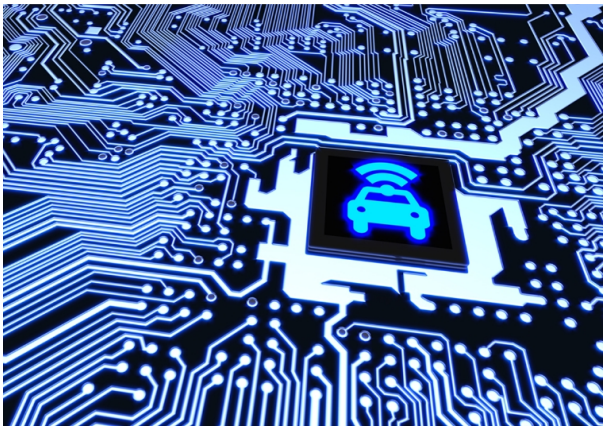
汽车网络安全

作为嵌入式系统安全评估和渗透测试的专业实验室，我们支持汽车行业在硬件、软件、通信和密码学层面的评估组件和抵御系统被最先进的信息安全攻击的能力。



新型汽车越来越多地由网络组件组成，这些组件使用有线和无线接口（CAN、LIN或自动以太网）进行内部通信，并与远程信息处理服务、电动汽车充电系统和智能驾驶系统进行外部通信。

汽车一级供应商负责开发嵌入汽车中的大多数关键信息安全组件。主机厂会要求这些产品有足够的保护和对策，以确保产品抵御潜在的攻击。

汽车和零部件信息安全的汽车标准和法规生态系统仍在发展中。UNECE WP.29是唯一的强制性法规，而主机厂有无数的行业标准和最佳实践可用于制定一级供应商通过的信息安全要求。

为了展示组件对最先进攻击的抵御能力，主机厂和一级制造商可以求助于专门的安全实验室来评估他们的产品。

汽车组件的信息安全评估

Applus+ IT实验室在评估硬件、软件、通信和密码学层面的嵌入式组件安全性方面有着丰富的经验。我们拥有从系统引导到系统间通信的完整OSI堆栈的专业知识。这种整体视角确保我们能够有高度的把握来评估复杂的系统。

威胁分析和风险评估(TARA)

- 对全球、每个项目和持续信息安全管理和活动的产品生命周期的概念、开发和后开发阶段进行审核，以达到所需的安全保障水平。
- TARA项目可以按照特定的汽车标准（如ISO/SAE 21434）和较少的系统框架（如ISO/IEC 62443）进行，甚至可以使用定制的TARA系统（如内部要求）。

为客户专门定制的安全评估

我们可以根据所需的保证水平（基本、适度和完全保证）调整评估工作。评估目标范围从单个组件（SoC、HSM、PCB）到设备（ECU、TCU、OBC）再到系统和网络（3GPP、蓝牙、CAN、100-BaseT1）。

- 设计审查、源代码审查（SCR）和漏洞分析（VA）
- 全栈渗透测试，以评估设备的抗攻击和恢复能力
- 针对自定义OEM/Tier合规性要求的定制评估

安全培训和最佳实践（设计和编程）

针对系统工程师、信息安全经理或软件架构师等职位的开放式信息安全培训和课程。我们培训的一些例子：

- 安全编码原则的最新技术以及如何将其应用于日常运营
- 从攻击者的角度出发所研发的汽车解决方案，以及设备如何受到攻击，有助于确定将这些知识应用于您的产品并使其更加强大的方法

为什么选择APPLUS+作为信息安全合作伙伴?

- 在汽车、支付、电信、工业、移动等行业具有多领域经验的高保证安全评估实验室
- 具备最新的攻击技术和设备，用于评估嵌入到车辆中的组件和设备，包括物理攻击、软件攻击以及网络和无线攻击
- 具备专业的知识，用于在产品开发过程中支持安全生命周期验证
- 我们的网络安全实验室足迹：（西班牙有3个实验室），北美（加拿大1个实验室和美国1个实验室）以及亚洲（中国上海有1个实验室）的配置
- 能够涵盖与汽车行业信息安全相关的多项标准和法规