ISO 26262：2018 功能安全管理体系
标准理解培训（3 天）

课程背景：

ISO 26262 于 2011 年 11 月份发布，是针对功能安全分析的标准，由 10 部分组成。ISO 26262：2018 版在 2018 年 12 月 20 号正式发布，新的 ISO 26262 第二版有什么变化，它将如何影响你？本课程在 2011 版基础上介绍 ISO 26262:2018,第 2 版 - 变化和亮点。

ISO26262 标准被美国和欧洲整车厂广泛采用，绝大部分整车厂都开始要求设计新的车型时采用 ISO 26262 的要求。同时一级供应商为了满足整车厂在询价阶段对 ISO26262 提出的要求，也正在接受该标准。该标准要求子系统、硬件/软件以及半导体供应商都满足 ISO2626。

丰田汽车刹车门的事件，也使软件和硬件的集成得以重视。众多整车厂的 CEO 和董事会开始对功能安全极其关注，认为新开发的电子、电控、软件和传感器等给企业带来很多的风险，因此采取要求实施 ISO2626 和汽车 ASIL 水平来降低风险。显然，ISO26262 的推行不可避免。

目前要求实施 ISO 26262 的驱动力量：欧洲的汽车客户如宝马 BMW, 博世 Bosch, 梅塞德斯 Mercedes, 菲亚特 Fiat 等；欧洲的法律法规也在促使企业满足 ISO26262。

ISO 26262 是以 IEC61508 为基础，为满足道路车辆上特定电子电气系统的需求而编写。ISO 26262 适用于道路车辆上特定的由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。 安全是未来汽车发展的关键问题之一，不仅在驾驶员辅助和动力驱动领域，而且在车辆动态控制和主被动安全系统领域，新的功能越来越多地触及到系统安全工程领域。这些功能的开发和集成将强化对安全的系统开发流程的需求，及提供证据证明全部合理的系统安全目标得到满足的需求。

随着技术日益复杂、软件内容和机电一体化应用不断增加，来自系统性失效和随机硬件失效的风险逐渐增加。ISO 26262 包含了通过提供适当的要求和流程来避免风险的指导。

系统安全是通过一系列安全措施实现的。安全措施通过各种技术（例如，机械、液压、气压、电子、电气、可编程电子等）实现且应用于开发过程中的不同层面。尽管 ISO 26262 针对的是电子电气系统的功能安全，但是它也提供了一个基于其它技术的与安全相关系统的框架。ISO 26262：

a) 提供了一个汽车安全生命周期(管理、开发、生产、运行、维护、报废)，并支持在这些生命周期阶段内对必要活动的剪裁；

b) 提供了一种汽车特定的基于风险的分析方法以确定完整性等级[汽车安全完整性等级(ASIL)；

c) 运用汽车安全完整性等级(ASIL)定义 ISO 26262 中适用的要求，以避免不合理的残余风险；

d) 提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

e) 提供了与供应商关系的要求。

电子电器功能安全受开发过程(例如包括需求规范、设计、实现、集成、验证、确认和配置)、生产过程、维护过程和管理过程的影响。 安全问题与常规的以功能为导向和以质量为导向的开发活动和工作成果相互关联。ISO 26262 涉及与安全相关的开发活动和工作成果。

目前司机辅助设备领域、车辆动力控制领域、主动和被动安全系统的设计研发都需要遵循

ISO26262。如：汽车防抱死制动系统（ABS)；车身稳定控制系统；电子刹车力分配系统；紧急制动辅助系统；防撞系统；车道偏离报警系统；自适应助力转向；主动停车辅助系统自适应悬架控制；安全气囊；司机瞌睡警示系统；自动巡航系统；胎压监控系统；等等；

课程目标：
三天课程详细讲解 ISO26262 标准内容和要求，包括标准第 1,2,3,4,5,6,7,8,9,10 部分的要求，（简要介绍 11，12 部分），并根据该标准要求阐述如何采取相应的行动实施功能安全管理体系，以满足 ISO26262 的要求。

三天课程，通过汽车某电子电器系统项目案例讲解，和六个小组练习（项目定义、危害分析和风险评估、功能安全概念、技术安全概念、硬件安全要求规格、FMEDA、软件安全要求规格），和功能安全专家的答疑和指导：
1.帮助学员理解了汽车安全生命周期和开发流程的功能安全要素；
2.帮助学员掌握了 ASIL 的含义以及如何利用 ASIL 来确定安全和技术要求从而达到可接受的残余风险；
3.帮助学员掌握了风险确认和认可的方法，确保安全水平达到可以接受的水平；
4.帮助学员掌握了 ISO 26262 企业内部实施策略和计划；
5.解决了学员在硬件开发和软件开发过程中，应用 ISO26262 中的难题；

学员背景要求：
因为该标准和汽车行业密切相关，建议参加培训的人员应了解基本的系统开发、软件开发硬件开发。

参加人员：
汽车行业管理层人员、系统、软件和硬件工程师，开发部和系统/软件/硬件经理，项目经理，功能安全经理

培训教材：
每位参加培训人员都会获得纸质版权培训教材，包括课程小组练习表格；

课程主要内容：
第一天
9:00-12:00
ISO 26262 介绍和标准第 1 部分

- ISO 26262 目的
- IATF 16949 产品安全要求
- ISO 26262 范围
- ISO 26262 –框架
- ISO 26262 方法
- ISO 26262：2011 – 10 Parts　10 个部份，ISO 26262：2018 版 12 个部分；
- 影响 ISO 26262 的相关标准
- ISO 26262 优势
- ISO 26262 OEM 驱动

