



自动驾驶面临的安全挑战

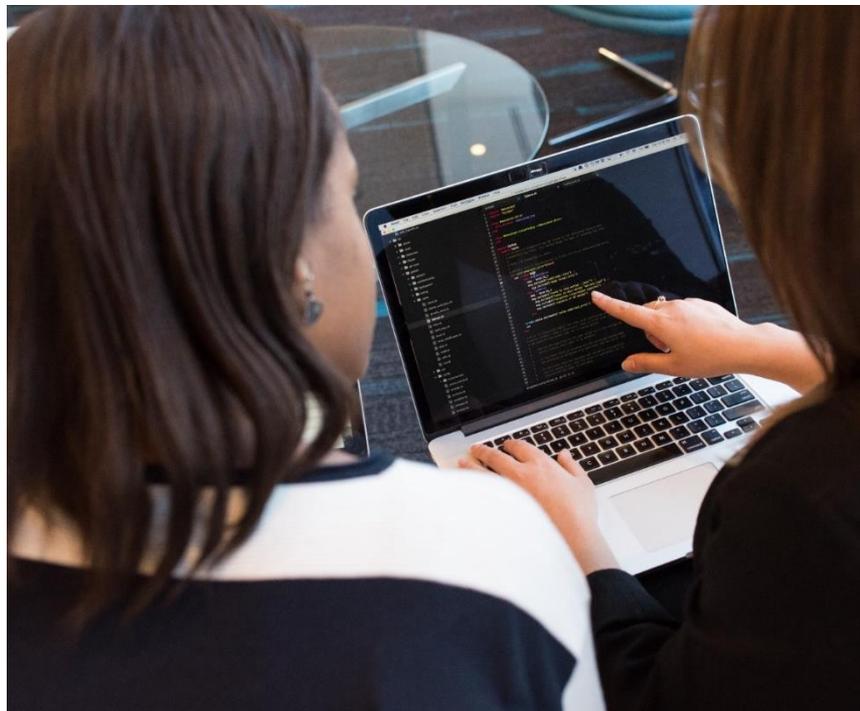
SAE-AWC

2019.08 - 深圳

Jose Almeida, Director Automotive Business Line
jose.almeida@sysgo.com

本地研发 全球布局

- SYSGO是欧洲领先的嵌入式操作系统供应商。
- 作为值得信赖的顾问，我们为客户提供安全与可靠性相关的技术与服务，成为世界物联网设备的高端软件解决方案。
- 成立于1991年 - 在安全关键系统认证方面拥有超过25年的经验
- Thales集团成员



产品与服务

作为欧洲领先的嵌入式操作系统供应商，我们已经为航空航天，汽车，铁路和IoT行业的功能安全和信息安全应用提供了超过25年的支持。我们与客户在其整个产品生命周期中都有密切合作。

