FSG（功能安全专家小组）

FSG Functional Safety Group

FSG（功能安全专家小组）是一个专门研究嵌入式功能安全的专家组织，汇集了在功能安全认证领域提供专业知识、封装方案和开发资源的顶尖企业。FSG提供功能安全相关的一站式服务，包括从功能安全标准的解读，到具体实施方案的制定，再到认证过程的全程指导，确保客户的产品在满足最高安全标准的同时，能够高效地推向市场。

我们随时准备根据您的需求提供帮助，共同推进功能安全技术的发展和应用。

FSG中国成员：

CETC 普华基础软件　iar　MUNIK　芯来科技 NUCLEI　NXP　PARASOFT　RENESAS 瑞萨

欧盟新机械法规下的海外出口影响和应对

机械法规REGULATION (EU) 2023/1230
和Ai ACT Regulation (EU) 2024/1689

Better Tech for Better Future

MUNIK

秒尼科技术服务有限公司

作为各类工业行业中专业的技术服务公司，MUNIK 主要面向汽车产业及相关半导体行业提供基于ISO 26262、IEC 61508、ISO 13849等功能安全标准的培训、咨询、辅导、预审核及评估等专业技术服务。我们的技术专家团队有汽车电子、芯片开发、功能安全、机械电气安全认证的专业背景，核心骨干由两名博士带队，与DEKRA德凯、TUV、CSA等权威第三方认证公司有广泛深入的合作，能够向客户提供从差距分析，到标准工程实施咨询，再到开发流程体系建设及产品认证、法规标准技术服务的全栈式解决方案。

公司部分核心成员曾在国际最大的第三方认证机构，从事电气安全、机械安全、功能安全业务线能力建设、技术管理等工作。**是国内最早从事AGV及机器人SIL认证、CE认证、北美认证一站式解决方案的技术团队。**曾为杭州海康机器人、上海仙工智能、深海柔创新、GEEK+、KUKA、优艾智合、沈阳新松、北京珞石等提供专业认证服务。

2019 年，我们从上海出发，带着“客户至上、专业引领、诚信为先、互利共赢”的初心，深耕功能安全、网络安全与软件质量领域。如今，上海总部联动西安、深圳子公司，辐射长三角、珠三角与中西部，用本地化团队的快速响应与全国资源的灵活调配，为每一位客户送去“家门口”的专业服务。

作为专业技术服务公司，我们是一个专业又充满激情和活力的团队，也希望有志之士加入我们，带来新鲜的思维和创新的力量，共创辉煌。

Better Tech for Better Future

MUNIK

新机械法规出台背景

发展历程

1973 年 首版机械安全指令 (73/123/EEC)

2006 年 修订为 2006/42/EC 指令

2023 年 升级为 REGULATION (EU) 2023/1230 (法规级别)

修订动因

1. 原有指令在产品覆盖范围存在不足
2. 数字技术发展带来新安全挑战（AI、物联网等）
3. 市场监管需求加强，需统一合规标准

> *"The social cost of the large number of accidents caused directly by the use of machinery can be reduced by inherently safe design and construction..."*

法规出台背景

欧盟工业机械制造场景

旧指令的不足

2006/42/EC 指令存在产品覆盖和合规评估程序的不足，无法适应新技术发展

经济支柱需求

机械行业作为欧盟经济支柱，需要更完善的安全规范保障产业竞争力

数字技术挑战

AI、物联网、机器人等新技术带来新型安全风险，需针对性应对措施

统一标准需求

消除成员国间实施差异，建立统一标准消除贸易壁垒

EU法规体系简介

1

法律基础

基于《欧盟运作条约》第 114 条制定，确保内部市场协调统一

2

法规升级

取代2006/42/EC 指令，升级为法规形式提高法律执行力

3

市场监管协同

与Regulation (EU) 2019/1020 市场监管法规协同实施

4

统一框架

参考Decision No 768/2008/EC 建立统一产品营销框架

Regulation (EU) 2023/1230 简介

1

正式通过

2023年6月14日由欧洲议会和理事会正式通过

2

核心目标

协调机械产品的健康与安全要求，确保统一标准

3

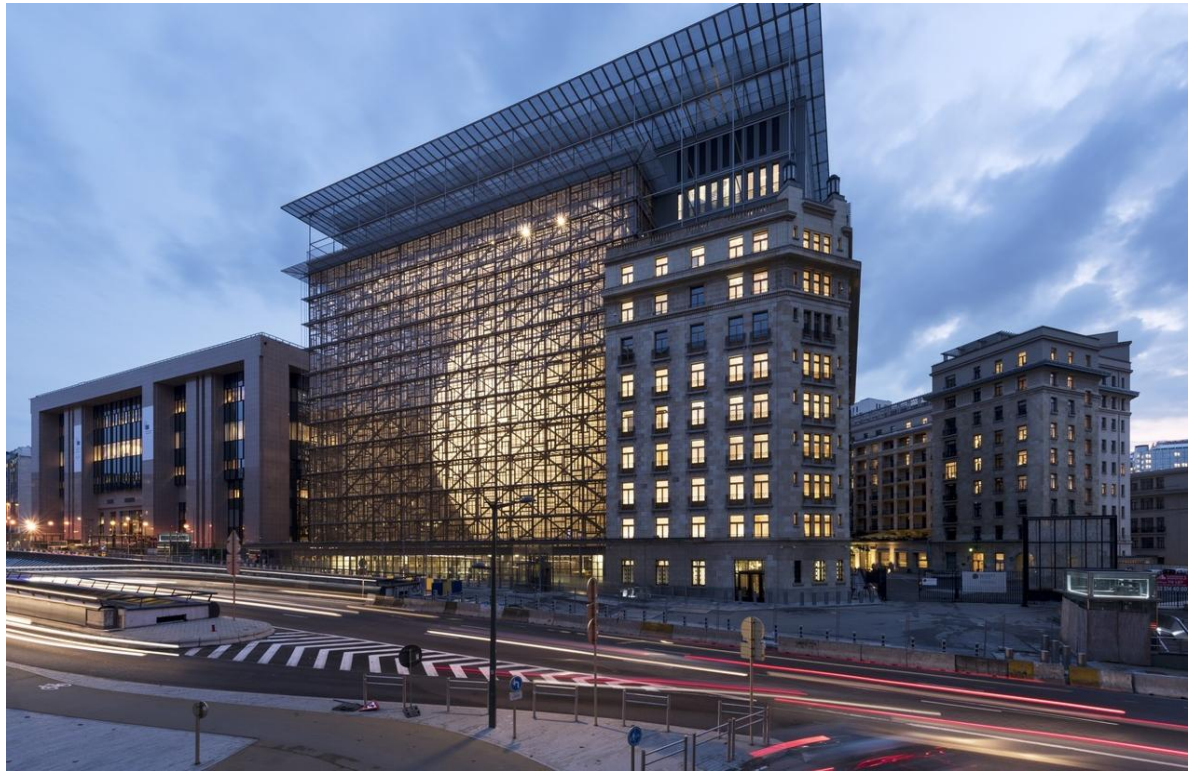
适用范围

适用于所有欧盟成员国及欧洲经济区 (EEA)地区

4

安全重点

关注机械的内在安全设计、正确安装和长期维护要求



与2006/42/EC 旧指令的对比

法律效力升级

从指令升级为法规，增强法律约束力和统一实施效力

覆盖范围扩大

纳入AI驱动机械、物联网设备等新型数字技术应用

评估程序简化

简化低风险产品自我声明流程，减少企业行政负担

市场监管强化

完善不合规产品处理机制，增强市场监督力度

与2006/42/EC旧指令对比

对比项目	2006/42/EC指令	2023/1230法规
法律层级	指令(需转化)	法规(直接适用)
数字技术	未明确覆盖	新增AI、网络安全要求
合规评估	8种模式	保留模式A-H，细化适用场景
市场监管	原则性规定	与2019/1020法规全面整合
技术文件	基本要求	强化电子文档与追溯要求

关键差异分析

1. 适用范围扩展：明确纳入软件作为安全组件
2. 责任划分细化：经济运营商义务更明确
3. 处罚措施强化：成员国需建立统一制裁机制

> *"Experience with the application of Directive 2006/42/EC has shown inadequacies and inconsistencies in the product coverage and conformity assessment procedures..."*

法规适用范围

✓包含产品

1. 机械（ Machinery ）
2. 相关产品（安全组件、起重配件等）
3. 部分完成的机械（ Partly completed machinery ）

排除产品

1. 武器及 firearms （受 EU 2021/555 指令管辖）
2. 主要用于运输人员 /货物的设备

机械

具有特定功能的可移动或固定设备组合

相关产品

包括可互换设备、安全组件、起重配件等

部分完成的机械

需进一步组装的机械系统

经济运营商

制造商、进口商、授权代表、经销商

关键术语定义精要

M 机械

具有特定功能的可移动或固定设备组合，通过非人力动力驱动执行特定操作

示例：加工设备、起重机械、输送系统等

R 相关产品

作为机械组成部分，对安全有重要影响且可单独投放市场的产品

示例：安全传感器、紧急停止装置、起重配件等

P 部分完成的机械

需进一步组装的机械系统，需附带技术文件和 EU 符合性声明

示例：未完成组装的机械框架、子系统组件等

E 经济运营商

在供应链中承担不同责任的主体，包括制造商、进口商、授权代表和经销商

示例：产品制造商、欧盟进口商、区域分销商等

机械产品类型介绍

1 按功能分类

加工机械（如数控机床）、起重机械（如起重机）、输送机械（如传送带系统）等。不同功能的机械针对特定工业流程设计，满足不同生产环节的需求。

2 按自动化程度

手动操作机械（需人工全程控制）、半自动机械（部分流程自动化）、全自动机械（完全自主运行）。自动化程度直接影响生产效率和人力需求。

3 按使用场景

工业用机械（工厂生产线）、农业用机械（收割机等）、消费用机械（家用电器）。不同场景对机械的安全性、耐用性和操作要求有显著差异。

4 新兴自主机械系统

具备AI学习能力的自主机械系统，能够根据环境变化自主决策和优化操作流程。这类系统代表了机械智能化的前沿发展方向。

相关产品及"部分完成的机械"定义

R 相关产品特征

1. 作为机械的组成部分，对机械安全有重要影响
2. 可单独投放市场（如安全传感器、紧急停止装置）
3. 需满足与整机相同的安全可靠性要求
4. 制造商需提供完整的技术文档和合规声明

P 部分完成的机械要求

1. 需附带技术文件和 EU 符合性声明
2. 提供明确的组装说明和安全要求
3. 最终组装者需承担产品合规责任
4. 必须包含风险评估和 CE 标志申请文件

安全开关 - 典型的相关产品示例

部分完成的机械组件示例

经济运营方义务概述

制造商

1. 设计和生产符合安全要求的产品
2. 进行风险评估并保留技术文件
3. 起草EU符合性声明并加贴CE标志

进口商

1. 确保进口产品符合欧盟法规要求
2. 验证制造商的技术文件和合规声明
3. 建立产品追溯系统

经销商

1. 只销售符合要求的产品
2. 配合市场监管机构的检查
3. 向制造商和进口商传递安全信息

数字技术和人工智能影响

1

AI 驱动机械安全要求

新增针对 AI 驱动机械的特定安全要求，包括决策透明度和可解释性

2

实时信息处理控制

实施实时信息处理系统的风险控制措施，确保数据处理的可靠性和安全性

3

自主学习系统边界

设定自主学习系统的安全边界，防止算法决策超出预定操作范围

4

非结构化环境保障

强化在非结构化环境中运行的机械安全保障机制，应对不可预测场景

软件作为安全组件的适用性

1

安全关键组件

软件被明确视为机械安全关键组件，需符合与硬件相同的可靠性要求

2

更新维护程序

建立软件更新和维护的合规程序，确保变更不影响安全功能

3

开源软件验证

开源软件组件的安全验证要求，需提供完整的安全评估报告

4

生命周期管理

软件全生命周期的安全管理，从设计到退役的完整安全控制

网络安全与自学习系统要求

1

网络连接防护

机械网络连接的安全防护措施，防止未授权访问和网络攻击

2

数据加密控制

数据传输加密和访问控制机制，确保敏感信息安全

3

算法可解释性

自学习算法的可解释性和可追溯性要求，确保决策透明

4

异常响应机制

异常行为检测与应急响应程序，保障系统安全运行

合规性评估程序新变化

1

简化自我声明流程

低风险产品可采用简化的自我声明流程，减少企业行政负担

2

高风险产品评估

高风险产品需由公告机构参与评估，确保安全合规

3

模块认证体系

引入模块认证体系，提高评估灵活性和效率

4

远程评估机制

允许远程评估和文档审查，适应数字化需求

说明文档与数字说明书的应用

1

电子形式提供

允许以电子形式提供说明书，减少纸质文档使用

2

交互式文档

交互式电子文档的技术要求，支持多媒体内容展示

3

多语言支持

多语言支持和易理解性要求，确保全球用户无障碍使用

4

更新追溯机制

数字说明书的更新和追溯机制，保持信息实时准确

扫码访问电子说明书

Better Tech for Better Future

MUNIK

其他关键变化

1 消费者场景安全考量

增强对消费者使用场景的安全考量，特别是非专业用户的操作风险

2 全生命周期管理

纳入机械全生命周期的安全管理，从设计到报废的完整安全控制

3 供应链责任强化

强化经济运营商的供应链责任，明确各环节安全义务

4 法规协调机制

改进与其他欧盟法规的协调机制，减少合规冲突

基本健康与安全要求（EHSR）总览

1 通用安全原则

机械设计和构造的通用安全原则，确保在各种工况下的安全运行

2 防护措施等级

防护措施的等级划分与应用，包括物理隔离和安全联锁装置

3 人体工程学设计

人体工程学设计要求，优化操作界面减少人为失误风险

4 有害物质控制

有害物质控制和排放限制，保护操作人员和环境安全

附录III要求架构

1 机械结构安全要求

机械整体结构强度、稳定性和耐久性要求，确保在各种工况下的安全运行

2 控制系统安全设计

控制系统的安全设计规范，包括故障安全原则和冗余设计

3 防护装置技术规范

防护装置的技术规范，包括固定防护、可移动防护和可调防护

4 安全联锁装置标准

安全联锁装置的性能标准，确保防护装置与机械运行的正确联动

移动式机器人的相关国际标准

- 欧盟

工业和商业用途AGV

- **EN ISO 3691-4:2023** Industrial trucks – Safety requirements and verification-Part 4: Driverless industrial trucks and their systems
- **EN ISO 13849-1:2023** Safety of machinery - Safety-related parts of control
- systems - Part 1: General principles for design
- EN1175:2020 Safety of industrial trucks -Electrical requirements - Part1: General requirements for battery powered trucks
- EN ISO 12100:2010 Safety of machinery -General principles for design- Risk assessment and risk reduction
- EN 60204-1:2018 Safety of machinery - Electrical equipment of machines - Part 1: General requirements

Note: 根据欧盟委员会官方发布OJ (April 16, 2020), MD指令对应的协调标准清单里已经删去了原适用标准EN 1525:1997，新标准EN ISO 3691-4:2023 **(EU) 2024/1329** Directive 2006/42/EC

