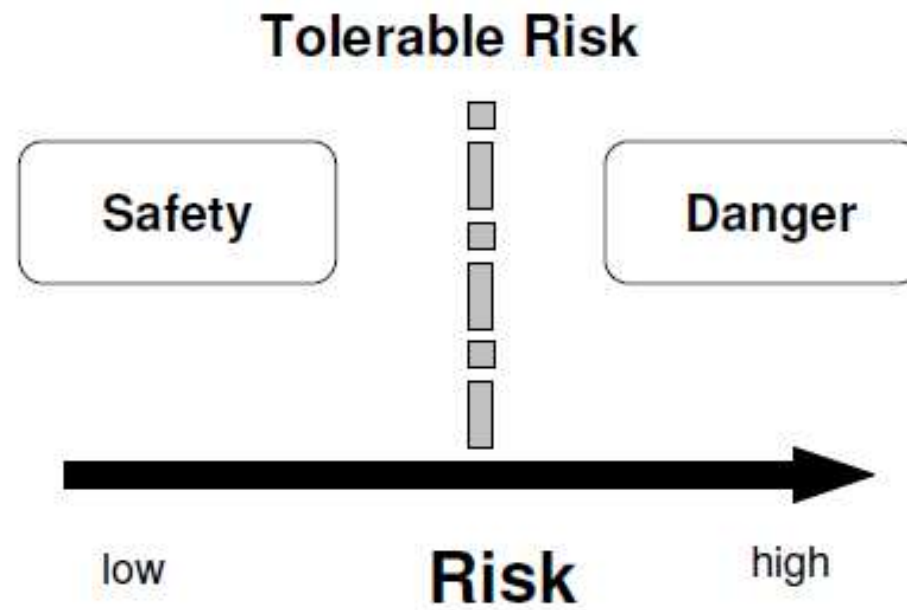


■ 基本定义

■ 什么是安全？

安全???

