TÜV 认证汽车网络安全 ISO/SAE 21434 及安全工程培训：二级（付费）

Agenda VectorAcademy

课程形式: 线下

课时: 2 天（基本内容） + 1 天（AUTOSAR 进阶培训，可选）

适用人员: 面向想了解和从事网络安全相关工作的汽车行业从业者

预备知识: 汽车软件开发 V 模型

目标: 了解汽车网络安全相关法规与标准，熟悉 ISO/SAE 21434 网络安全管理体系相关的概念、方法论和实践，以及掌握安全工程和安全测试的基本原理和实践。（可选内容：深入了解 AUTOSAR 中网络安全机制的原理，应用，及配置练习）

1. 基础内容（2 天）

网络安全挑战、标准、法规和行业术语

- 行业趋势及术语介绍
- 标准与法规解读（ISO/SAE 21434:2021，UNECE R.155，GB 44495-2024 等）

网络安全管理

- 标准解读与经验分享之组织级网络安全管理
- 标准解读与经验分享之基于项目的网络安全管理
- 标准解读与经验分享之分布式网络安全活动

基于风险的网络安全和网络安全分析

- 基于风险的网络安全及其核心要点
- TARA 方法论、最佳实践分享、练习

系统化的网络安全工程

- 密码学基础知识简介
- 安全设计之安全编码落地指南
- 信任根 - 硬件安全模块介绍 （HSM）
- 防御机制介绍与经验分享之安全更新（Secure Update/Download/Flashing）

VECTOR

TÜV 认证汽车网络安全 ISO/SAE 21434 及安全工程培训：二级（付费）

Agenda VectorAcademy

- 防御机制介绍与经验分享之安全启动（Secure Boot）
- 防御机制介绍与经验分享之安全通信（SecOC）
- 防御机制介绍与经验分享之安全诊断（0x27、0x29）
- 防御机制介绍与经验分享之安全日志（Secure Logging）
- 防御机制介绍与经验分享之 Adaptive AUTOSAR（安全通信，安全诊断等）

网络安全验证与确认

- 方法论、工具及最佳实践分享之静态代码分析
- 方法论、工具及最佳实践分享之功能测试
- 方法论、工具及最佳实践分享之漏洞扫描
- 方法论、工具、最佳实践分享及实操练习之模糊测试
- 方法论、工具、最佳实践分享及实操练习之渗透测试

后开发阶段的网络安全防护

- 标准解读与经验分享之生产
- 标准解读与经验分享之结束网络安全支持
- 标准解读与经验分享之报废
- 标准解读与经验分享之持续性网络安全活动
- 标准解读与经验分享之网络安全事件响应
- 标准解读与经验分享之更新

考试与证书

- Vector 证书：参加并通过 Vector 组织的考试，获得二级证书
- TÜV 证书：
  - 参加考试的前提是完成 Vector 网络安全培训
  - 参加并通过 TÜV 组织的一级考试，获得一级证书
  - 参加并通过 TÜV 组织的二级考试，获得二级证书
  - 参加二级考试的前提是持有一级证书
- 不参加考试：获得 Vector 培训证明

TÜV 认证汽车网络安全 ISO/SAE 21434 及安全工程培训：二级（付费）

Agenda VectorAcademy

2. 基于 AUTOSAR 进阶培训（1 天，可选）

以下内容为可选内容

基本概念

- 基本概念原语
- 基本概念密钥
- 基本概念作业
- 基础 AUTOSAR 加密栈

演练示例：基于密码的消息认证码 (CMAC)

- 演示用于 CMAC 生成和验证的加密作业的详细配置
- 演示加密栈的配置（Csm、CryIf 和 Crypto 驱动程序）

实操练习 (DaVinci Configurator)

- 加密栈的配置（通过 SW Crypto 驱动程序）
- 加密密钥配置
- 加密作业配置（加密和解密、MAC 生成和验证）

证书

- 学员出勤时间不低于课程时长的 80%，且通过考试