风险评估与减轻方法

1 风险识别流程

系统化的风险识别流程，涵盖设计、制造、使用和维护全生命周期

2 评估矩阵

风险等级评估矩阵，综合考虑严重程度和发生概率确定风险等级

3 控制优先级

风险控制措施的优先级排序，从源头消除到个人防护的分级策略

4 残余风险标准

残余风险的可接受性标准，确保风险控制在合理可行范围内

合规评估程序路径

自我声明路径

适用于低风险机械

1. 制造商自行完成评估
2. 保留技术文件10年
3. 签署EU符合性声明

第三方机构路径

适用于高风险机械

1. 公告机构参与评估
2. 型式检验或全面质量保证
3. 持续监督要求

技术文件要求（附录IV）

1

机械设计和制造图纸

详细的设计图纸、技术规格和制造工艺说明

2

风险评估报告

完整的风险评估报告，包括识别、分析和控制措施

3

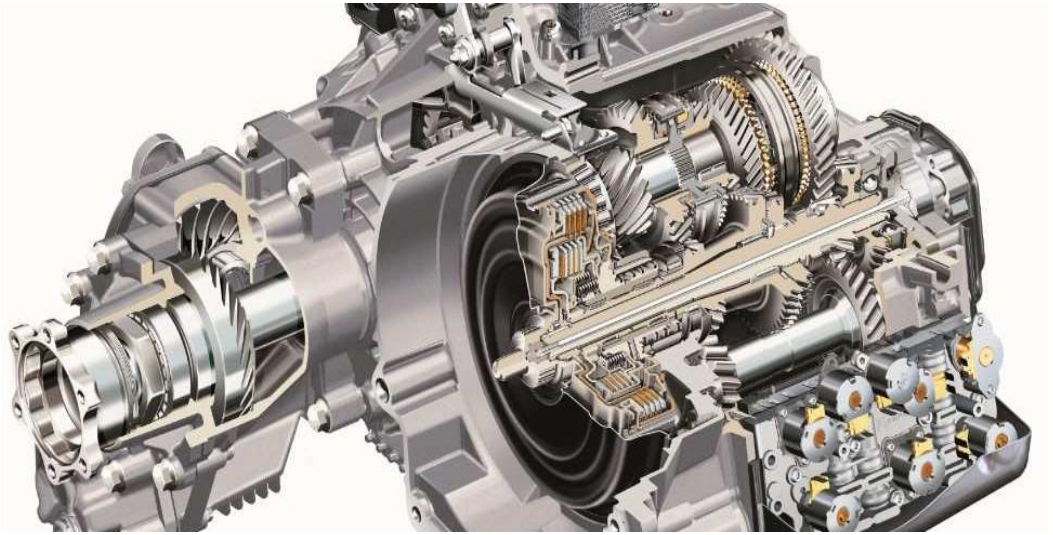
合规性评估记录

合规性评估的详细记录和测试结果

4

操作维护说明书

详细的操作、维护和安全使用说明书



文件保存要求

- 电子或纸质格式
- 保存期限10年
- 随时可提供审查

CE标志及其要求

1

规格与放置位置

CE标志必须符合规定比例，清晰可见地加贴在产品上

2

附加信息标注

需标注公告机构编号及其他必要信息

3

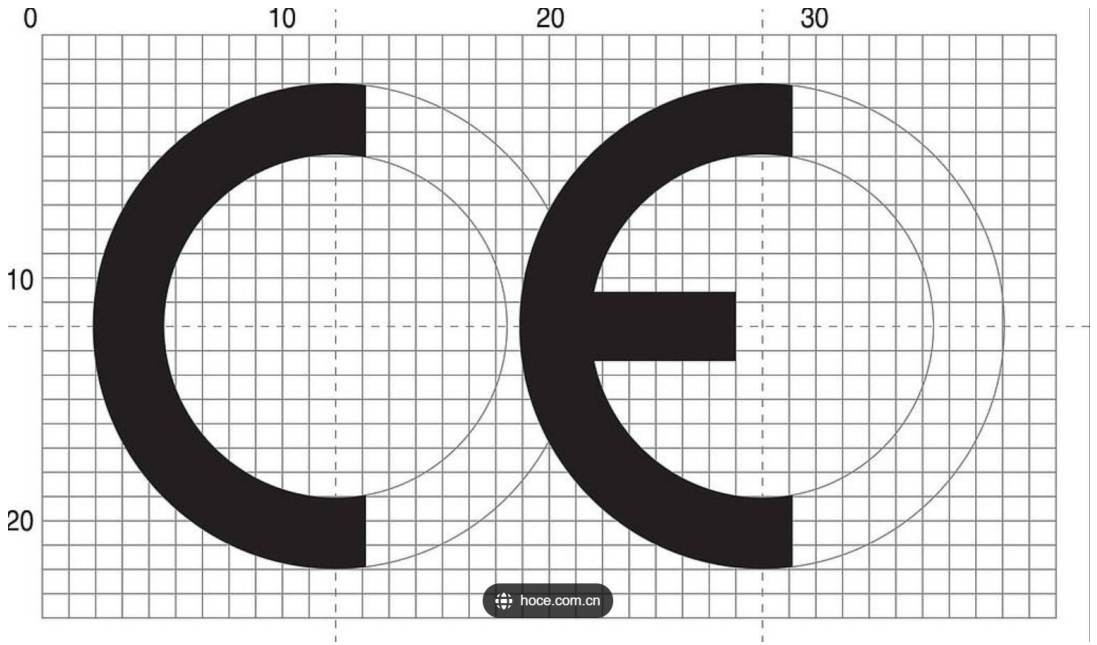
虚假标志后果

使用虚假CE标志将面临高额罚款和产品召回

4

进口产品责任

进口商需确保产品CE标志真实有效



CE标志规格要求

最小高度：5mm
比例必须保持
清晰可辨

协调标准作用

1 法律地位

harmonized standards提供合规性推定，符合标准即推定符合法规基本要求

2 合规证明

使用标准证明产品合规性的方法和流程，包括测试报告和技术文件

3 更新与过渡期

标准更新与过渡期安排，确保企业有足够时间适应新要求

4 非标准解决方案

非标准解决方案的接受条件，需提供等效安全证明和技术论证

软件源代码要求与披露

1

源代码审查要求

安全关键软件的源代码审查要求，确保算法透明可靠

2

质量验证

代码质量和可靠性验证，包括静态分析和动态测试

3

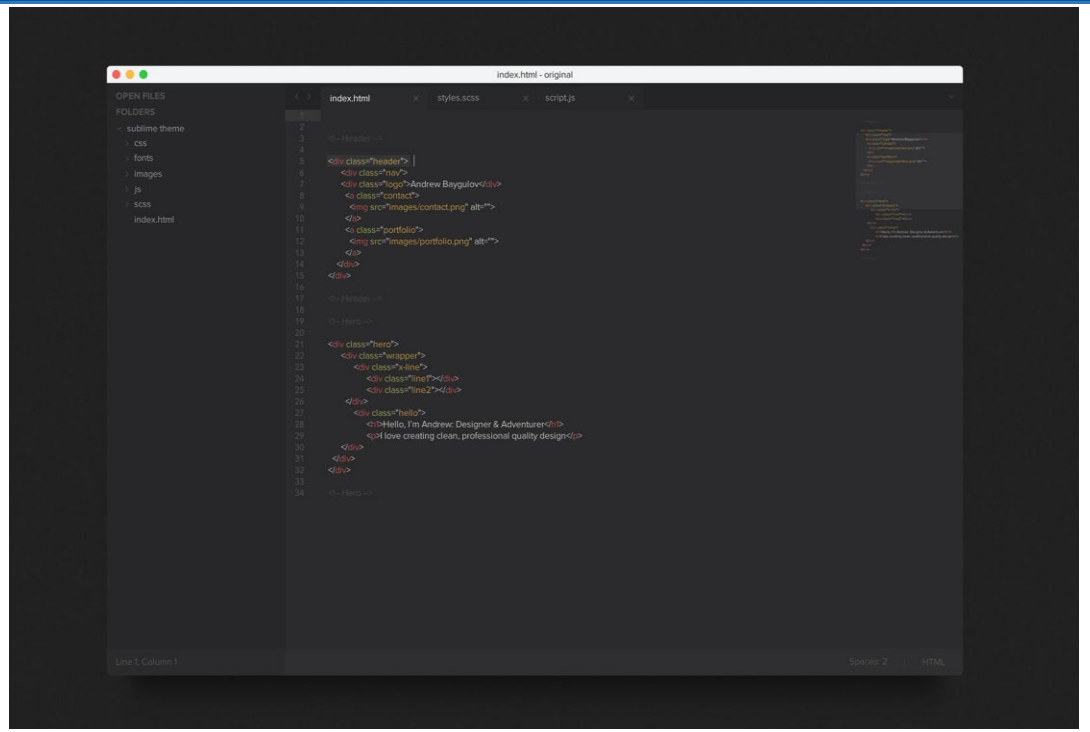
知识产权平衡

知识产权保护与合规需求的平衡机制

4

漏洞管理

漏洞披露和修复机制，建立安全响应流程



披露要求

- 安全关键模块需披露
- 提供可审计版本
- 签署保密协议

重大修改的定义与后果

1

技术判断标准

影响安全性能、基本设计或预定用途的变更视为重大修改

2

重新评估义务

修改后需进行重新评估，确保产品仍符合法规要求

3

通知程序要求

必须通知市场监管机构和相关方的正式程序

4

CE标志重新申请

重大修改后需重新申请CE标志，更新符合性声明

未申报后果

- 产品下架
- 高额罚款
- 法律责任

二手机械处理要求

1

进口合规评估

进口二手机械需进行合规性评估，确保符合当前安全标准

2

安全升级标准

必须按照最新安全标准进行必要的升级和改造

3

使用寿命评估

进行使用寿命评估和剩余价值计算，确定继续使用的可行性

4

追溯文件要求

提供完整的追溯性文件，包括原始技术文件和改造记录

附录I中高风险类别

1

木工机械

特殊安全要求包括刀具防护、紧急制动系统和防反弹装置

2

塑料橡胶加工机械

高温防护、熔融材料防喷溅装置和自动送料安全联锁

3

高空作业平台

稳定性要求、防倾覆装置和紧急下降系统

4

游乐园设备

额外安全措施包括多重制动系统、载荷监控和紧急疏散通道

纳入附录I的标准与程序

1 技术标准

高风险类别确定的技术标准，基于事故数据和风险评估

2 动态调整机制

产品分类的动态调整机制，适应技术发展和新风险

3 申报流程

新风险产品的申报流程，包括技术文件提交和评估

4 过渡期安排

过渡期安排与 grandfathering 条款，确保平稳过渡

法案概述

立法里程碑

2024 年 6月，欧盟正式通过Regulation (EU) 2024/1689
《人工智能法案》，成为全球首个综合性AI监管框架

核心目标

确保 AI 系统安全、保护基本权利、促进创新与竞争

监管范围

覆盖 AI 系统全生命周期，从研发、投放市场到使用阶段

合规原则：基于风险等级分类监管，采取 "禁止 -限制 -允许 "的分级管控模式

EU Artificial Intelligence Act

欧盟 AI 法案标志性元素

欧盟AI法案概述

立法背景

确保AI系统安全与基本权利保护（如《欧盟基本权利宪章》），防范AI对健康、安全及民主价值观的潜在风险

核心目标

建立统一的欧盟AI监管框架，促进单一市场运作；推动以人为本的可信AI发展，同时支持创新

适用范围

覆盖欧盟境内及向欧盟输出的AI系统；例外情况：军事/国防用途、纯个人非专业使用

欧盟议会大楼 - AI法案立法机构

禁止的 AI 实践

1

利用人类脆弱性的操纵性系统

如通过潜意识技术或欺骗性方法扭曲行为，导致重大伤害

2

社会评分系统

基于社会行为或个人特征对自然人进行评分，导致歧视性待遇

3

公共空间实时远程生物识别

仅允许例外情况：反恐、寻找失踪人员、严重犯罪调查

4

工作 /教育场景的情感识别

禁止通过生物数据推断情绪状态（医疗 /安全目的除外）

5

未经授权构建面部识别数据库

禁止通过互联网或监控 footage 无目标抓取面部图像

禁止的潜意识操纵技术示例

高风险 AI 系统分类（ Annex III ）

1. **生物识别系统**

   远程生物识别、情感识别、敏感属性分类

2. **关键基础设施管理**

   能源、交通、供水等关键设施的安全组件

3. **教育与职业培训**

   入学筛选、学习成果评估、考试监控

4. **就业与劳动力管理**

   招聘、绩效评估、工作任务分配

5. **医疗、金融等关键服务**

   医疗诊断、信贷评分、保险风险评估

6. **执法与边境控制**

   风险评估、身份识别、犯罪预测

7. **司法与民主进程**

   司法决策辅助、选举干预

生物识别门禁系统 - 高风险 AI 应用示例

高风险AI系统合规要求（一）

风险管理系统（Article 9）

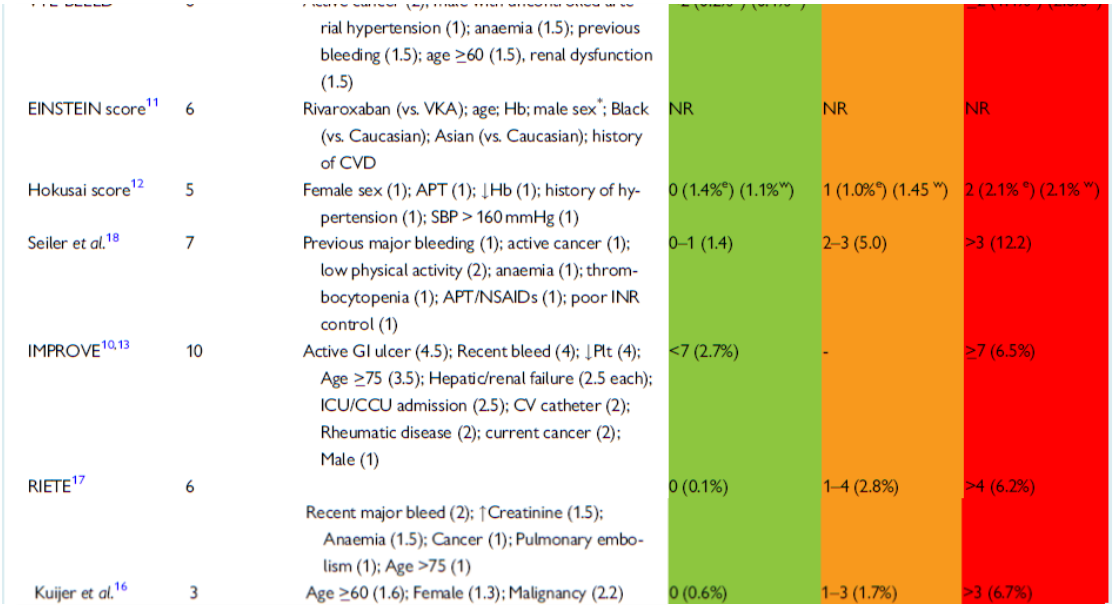
全生命周期风险评估，包括可预见滥用场景；风险 mitigation 措施文档化

数据治理（Article 10）

训练数据需代表性、完整性、无偏见；特殊类别个人数据处理需额外 safeguards

技术文档与记录保存（Articles 11-12）

技术文档需包含算法逻辑、数据来源、测试结果；自动日志记录，保存至少6个月



		rial hypertension (1); anaemia (1.5); previous bleeding (1.5); age ≥60 (1.5), renal dysfunction (1.5)			
EINSTEIN score[11]	6	Rivaroxaban (vs. VKA); age; Hb; male sex*; Black (vs. Caucasian); Asian (vs. Caucasian); history of CVD	NR	NR	NR
Hokusai score[12]	5	Female sex (1); APT (1); ↓Hb (1); history of hypertension (1); SBP > 160 mmHg (1)	0 (1.4%ᵉ) (1.1%ᵂ)	1 (1.0%ᵉ) (1.45 ᵂ)	2 (2.1% ᵉ) (2.1% ᵂ)
Seiler *et al.*[18]	7	Previous major bleeding (1); active cancer (1); low physical activity (2); anaemia (1); thrombocytopenia (1); APT/NSAIDs (1); poor INR control (1)	0–1 (1.4)	2–3 (5.0)	>3 (12.2)
IMPROVE[10,13]	10	Active GI ulcer (4.5); Recent bleed (4); ↓Plt (4); Age ≥75 (3.5); Hepatic/renal failure (2.5 each); ICU/CCU admission (2.5); CV catheter (2); Rheumatic disease (2); current cancer (2); Male (1)	<7 (2.7%)	-	≥7 (6.5%)
RIETE[17]	6	Recent major bleed (2); ↑Creatinine (1.5); Anaemia (1.5); Cancer (1); Pulmonary embolism (1); Age >75 (1)	0 (0.1%)	1–4 (2.8%)	>4 (6.2%)
Kuijer *et al.*[16]	3	Age ≥60 (1.6); Female (1.3); Malignancy (2.2)	0 (0.6%)	1–3 (1.7%)	>3 (6.7%)

AI系统风险评估流程示意图

高风险AI系统合规要求（二）

透明度与人类监督（Articles 13-14）

向部署者提供清晰的使用说明和性能限制；关键决策需人类可干预，避免完全自动化

准确性、鲁棒性与网络安全（Article 15）

定期测试以确保准确性，防范对抗性攻击；数据加密与访问控制措施

欧盟合规声明与CE标识（Articles 47-48）

需签署合规声明，加贴CE标识；高风险系统需在欧盟数据库注册

人类监督在AI系统中的应用示例

通用AI模型监管框架

系统性风险模型分类标准（Article 51）

基于参数规模（如>10^{25} FLOPs）或能力评估；委员会可指定特定模型为系统性风险

额外义务（Article 55）

强制 adversarial testing 和风险评估；持续监控与事件报告机制

开源模型豁免（Article 53(2)）

开源模型可豁免部分透明度要求；但需遵守版权合规与训练数据摘要公开

大型AI服务器集群 - 通用AI模型基础设施

市场监督与执法机制

欧盟数据库注册（Article 71）

高风险AI系统需提交技术文档与合规声明；公众可查询非敏感信息

成员国监管沙盒（Article 57）

提供安全测试环境，支持创新企业合规

处罚措施（Article 99）

最高罚款：全球营业额7%（非合规禁止实践）；3%营业额罚款（其他违规，如文档缺失）

欧盟AI系统数据库注册界面示例

合规时间节点

1 高风险禁令

2025年2月2日

不可接受风险AI应用立即禁止，包括认知操纵、社交评分等

2 行为守则

生效后9个月

行业自律规范开始执行，建立初步合规框架

3 透明度要求

生效后12个月

所有AI系统需提供使用说明和数据来源

4 全面合规

生效后36个月

高风险系统完成全面合规改造，通过强制性评估

注：法案正式生效日期以欧盟官方公告为准，预计为2024年第四季度

实施时间表

2025年2月2日

禁止实践条款生效

2025年8月2日

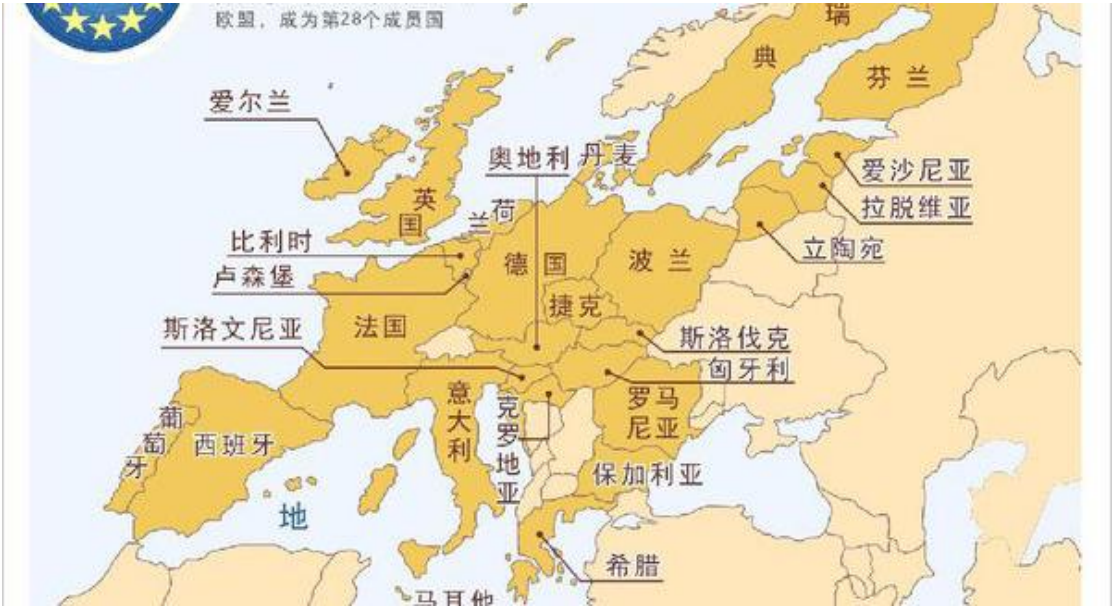
通用AI模型义务生效

2026年8月2日

法案全面生效

2030年8月2日

公共部门系统合规截止



欧盟成员国分布图 - 法案适用范围

对企业的影响

1 合规成本增加

中小企业需投入资源进行风险评估与文档编写

2 供应链责任延伸（Article 25）

分销商、进口商对产品合规承担连带责任

3 全球AI治理标杆效应

非欧盟企业需遵守同等标准以进入欧盟市场

中小企业办公场景 - 合规成本增加的影响

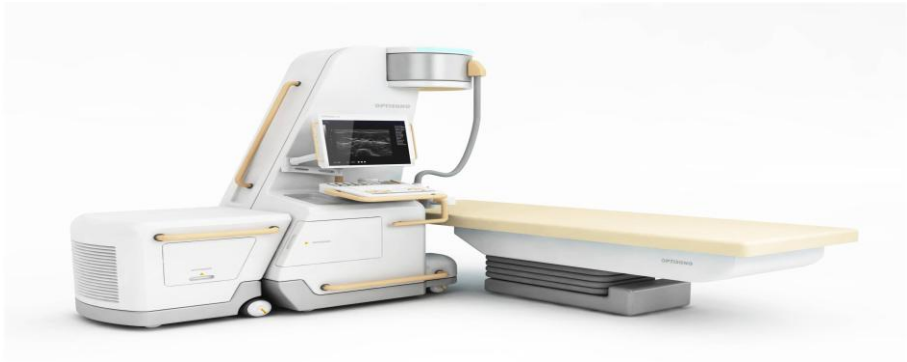
高风险 AI 系统分类

产品安全法规覆盖领域

1. 玩具安全
2. 航空设备
3. 汽车系统
4. 医疗设备
5. 电梯与索道设备

特定领域应用系统

1. 关键基础设施管理（能源、交通、水利等）
2. 教育与职业培训（评分系统、招生筛选）
3. 就业与劳动力管理（招聘、绩效评估）
4. 公共服务与福利分配（社会保障、医疗服务）
5. 执法与司法系统（风险评估、法律适用辅助）
6. 移民与边境管制（签证审核、身份识别）



医疗设备属于高风险 AI 系统监管范围

监管要求：所有高风险系统需通过强制性合规评估并在欧盟数据库注册

不可接受风险应用

⚠ 全面禁止的 AI 应用

1. 认知行为操纵：如鼓励危险行为的儿童智能玩具
2. 社交评分系统：基于社会经济地位或个人特征的歧视性分类
3. 生物特征识别分类：利用生物数据进行不合理人群划分
4. 实时远程生物特征识别：公共场所无差别面部识别

i 有限例外情况

1. 严重犯罪调查可使用"实时"远程生物特征识别（需司法批准）
2. 重大犯罪起诉可使用"事后"远程生物特征识别（需法院授权）

ISO/IEC 22989:2022

AI领域基础概念与术语标准

建立全球统一的 AI基础术语体系，为人工智能领域的标准化工作提供共同语言基础。

统一全球 AI术语定义

明确定义人工智能、机器学习、算法偏见等核心概念，消除跨领域交流障碍。

标准制定的基础框架

为后续 AI技术标准、管理体系标准和评估认证标准提供术语参考框架。

AI 术语标准参考书籍 - 统一概念定义

ISO/IEC 42001:2023

全球首个 AI 管理体系国际标准

建立组织级 AI治理框架，规范人工智能系统的开发、部署和运营全过程。

基于 PDCA 循环的治理框架

采用计划 (Plan)- 实施 (Do)- 检查 (Check)- 改进 (Act) 的持续改进机制。

多领域要求的整合

融合质量管理、信息安全、隐私保护等多维度要求，实现全面风险管理。

ISO/IEC 5338:2023

1

规划设计

需求分析与系统架构设计，明确　　AI 系统目标和约束条件

2

开发实现

数据准备、模型训练与验证，确保算法符合设计要求

3

部署集成

系统集成与上线部署，完成与现有　　IT 环境的无缝对接

4

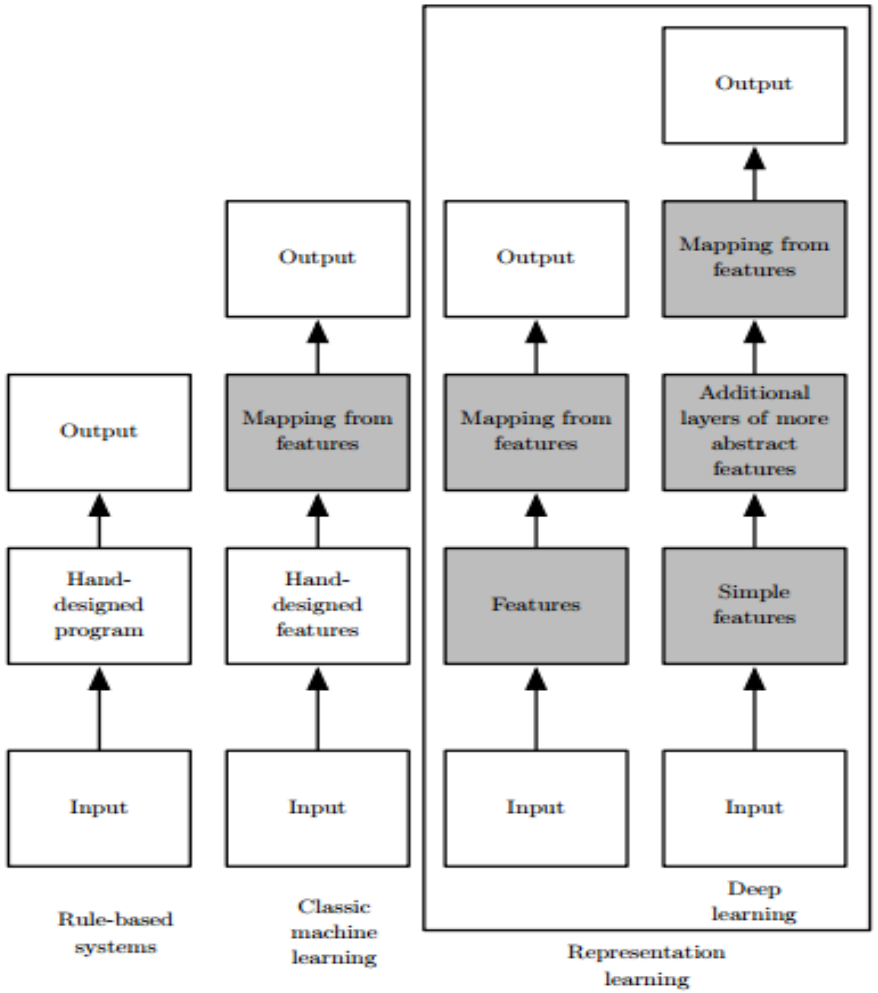
监控评估

持续性能监控与效果评估，确保系统稳定可靠运行

5

更新维护

模型迭代与系统优化，适应业务需求变化和技术演进



1.5: 流程图展示了 AI 系统的不同部分如何在不同的 AI 学科中彼此相关。阴影框表示能从中学习的组件。

风险管理与数据质量标准

23894 ISO/IEC 23894: AI 风险管理

六阶段风险管理流程：

- 沟通协商：利益相关方参与风险识别
- 范围界定：明确系统边界与风险维度
- 风险评估：量化风险概率与影响
- 风险应对：制定缓解与控制措施
- 持续监控：实时跟踪风险变化
- 完整记录：建立风险档案与审计追踪

5259 ISO/IEC 5259 系列 ： 数据质量标准

20 项核心数据质量指标：

- 完整性：数据字段完整度 ≥98%
- 准确性：关键数据准确率 ≥95%
- 分布偏差：特征分布偏移监测
- 时效性：数据更新时效要求
- 一致性：跨源数据一致性验证