PikeOS®

基于分离内核的RTOS，集成和认证的虚拟化技术（Hypervisor）

ELinOS

具有实时扩展的嵌入式系统的工业级Linux发行版

Board Support Packages

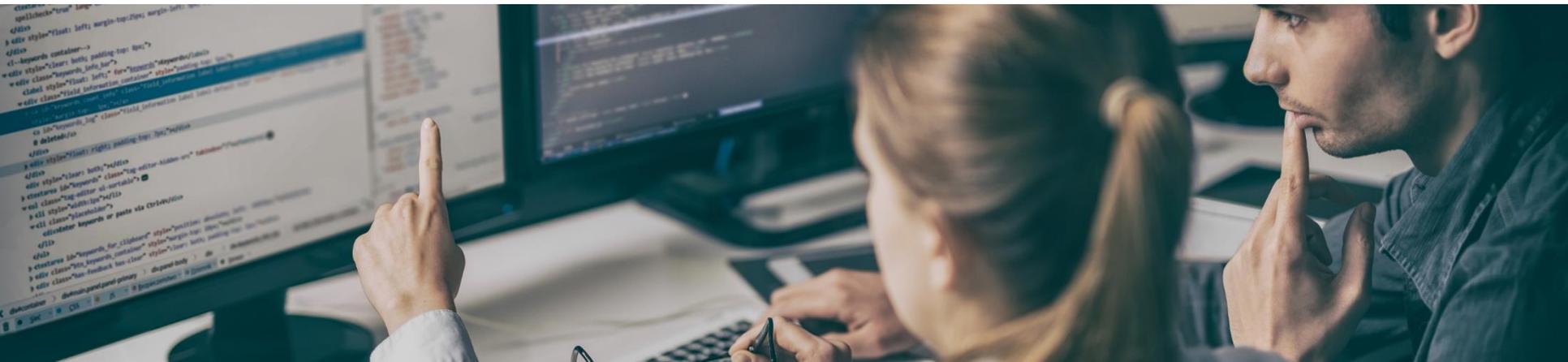
适应所选的架构，板特定的初始化和驱动程序

Certification Kits

广泛收集所有主要通用和行业特定标准的认证文档

Professional Services

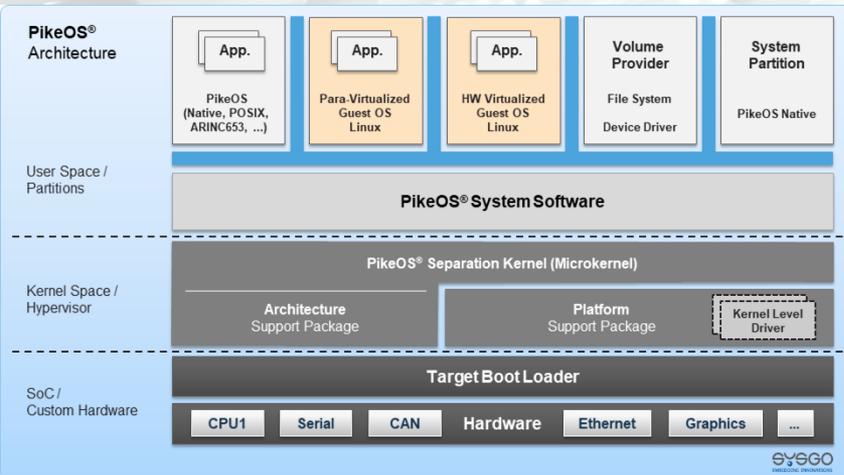
我们确保客户可以优化使用我们的技术，从原型设计到认证



产品与服务

PikeOS®

嵌入式RTOS和HV



- **硬实时操作系统和虚拟化系统**

- 凭借安全可靠的虚拟化，与多个客户操作系统的混合关键性和高度可移植性，支持所有重要的CPU架构

- **客户操作系统**

- 可以在单个或多核处理器上的并行分区中运行，以满足特定用例的需要

- **混合关键性**

- 严格的空间和时间划分

- **基于Eclipse的CODEO**

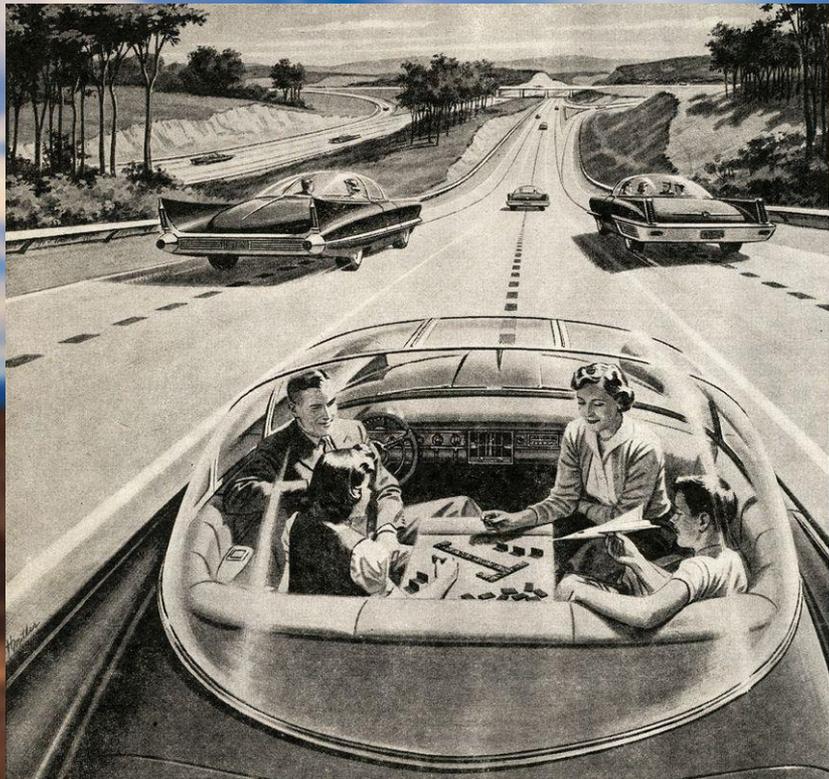
- 一个支持C / C++的综合集成开发环境

- **没有任何出口限制**

- ITAR free

自动驾驶 愿景





自动驾驶

WHY

Self
Driving

提高安全性 (69%)

道路通行能力 (65%)

流动性、压力 (~50%)

减少排放 (31%)