■ 达到什么程度才算安全？



■ 功能安全

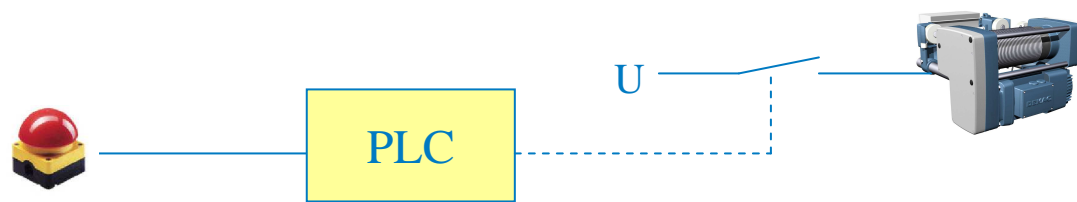
满足下列条件，安全系统是符合功能安全的：

- 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

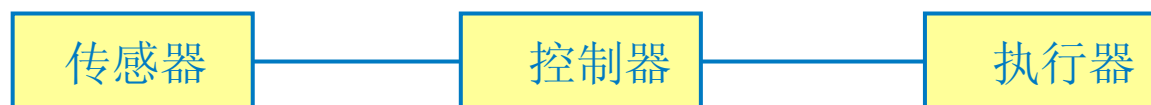
在正常条件及存在故障条件下，控制设备、系统的安全功能必须都能够保证

■ 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



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



■ 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

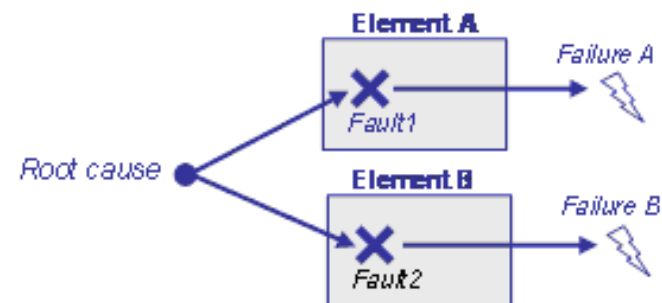
能够警告司机，以便于司机能够及时采取措施避免失效的影响

■ 级联失效和共因失效

级联失效

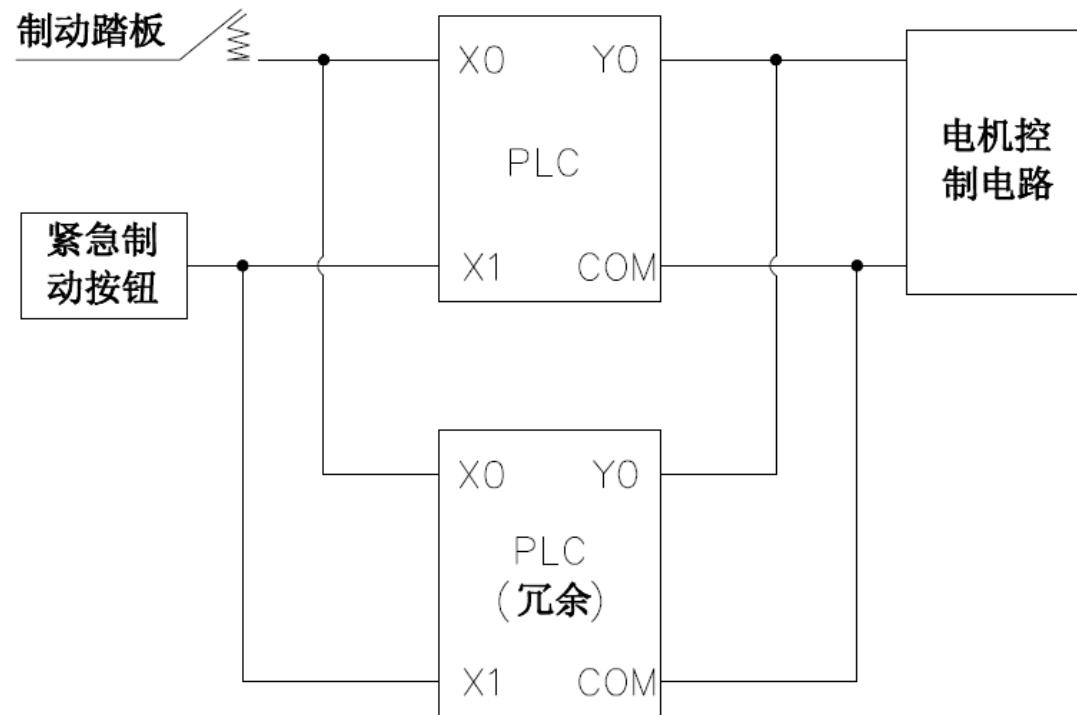


共因失效



■ 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



■ 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**ISO 26262**开发安全产品？