数据质量监控设备 - 确保 AI 系统输入质量

协同机制要求

- 数据来源可追溯：建立完整数据谱系与元数据管理
- 隐私保护强制性： GDPR 等合规要求嵌入数据处理流程
- 质量与风险联动：数据异常自动触发风险评估流程

应用指南与功能安全

5339

ISO/IEC 5339: AI 应用实践框架

提供 AI 系统全生命周期实施指南，覆盖从需求分析到退役的全过程管理。

- 需求定义与范围界定
- 系统设计与模型开发
- 验证、部署与持续监控

5469

ISO/IEC TR 5469: 功能安全指南

针对安全关键领域 AI 系统的特殊要求，确保高风险场景下的可靠运行。

- 自动驾驶系统安全阈值
- 医疗诊断 AI 的容错机制
- 工业控制系统的故障安全设计

与传统安全标准的协同

ISO 26262

汽车功能安全标准

IEC 61508

工业控制系统安全

IEC 62304

医疗设备软件安全

核心框架与实施要点

ISO/PAS 8800:2024　　安全标准实践指南

AI 安全生命周期

需求定义

明确 AI 系统功能需求与安全目标

架构设计

选择 AI 技术，确定数据需求与接口规范

数据管理

确保训练数据质量与多样性

验证确认

虚拟与物理测试结合评估性能

部署监控

持续监测系统状态，定期更新模型

风险管控措施

系统性失效

- 多传感器融合
- 算法冗余设计
- 双 AI 系统交叉验证

硬件故障

- 传感器冗余配置
- 电磁干扰防护

功能不足

- 扩大训练数据覆盖
- 迁移学习增强泛化

操作不当

- 异常输入检测机制
- 模型输出概率阈值过滤

行业实践案例

吉利汽车

全球首家通过认证车企，构建全域安全体系

MUNIK

整合 ISO 26262 与 8800 流程，获 DEKRA 全球首张开发流程认证

标准协同

与 ISO 26262(ASIL 等级)、 ISO 21448(SOTIF) 形成互补安全体系

AI标准体系层次结构

基础层 - 概念术语　管理体系层 - 组织治理　支撑层 - 技术实施　认证层 - 第三方评估

标准间相互作用机制

1

管理体系整合

42001 整合引用生命周期、风险管理、数据质量等专项标准，形成完整的 AI 治理框架。

2

风险协同控制

数据质量 (5259) 与风险管理 (23894) 协同工作，共同控制算法偏见与数据偏差风险。

3

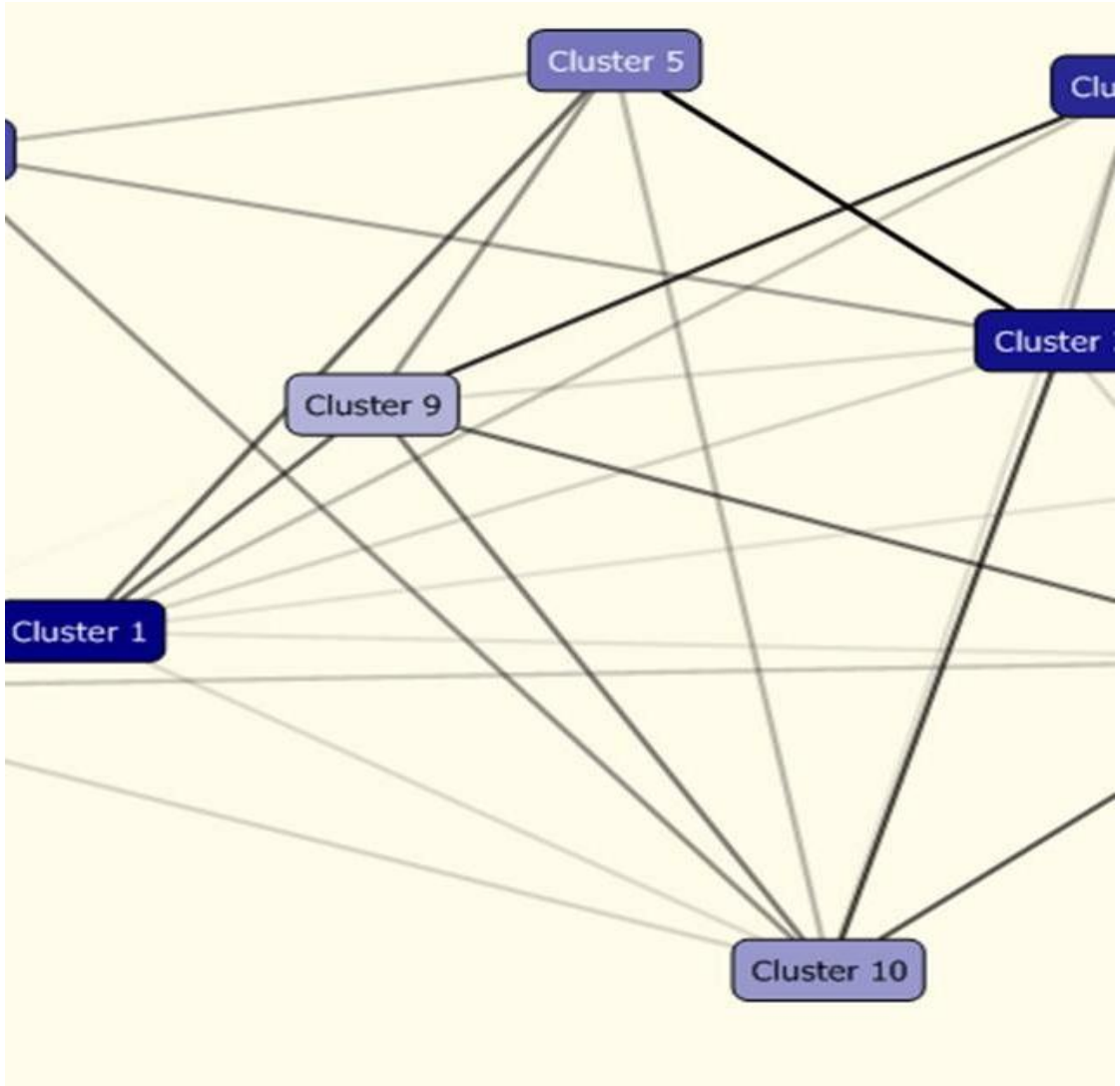
全流程互补

生命周期标准 (5338) 与应用指南 (5339) 互补，实现从开发到运营的全流程管理。

4

高危领域覆盖

功能安全指南 (TR5469) 填补自动驾驶、医疗诊断等高危领域标准空白。



AI 认证市场需求驱动

1

企业竞争力提升

第三方认证成为市场差异化要素，提升企业信誉与市场竞争力

- 认证作为技术能力背书
- 增强客户信任与品牌价值
- 获得市场竞争优势地位

2

监管合规要求

欧盟 AI 法案等法规推动强制性合格评定，确保 AI 系统合规

- 高风险 AI 系统强制认证
- 避免法律处罚与合规风险
- 满足跨境业务准入条件

3

行业信任建设

金融、医疗等领域率先推行认证机制，建立行业自律与公众信任

- B2B 业务准入必要条件
- 公共采购的准入门槛
- 增强公众对 AI 技术信任

AI认证主要类型

1

管理体系认证

ISO/IEC 42001 组织级 AI治理能力评估

- 组织治理架构评估
- 风险管理体系审核
- 合规性能力验证

2

产品/系统认证

特定AI应用安全性能评估

- 自动驾驶系统安全测试
- 医疗诊断 AI准确性验证
- 工业控制系统可靠性评估

3

服务认证

AI服务伦理合规性验证

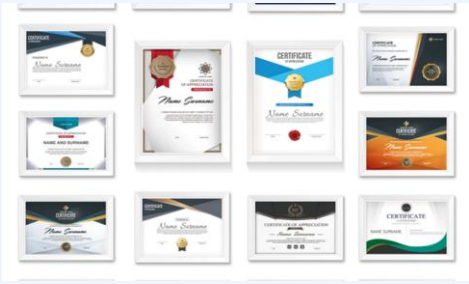
- 生成式 AI服务内容审核
- 算法透明度验证
- 用户隐私保护评估

4

人员认证

AI从业人员能力资质评定

- 算法工程师能力认证
- AI伦理审核员资质
- 系统安全评估师认证



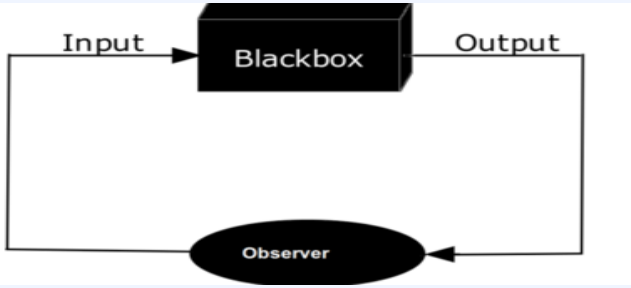
认证实施技术挑战

1

黑箱特性评估困难

AI 系统内部决策过程不透明，可解释性不足影响审核判断

- 复杂模型决策路径难以追踪
- 特征重要性分析存在偏差
- 因果关系与相关性混淆



2

动态模型监控需求

持续学习模型需要实时监控，传统静态认证模式不适用

- 模型漂移检测机制缺乏
- 数据分布变化实时响应不足
- 概念漂移预警系统不完善

3

新兴技术标准缺失

大模型等前沿技术评估标准滞后，验证方法不成熟

- 生成式 AI 伦理评估框架缺失
- 多模态模型测试方法不统一
- 对抗性攻击防御验证不足
- 鲁棒性测试基准未建立

合规挑战与建议

挑战

1

动态监管要求

标准与指南持续更新，企业需不断调整合规策略

2

跨境数据流动

GDPR与AI法案协同要求，增加数据处理复杂性

3

技术实施成本

高风险系统需投入大量资源满足技术合规要求

建议

1

早期合规评估

借助监管沙盒测试创新方案，降低合规风险

2

员工AI素养培训

确保人类监督有效实施，满足透明度要求

3

第三方审计

验证风险控制措施有效性，增强合规可信度


更多咨询关注“MUNIK秒尼科”公众号和联系我们
Lillian Luo
上海 黄浦
Ice
广东 深圳
Better Tech for Better Future
MUNIK

Fast-Track to Functional Safety with Certified Software Tools

Brendan Pan (潘锋)
FAE
July 23, 2025

Agenda

- Functional Safety and Standards
- Requirements for software tools in IEC 61508
- IAR Solutions for IEC 61508
- Latest update
- Summary and Q&A

IAR Introduction

IAR总部位于瑞典，全球有***200***多名员工，分布在亚洲、欧洲和美洲共***13*** 个办事处为客户提供支持

Customers are supported by 200+ employees in ***13 offices*** in Asia, Europe and the Americas

IAR在***瑞典*** 纳斯达克斯德哥尔摩中型股上市，股票代码为 ***IAR B***

Listed on Nasdaq Stockholm MidCap, under the ticker symbol ***IAR B***

IAR在2024年的全年收入为 ***4.87*** 亿瑞典克朗（***4800万*** 美元）

The revenue in 2024 was ***487 MSEK*** ($48M USD)

IAR可支持 ***20*** 种以上指令架构，共计***15000*** 多款MCU/SOC，来自国内外***70*** 多家芯片厂商

We support ***15 000+*** MCU/SOC devices from ***70+*** silicon vendors, built on ***20+*** architectures

IAR为全球超过***30,000*** 名开发人员提供了方案与技术支持

30,000+ developers worldwide are empowered by our solutions

我们日常能够接触到通过IAR开发的产品，每日可达***30***余次。

People interact with IAR ***30+ times*** a day when using a product programmed by one of our customers

Functional Safety and Standards

Standards for Functional Safety

- IEC 61508 Industrial
  Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- ISO 26262 Automotive
  Road vehicles – Functional safety
- IEC 62304 Medical
  Medical device software – Software life cycle processes
- EN 50128 EN50567 Rail
  Railway applications – Communication, signaling and processing systems - Software for railway control and protection systems
- Other: ISO 25119/ISO 13849 IEC 62061/IEC 61511/IEC 60730

Start from IEC 61508

- deals with functional safety
  - Safety: freedom from unacceptable risk
  - Functional Safety: part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

Start from IEC 61508

- deals with functional safety
- forms the basis of other functional safety standards including ISO13849

Start from IEC 61508

- deals with functional safety
- forms the basis of other functional safety standards including ISO13849
- categorized as random hardware failures or systematic failures
  - random hardware failure: failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware
  - systematic failure: failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Start from IEC 61508

- deals with functional safety
- forms the basis of other functional safety standards including ISO13849
- categorized as random hardware failures or systematic failures
- defines a set of Safety Integrity Levels (SILs)
  - How often can we tolerate the safety function failing?

SIL	Probability of failure per hour (continuous operation)	Probability of failure on demand (on-demand operation)
1	$\geq 10^{-6}$ to 10^{-5}	$\geq 10^{-2}$ to 10^{-1}
2	$\geq 10^{-7}$ to 10^{-6}	$\geq 10^{-3}$ to 10^{-2}
3	$\geq 10^{-8}$ to 10^{-7}	$\geq 10^{-4}$ to 10^{-3}
4	$\geq 10^{-9}$ to 10^{-8}	$\geq 10^{-5}$ to 10^{-4}

Start from IEC 61508

- deals with functional safety
- forms the basis of other functional safety standards including ISO13849
- categorized as random hardware failures or systematic failures
- defines a set of Safety Integrity Levels (SILs)
- defines sets of:
  - Processes—e.g., impact analysis, regression testing
  - Techniques—e.g., (semi-)formal methods, boundary value analysis
  - Tools—e.g., certified code translator, coding standards, fault tree analysis

  that are not recommended, recommended or highly recommended at each SIL.

IEC 61508 Overall framework

1. General Requirements. Concept, hazard and risk analysis.
2. System & Hardware.
3. Software.
4. Definitions.
5. Methods for determining Safety Integrity Levels (SILs).
6. Guidelines for applying parts 2 and 3.
7. Techniques and Measures.

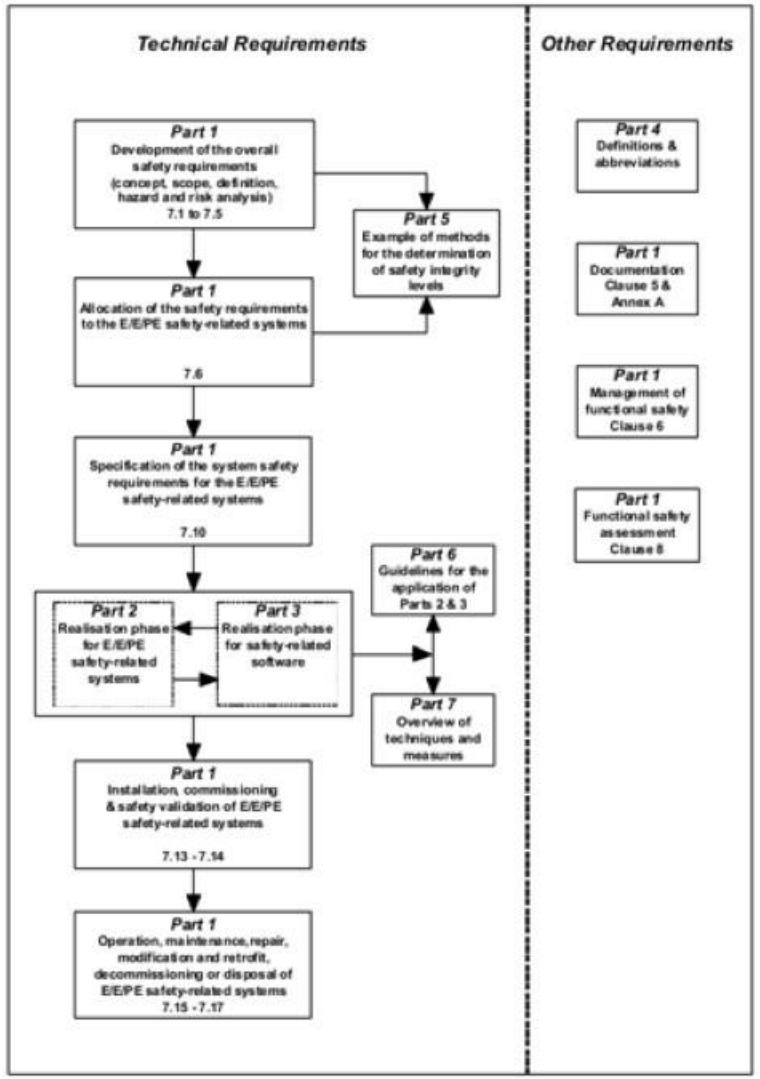


Figure 1 – Overall framework of the IEC 61508 series

IEC 61508 Overall framework

1. General Requirements. Concept, hazard and risk analysis.
2. System & Hardware.
3. Software.
4. Definitions.
5. Methods for determining Safety Integrity Levels (SILs).
6. Guidelines for applying parts 2 and 3.
7. Techniques and Measures.

Independent from the Safety Integrity Level, it has the requirements for the development tools in all functional safety standards

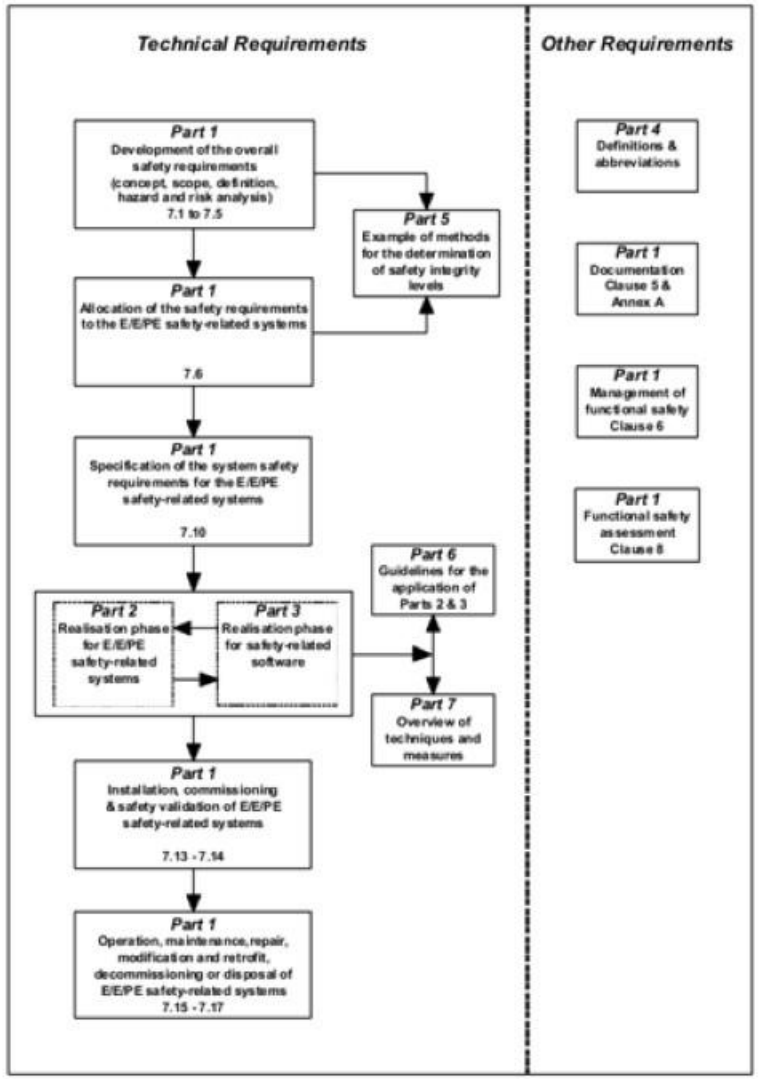
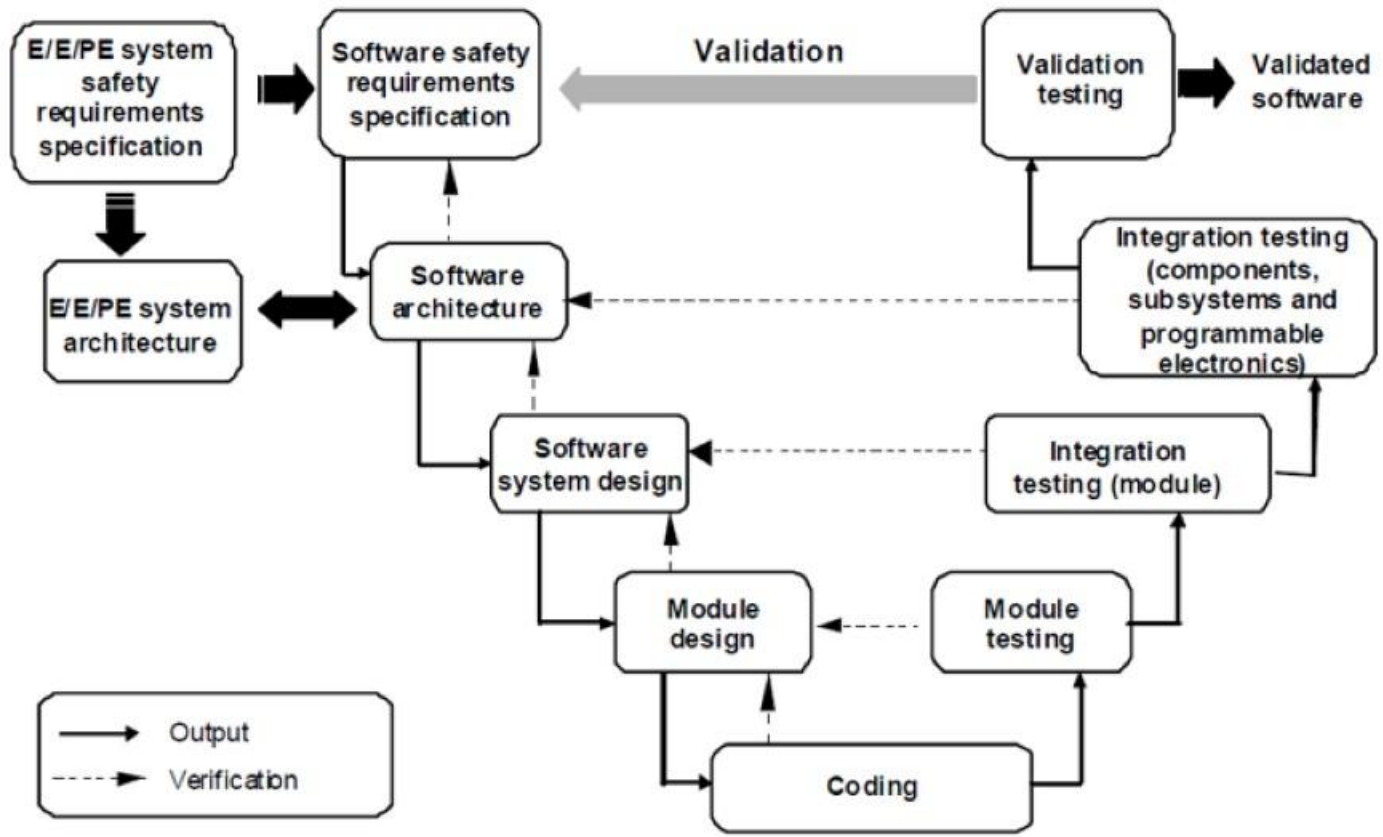


Figure 1 – Overall framework of the IEC 61508 series

Requirements for software tools in IEC 61508

IEC 61508 Software V-Model

- Requirements for software tools are mainly covered in **7.4.4** “Requirements for support tools, including programming languages” (IEC61508-3)
- Focus on the off-line software tools



General requirements for Tool qualification

- **Identification**
  - Identify tools that are appropriate for the specific application and meet the required safety integrity level
- **Classification**
  - Classify tools based on their impact on safety-related functions. It helps determine the level of scrutiny and validation needed.
- **Specification**
  - Define tool's behavior and usage constraints
- **Assessment**
  - Assess whether the tool meets its specification, check compliance, and identify any limitations or risks.
- **Validation**
  - Perform validation activities to ensure the tool conforms to specification.
- **Configuration**
  - Implement configuration management for the tool's and keep track of known issues with the tool.

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **7.4.4.2** Software off-line support tools shall be selected as a coherent part of the software development activities.

NOTE 2 Appropriate off-line tools to support the development of software should be used in order to increase the integrity of the software by reducing the likelihood of introducing or not detecting faults during the development. Examples of tools relevant to the phases of the software development lifecycle include:

a) transformation or translation tools that convert a software or design representation (e.g. text or a diagram) from one abstraction level to another level: design refinement tools, compilers, assemblers, linkers, binders, loaders and code generation tools;

b) verification and validation tools such as static code analysers, test coverage monitors, theorem proving assistants, and simulators;

c) diagnostic tools used to maintain and monitor the software under operating conditions;

d) infrastructure tools such as development support systems;

e) configuration control tools such as version control tools;

f) application data tools that produce or maintain data which are required to define parameters and to instantiate system functions. Such data includes function parameters, instrument ranges, alarm and trip levels, output states to be adopted at failure, geographical layout.

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- Tools impact on the executable code (**3.2.11** in IEC 61508-4)

Tool Class	Definition	Example
T1	Tools which generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system	Text Editor
T2	Tools which supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software	Static Analysis Tool
T3	Tools which generates outputs which can directly or indirectly contribute to the executable code of the safety related system	Compiler

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **7.4.4.4** All off-line support tools in classes T2 and T3 **shall have a specification or product documentation** which clearly defines the behaviour of the tool and any instructions or constraints on its use.

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **7.4.4.5 An assessment shall be carried out** for offline support tools in classes T2 and T3 to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures shall be taken.

