目录

守护你的座驾：汽车安全

- 最新版本：`v1.1`
- 更新时间：`20221028`

简介

介绍如何加强汽车安全，守护你的座驾。先对汽车安全进行概览说明。再对汽车安全事件和攻击方式和角度进行详述；介绍了汽车相关的基础知识，比如车联网的V2X、T-Box、OTA等，总线中的CAN、FlexRay等；各种模块，比如IVI、ECU、车载网关等；介绍了汽车安全相关的协议和规范，比如WP.29、ISO/SAE 21434、ISO 26262、SAE、J3061等；介绍了一些汽车安全相关方案；以及其他汽车安全相关知识，比如AutoSar、NHTSA等。最后给出参考资料。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

HonKit源码

- crifan/guard_your_car_safety: 守护你的座驾：汽车安全

如何使用此HonKit源码去生成发布为电子书

详见：crifan/honkit_template: demo how to use crifan honkit template and demo

在线浏览

- 守护你的座驾：汽车安全 book.crifan.org
- 守护你的座驾：汽车安全 crifan.github.io

离线下载阅读

- 守护你的座驾：汽车安全 PDF
- 守护你的座驾：汽车安全 ePub
- 守护你的座驾：汽车安全 Mobi

版权和用途说明

鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

更多其他电子书

本人 `crifan` 还写了其他 `150+` 本电子书教程，感兴趣可移步至：

crifan/crifan_ebook_readme: Crifan的电子书的使用说明

汽车安全概览

如之前在信息安全概览中所总结的，信息安全方向，有几个大的方向：

- 线上或线下
  - 侧重线下的
    - 侧重windows系统的：漏洞和安全
  - 侧重线上的
    - 侧重远程Web网络的：渗透测试
    - 侧重远程工控设备的：工控安全 ~= 物联网安全
- 设备和端
  - 侧重移动端：移动端安全和破解
    - 安卓的安全和破解
    - iOS的安全和破解
  - PC端
    - Windows安全
    - Linux安全
    - Mac安全

而其中：

- 工控安全 ~= 物联网安全
  - 涉及到 汽车领域就是
    - 汽车安全

而汽车安全又涉及到：

- 汽车安全
  - 汽车内部的操作系统 相关安全
  - 用户使用的app 相关安全
    - 移动端安全
    - app和汽车的交互
      - 各种无线协议
        - NFC
        - 等

背景

- 汽车向智能手机方向进化
  - 新四化
    - 智能化
    - 网联化
    - 共享化
    - 电动化

汽车安全概况

- 汽车网络安全防护还很薄弱
  - 相对传统汽车厂商而言，特斯拉无疑在网络安全防护方面表现得更好一些，但依然无法有效防范各种漏洞利用、数据泄露和服务中断等问题
- 汽车行业在信息安全方面的防护基础整体还较为薄弱
  - 汽车端

        - 三类问题较为突出
            - 首先，受限于成本、技术成熟度等因素，目前车内防护仍以软件措施为主，身份认证、加密隔离等应用不足
            - 其次，对关键零部件、整车系统级软硬件的风险评估能力不足
            - 第三，网络安全测试评价基础薄弱，在车内部件、整车等方面测试验证能力不足，整车渗透还主要依赖于人工实施，渗透深度和水平缺乏可量化评估标准

功能安全

- 按是否需要功能安全划分应用类别
    - `非功能` 安全
        - 车身控制和车载ECU
            - 举例：座椅，空调面板，照明灯控，Tbox,OBC，车载无线充，车载显示屏协控制器等
    - `ASIL`
        - `ASIL-B`
            - 汽车车身控制
                - 举例：BCM、空调电源、电源管理，BMS,仪表盘控制、前照明大灯等
                - 说明：有时候非功能安全和ASIL-B的应用场景会稍微有交叉，主要看主机厂是如何做的规定
        - `ASIL-D`
            - 强功能安全应用
                - 举例：
                    - 汽车安全气囊、刹车制动 `ABS` 、 `ESP`
                    - 电驱动、电池包BMS、变速箱和三电系统（VCU，MCU，BMS）
            - 常见方案商=芯片厂商
                - 能够提供D等级的MCU厂家
                    - 英飞凌的TC系列MCU
                    - 瑞萨的RH850系列MCU
                    - NXP最新推出的S32K3系列MCU

汽车安全攻击和破解

TODO：

- CIVC王羽：《汽车自动驾驶技术路线图》 信息安全技术 - 安全内参 | 决策者的网络安全知识库
  - https://www.secrss.com/articles/9404