安全问题/故障安全概念

法律上的限制

网络安全

主要的挑战

新想法



新想法

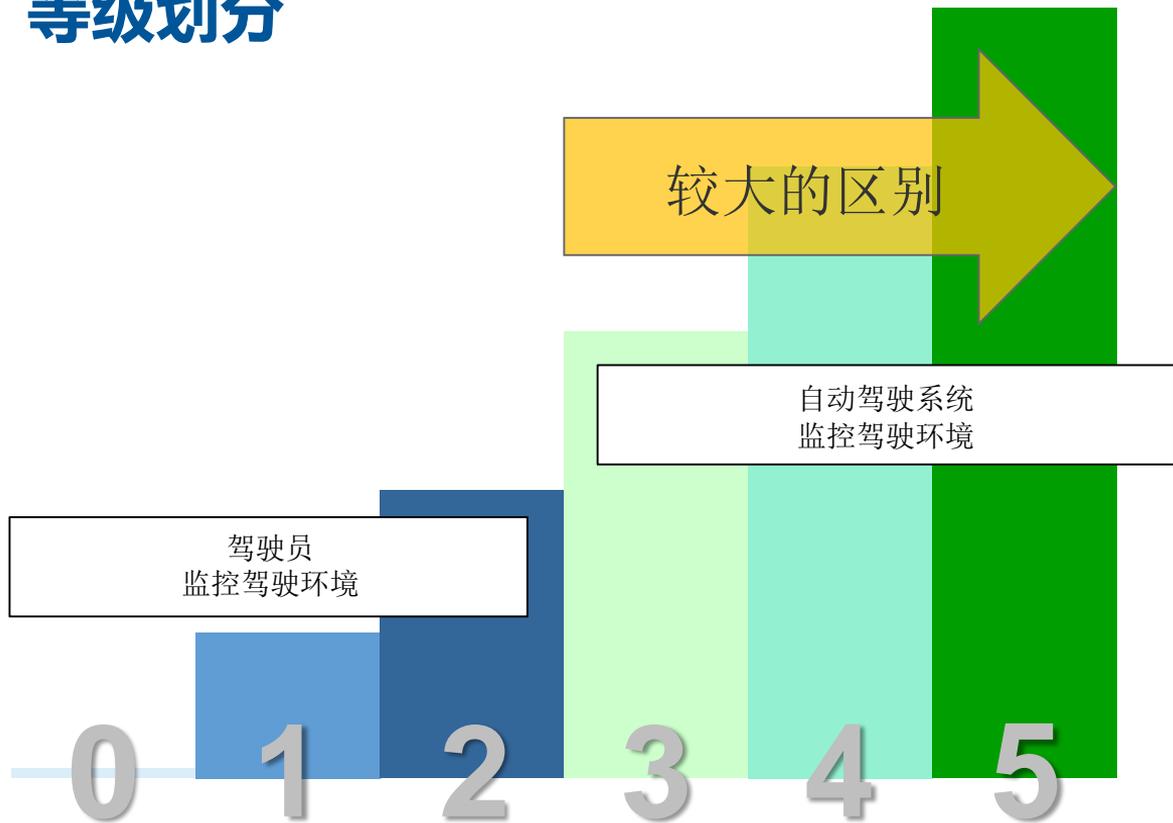


连接与安全

复杂性——
域集成

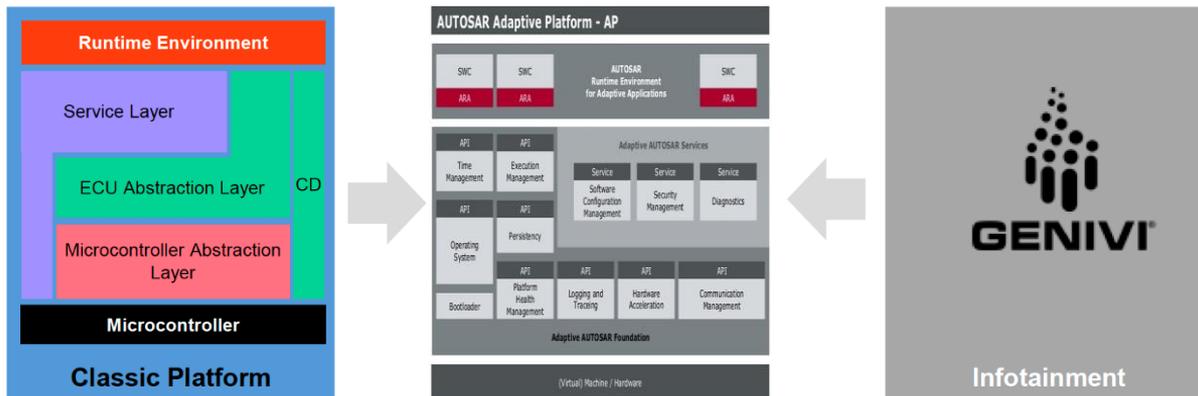
生命周期&
开发过程

自动驾驶的 等级划分



Real time requirements

Safety relevance

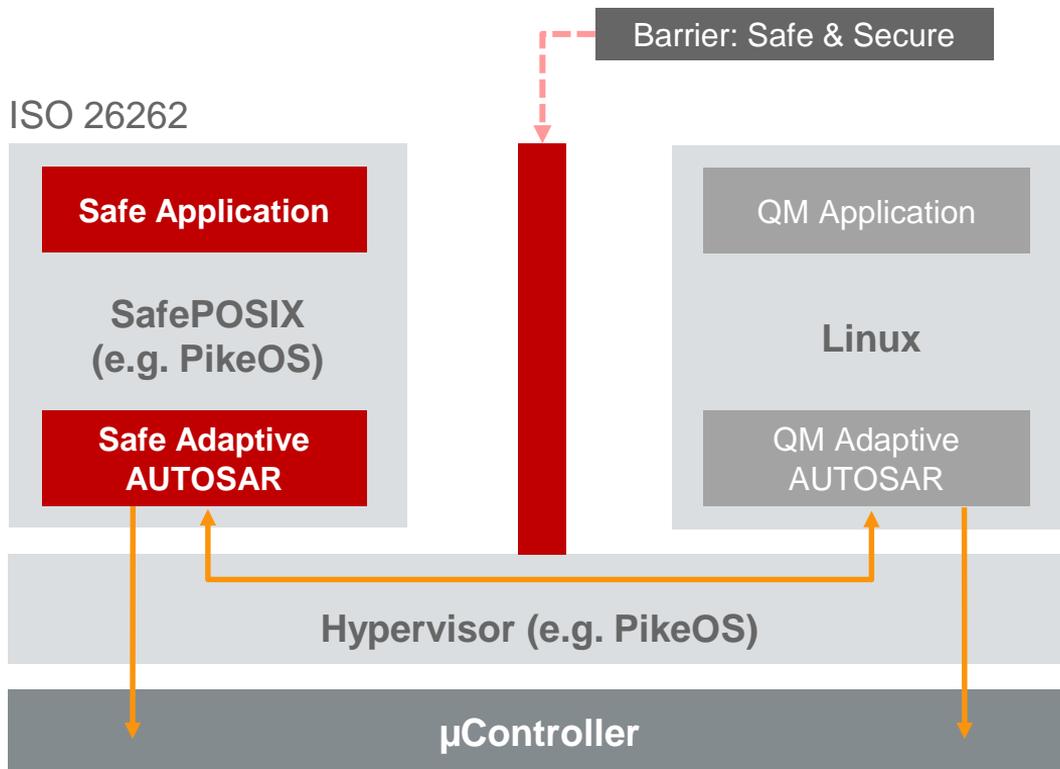


Security

Computing power

AUTOSAR: “另一种针对应用开发的平台”