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **7.4.4.6 For each tool in class T3, evidence shall be available that the tool conforms to its specification or documentation.** Evidence may be based on a suitable combination of history of successful use in similar environments and for similar applications (within the organization or other organizations), and of tool validation as specified in 7.4.4.7
- **7.4.4.7** The results of tool validation **shall be documented** covering the following results:

  a) a chronological record of the validation activities;

  b) the version of the tool product manual being used;

  c) the tool functions being validated;

  d) tools and equipment used;

  e) the results of the validation activity; the documented results of validation shall state either that the software has passed the validation or the reasons for its failure;

  f) test cases and their results for subsequent analysis;

  g) discrepancies between expected and actual results.

Requirements for software tools in IEC 61508

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **7.4.4.15** Where off-line support tools of classes T2 and T3 generate items in the configuration baseline, configuration management shall ensure that information on the tools is recorded in the configuration baseline.
- **7.4.4.16** Configuration management shall ensure that for tools in classes T2 and T3, **only qualified versions are used**.

Specific requirement for Translator

- **7.4.4.10** To the extent required by the safety integrity level, the software or design representation (including a programming language) selected shall:

  a) have a translator which has been assessed for fitness for purpose including, where appropriate, assessment against the international or national standards;
  b) use only defined language features;
  c) match the characteristics of the application;
  d) contain features that facilitate the detection of design or programming mistakes;
  e) support features that match the design method.

Support Tools & Programming Language

- Tables of recommended and highly-recommended tools and techniques. From IEC 61508:.

Table A.3 – Software design and development – support tools and programming language

(See 7.4.4)

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Suitable programming language	C.4.5	HR	HR	HR	HR
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR
3	Language subset	C.4.2	---	---	HR	HR
4a	Certified tools and certified translators	C.4.3	R	HR	HR	HR
4b	Tools and translators: increased confidence from use	C.4.4	HR	HR	HR	HR

Certified Tools and Certified Translators

C.4.3 Certified tools and certified translators

NOTE This technique/measure is referenced in Table A.3 of IEC 61508-3.

Aim: Tools are necessary to help developers in the different phases of software development. Wherever possible, tools should be certified so that some level of confidence can be assumed regarding the correctness of the outputs.

Description: The certification of a tool will generally be carried out by an independent, often national, body, against independently set criteria, typically national or international standards. Ideally, the tools used in all development phases (specification, design, coding, testing and validation) and those used in configuration management, should be subject to certification.

To date, only compilers (translators) are regularly subject to certification procedures; these are laid down by national certification bodies and they exercise compilers (translators) against international standards such as those for Ada and Pascal.

It is important to note that certified tools and certified translators are usually certified only against their respective language or process standards. They are usually not certified in any way with respect to safety.

Language subset and static analysis

C.4.2 Language subsets

NOTE This technique/measure is referenced in Table A.3 of IEC 61508-3.

Aim: To reduce the probability of introducing programming faults and increase the probability of detecting any remaining faults.

Description: The language is examined to determine programming constructs which are either error-prone or difficult to analyse, for example, using static analysis methods. A language subset is then defined which excludes these constructs.

Language subset and static analysis

Table C.1 – Recommendations for specific programming languages

	Programming language	SIL1	SIL2	SIL3	SIL4
1	ADA	HR	HR	R	R
2	ADA with subset	HR	HR	HR	HR
3	Java	NR	NR	NR	NR
4	Java with subset (including either no garbage collection or garbage collection which will not cause the application code to stop for a significant period of time). See Annex G for guidance on use of object oriented facilities.	R	R	NR	NR
5	PASCAL (see Note 1)	HR	HR	R	R
6	PASCAL with subset	HR	HR	HR	HR
7	FORTRAN 77	R	R	R	R
8	FORTRAN 77 with subset	HR	HR	HR	HR
9	C	R	–	NR	NR
10	C with subset and coding standard, and use of static analysis tools	HR	HR	HR	HR
11	C++ (see Annex G for guidance on use of object oriented facilities)	R	–	NR	NR
12	C++ with subset and coding standard, and use of static analysis tools (see Annex G for guidance on use of object oriented facilities)	HR	HR	HR	HR
13	Assembler	R	R	–	–
14	Assembler with subset and coding standard	R	R	R	R
15	Ladder diagrams	R	R	R	R
16	Ladder diagram with defined subset of language	HR	HR	HR	HR

Why using Certified Tools?

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

Why using Certified Tools?

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **Self-validation**
  - 6-12 months of engineering effort
  - 2-4 full-time engineers
  - external assessments, documentation, and certification audits
  - Comprehensive estimates : $150k~300k per project

Why using Certified Tools?

- Identification
- Classification
- Specification
- Assessment
- Validation
- Configuration

- **Self-validation**
  - 6-12 months of engineering effort
  - 2-4 full-time engineers
  - external assessments, documentation, and certification audits
  - Comprehensive estimates : $150k~300k per project

- **Certified tools mean**
  - Certification included thorough assessment of development, testing, and support.
  - Tool is certified for safety-related applications per functional safety standards.
  - No need for self-evaluation or compliance testing; third-party accredited body has certified it.
  - Focus on product development to accelerate safety product development and certification.

IAR Solutions for IEC 61508

Functional Safety Certified Toolchain

Arm Functional Safety Partner
Software & Tools

- Certified toolchain
  - A special functional safety edition of IAR Embedded Workbench/Build Tools
- Simplified validation
  - Functional Safety certificate
  - Safety report
  - Safety guide
- Guaranteed support through the product life cycle
  - Prioritized support
  - Validated service packs
  - Regular reports of known problems

TÜV SÜD Safety tested Production monitored Functional Safety

Broad Coverage of Standards

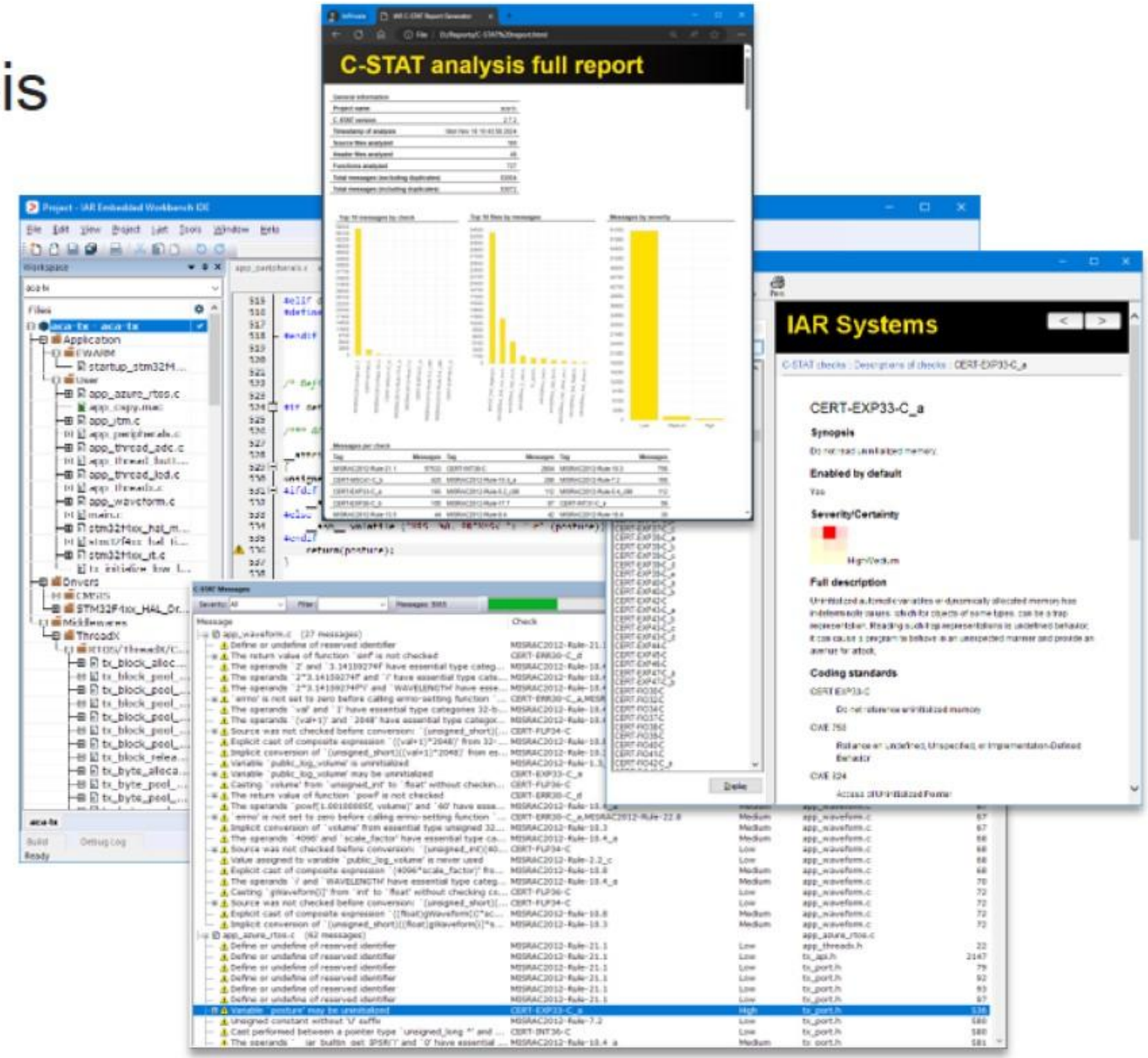
	Industrial IEC 61508	Automotive ISO 26262	Railway EN 50128 EN 50657	Medical IEC 62304	Agriculture & forestry ISO 25119	Machinery control ISO 13849 IEC 62061	Process industry IEC 61511	Household appliances IEC 60730
Arm	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓
RISC-V	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓
Renesas RL78	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓	● ✓
Renesas RX	●	●	●	●				
Renesas RH850	●	●	●	●				
STM8	●	●	●	●				

Functional Safety Release cycle

- A new Functional Safety Edition is generally released every 12~18 months
- Functional Safety editions come with `feature frozen` toolchains certified by TÜV SÜD
- Upgrade path conveniently allows active customers to move forward to newer releases

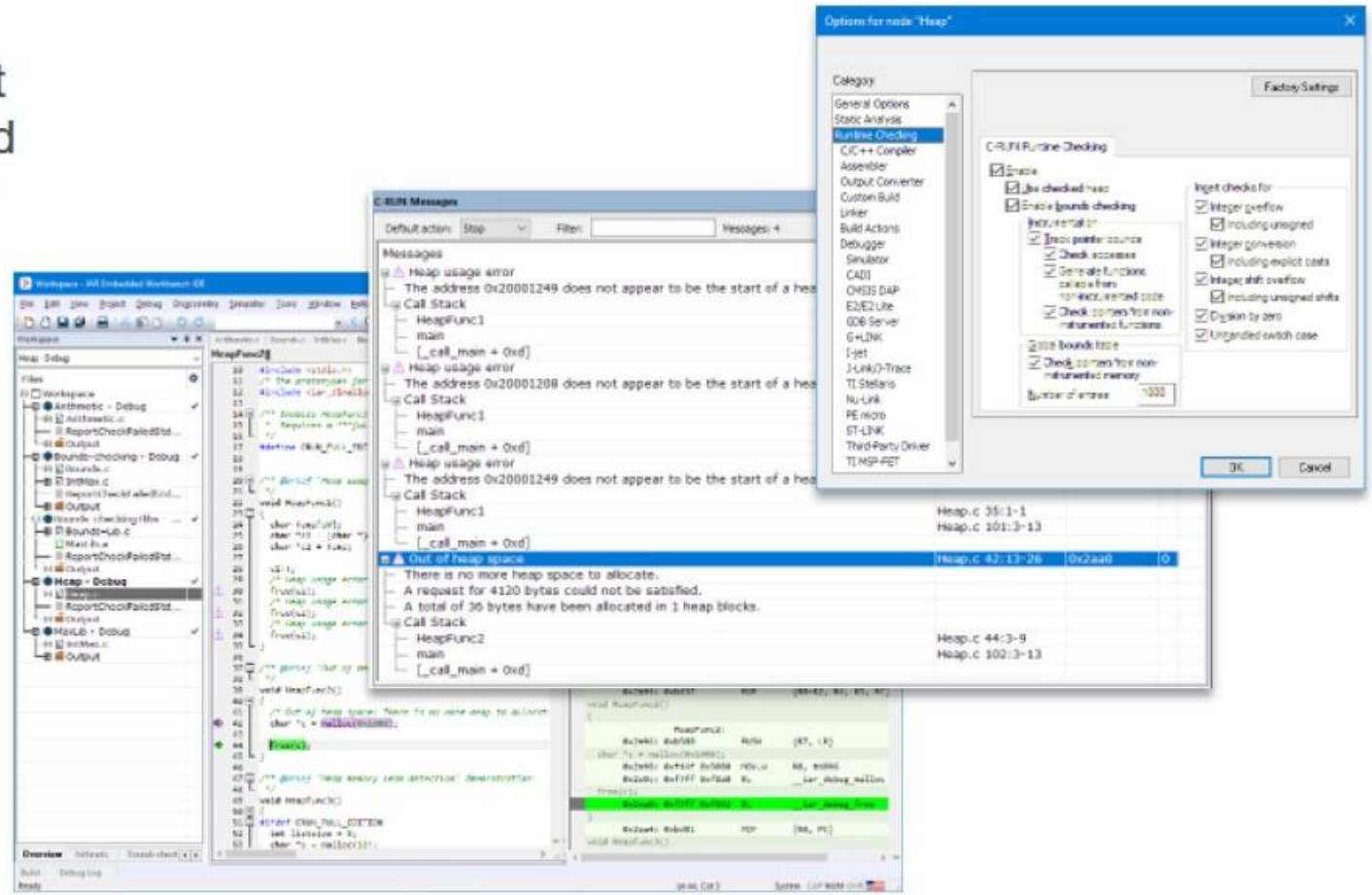
C-STAT: Static Code Analysis

- Ensure C and C++ code quality throughout the development cycle
- Checks code compliance with
  - MISRA C (2023, 2012, 2004)
  - MISRA C++ (2023, 2008)
  - SEI CERT C (Secure Coding)
  - CWE (Common Weaknesses Enumeration)
- Detailed list with context-sensitive help
- Full analysis report generation
- TÜV SÜD certified version available
  - Arm, RISC-V and Renesas RL78



C-RUN: Runtime Analysis

- Takes the debugging experience to the next level, by automatically equipping your C and C++ code for quickly detecting preventable errors such as
  - Bit losses in shifting operations
  - Buffer overflow
  - Division by Zero
  - Heap memory corruption and leaks
  - Out-of-bounds access for arrays and objects
  - Type casting inadvertent value changes
- Available for Arm and Renesas RX targets
- Evaluation hands-on guide available

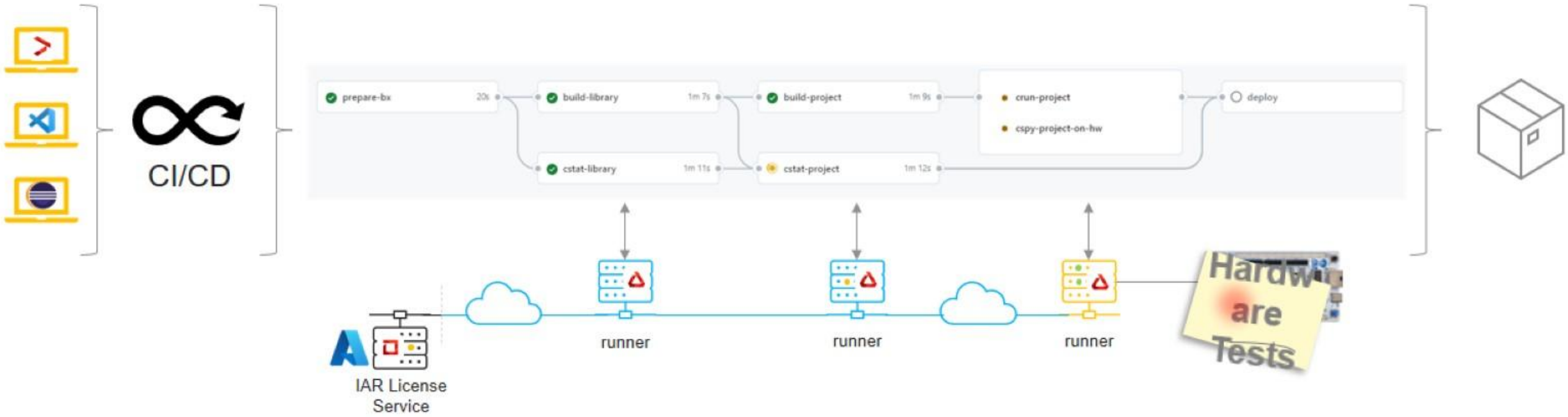


IAR Build Tools – Ideal solution for CI/CD workflow

- Deployable on typical CI/CD environments
  Self-Hosted & Cloud-Hosted
- Cross-platform
  - Linux (Ubuntu,RedHat)
  - Windows
- Command-line tools
  - Compiler, assembler, linker, etc.
  - IAR Command line build utility (iarbuild)
  - C-STAT & C-RUN
- CSpy for non-interactive debugging
  - Used in automated tests

```
# Build
> iarbuild project.ewp –build Release
[...]
Total number of errors: 0
Total number of warnings: 0

Build succeeded


# Static Code Analysis (C-STAT)
> iarbuild project.ewp –cstat_analyze Release
[...]

Analysis completed. 128 message(s)


# Runtime Analysis (C-RUN)
> CSpyBat ... --rtc_enable --debug-file=/path/to/executable.out
[...]

CSpyBat terminating.


# Flash the target
> CSpyBat ... --download_only --debug-file=/path/to/executable.out
[...]

CSpyBat terminating.
```