■ 功能安全：5个步骤实现

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**

Step 1

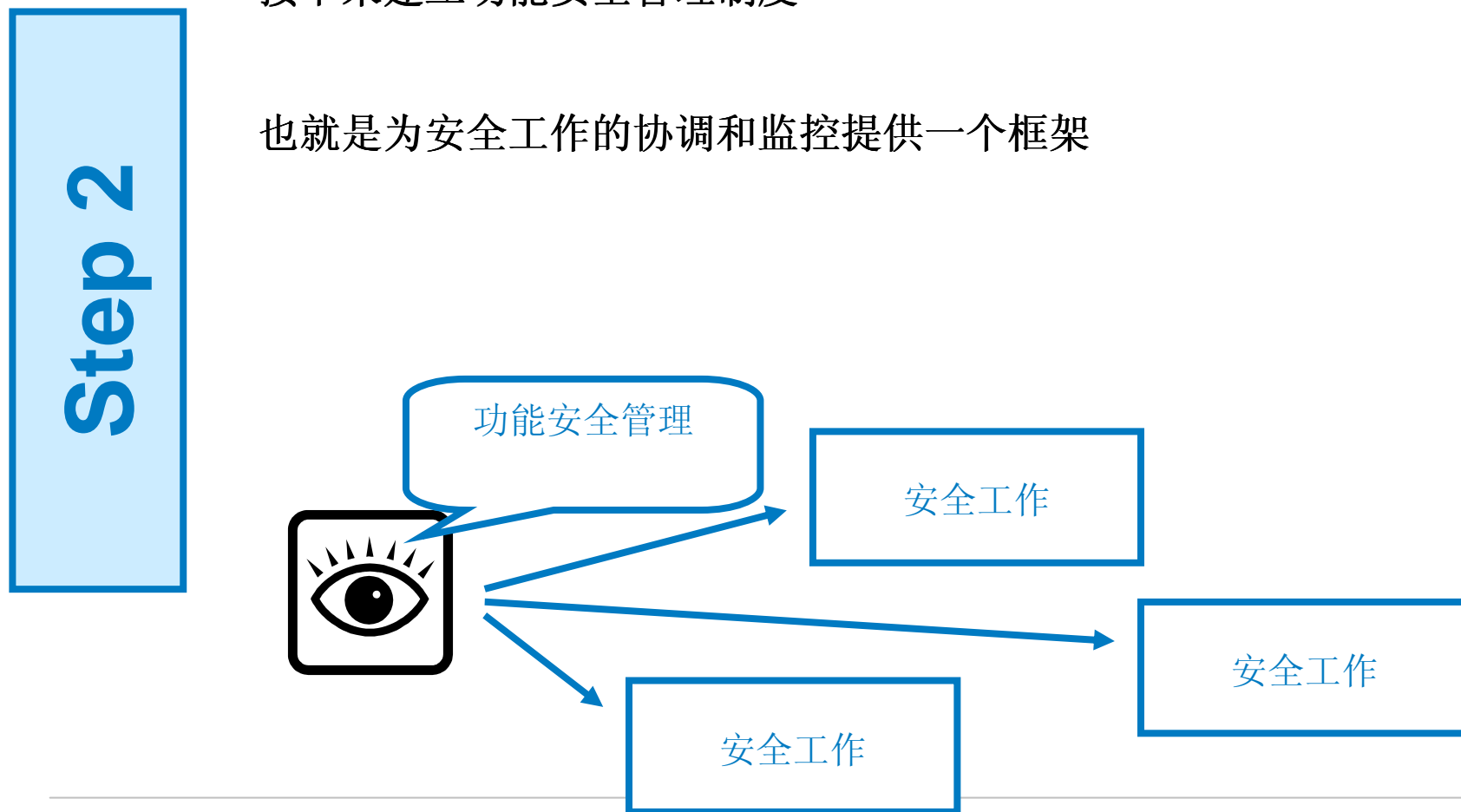


需要安全功能吗？

■ 功能安全：5个步骤实现

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



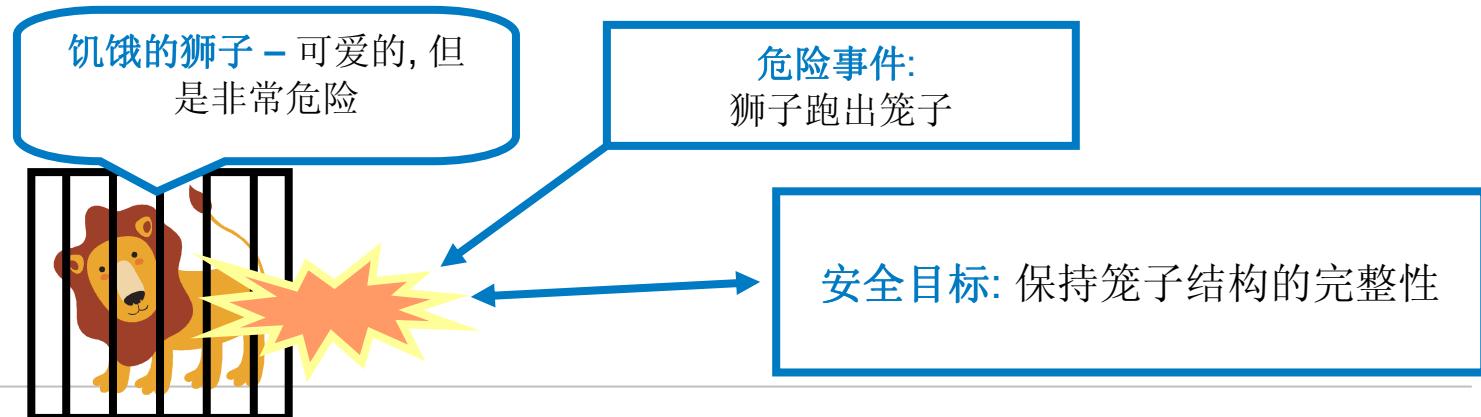
■ 功能安全：5个步骤实现

通过危险分析和风险评估来确认哪些危险事件应该考虑

Step 3

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



■ 功能安全：5个步骤实现

Step 4

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

■ 功能安全：5个步骤实现

Step 5

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。

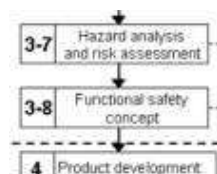
功能安全管理



■ 功能安全管理

ISO/DIS 26262-2

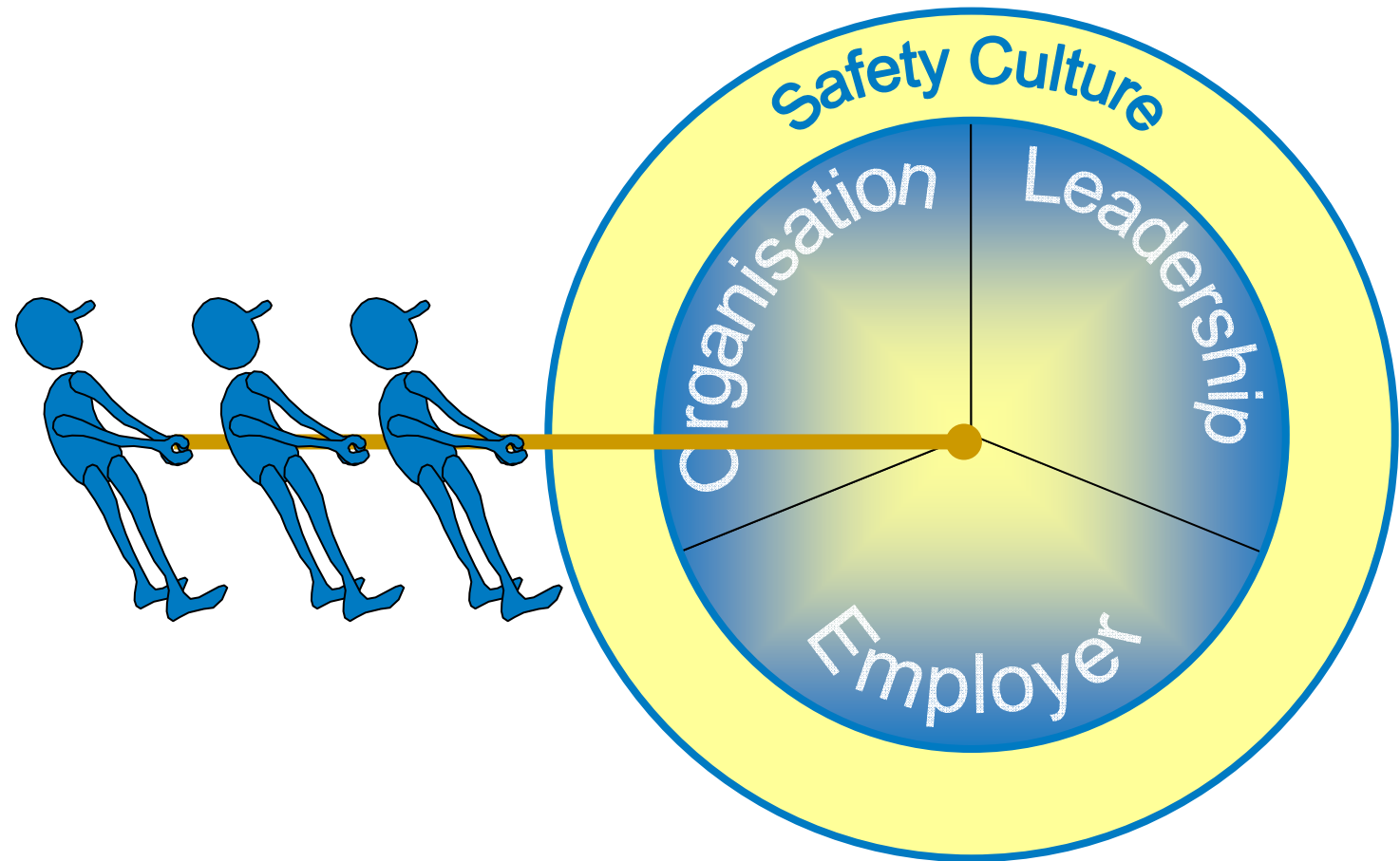
安全管理:



- 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



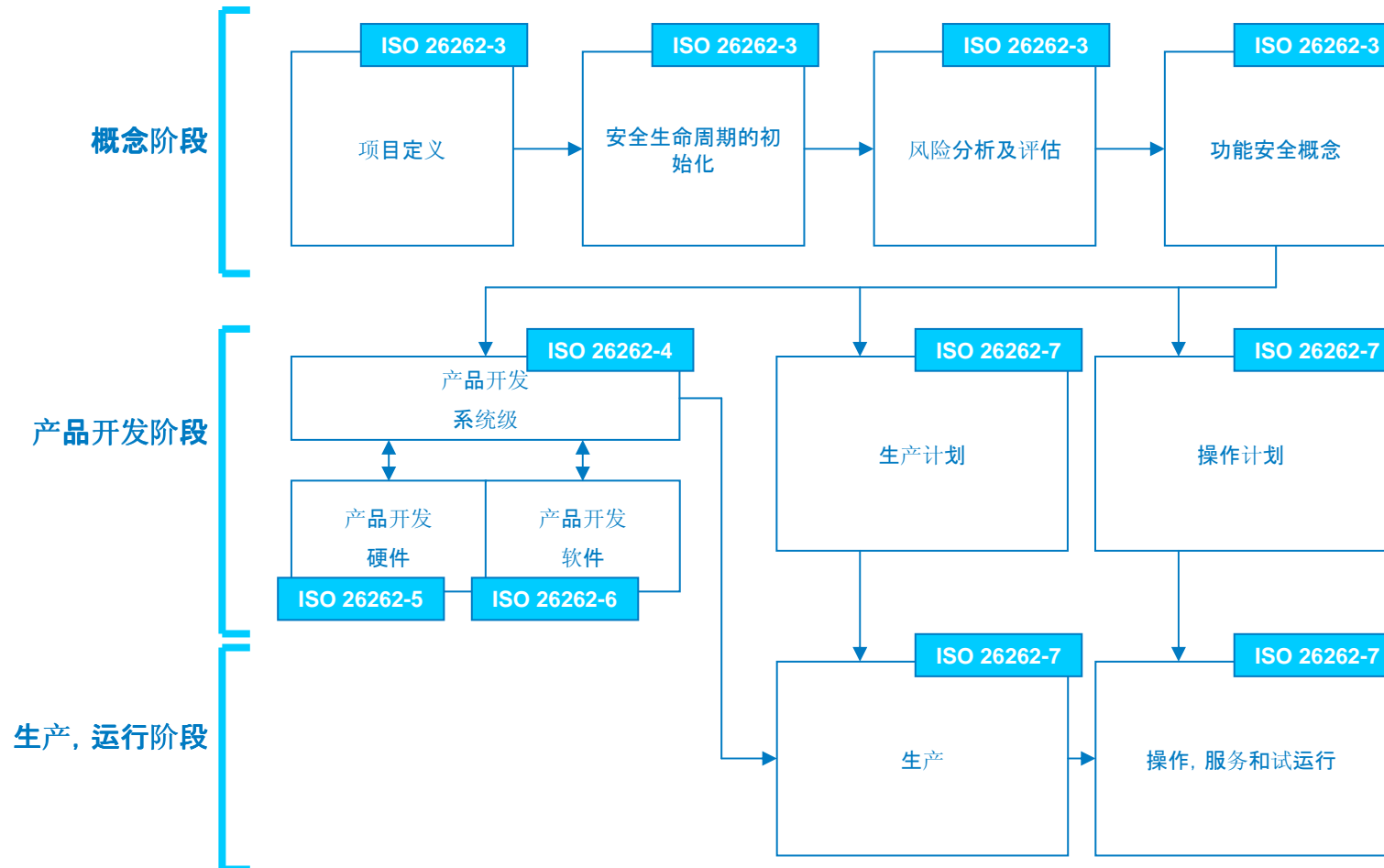
■ 功能安全需要做什么



■ 开发阶段安全生命周期模型



■ ISO/DIS 26262 – 安全生命周期模型



项目定义

■ 项目和其他相关概念

ISO/DIS 26262-10 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 **Item definition** 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

ISO/DIS 26262-3 Clause 5

在项目定义过程中，必须考虑所有相关需求

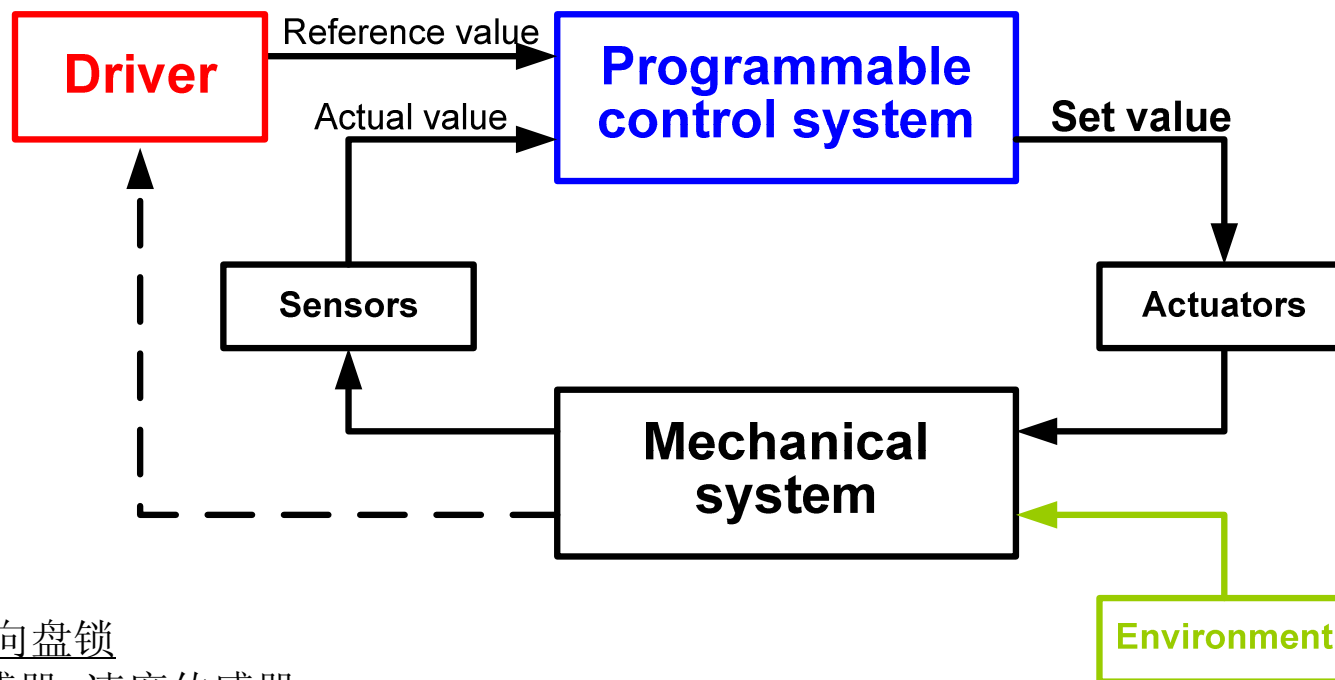
- 功能性的需求
- 非功能性需求 (费用, 尺寸, 环境要求, ASIL...)
- 法规要求
- 标准, 导则

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

■ 项目定义

ISO/DIS 26262-3 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

危险分析、风险评估和安全目标

■ 执行危险分析和风险评估

ISO/DIS 26262-3, 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

安全目标应确保项目的运行风险低至可以接受。

■ 汽车领域项目基本流程

ISO/DIS 26262-3, clause 7; ISO/DIS 26262-3, annex B



■ 车辆安全完整性等级评估(4)