AUTOSAR Adaptive – 新标准、新功能



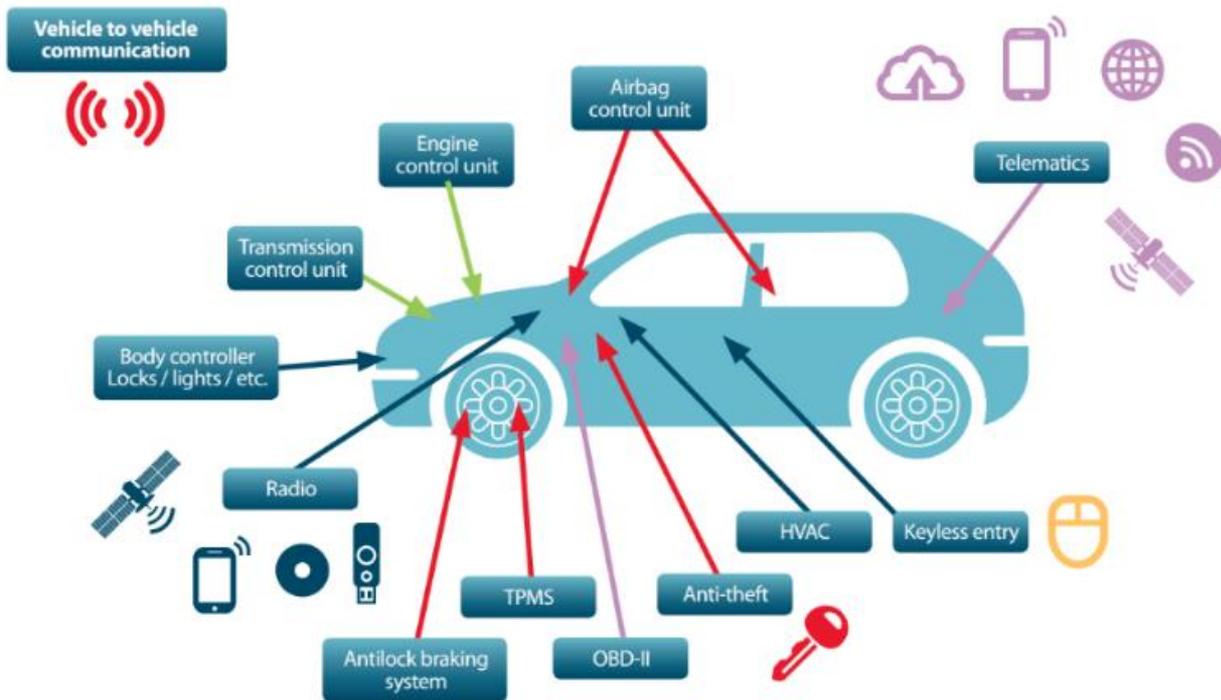
Hypervisor
连接
安全和Linux

安全意味着...