IAR DevOps Workflow



Cloud

On-prem

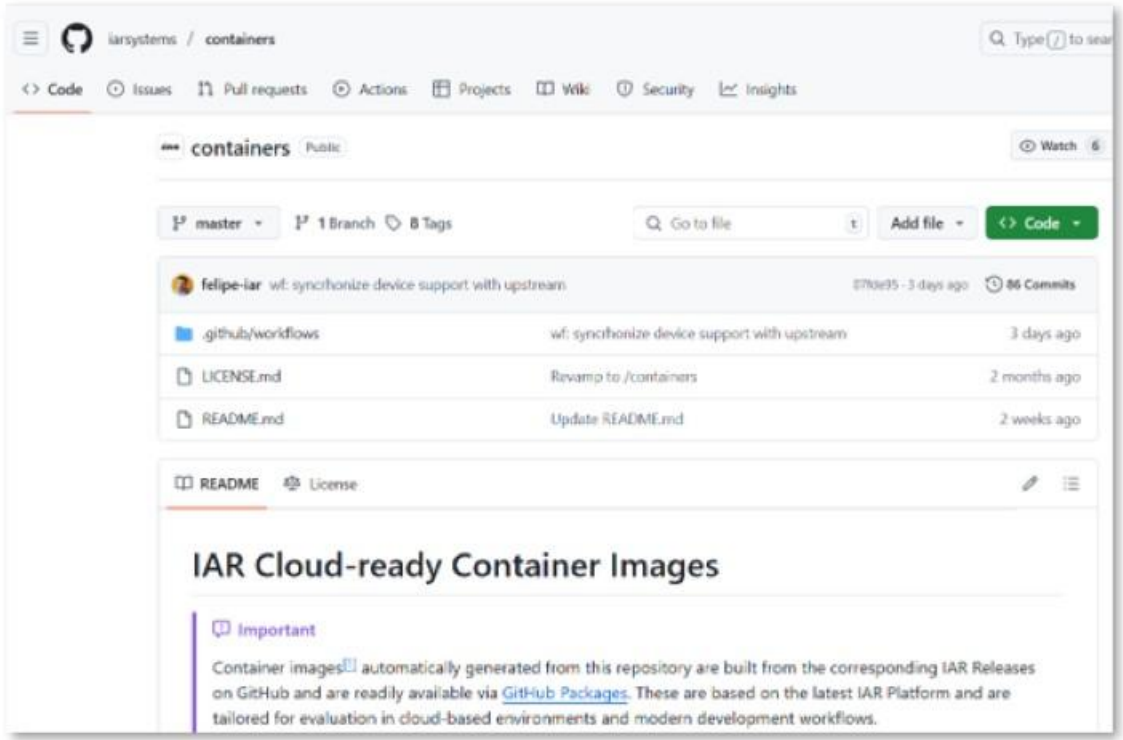
IAR Embedded Workbench

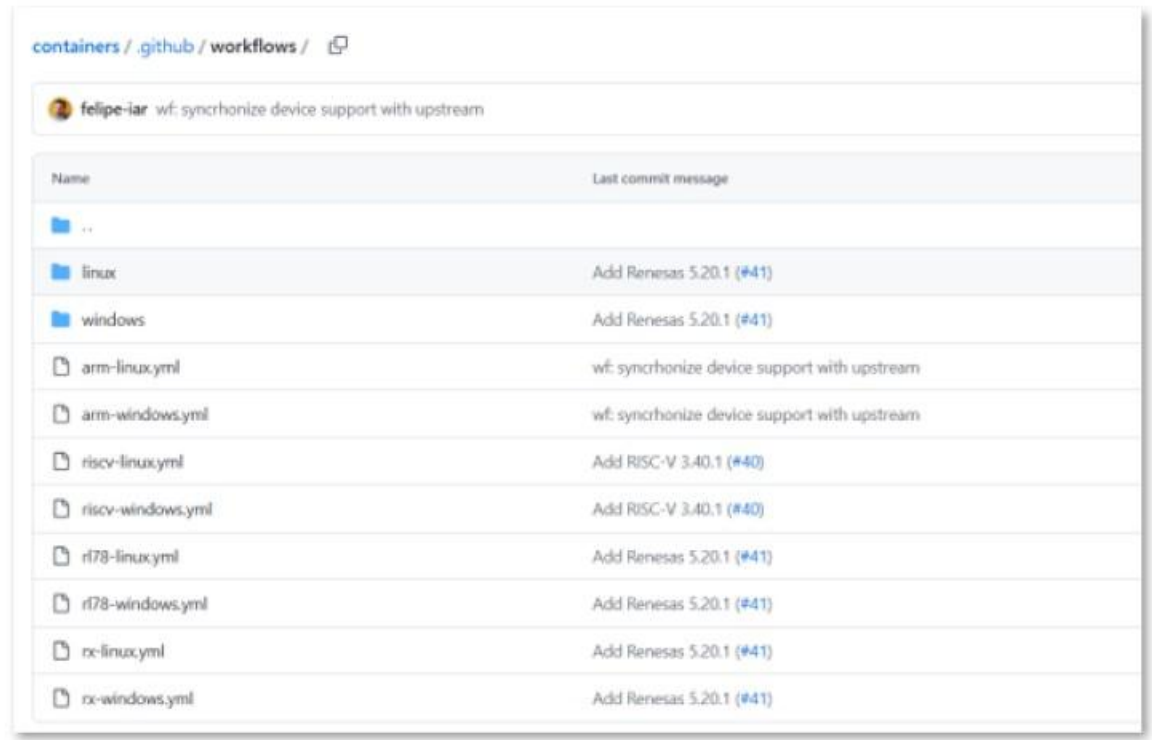
Visual Studio Code

IAR Build Tools

IAR License Service

Out-of-box container images

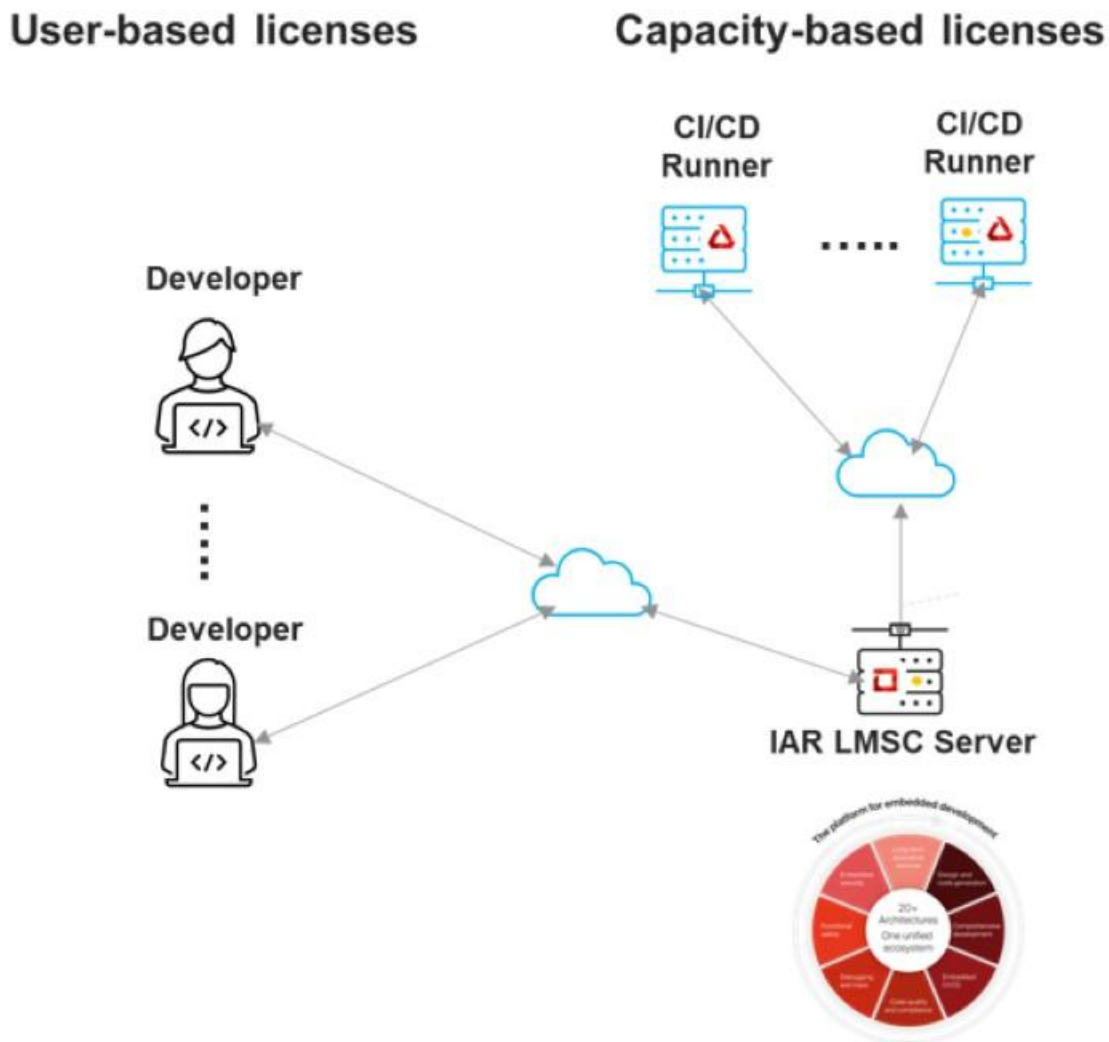




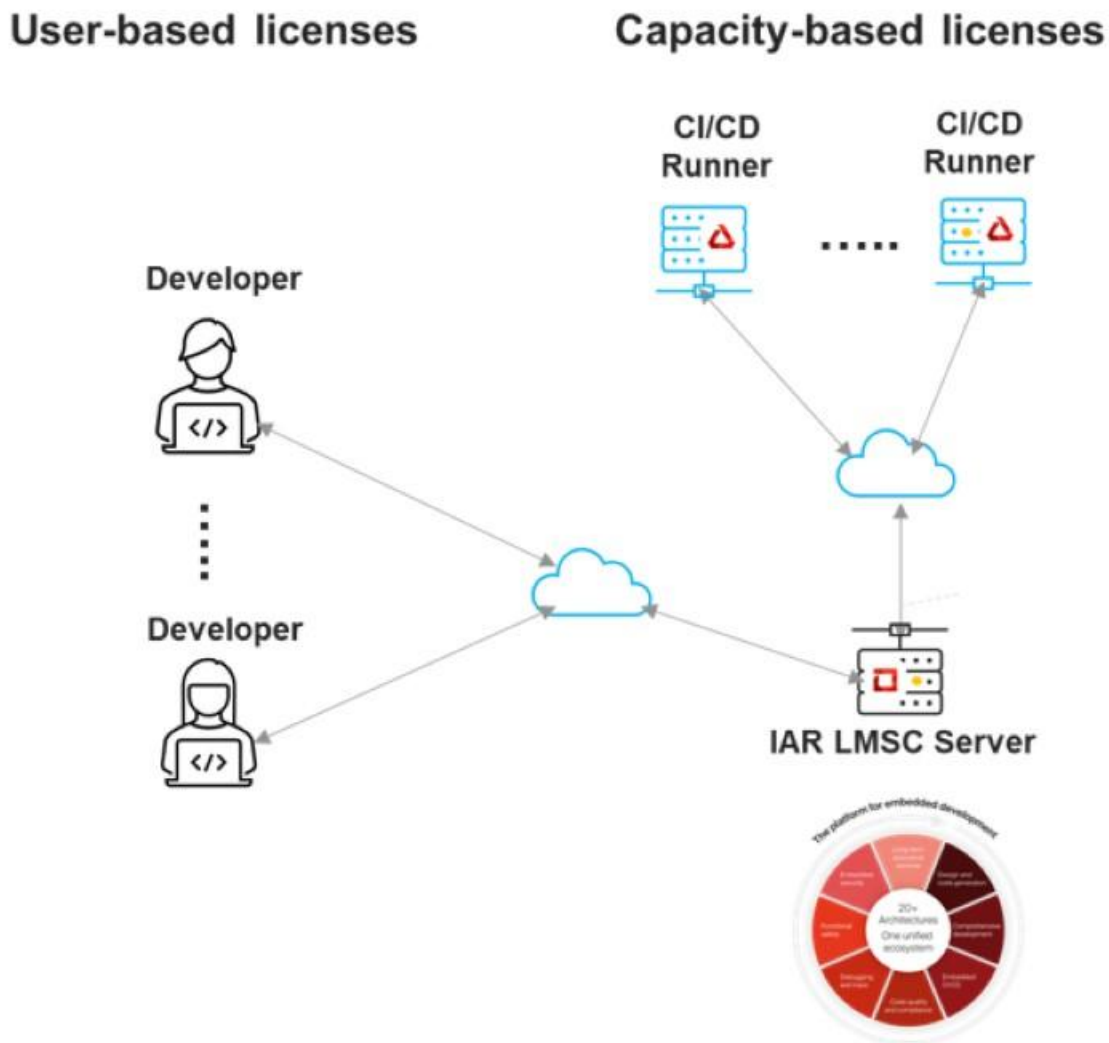
Source: https://github.com/iarsystems/containers/

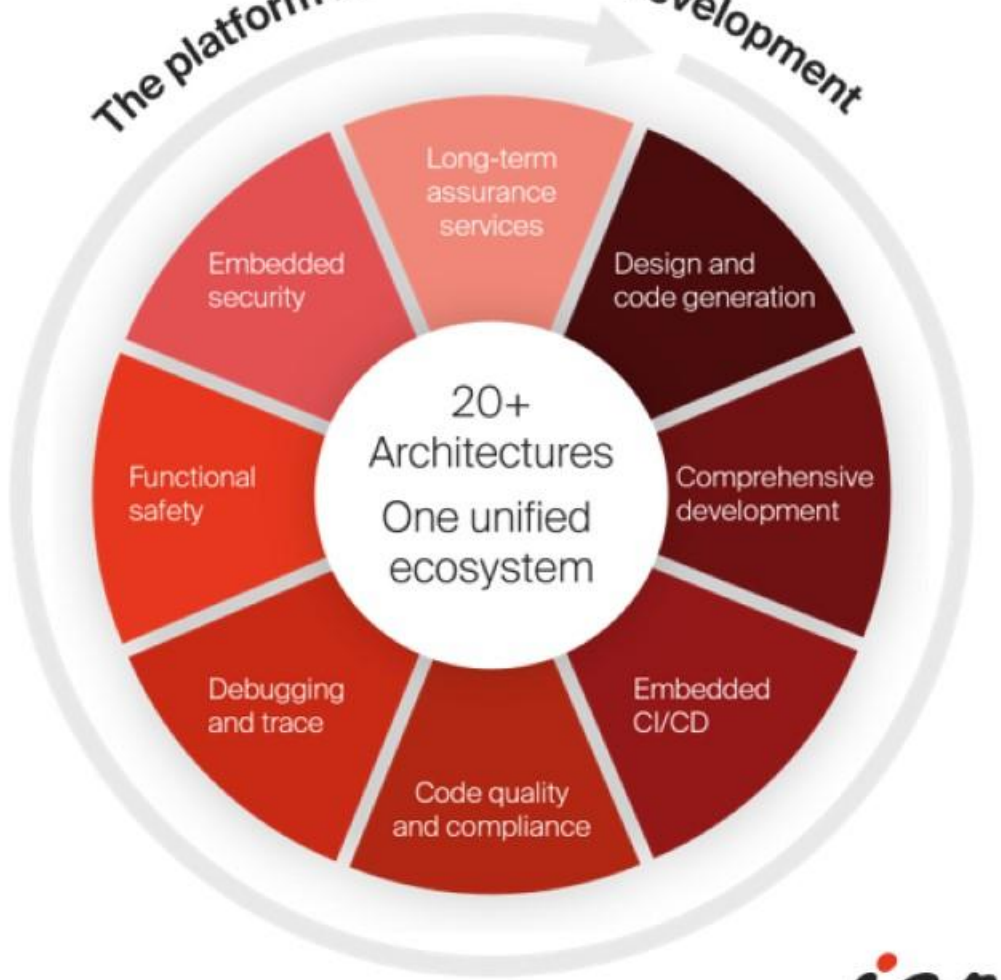
Latest update: IAR Platform

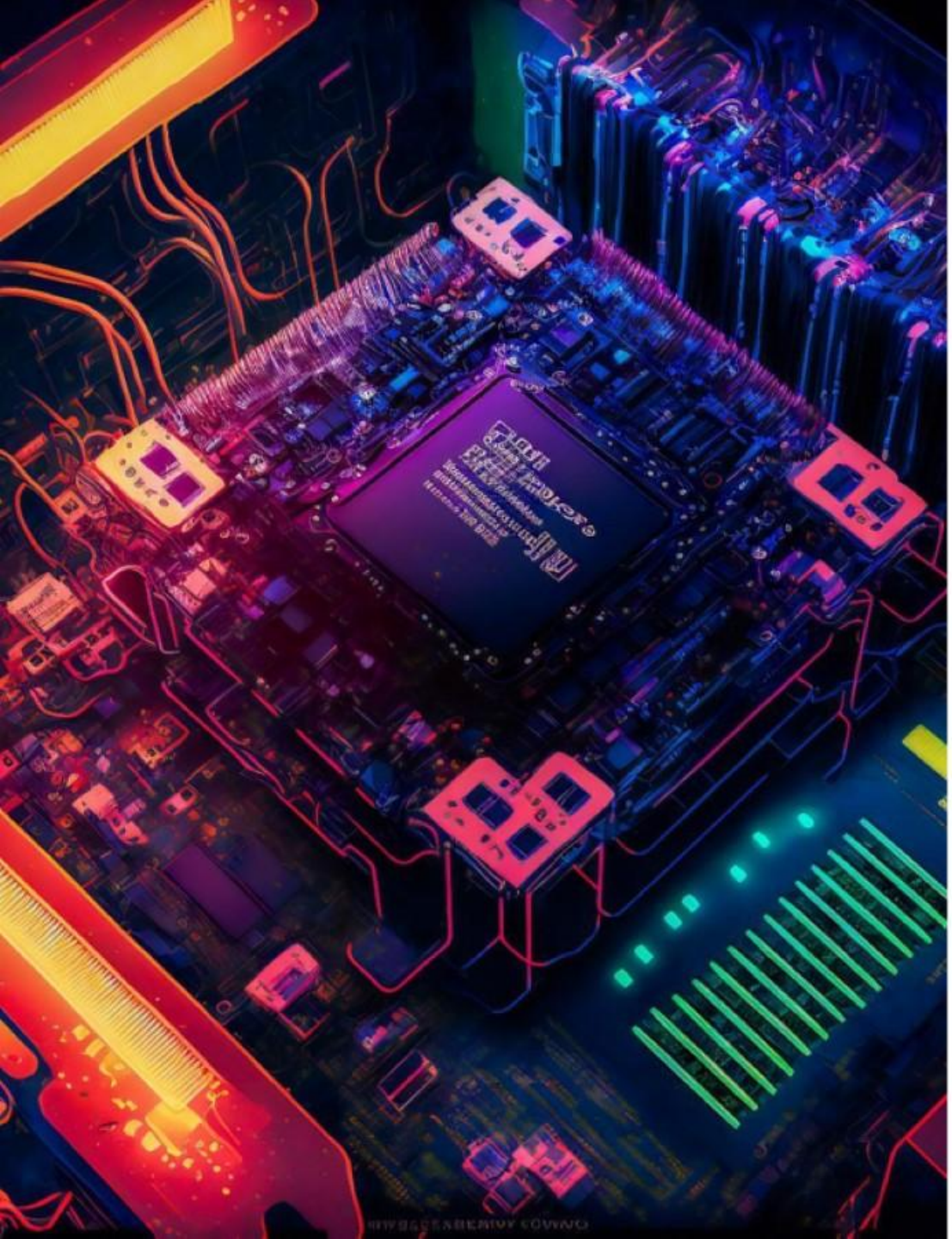
The IAR Platform



The IAR Platform







Summary

- All functional safety standards have corresponding requirements for software tools.
- Use certified tools can significantly accelerate the functional safety product development and certification.
- IAR offers a comprehensive functional safety solution covering compilers, code analysis, and CI/CD automation.
- The latest IAR Platform provides full access to all IAR solutions.


Thank you

PARASOFT

出海功能安全合规—
Parasoft 自动化测试验证体系构建与认证加速方案

徐晨英
Selina Xu

演讲大纲

1 出海合规第一步

2 出海合规白盒级测试解决方案

3 统一的软件质量管理控制平台

出海合规第一步，我们需要做什么

核心步骤：合规风险评估与法规识别

行业特定法规：

1）汽车行业：需符合ISO 26262（ASIL分级）功能安全标准，欧盟ELV指令限制有害物质使用

2）医疗设备：遵循IEC 62304（软件生命周期要求），美国FDA 21 CFR Part 820（质量体系法规）

3）工业设备：IEC 61508（功能安全基础标准），欧盟ATEX指令（防爆设备认证）

即必须符合对应的功能安全认证标准

什么是功能安全?

安全　远离不可接受的风险

风险　伤害发生的可能性和严重程度的组合

功能安全的目标是把风险降低到可接受的程度.

出海合规——汽车软件代码级测试解决方案 (ISO26262)

IEC 61508
E/E/PE 通用标准

ISO 26262
道路车辆

IEC 61511
工业过程

IEC 61513/60880
核能工业

IEC 62061
机器安全

EN 50128
轨道交通

ISO26262危害分析以及风险评估

1.严重度的划分

	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害

2.暴露率等级

	E0	E1	E2	E3	E4
描述	不可能	非常低的概率	低概率	中等概率	高概率

3.可控性描述

	C0	C1	C2	C3
描述	原则上可控（一般，易控），可控	简单可控	正常可控（一般）	难以控制或不可控

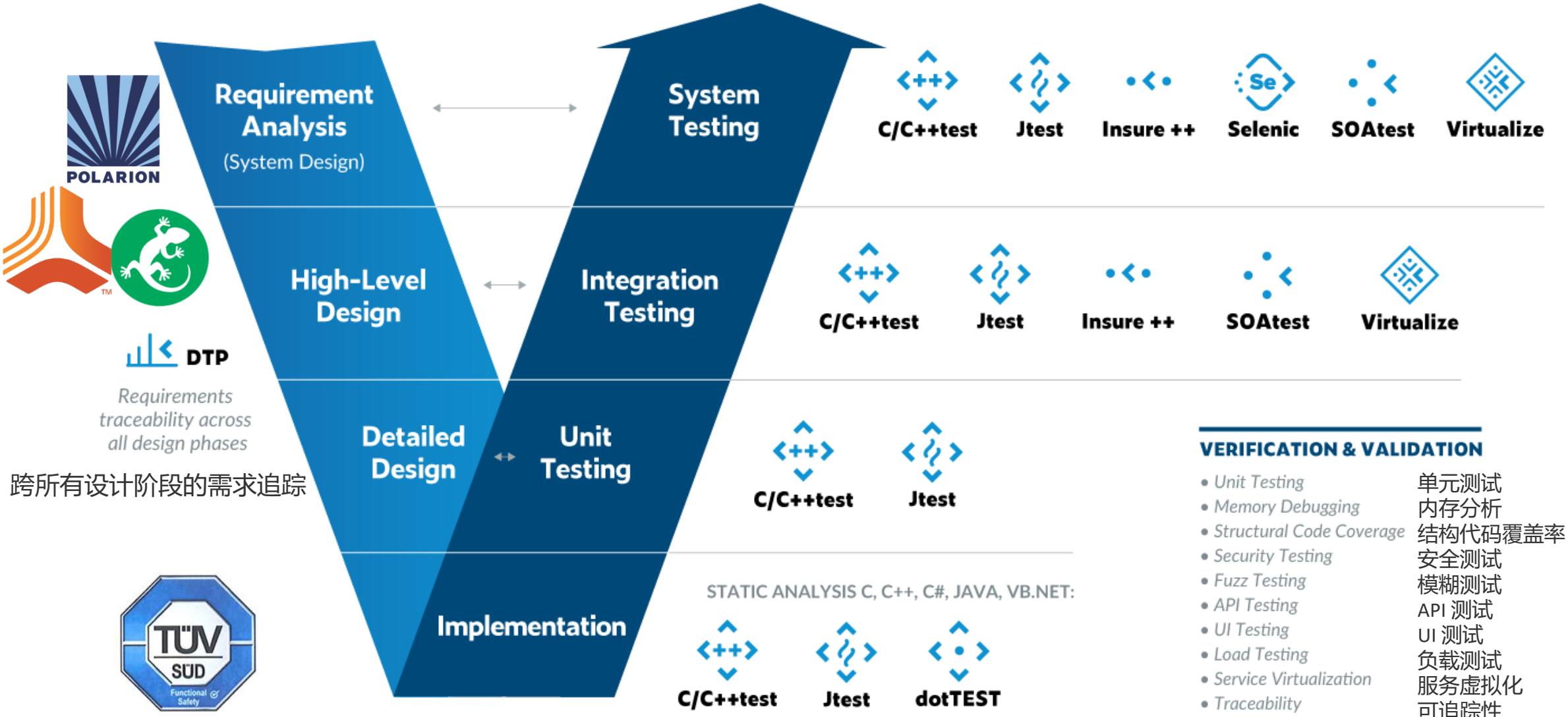
演讲大纲

1 出海合规第一步

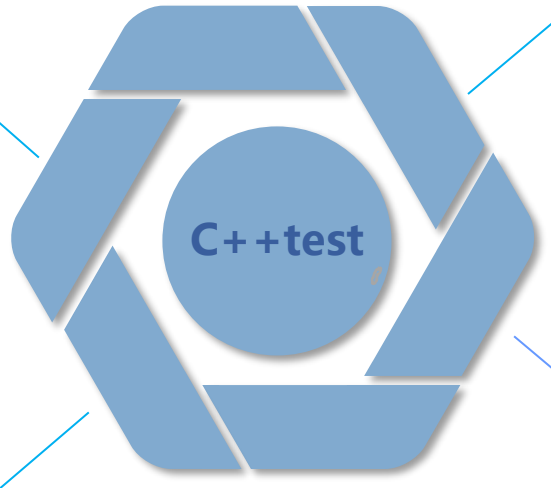
2 出海合规白盒测试解决方案

3 统一的软件质量管理控制平台

贯穿整个软件开发生命周期不同阶段



出海合规白盒测试解决方案— 全球最完整技术链条



代码逻辑分析-FA

分析代码逻辑，查找运行时错误问题，指向问题根源，Parasoft 专利技术

静态语法分析-STA

逐行分析代码确认代码质量，扫描效率，误报率，漏报率全球领先

代码度量分析

分析代码度量指标，检测代码复杂度、合理性，降低代码维护、迭代成本

持续集成能力

灵活方便的集成多种不同继续构建系统，集成多种不同管理系统

单元测试

通过分析代码，指导使用者快速创建并评估单元测试用例，快速达成单元测试要求

AI赋能，静态分析效率破局，加速出海合规认证流程

静态分析效率的瓶颈，在于传统技术的局限性

传统静态分析技术

VS

AI大模型

简单、高效、稳定

数据流、函数上下文信息充足

管报不管修，修复建议缺乏针对性

代码修改效率低

推理能力出众

提供针对性的修复建议

自动修复违规代码

代码修改效率高

针对违规代码结合AI分析，提供针对性的修复建议

结合AI智能判断缺陷真实性

Parasoft C/C++test

诊断

代码违反了 `BD-PB-ZERO` 规则，因为 `person->daysWorkedInPassedMonth` 可能为零，这会导致在计算日薪时发生除以零的错误。