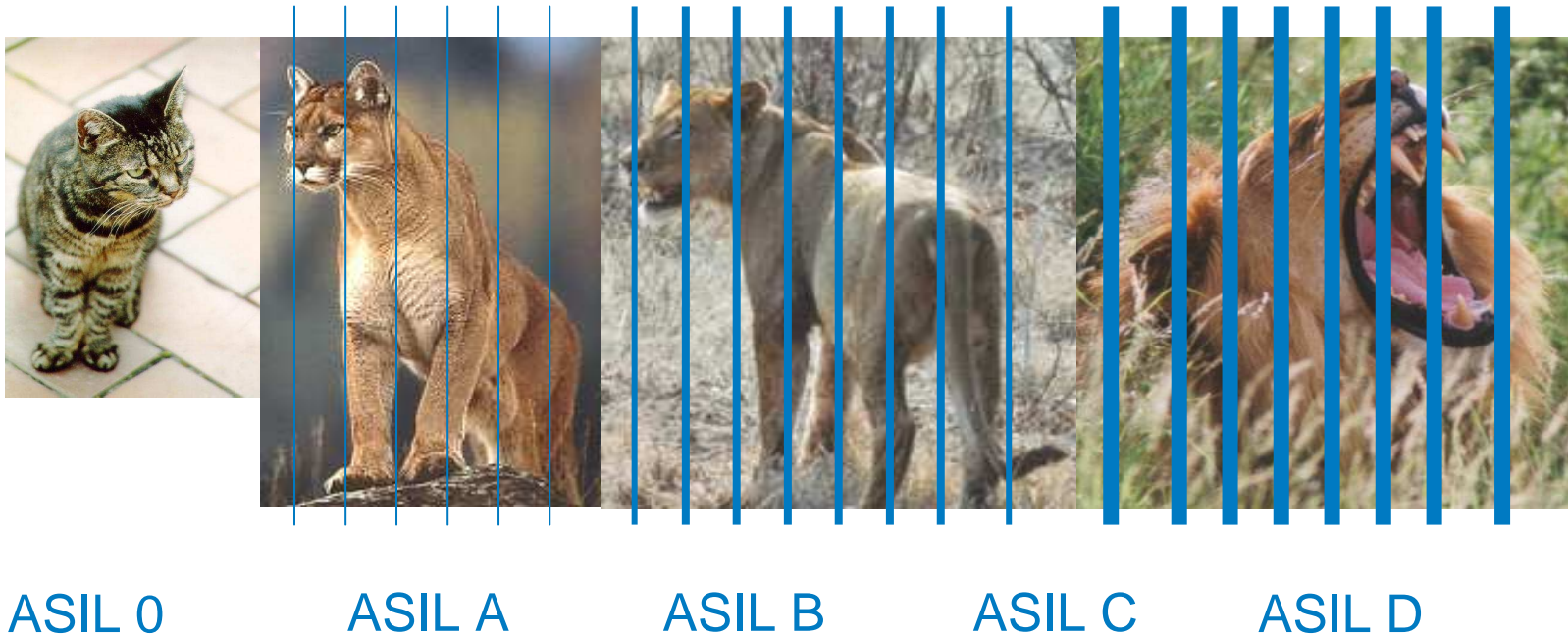
S: 严重性

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

■ 车辆安全完整性等级



■ 汽车安全完整性等级举例

TSR – 交通标识识别

- 正确识别: QM or ASIL A

电磁方向盘锁定系统

- 驾驶时防止锁定: ASIL D

安全气囊

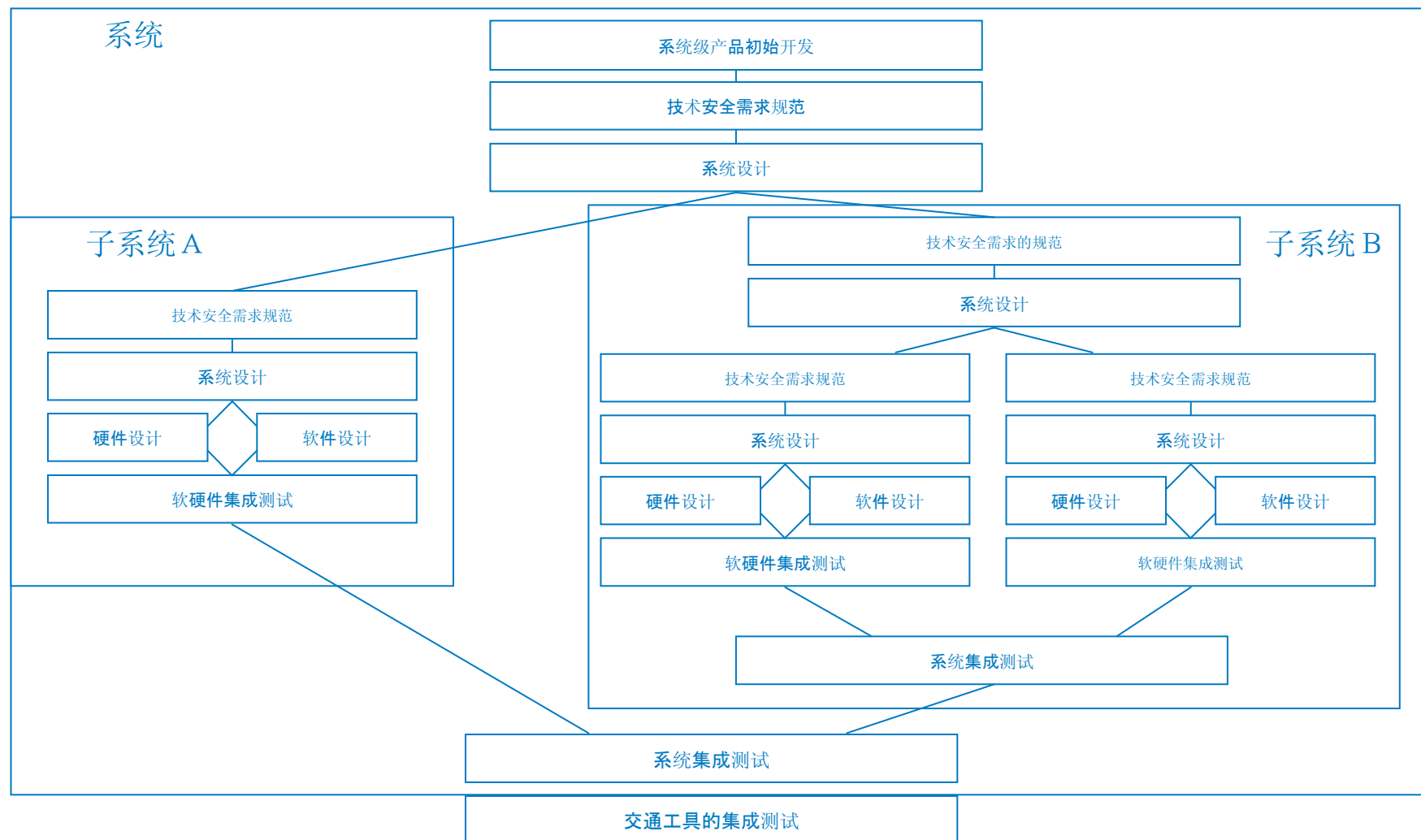
- 需要时打开安全气囊: ASIL A
- 不需要时不能打开气囊: ASIL D