- ISO26262 标准开发时间轴
- 为何需要 ISO 26262
- 小组练习题练习（测试）

标准第 2 部分：功能安全管理

- 标准第 2 部分主要条款和内容
- 安全管理概要：批量前和批量后
- 新产品开发的角色和安全经理、项目经理
- 在概念阶段和产品开发阶段的安全管理
- 项目计划与功能安全计划
- 安全档案
- 审核、评估、评审
- 认可评审和认可评审措施报告
- 功能安全审核、功能安全评估计划
- 产品放行后的活动
- 小组练习题练习（测试）

13:30-17:30

标准第 3 部分：概念阶段

- 概念开发流程说明、小组流程练习
- 项目定义：定义和描述项目，提供对项目的充分理解，以便使得安全生命周期中定义的每一项活动可以执行。
- 汽车某电子电器系统项目，项目定义案例讲解
- 项目定义小组练习（企业或学员公司产品）
- 安全生命周期启动和定义将要执行的安全生命周期活动
- 危险分析和风险评估
- 汽车某电子电器系统项目，危害分析和风险评估案例讲解
- 危害分析和风险评估小组练习（企业或学员公司产品）

第二天

9:00-12:00

第一天内容复习

标准第 3 部分：概念阶段

- 功能安全概念（功能安全需求和初级架构元素或外部降低风险的措施）
- 汽车某电子电器系统项目，功能安全概念案例讲解
- 功能安全概念小组练习（企业或学员公司产品）
- 小组练习题练习（测试）

13:30-17:30

第 4 部分：产品开发 - 系统级

- 系统级开发流程说明、小组流程练习
- 系统级产品开发的启动
- 技术安全要求中的规格
- 系统设计
- 项目集成和测试
- 安全验证
- 功能安全评估

- 产品发布
- 汽车某电子电器系统项目，技术安全概念案例讲解
- 技术安全概念小组练习（企业或学员公司产品）
- 小组练习题练习（测试）

第三天
9:00-12：00
第二天内容复习
第 5 部分：产品开发 - 硬件级

- 硬件级开发流程说明、小组流程练习
- 硬件产品开发的启动
- 硬件开发的目标
- 硬件设计开发的原则
- 硬件安全规格的要求
- 汽车某电子电器系统项目，硬件安全要求规格案例讲解
- 硬件安全要求规格小组练习（企业或学员公司产品）
- 失效率的要求和随机失效率目标值
- 硬件架构设计和详细设计

第 9 部分：分解

- ASIL 分解、基本原则
- ASIL 分解的逻辑
- ASIL 分解案例与场景
- 小组练习题练习（测试）

回到第 5 部分：产品开发 - 硬件级

- 硬件的认证
- 安全分析与硬件
- 硬件的设计安全分析
- 硬件要求验证
- 硬件设计验证
- 硬件设计分析、硬件集成
- 硬件集成测试用例、集成测试
- 硬件安全机制
- 硬件架构指标总结：诊断覆盖率；安全可靠性指标
- FMEDA 案例和练习
- 小组练习题练习（测试）

第三天(续)
13:00-17:30
第 6 部分：产品开发 – 软件级

- 软件开发流程说明、小组流程练习
- 软件级产品开发的启动
- 软件安全要求的规格
- 汽车某电子电器系统项目，软件安全要求的规格案例讲解
- 软件安全要求的规格小组练习（企业或学员公司产品）
- 软件架构设计

- 软件单元设计与执行
- 软件单元测试
- 软件集成和测试
- 软件安全要求的验证
- 小组练习题练习（测试）

回到第 4 部分：产品开发 - 系统级

- 项目系统集成和测试
- 安全确认
- 功能安全评估
- 产品发布（投产）

回到标准第 2 部分：安全档案

- 安全档案
- 安全档案实例
- 小组练习题练习（测试）

标准第 7 部分: 生产和运营

- 生产：建立一个安全相关产品的生产计划，通过相关产品制造商或主管生产过程的人或组织来达到功能安全。
- 操作、维护和废弃：为了维持车辆操作期间的功能安全；定义了安全相关产品的维护、客户信息和维修指南的范围；提供拆卸前涉及的有关安全的活动要求

标准第 8 部分：支持流程

- 分布式开发接口；安全需求管理
- 配置管理或技术状态管理；变更管理
- 验证；文件
- 软件工具使用的信心；软件组件的认可
- 硬件组件的认可；使用中数据证明；独立安全元件

标准第 9 部分：安全分析

标准第 10 部分-指南

ISO26262 体系企业推行计划

- 小组练习题练习（测试）

ISO 26262:2018,第 2 版 - 变化和亮点总结

ISO 26262：2018 版在 2018 年 12 月 20 号正式发布。新的 ISO 26262 第二版有什么变化，它将如何影响你？

- 第 1 部分到 10 部分变化和亮点
- **第 11、12 部分简要介绍**

第三天内容复习、课程总结和考试