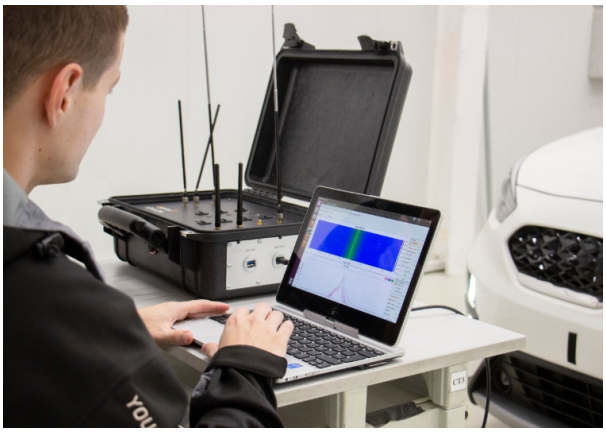
idiada_china@idiada.com

网络安全

面对层出不穷的网络安全问题，汽车行业积极应对，推出了风险验证及评估技术，对车辆软硬件的正常工作带来了深远影响。与此同时，我们也察觉到了黑客们入侵车辆系统的新方法。为了减少黑客们的影响，对车辆进行全方位保护事关重要。



我们的团队拥有**车辆网络安全**方面的专家，可在开发全程提供丰富经验，包括：

- 基于ISO/SAE 21434和SAE J3061标准的**网络安全概念**
  - 风险分析危险评估
  - 网络安全功能要求
  - 制定安全目标
  - 评估不同功能/项目的网络安全
- **车辆网络安全对标**
- **网络安全架构设计**
- **汽车网络安全培训**
- 差距分析以及为即将生效的法规和标准提供**合规支持**
- **无线安全系统更新及流程**

网络工具箱

借助自主开发的网络工具箱系统，Applus IDIADA可以评估车辆安全程度，为车辆制造商和不同层级的供应商提供解决方案，避免潜在的市场召回风险。该系统可应对汽车行业日益增长的网络安全需求，提供综合全面的解决方案，方便**开发网络安全性汽车**。该系统还具有充分的灵活性，能在满足标准和认证项目要求的前提下融入未来可能出现的新的攻击途径。虽然网络安全问题并不一定影响用户的身体安全，但可能会对**车辆的隐私及/或功能**

造成影响。与未受攻击的车辆系统相比，我们发现受攻击的车辆系统存在诸多关键弱点，也就是说这些车辆的某些系统未经过安全测试，如经过测试也许就能发现弱点并予以纠正。

Applus IDIADA开发的**网络安全评估工具**可结合不同**硬件和软件**，实现自动运作，还可分析网络攻击下可能影响**车辆功能、完整性或隐私**及/或用户的连结向量。我们还为基础应用配备了网络界面，用于配置、管理和执行测试以及生成可供分析的详细测试报告。