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。

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

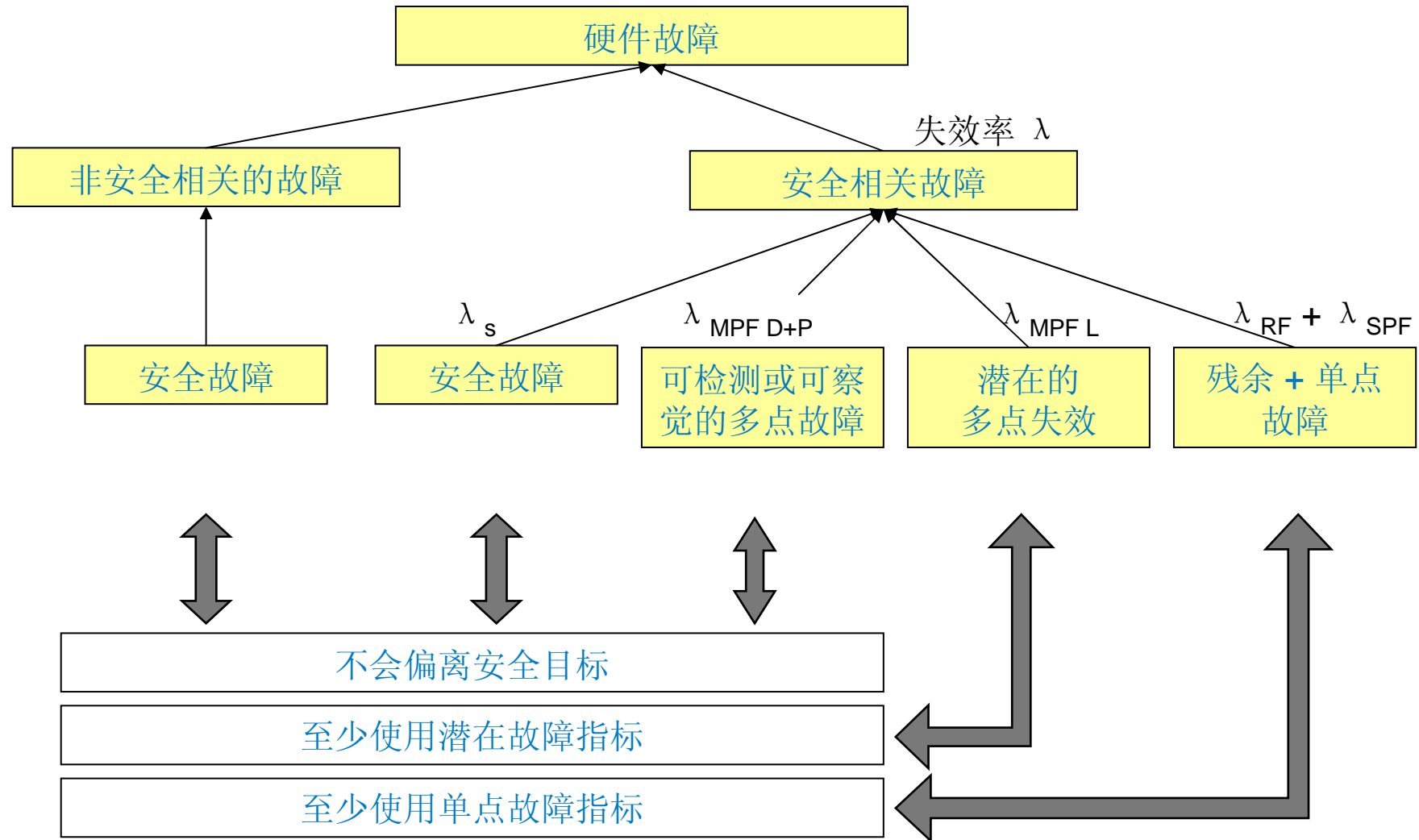


■ 硬件安全需求规范

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

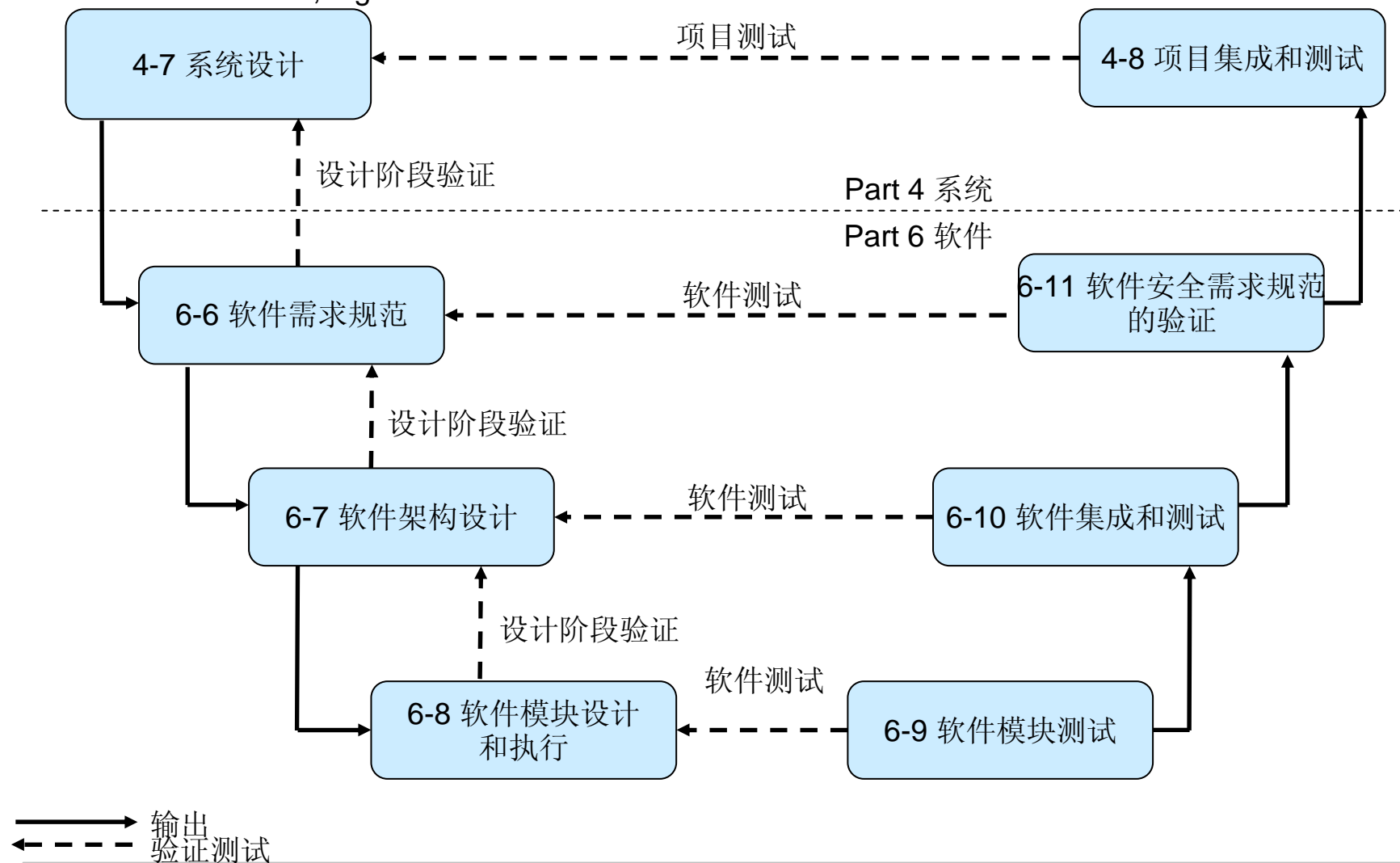


■ 讨论: 软件设计时会遇到什么问题?

