

ISO 26262 (GB/T 34590.1-10-2017) 功能安全管理体系

培训大纲

课程简介：

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。ISO 26262 于 2011 年 11 月份发布，我国于 2017 年根据我国国情修改 (MOD) 采用该系列标准，标准号为 GB/T 34590-2017，该标准是针对功能安全分析的标准，由 10 部分组成。

ISO26262 标准被美国和欧洲整车厂广泛采用。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 ISO26262。电子 (包括 PCB) 和半导体的客户也要求符合 ISO26262。

很多整车厂的 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 ISO26262 和汽车 ASIL 水平来降低风险。

显然，ISO26262 的推行不可避免。提供一系列的课程，帮助发现、分析、评估这些风险，并且提供全面的软件系统来帮助有效实施和管理 ISO26262。

课程目的：

- 理解汽车安全生命周期，包括管理、开发、生产、操作、服务和废止。
- 理解开发流程的功能安全要素，包括要求制定、设计、实施、集成、验证、认可和配置等。
- 掌握 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。
- 了解制定 ISO 26262 实施策略的必要信息。
- 掌握汽车行业独特的基于风险模式的风险分级汽车安全完整水平 - ASIL (Automotive Safety Integrity Levels, ASILs)。
- 掌握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。

课程大纲：

第零部分：ISO 26262 介绍

- ISO 26262 介绍
- ISO 26262 和 ISO 9001 或 ISO/TS 16949 的集成

第一部分：GB/T 34590.1-2017 道路车辆 功能安全 第 1 部分：术语

- 142 个概念选择介绍

第二部分：GB/T 34590.2-2017 道路车辆 功能安全 第 2 部分：功能安全管理

- 安全管理概要
- 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
- 安全档案实例
- 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

第三部分：GB/T 34590.3-2017 道路车辆 功能安全 第3部分：概念阶段

- 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。
- 项目定义小组练习
- 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
- 危害分析和风险评估小组练习
- 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）
- 功能安全概念小组练习

第四部分：GB/T 34590.4-2017 道路车辆 功能安全 第4部分：产品开发：系统层面

- 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
- 技术安全概念小组练习

- 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）

第五部分：GB/T 34590.5-2017 道路车辆 功能安全 第5部分：产品开发：硬件层面

- 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
- 硬件安全要求规格小组练习
- 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

- 硬件的认证
- 认证硬件
- 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
- 对由于硬件系统性失效引起的违反安全目标进行的评估（诊断覆盖率）
- 对由于硬件随机失效引起的违反安全目标进行评估（安全可靠性指标）

第六部分：GB/T 34590.6-2017 道路车辆 功能安全 第6部分：产品开发：软件层面

- 软件级产品开发的启动
- 软件安全要求的规格
- 软件安全要求的规格小组练习
- 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

第七部分：GB/T 34590.7-2017 道路车辆 功能安全 第7部分：生产和运行

- 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

第八部分：GB/T 34590.8-2017 道路车辆 功能安全 第8部分：支持过程

- 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

第九部分：GB/T 34590.9-2017 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析

- ASIL 分解、基本原则
- ASIL 分解的逻辑
- ASIL 分解案例与场景

第十部分：GB/T 34590.10-2017 道路车辆 功能安全 第10部分：指南

第十一部分：ISO26262 体系企业推行计划