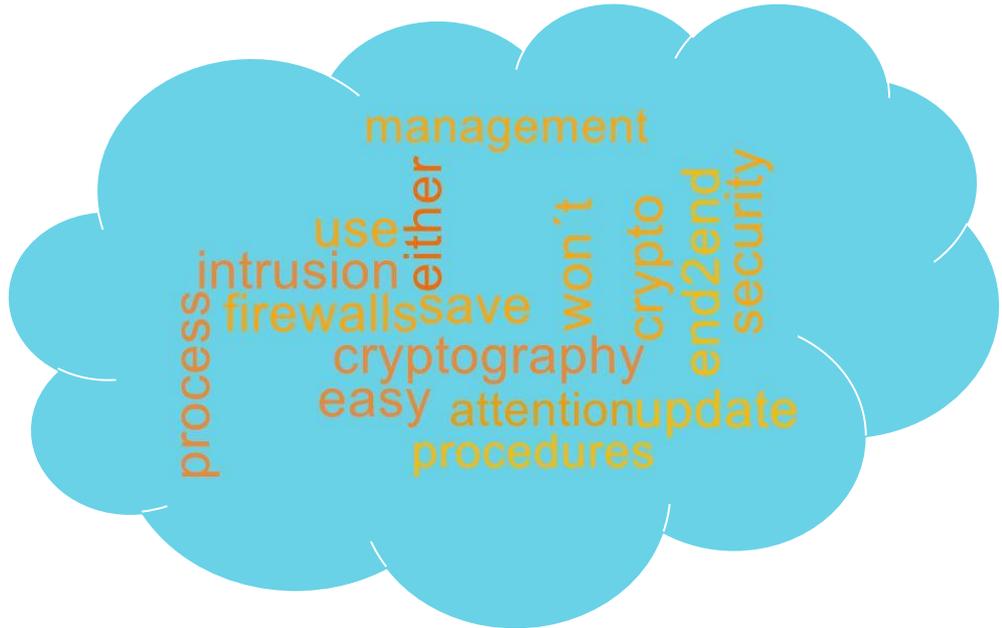
数据安全 - 隐私

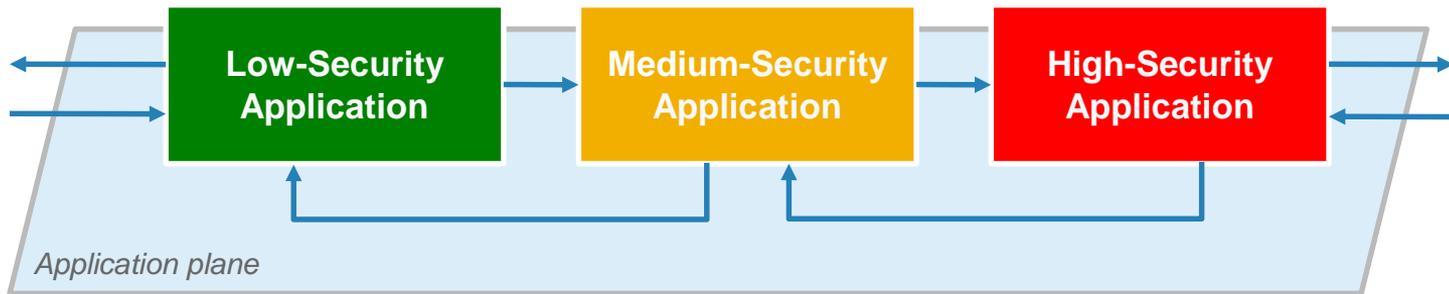
安全保障

凯迪拉克ELDORADO的受攻击点

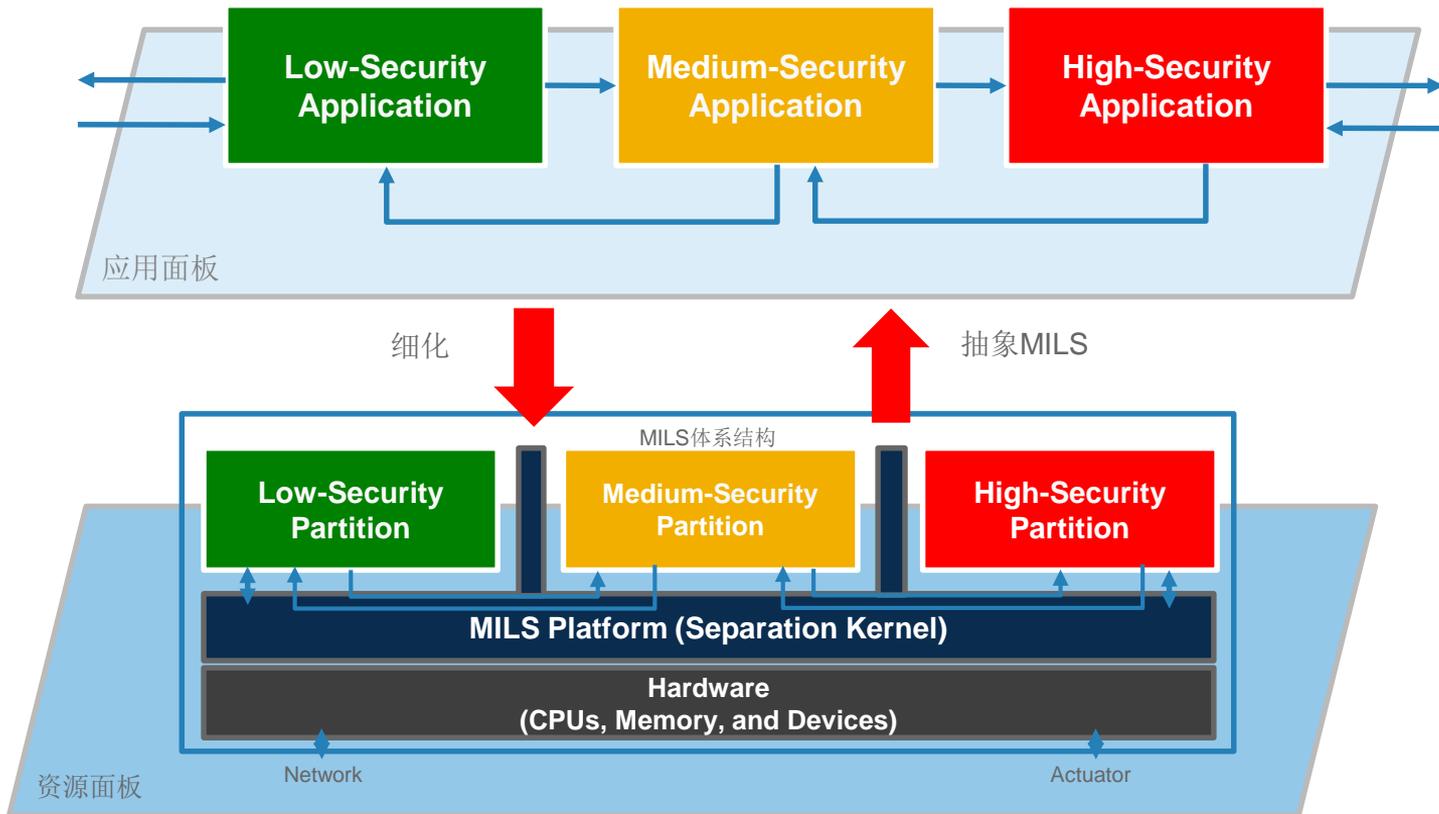


从IT行业中学习安全





MILS是一种高度可靠的安全体系结构，支持基于可验证的分离机制和受控信息流的不可靠和可靠组件的共存。