- 不同的开发人员有不同的编码观点和方式
- 高复杂性:
 - 接口
 - 算法
 - 诊断
 -
- 软件实现比硬件实现更便宜
- 配置管理/版本控制
- 与开发、验证工具高度相关
- 对于每个工具的使用, 开发人员都需要受到培训
- 完整的并且易理解相关文档
- 软件可以持续更改

■ 软件开发 V 模型

ISO/DIS 26262-6, Figure 2



安全分析、安全确认与安全论证

■ 安全分析

ISO/DIS 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

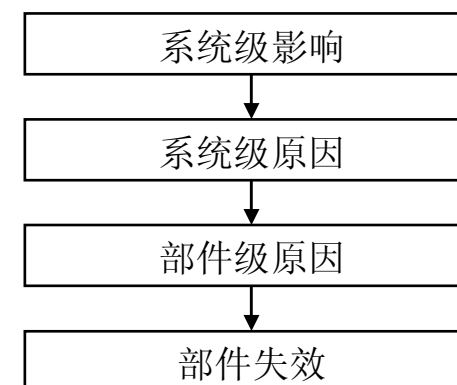
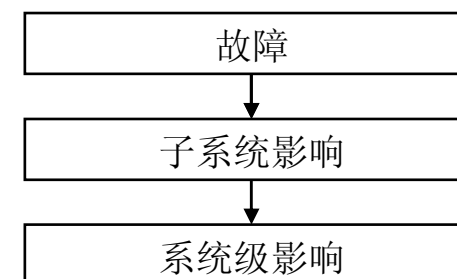
ISO/DIS 26262-9 Section 8

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 (FMEA)
- 故障树分析 (FTA)
- 马尔可夫模型
- 可靠性框图



■ 安全确认

ISO/DIS 26262-4 Clause 9

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

■ 什么是安全论证?

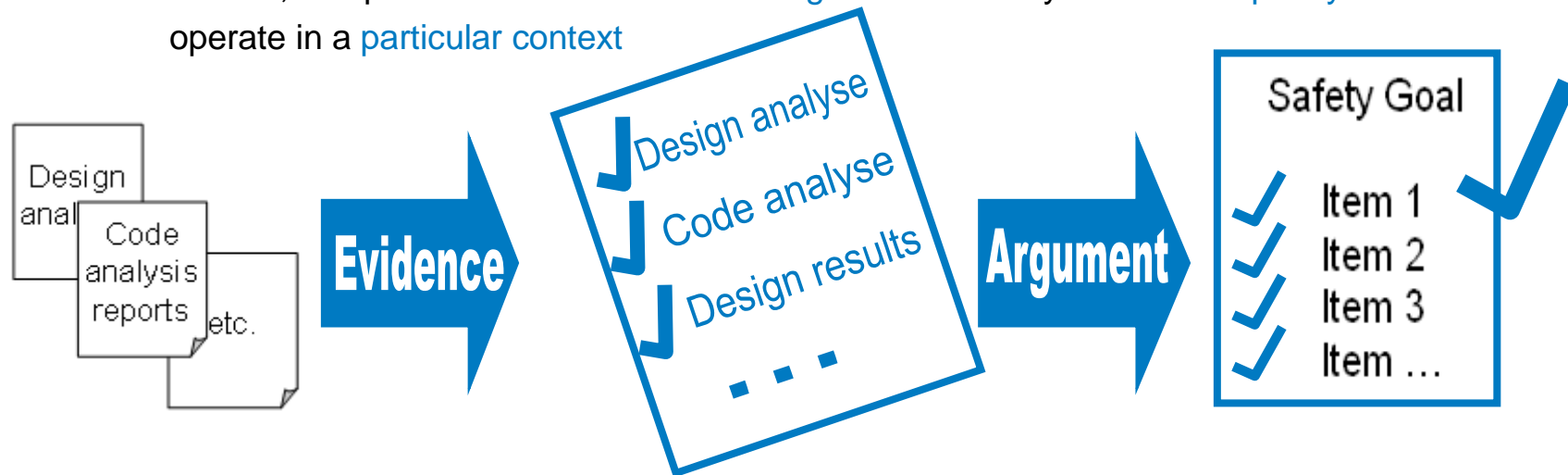
ISO/DIS 26262-2, 6.4.5

ISO 26262-1, 1.103

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

通常说法^[1] 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
A clear, comprehensive and defensible **argument** that a system is **acceptably safe** to operate in a **particular context**



[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

ISO/DIS 26262-2 Table 1

I0, I1, I2, I3 说明独立性水平



证明措施			ASIL			
Type	Target	A	B	C	D	
复核	危险分析和风险评估	I3	I3	I3	I3	
复核	安全计划	—	I1	I2	I3	
复核	集成和测试计划	I0	I1	I2	I2	
复核	确认计划	I0	I1	I2	I2	
复核	安全分析 (FMEA, FTA, ...)	I1	I1	I2	I3	
复核	软件工具的考核	—	I0	I1	I1	
复核	预先使用的论证	I0	I1	I2	I3	
复核	安全论证的完成	I0	I1	I2	I3	
审核	功能安全过程	—	I0	I2	I3	
评估	功能安全评估	—	I0	I2	I3	