OpenAI deepseek

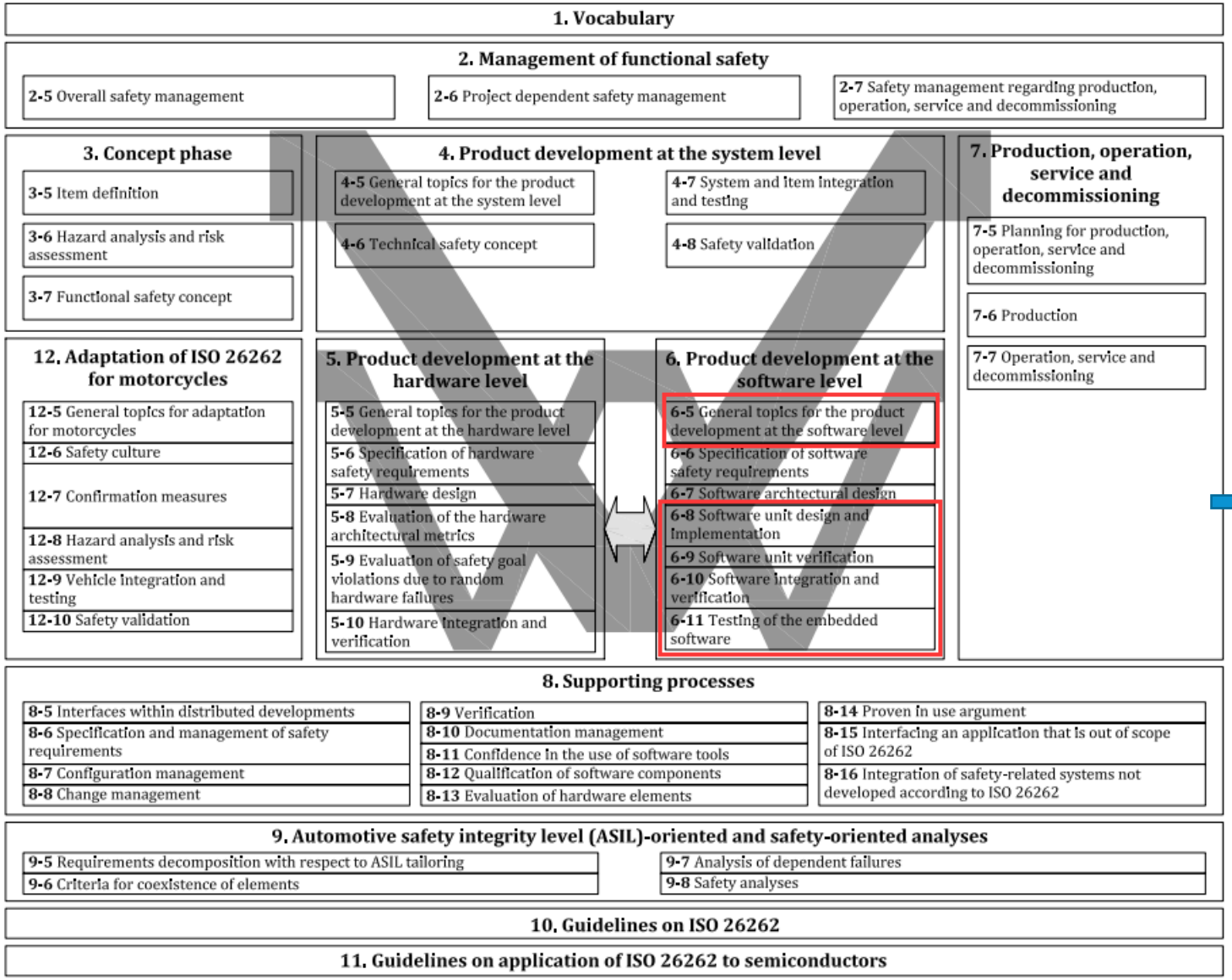
一键生成修复建议

```
void displayPersonalInfo(Person *person)
{
    printf("Name: %s\n", person->name);
    printf("Salary: %d\n", person->salary);
    if (person->daysWorkedInPassedMonth != 0)
    {
        printf("Day's pay: %d\n", person->sal
    }
    else
    {
        printf("Day's pay: N/A (days worked i
    }
}
```

此修复确保仅在 `person->daysWorkedInPassedMonth` 不为零时执行除法操作，从而避免除以零的错误。

不仅能发现问题，更能解决问题！

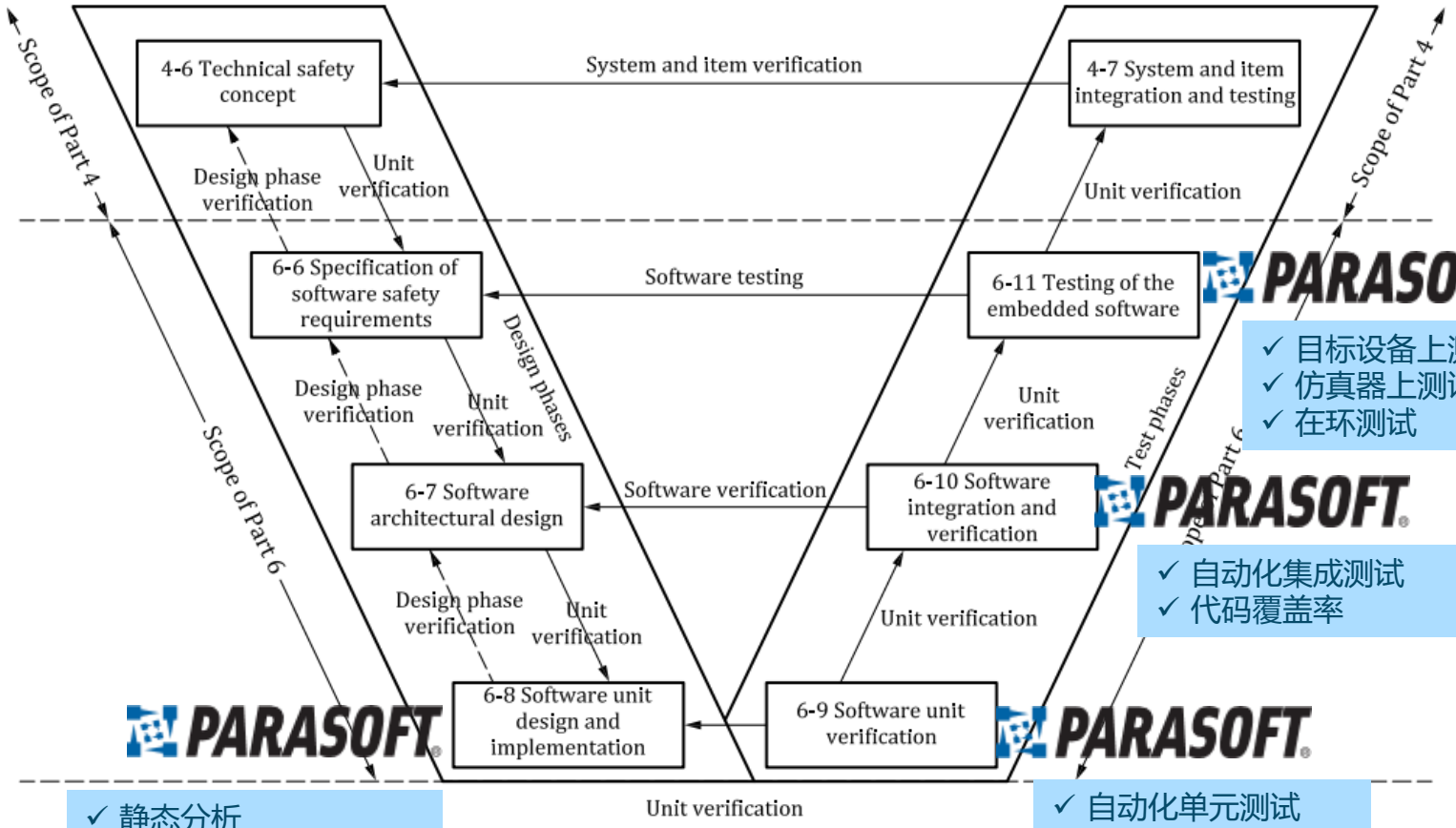
Parasoft 对应 ISO 26262 软件产品开发验证过程



Part 6： 产品开发：软件级

- 6-5 软件产品开发总则
- 6-8 软件单元设计和实现
- 6-9 软件单元验证
- 6-10 软件集成和验证
- 6-11 嵌入式软件的测试

ISO26262 软件级产品开发的参考阶段模型



PARASOFT

- ✓ 目标设备上测试
- ✓ 仿真器上测试
- ✓ 在环测试

PARASOFT

- ✓ 自动化集成测试
- ✓ 代码覆盖率

PARASOFT

- ✓ 静态分析
- ✓ 代码审查
- ✓ 流分析
- ✓ 度量指标分析

PARASOFT

- ✓ 自动化单元测试
- ✓ 需求测试双向追溯
- ✓ 代码覆盖率

Part 6：产品开发：软件级

- 6-5 软件级产品开发的总论
- 6-6 软件安全需求规范拟定
- 6-7 软件架构设计
- 6-8 软件单元设计和实现
- 6-9 软件单元验证
- 6-10 软件集成和验证
- 6-11 嵌入式软件测试

ISO26262软件需求与Parasoft技术能力点映射

<<ISO 26262-6-2018 Part6>> 5.4.6 实现软件设计和实现正确性的需求。这里描述的方法适用于包括建模和编程语言	
需求	**PARASOFT 的能力**
Enforcement of low complexity （低复杂度的实施）	•报告圈复杂度，基本复杂度，Halsted 复杂度和其他代码度量
Use of language subsets （使用的语言子集）	•实施编码标准，例如检测不安全的语言结构
Enforcement of strong typing （强类型的实施）	•隐式转换检测
Use of defensive implementation techniques （使用防御性实现技术）	•根据适当的编码标准规则，实施防御性编程，例如检查malloc的返回值，检查被调用函数返回的错误代码值等等。
Use of well-trusted design principles （使用可靠的设计原则）	•实施行业编码标准规则集，例如MISRA C/C++， JSF，HIS源代码度量等等。
Use of unambiguous graphical representation （使用明确的图形表示）	•执行特定的格式化约定
Use of style guides （使用样式指南）	•执行特定的编码约定
Use of naming conventions （使用命名约定）	•执行特定的命名约定

<<ISO 26262-6-2018 Part6>> 8.4.4规定软件单元设计和实现的设计原则。	
需求	**PARASOFT 的能力**
Design principles for software unit implementation, e.g. Initialization of variables, No implicit type conversions, etc （软件单元实现的设计原则，例如变量的初始化，没有隐式类型转换，等等）	静态分析: • MISRA C规则 • MISRA c++规则 • MISRA C 2012 • MISRA 2004 • 其他标准

<<ISO 26262-6-2018 Part6>> 8.4.5规定了检查软件单元设计和实现的验证方法。	
需求	**PARASOFT 的能力**
Control flow analysis （控制流分析）	•控制流分析
Data flow analysis （数据流分析）	•数据流分析
Static code analysis （静态代码分析）	•编码标准执行
Inspection of the source code （检查源代码）	•DTP变更仪表板视图
Walkthrough of the source code （源代码走查）	•DTP变更仪表板视图

ISO26262软件需求与Parasoft技术能力点映射

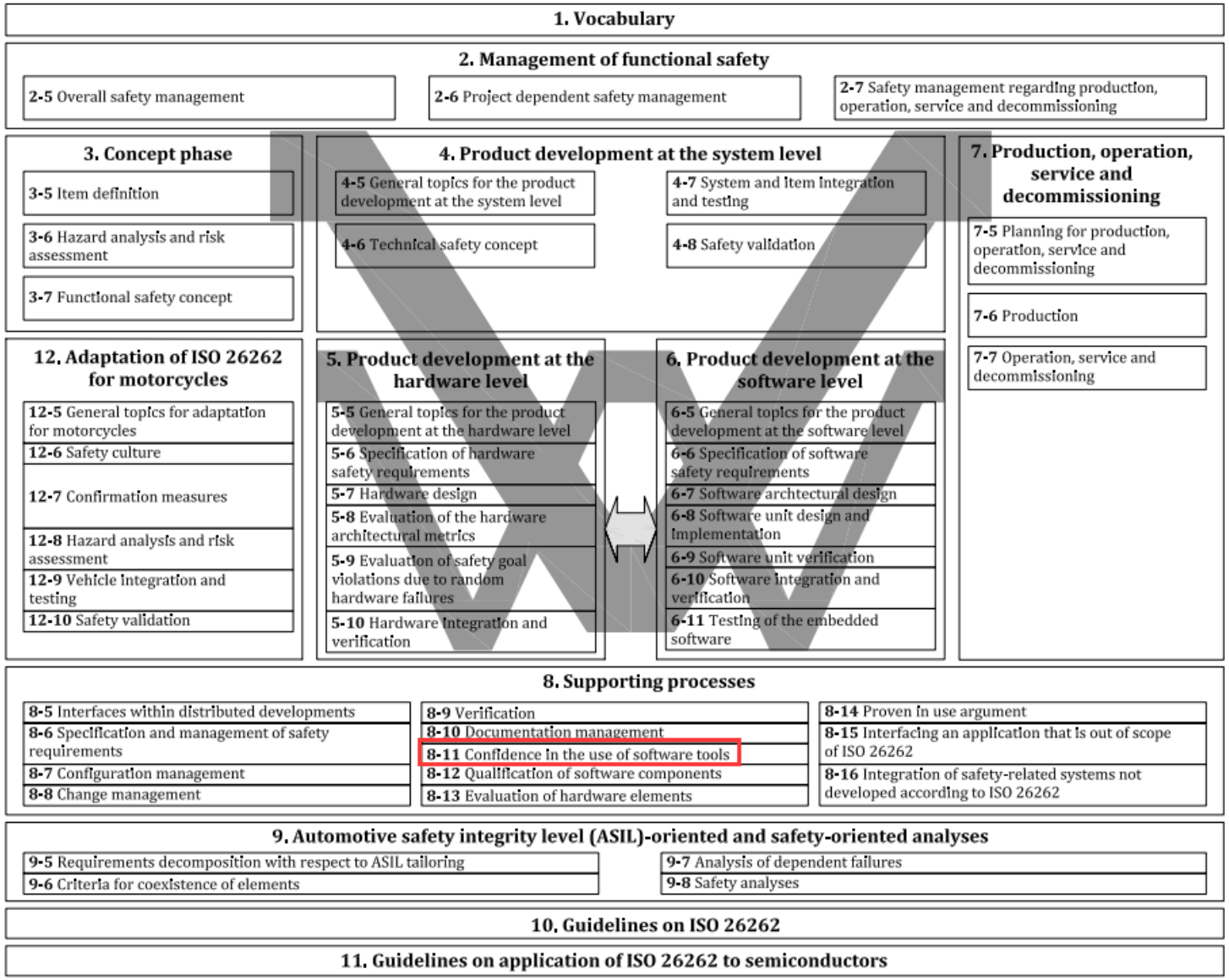
<<ISO 26262-6-2018 Part6>> 9.4.1描述关于单元测试执行的一般信息。	
需求	**PARASOFT 的能力**
Unit test execution （单元测试执行）	•单元测试执行模块 •报告模块，用于展示结果
Unit test specification （单元测试规范）	•根据已定义的规范可配置的单元测试生成模块创建测试 •测试用例资源管理器模块显示所有已定义具有通过/失败状态的测试用例的列表

<<ISO 26262-6-2018 Part6>> 9.4.2描述用于指定和执行单元测试的方法。	
需求	**PARASOFT 的能力**
Requirement-based tests （基于需求的测试）	•测试和要求的双向可追溯性 •需求测试覆盖率报告
Unit test specification （单元测试规范）	•将测试用例与需求和/或缺陷结合到DTP中 •支持手动创建的用户定义测试用例和使用测试用例编辑器创建的测试
Interface tests （接口测试）	•使用函数打桩和数据源来模拟外部组件的行为，以便自动执行单元测试
Fault injection tests （故障注入测试）	•使用函数打桩强制执行故障条件 •使用不同的前置条件集(如最小、最大、启发式值)自动生成单元测试

<<ISO 26262-6-2018 Part6>> 9.4.3定义应该用于创建测试用例的方法。	
需求	**PARASOFT 的能力**
Analysis of requirements （需求分析）	•Parasoft DTP提供了需求到代码和需求到测试的可跟踪性
Generation and analysis of equivalence classes （等价类的生成和分析）	•使用工厂函数为自动化单元测试生成准备输入参数值 •使用数据源以在测试中有效地使用广泛的输入值
Analysis of boundary values （边界值分析）	•自动生成的测试用例(如启发式值、边界值) •使用数据源以在测试中使用广泛的输入值
Error guessing （错误猜测）	•使用函数打桩机制将故障条件注入测试代码

<<ISO 26262-6-2018 Part6>> 9.4.4定义证明测试用例完整性的方法。	
需求	**PARASOFT 的能力**
Statement coverage （语句覆盖率）	•代码覆盖模块
Branch coverage （分支覆盖率）	•代码覆盖模块
MC/DC (modified condition/decision coverage) （修改条件/判定覆盖率）	•代码覆盖模块

Parasoft 对应ISO26262支持过程



Part 8： 支持过程

8-11使用软件工具的置信度

根据ISO 26262的工具鉴定(Qualification)

» 根据工具影响(TI)和工具错误检测(TD)确定软件工具置信度鉴定的级别(TCL)

» 软件工具鉴定证明的目的是提供软件工具在开发安全相关项目或元素时是否适合使用的证据，以便在正确执行ISO26262所要求的活动和任务时获得信心。

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

TI：工具影响
TD：工具错误检测

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]	+	+	++	++

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.

EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508, EN 50128 or RTCA DO-178C.

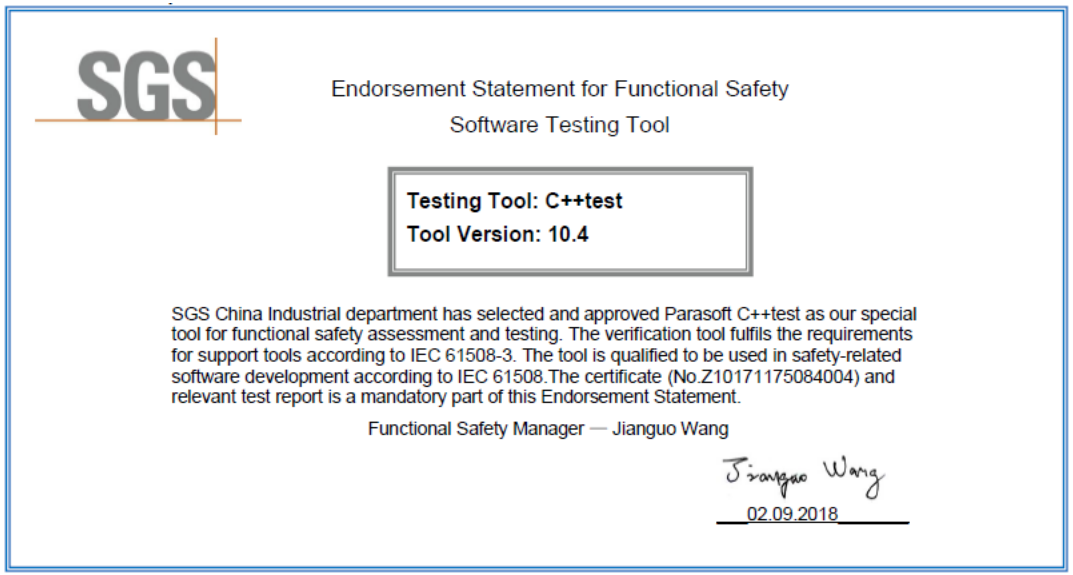
1a：使用中积累置信度，按照11.4.7
1b：工具开发流程评估，按照11.4.8
1c：软件工具确认，按照11.4.9
1d：按照安全标准开发

属于TCL3等级的软件工具需要
ASIL A、ASIL B 适用1a，1b方法
ASIL C、ASIL D 适用1c，1d方法

Parasoft C/C++test鉴定套件(Qualification Kits)

提供符合最高TCL3等级要求的鉴定套件，套件输出包括：

- Tool Classification Report--工具分类报告（TCR）；
  -- 根据功能和用例确定工具的置信度
- Tool Qualification Plan--工具资质计划（TQP）；
  -- 测试用例和资质阶段
- Tool Qualification Report--工具资质报告（TQR）；
  -- 测试和资质证明过程的状态
- Tool Safety Manual--工具安全手册（TSM）；
  -- 配置工具以确保正确使用和减少已知错误



SGS

Endorsement Statement for Functional Safety
Software Testing Tool

Testing Tool: C++test
Tool Version: 10.4

SGS China Industrial department has selected and approved Parasoft C++test as our special tool for functional safety assessment and testing. The verification tool fulfils the requirements for support tools according to IEC 61508-3. The tool is qualified to be used in safety-related software development according to IEC 61508.The certificate (No.Z10171175084004) and relevant test report is a mandatory part of this Endorsement Statement.

Functional Safety Manager — Jianguo Wang

Jianguo Wang

02.09.2018

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE
No. Z10 075084 0005 Rev. 03

Holder of Certificate: Parasoft Polska Sp. z o. o.
Kielkowskiego 9
30-704 Krakow
POLAND

Certification Mark:

Product: Software Tool for Safety Related Development

Model(s): C/C++test

Parameters: Tool classification: T2 (acc. to IEC 61508)

The verification tool fulfills the requirements for support tools according to IEC 61508-3. The tool is qualified to be used in safety-related software development according to IEC 61508, EN 50128 and ISO 26262. It is suitably validated for use in safety-related development according to IEC 62304. The test report is a mandatory part of this certificate.