优点

MILS OS作为未来汽车平台的基础

创建多域平台支持新的移动服务

确保严格的分离，域集成提高数据隐私，最大限度地降低安全风险

降低开发成本，最大限度地降低第三方组件的风险

Adaptive
Autosar

Genivi /
AGL

Other OEM
Innovations

常见的功能安全和信息安全标准

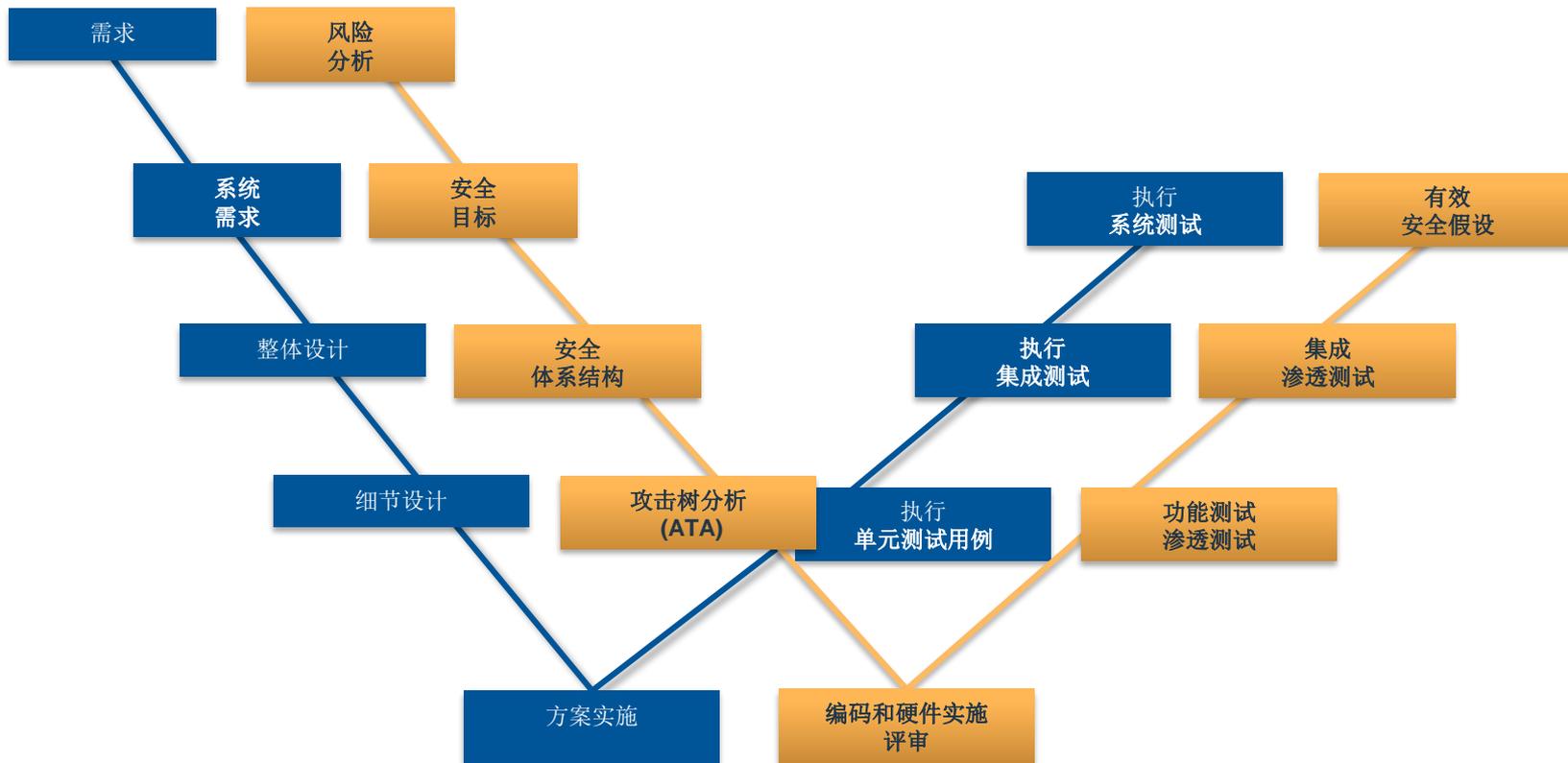