■ 第三方功能安全评估

为了增加项目符合**ISO 26262** 的可信度，可以由第三方评审人员做功能安全评估

对**ASIL C** 和 **ASIL D**，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：

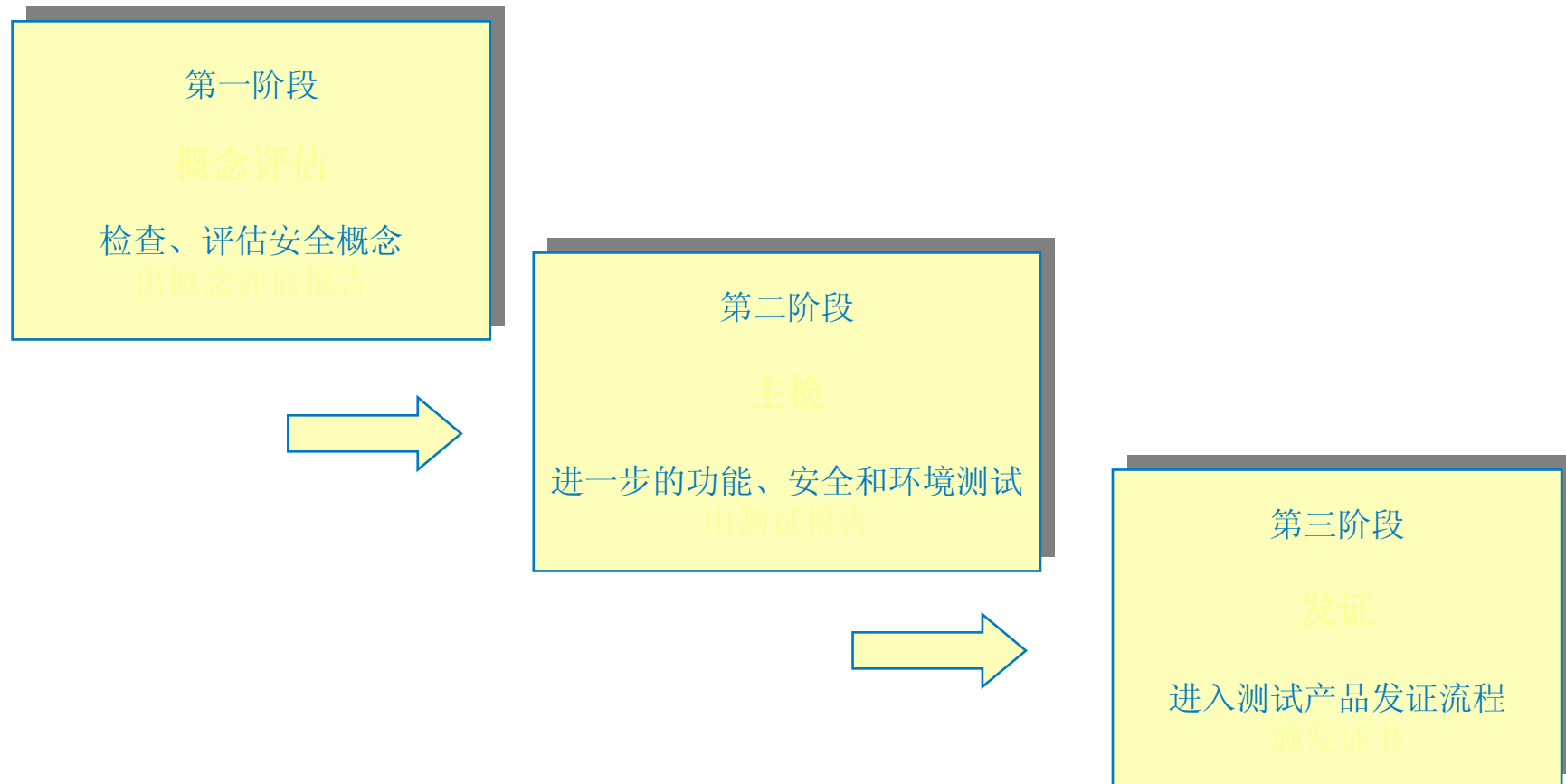
- 另一种角度
- 功能安全评估专业知识
- 公司外的人力资源



认证流程



■ 认证与产品研发应该并行



■ 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. 968/EZ 897.00/08

Prüfgegenstand Product tested	Programmierbare Sicherheitssteuerung Programmable Safety Controller	Lizenznehmer License Holder	ZPOK Corp. Post code 318-0893 1-7 Kita-Huomay, Plokiropy Nowhere-City, Kichina China
Typbezeichnung Type designation	S-PLC - PCS-H Version 3.6.9	Verwendungszweck Intended application	Maschinensicherheit Anwendungen, in denen der energie-lose Zustand der sichere Zustand ist. Safety of machinery, applications, where the de-energised state is the safe state.
Prüfgrundlagen Codes and standards forming the basis of testing	IEC 61508:1998 & 2000 EN 954-1:1996 EN 62044-1:2006 NFPA 79:2007 (chapters 4.4, 6, 9.4.3) UL 1998:2004 (Revision 4/5/2004) EN ISO 13849-1:2006 EN ISO 13849-2:2003 EN 50178:1997		
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 eingesetzt 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 Specific requirements	Die Hinweise in der Bedienungsanleitung sind zu beachten. The information provided in the instruction manual must be considered.		



Der Prüfbericht-Nr.: 968/EZ 897.00/08 vom 29.08.2008 ist Bestandteil dieses Zertifikates.
 Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.
 The test report no.: 968/EZ 897.00/08 dated 2008-08-29 is an integral part of this certificate.
 The holder of a valid licence certificate for the product tested is authorised to affix the test mark shown opposite to products which are identical with the product tested.

29.08.2008
 Datum/Date

TÜV Rheinland Industrie Service GmbH
 Geschäftsfeld ASI
 Automation, Software und Informationstechnologie
 Am Grauen Stein, 51105 Köln
 Postfach 91 00 51, 51101 Köln


 Dipl.-Ing. Stephan Hab



总结



■ ISO 26262 – 总结



ISO 26262 将在2011年中正式发布

- 描述汽车系统功能安全当前发展水平

ISO 26262 目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ISO 26262 是非常必要的

- 对于产品设计、开发、生产所有方面有大量的要求

■ ISO 26262 – 总结

功能安全管理

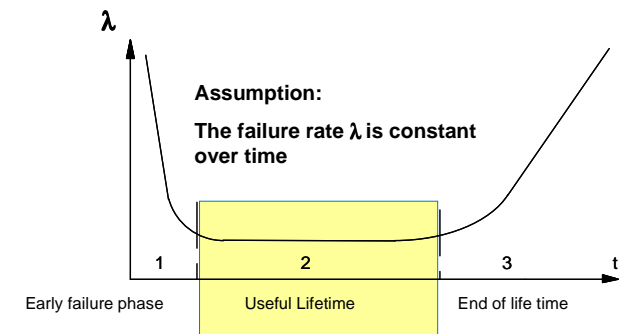
- 安全组织机构的管理
- 人员资质的要求
- 安全文化是必要的

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



Any question???