Tested according to:
IEC 61508-3:2010
IEC 62304:2015
ISO 26262-8:2018
EN 50128:2011/A2:2020

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. This certificate is valid until the listed date, unless it is cancelled earlier. All applicable requirements of the testing and certification regulations of TÜV SÜD Group have to be complied. For details see: www.tuvsud.com/ps-cert

Test report no.: PK83996C

Valid until: 2026-07-05

Date, 2021-07-06

(Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

演讲大纲

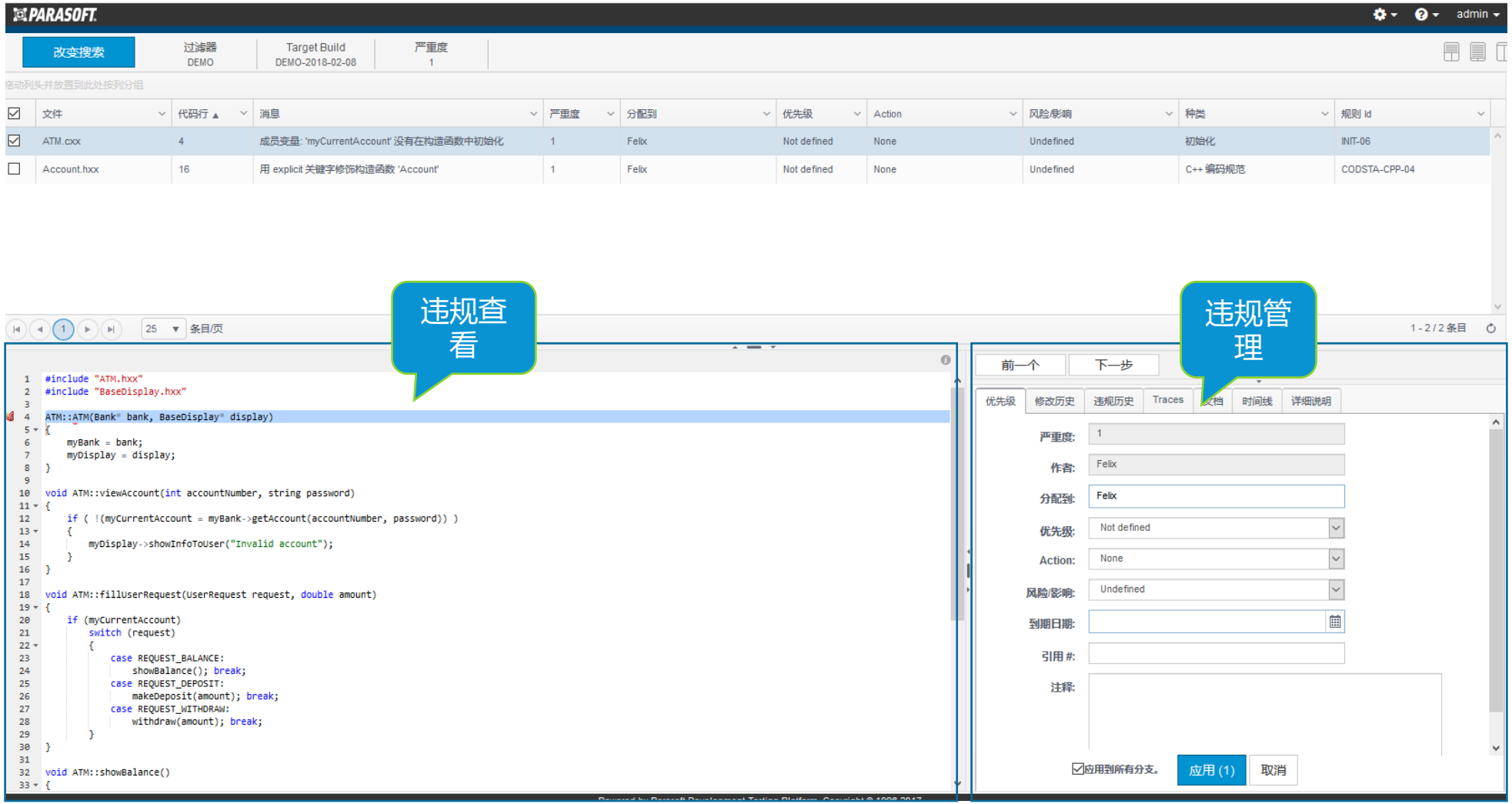
1 出海合规第一步

2 出海合规白盒级测试解决方案

3 统一的软件质量管理控制平台

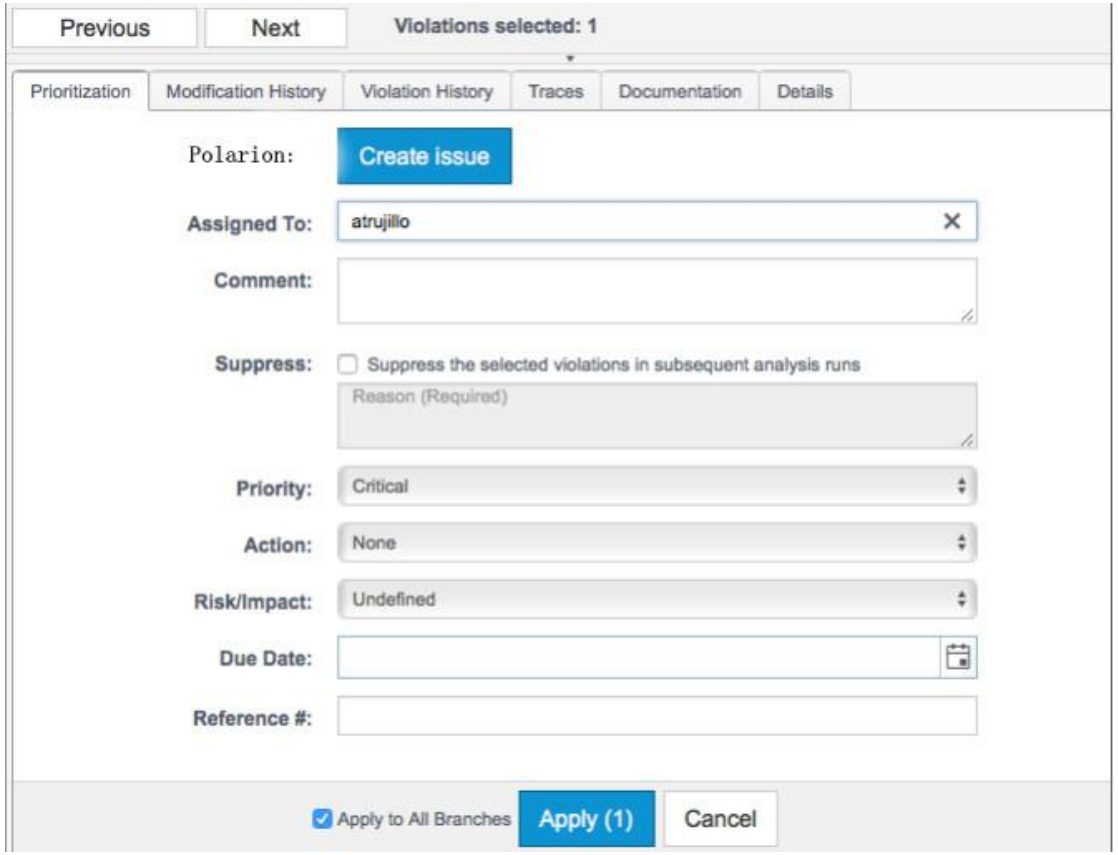
Parasoft DTP **报告中心**

Parasoft DTP **报告中心**

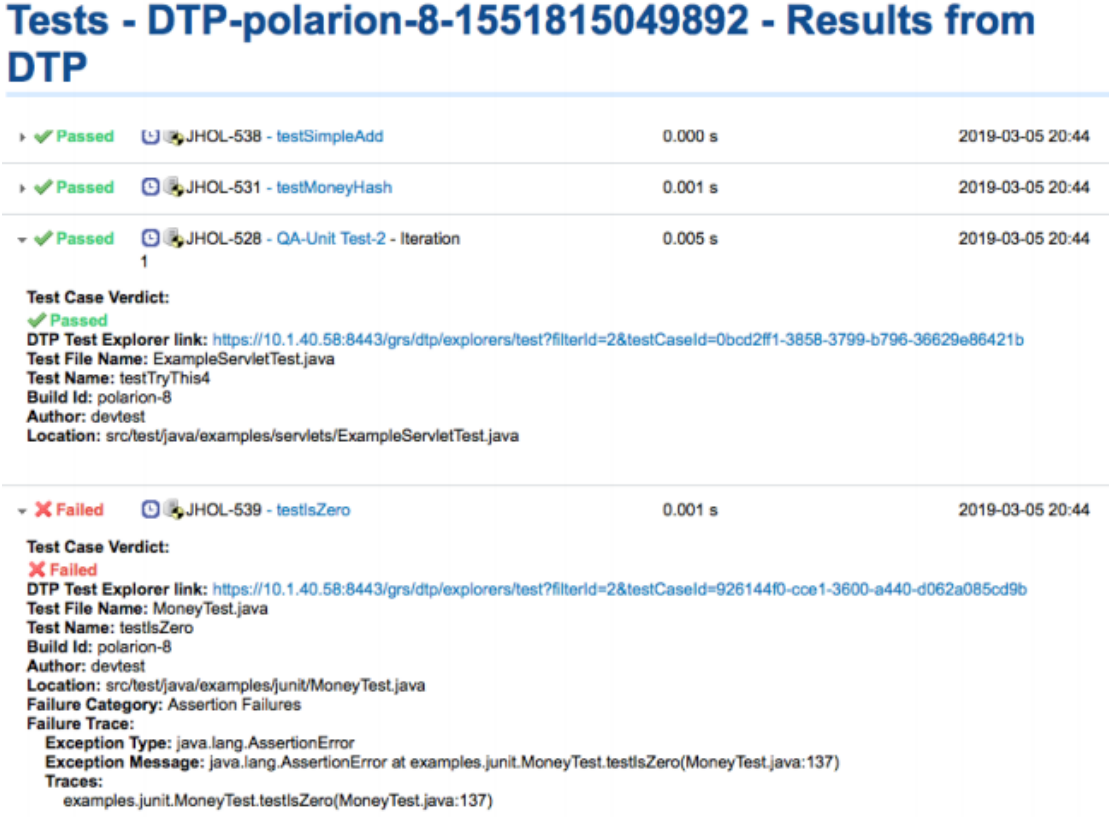


代码级解决方案 —Polarion无缝集成实现实时追溯性

PARASOFT® ⟷ 自动同步 ⟷ Polarion® ALM™

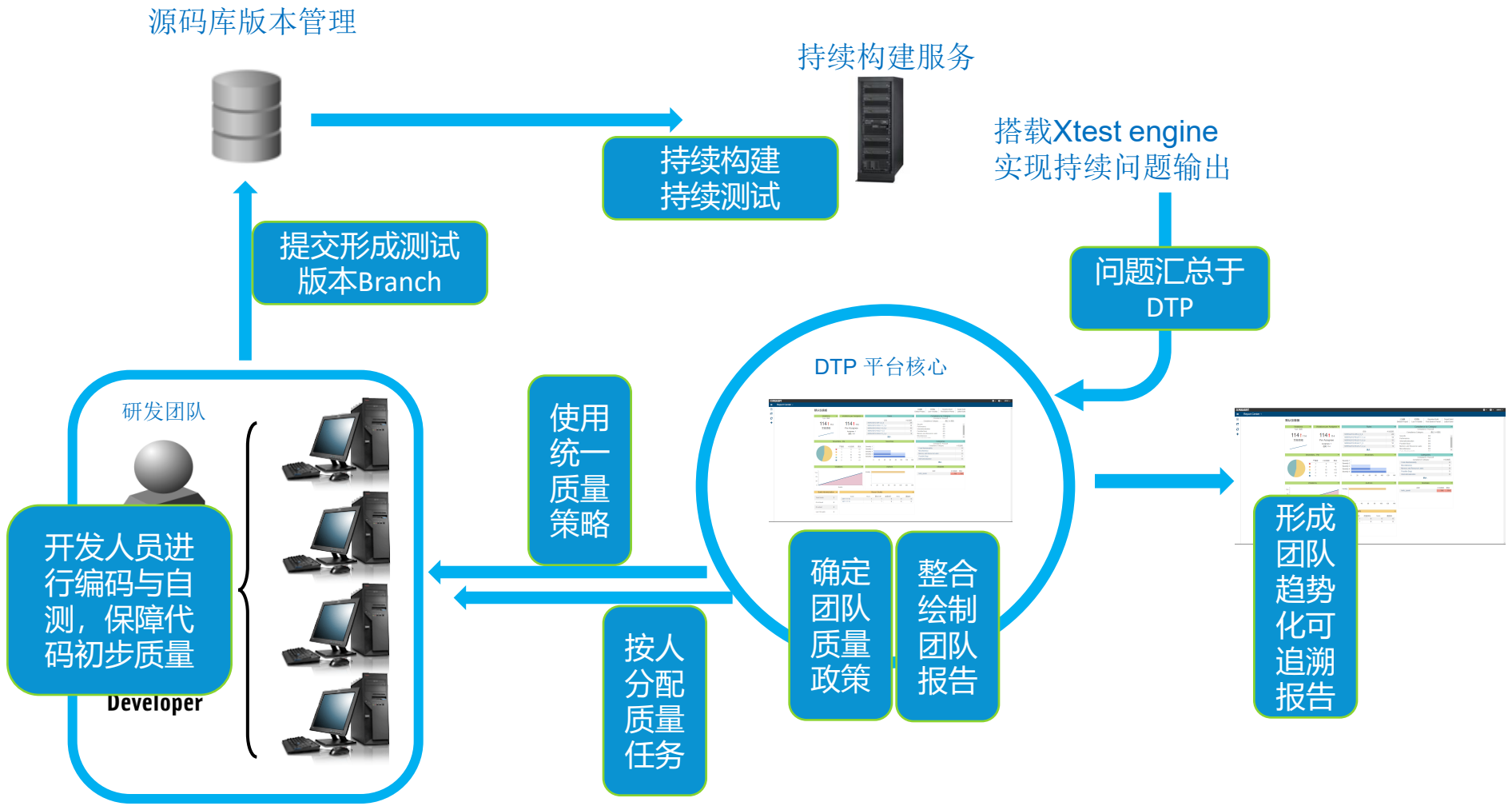


在Parasoft测试结果上直接创建Polarion Issue



在Polarion上直接通过Parasoft生成的测试用例代码验证需求

代码级解决方案 — 质量控制平台



德国大众集团对Parasoft的选择– 案例学习

CASE STUDY: VW Group

E3 (End-to-End Electronics) MEB Architecture that will be used in the next 10-15 years for all their cars.

Challenge:

Modernization of software development and testing platform triggered the need to acquire best-of-breed product for safety critical and security standards including MISRA2012, CERT C, CERT C++, AUTOSAR C++14, ISO26262.

Solution:

Modern, open architecture of C/C++test, combined pattern, flow and metrics analysis combined with unit testing + coverage in one vendor solution, ability of custom rules creation with RuleWizard, enterprise CI/CD integration, leading combination of safety critical and security solutions, advanced reporting and analytics (DTP).

Benefits:

- Full support for ISO26262 Static Analysis and Unit Testing requirements **in one tool**
- Support for containerized development and test environment
- Responsive and agile product team
- Integrated support for MISRA and AUTOSAR standards

Parasoft Complete Quality Suite

Unit Testing | Static Analysis | API Testing + SV

"Parasoft is the only company that provides everything to fulfill complete ISO26262 requirements."

PARASOFT

Perfecting software

谢谢您的观看指导!

We help our customers mitigate risk, drive higher software quality, and achieve their corporate objectives.

全球工业准入介绍

以更高标准把握未来

演讲：季方舟 Joe Ji

内容

1. CSA集团简介；
2. 北美工业整机及及产线合规路径
3. 欧盟CE-机械指令
4. 合规建议及最佳实践分享

CSA集团简介

CSA集团介绍

- CSA Group is one of the largest standards development organizations in North America
- CSA集团是北美最大标准开发机构之一，拥有1万余标准专业会员，约1115个标准技术委员会，跨越12个重点领域；
- World-famous certification body in Testing, Inspection and Certification；
- 全球知名认证机构，专业于测试，检验，认证；
- Accredited and recognized by numerous organizations around the world: SCC, OSHA, ANSI, IEEECB, ATEX, EMC, RED, etc.
- 拥有各个官方权威资质授权，如SCC, OSHA, ANSI等；

3,000+
发布的规范和标准
我们为加拿大、美国和世界其他地区在12个重点领域开发编制标准。

100+年
认证经验
公司凭借百年经验蜚声国际，不负重托。

140多个
国际市场
我们的全球实验室提供认证服务，协助您打入全球140多个市场。

行业知识与技术熟练程度相结合

THE CONFIDENCE TO GET IT RIGHT THE FIRST TIME

家庭和商业
电器
工具+户外设备
建筑与建筑产品
照明
信息和通信技术

工业
工业与危险区域防爆
设备
发电与储能
个人防护装备

医疗
医疗和实验室及测量
设备

新兴技术
网络安全
电磁
功能安全
全球市场准入
特殊检验/现场评估

为您提供可靠的产品测试、检验和认证

我们的服务不断完善

创建解决方案，促进业务发展

消费者产品评估

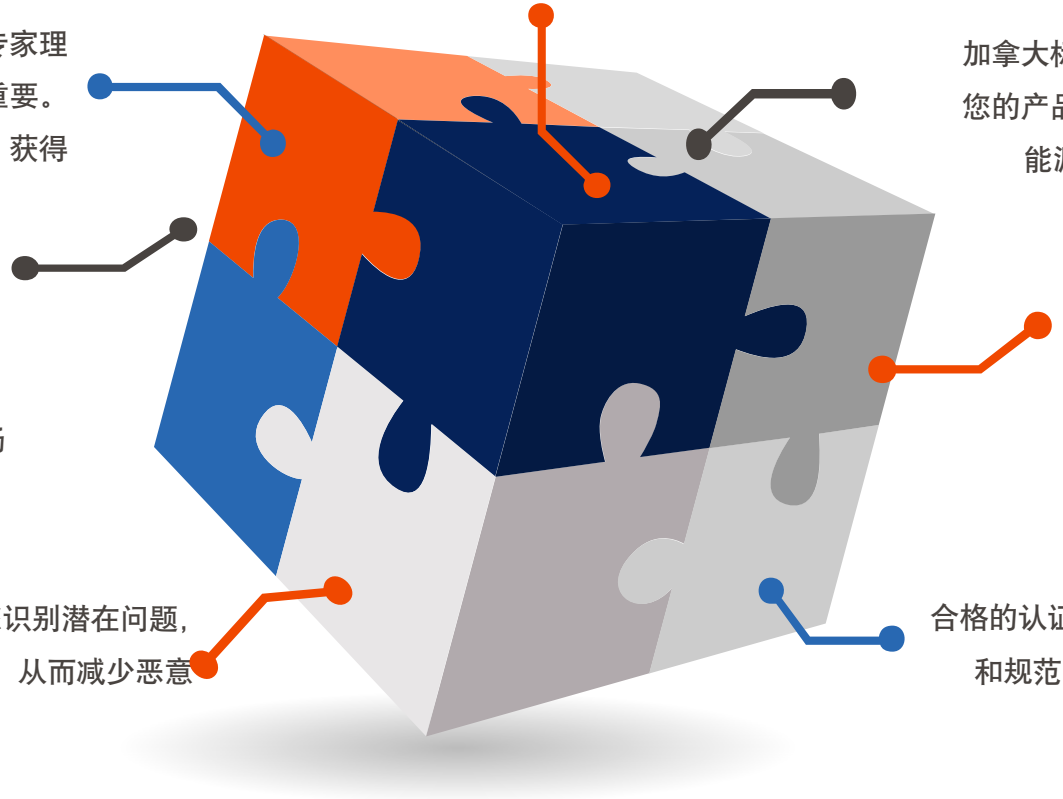
为一系列零售产品提供第三方独立验证、检验和检测服务，因此您可以做出知情决策，确保客户满意。

认证

跟上全球市场机遇的快速步伐。我们的认证专家理解可靠且可预测的服务对您的业务发展至关重要。我们可以帮助您充分利用当今的全球化经济，获得准入全球新市场所需的认可。

能效验证

加拿大标准协会集团提供能源效率验证服务，以显示您的产品符合北美能效要求。我们的服务包括一整套能源效率标准，包括ENERGY STAR®等。



全球市场准入

获得一站式认证服务，帮助您准入多达200个国家的市场

功能安全

通过快速高效的安全评估服务、技术指导和培训，为客户提供定心丸

网络安全

与您密切合作，开发定制解决方案，助您识别潜在问题，执行覆盖整个产品生命周期的安全措施，从而减少恶意入侵和攻击的机会。

现场评估/特殊检验

合格的认证专家将参照安全及其他适用标准和规范，评估贵司未经认证的产品。

北美工业整机及及产线合规路径

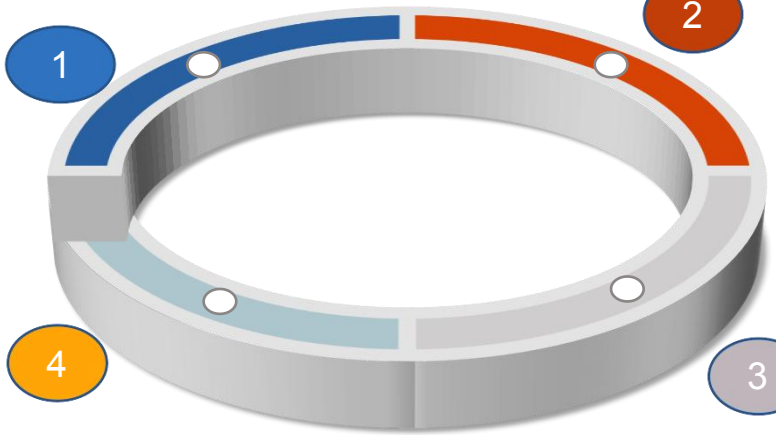
北美监管体系

Writes Regulations/制定法规
Adopts Codes and Product Standards/采纳法规与标准
Recognizes Certification Schemes/批准认证程序
Recognizes work performed by Accredited CB's/认可审核机构工作

Creates product/产品生产
Decides where product will be sold/决定产品目标市场
Must comply with regulations/确保符合当地法规

1 Regulatory Body / 监管机构

2 Manufacturer / 制造商



4 Accreditation Body /资质审核机构

3 Certification Body / 认证机构

Recognized by Regulatory Body/由监管机构认可
Assesses CB's compliance with Certification Scheme/审核认证机构工作程序的符合性
Gets Direction from Reg. Body/监管机构指导工作

Gains Accreditation for Certification Scheme/获取相应认证资质
Evaluates Products/评估产品
Makes Statement of Conformity/颁发符合性证书或声明

The Role of the AHJ

Authority having jurisdiction (AHJ) — **the organization, office, or person** authorized to determine what electrical equipment, appliance, or device may be installed, used, or sold within their area of jurisdiction.

(From SPE-1000-21)

Authority Having Jurisdiction (AHJ) **— An organization, office or individual** responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

(From NFPA70)

典型AHJ:

- 地方政府:建筑部门、消防部门
- 州政府:州消防局长、州卫生部
- 联邦政府:医疗保险和医疗补助服务中心(CMS)
- 私营部门:保险公司（限保险事宜）

AHJ职责:

- 解释当地的法规决定产品上认证标志是否可接受
- 保障群众生命、财产和安全

Access to Canada

"Approved (as applied to electrical equipment) —

a) equipment that has been certified by a certification organization accredited by the Standards Council of Canada in accordance with the requirements of …

b) equipment that conforms to the requirements of the regulatory authority (see Appendix B).

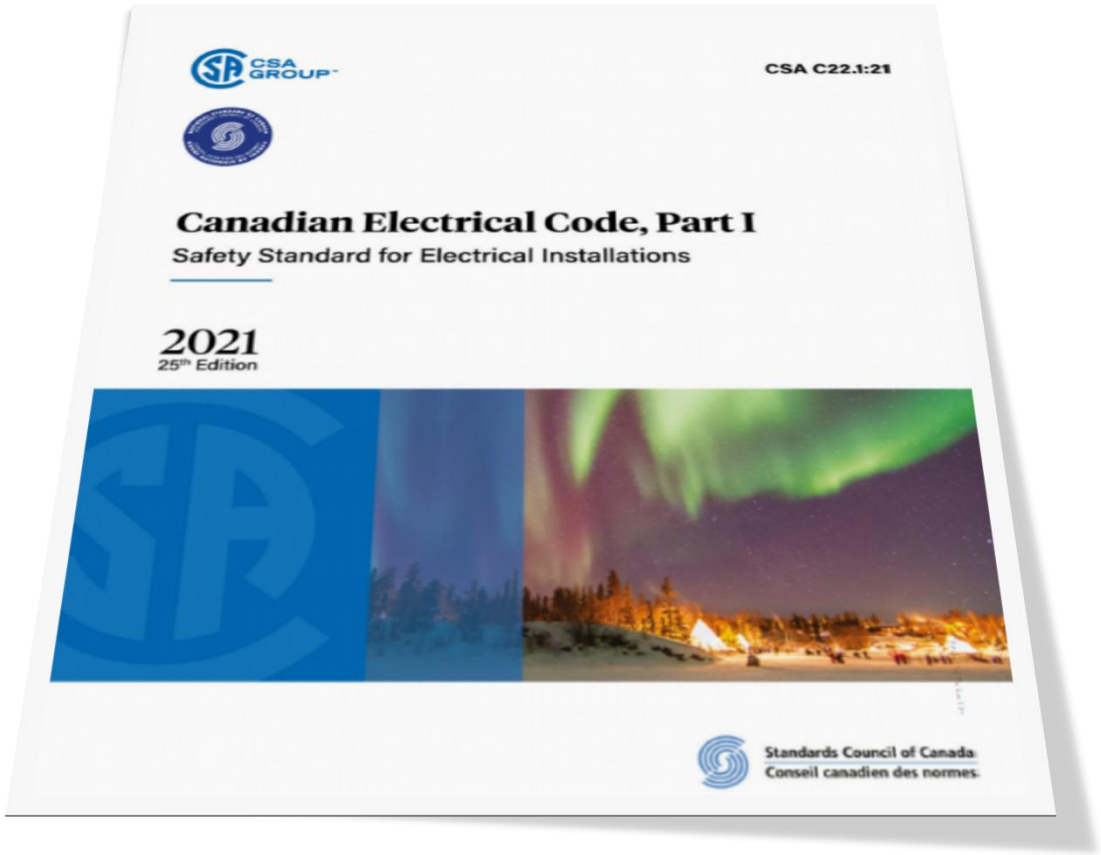
Notes:

1) This is the Canadian Electrical Code, Part I definition.