ISO 26262

SAE J3101

地面车辆应用的硬件保护安全

**ISO/SAE 21434 -
SAE J3061**

网络物理车辆系统的网络安全指南



安全启动

安全更新

防火墙

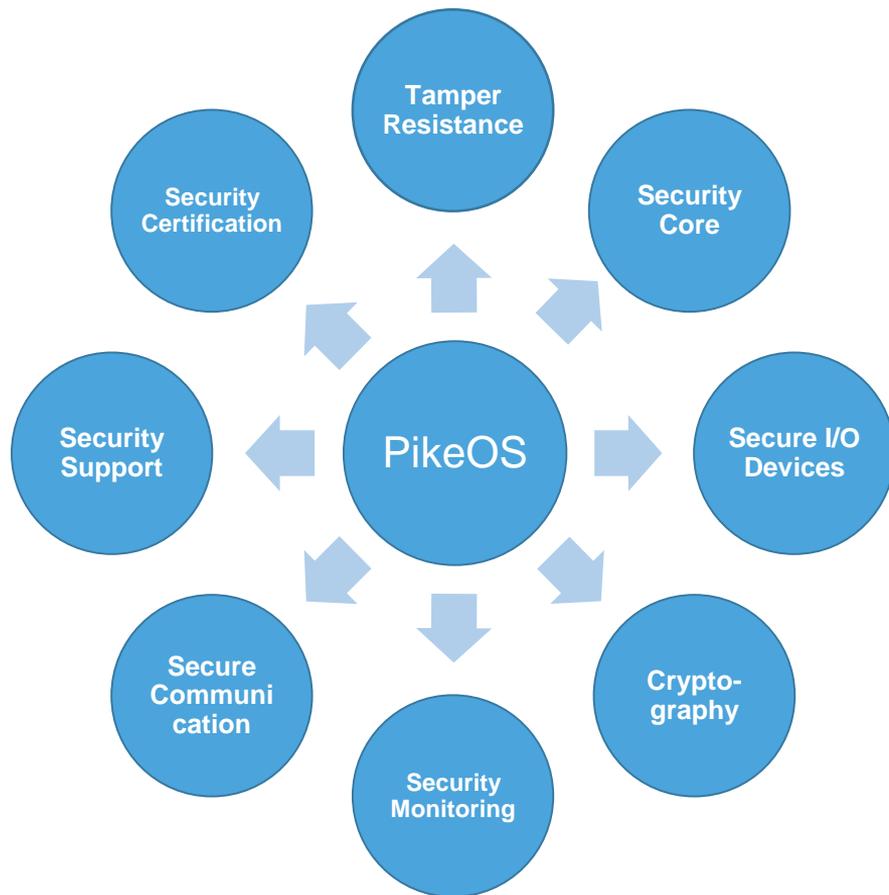
入侵检测系统

受控通信流

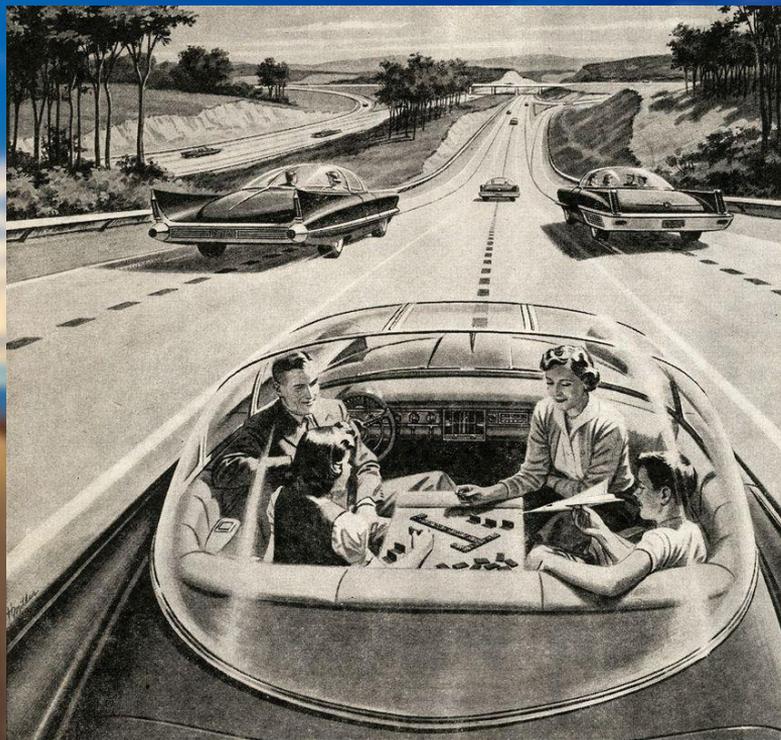
MILS分离内核

- 理解标准和建议
- 首先保障硬件安全
- 其次保障软件安全

- 系统集成概念,
即架构是最重要的安全准则
- 询问您的软件是否有:
 - 监控
 - 评定
 - 通知
 - 调控措施
 - 安全可靠的软件生命周期
 - 建立端到端的安全性



自动驾驶 让我们一起来实现



和我们一起解决

自动驾驶的功能安全和信息安全的挑战

SYSGO
EMBEDDING INNOVATIONS

EPT 烽星科技