2) Item b) covers field-evaluated equipment."

From CSA C22.1

CE Code and use of "*Approved*" equipment are enforced through regulation and inspection



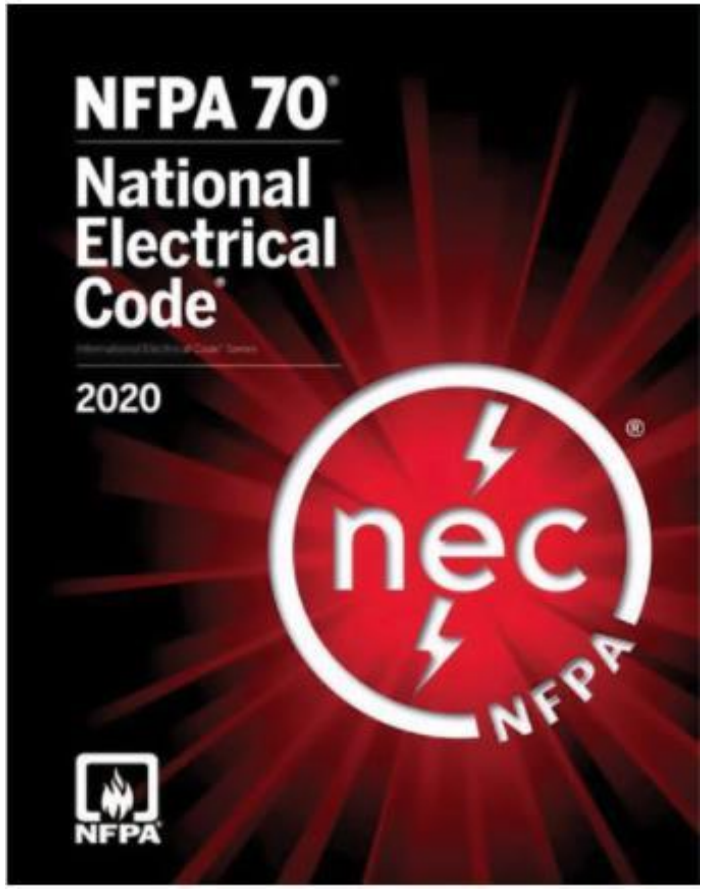
Access to United States

"Approved. Acceptable to the authority having jurisdiction.

Labeled - Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner."

From NFPA 70

44,000+ AHJ



现场评估的特点

基于现场的评估服务

被监管机构认可

非认证程序（没有厂检、年费）

限量销售/型号/年/制造商的设备

不适用于零部件的进一步评估

不适用于载人升降平台、电梯、上爬辅助设备和相似的系统（控制柜除外）

不适用于导线、线缆、接线装置、特定医疗设备

不适用于危险区域

现场评估围绕的关注点

一般审核事项包括：

- 耐压测试；
- 温升测试；
- 漏电流测试
- 拉不脱测试
- 淋雨测试
- 零部件认证和使用条件
- 铭牌、警示标识
- 机械组装和防护；
- 电源隔离
- 接地可靠性

...

现场评估流程

前期审核

技术会议；
符合性要求解释沟通；
设计资料准备；

设计确认

铭牌信息
零部件符合性
安装要求
电气设计等

初次检验

- 申请范围一致性检查
- 现场查验零部件认证信息、安装、应用
- 核对整机设备的安装、应用、设计合规性
- 不符合项总结和通知

最终检检

- 核对整改要求
- 现场开展必要测试

符合性交付

- 现场贴标
- 评估性报告

特殊检验/现场评估比较

CSA

CAN-Special Inspection

U.S Field Evaluation

SI Special inspection 加拿大特殊检验	USFE US field evaluation 美国现场评估
标准 SPE-1000-21和相关产品标准	**标准** NFPA 790, NFPA 791, ANSI/UL 及相关产品标准
数量 不超出500台/型号/年	**数量** 有限数量
检验地点 安装现场、CSA实验室、制造商工厂或指定场所	**检验地点** 在任何现场、制造商、CSA实验室
贴标地点 安装现场、CSA实验室、制造商，或指定场所	**贴标地点** 依据AHJ要求
	

产品范围

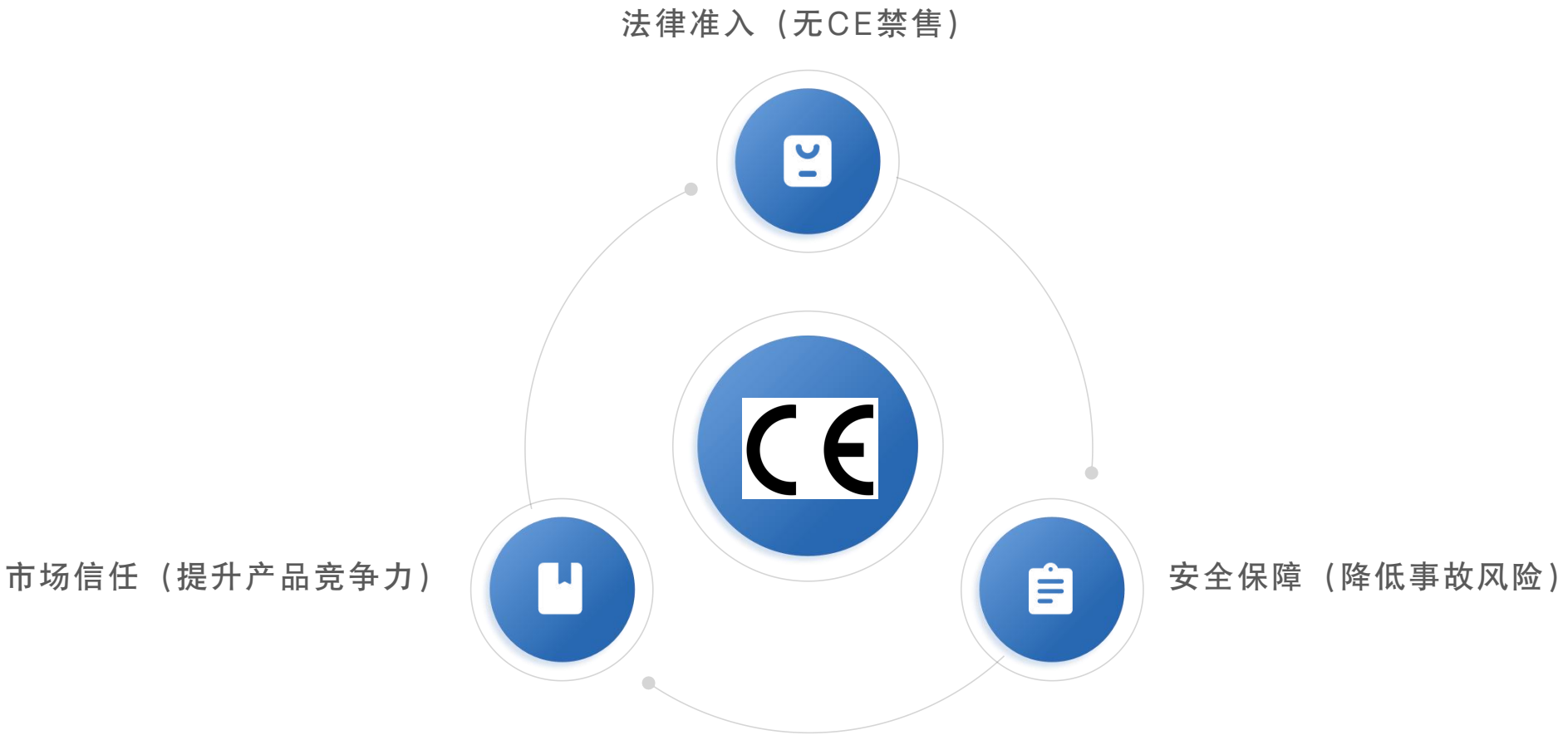
CSA集团可进行现场评估的产品包括，不限于：

- 工业控制面板（ICP)
- 自动制造、组装和包装设备
- 半导体制造设备
- 灯具、打标机和展示柜
- 配电盘，控制盘柜和电机控制中心
- 加热和制冷设备
- 商用烹饪和食品服务设备
- 变压器
- 自动引导车辆（AGV),
- 智能辅助设备
- 机器人和机器人设备
- 分布式发电设备
- 储能设备
- 光伏设备和产线
- 微电网系统
- 数据中心
- ...

欧盟CE-机械指令

CE认证是什么?

进入欧洲市场的强制性安全合格标志



认证流程

风险评估

标准：EN ISO 12100

方法：识别危险 → 设计防护

技术文件准备

内容：设计图、测试报告、说明书、风险评估记录

签署符合性声明（DoC）

法律文件，随产品提供，欧代

加贴CE标志

最小尺寸5mm，需永久附着

新旧机械法规的变化

升级方向	原指令 2006/42/EC	新法规 (EU) 2023/1230
法规性质	指令（成员国需转化）	法规（直接适用，统一执行）
技术要求	传统安全标准	新增网络安全、AI 安全、自动机械自检等
覆盖范围	传统机械	纳入平衡车、3D 打印机、电动家具等新兴产品

工业中其他常见法规

低电压指令（LVD）-2014/35/EU

适用范围：交流50V~1000V、直流75V~1500V 的电气设备，如工业电机、控制器、开关电源、变压器等。

电磁兼容指令(EMC)-2014/30/EU

适用范围：所有电子电气设备,确保设备在电磁环境中正常工作，且不干扰其他设备.

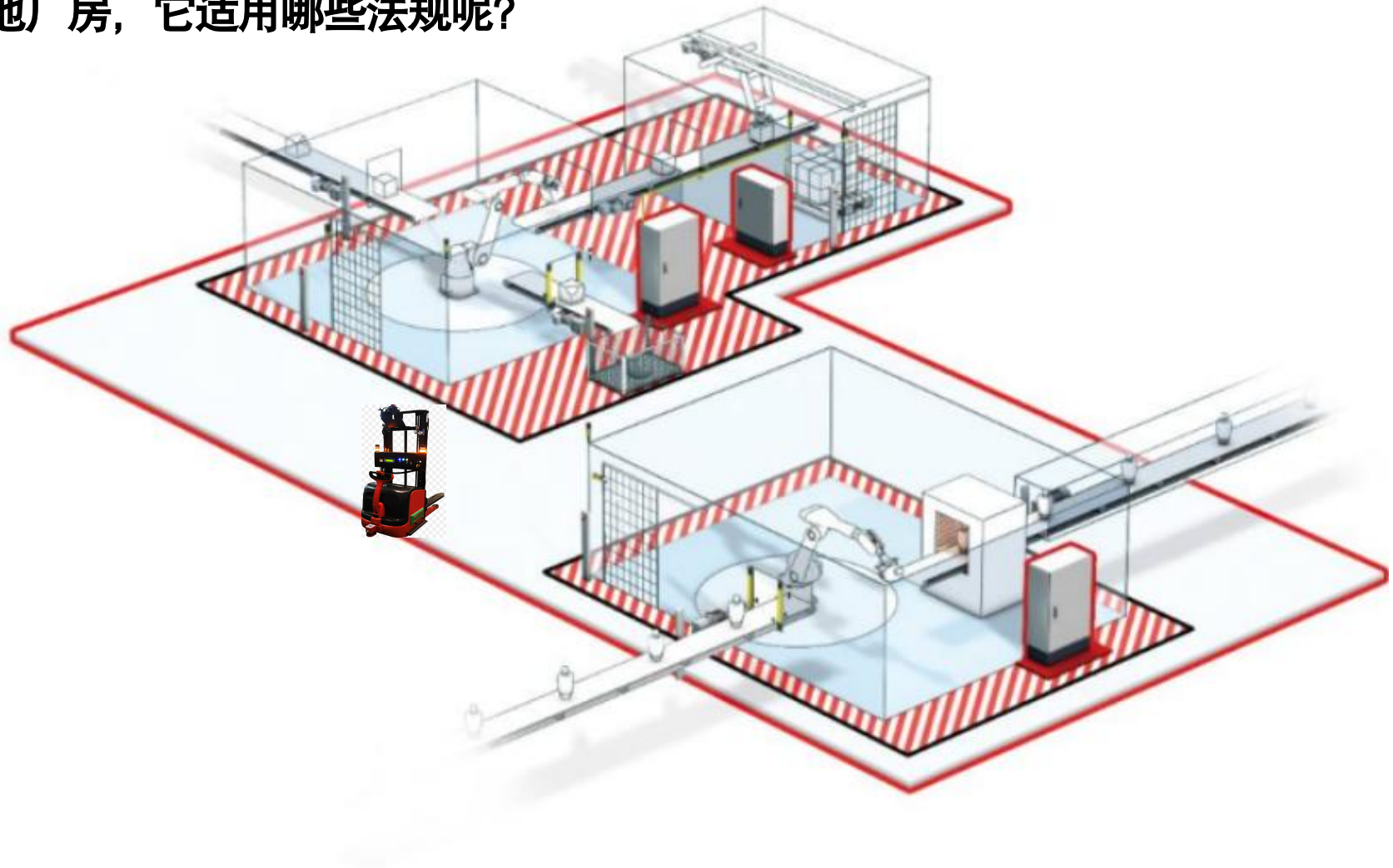
潜在爆炸性环境设备指令（ATEX）-2014/34/EU

适用范围：在爆炸性气体、粉尘环境中使用的设备，如石油化工行业的电机、灯具、传感器、阀门等。

合规建议及最佳实践分享

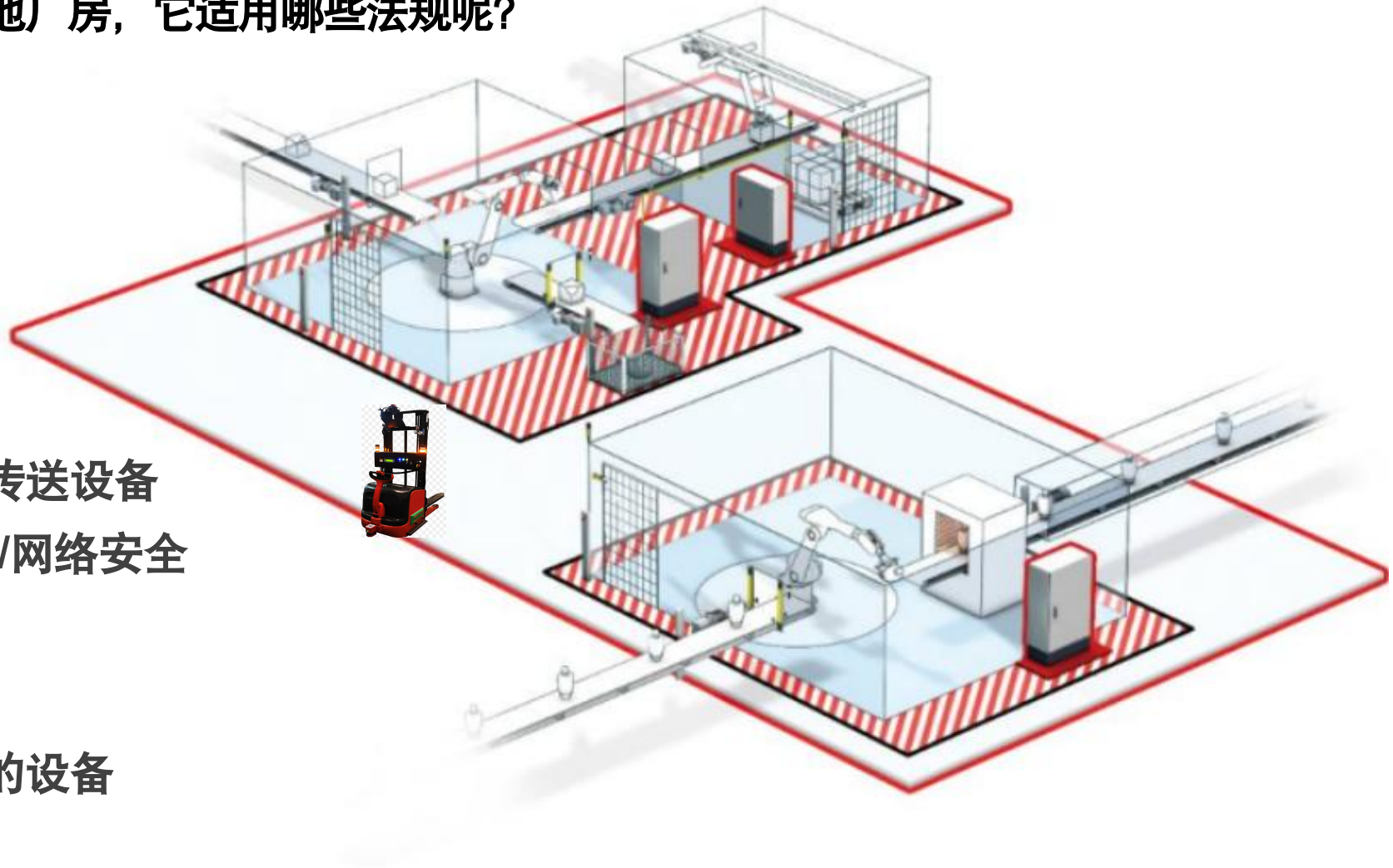
标准之间的互动---*CE*

如果这是一个锂电池厂房，它适用哪些法规呢?



标准之间的互动---*CE*

如果这是一个锂电池厂房，它适用哪些法规呢?



1. 机械（MD）

- 例如：机器人，传送设备

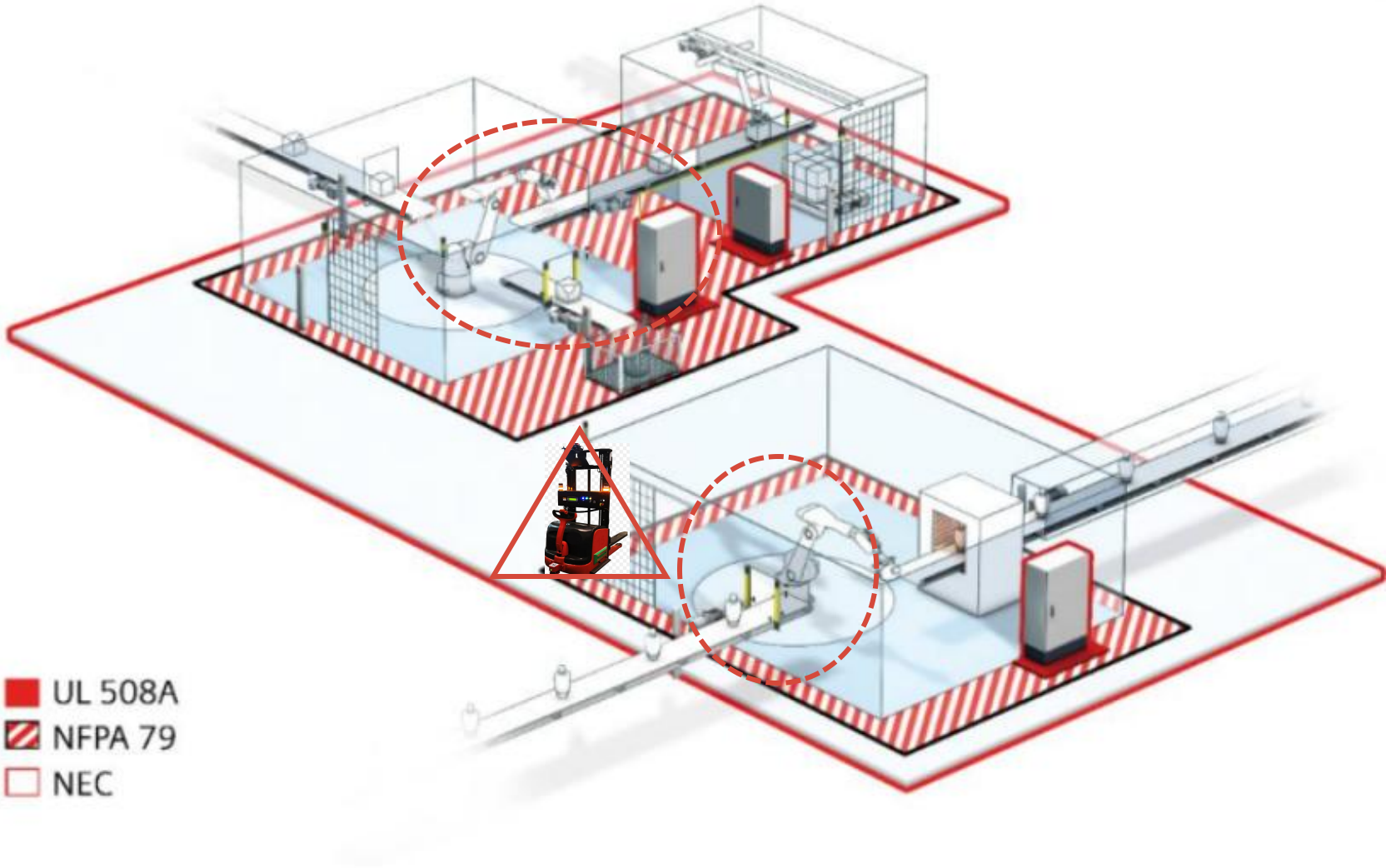
2. LVD/EMC/RED/网络安全

- 产线各设备

3. 防爆（ATEX）

- 潜在爆炸环境下的设备

标准之间的互动---北美



Thank you.

Address:
上海市宜山路889号4号楼1楼
中国，上海

Phone Number:
15300504841

Email:
Joe.ji@csagroup.org

FSG（功能安全专家小组）

FSG Functional Safety Group

FSG（功能安全专家小组）是一个专门研究嵌入式功能安全的专家组织，汇集了在功能安全认证领域提供专业知识、封装方案和开发资源的顶尖企业。FSG提供功能安全相关的一站式服务，包括从功能安全标准的解读，到具体实施方案的制定，再到认证过程的全程指导，确保客户的产品在满足最高安全标准的同时，能够高效地推向市场。

我们随时准备根据您的需求提供帮助，共同推进功能安全技术的发展和应用。

FSG中国成员：

CETC 普华基础软件　iar　MUNIK　芯来科技 NUCLEI　NXP　PARASOFT　RENESAS 瑞萨