传统汽车，往往是不联网的。

现在的汽车，往往联了网，常被叫做：`智能网联汽车` = `ICV` = `Intelligent Connected Vehicle`

汽车，一旦联网，就增加了各种安全风险。

破解

破解案例

- 汽车黑客揭秘：我是如何通过逆向API接口黑掉宝马i3的
  - Github
    - https://github.com/edent/BMW-i-Remote/
  - 中文翻译
    - [翻译]对宝马车载apps协议的逆向分析研究-『智能设备』-看雪安全论坛

防护

希望可以防止未授权的攻击：

攻击风险和角度

此处整理汽车安全攻击相关内容。

汽车安全类型

- 汽车安全类型
  - 根据风险类型分
    - 智能汽车的网络安全威胁：7类
      - 手机App漏洞
      - 云端服务器漏洞
      - 不安全的外部连接
      - 远程通信接口漏洞
      - 不法分子反向攻击服务器以获取数据
      - 车载网络指令被篡改
      - 车载部件系统因固件刷写、提取、植入病毒等被破坏

攻击风险

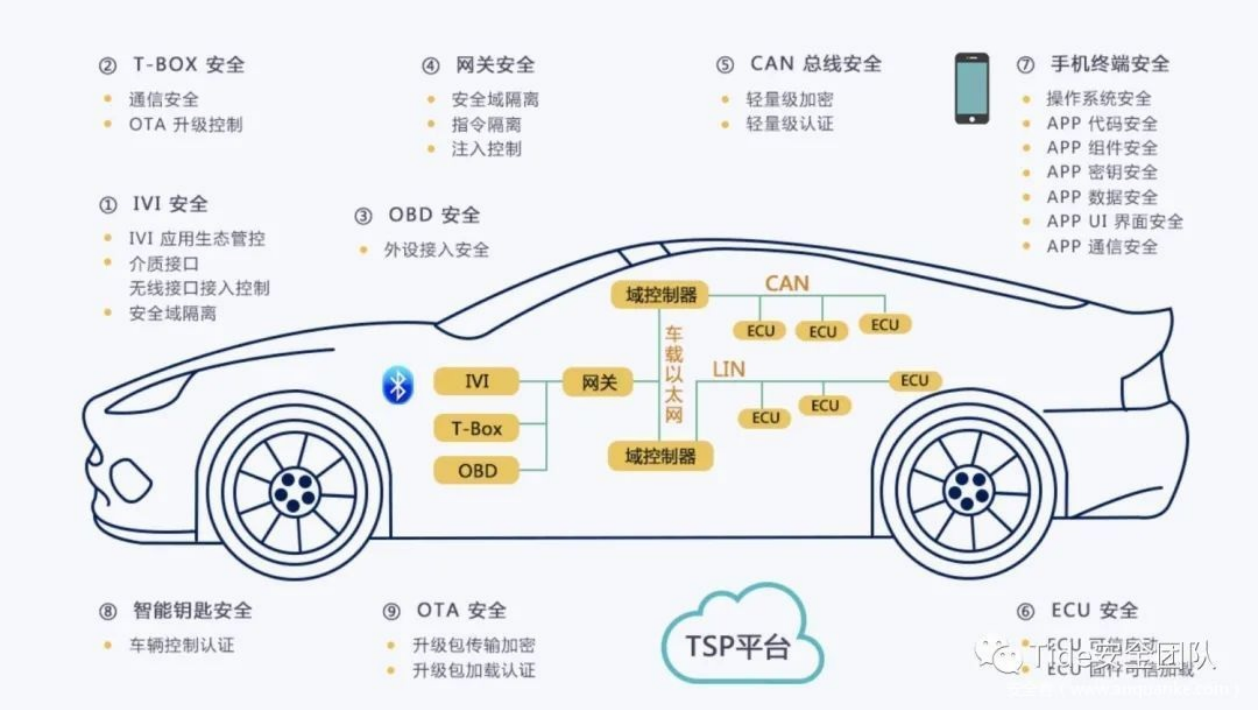
- 2020车联网信息安全十大风险
  - 数据来源：中汽数据
  - 概述
    - 文字
      - 相较于2019车联网安全风险TOP来说，不安全的生态接口问题仍然占据第一位置，总占比约25%，系统固件可被提取及逆向问题由2019年年的第六名，提升到了今年的第五名，总占比约10%，已知漏洞的组件问题 在排名由第七名上升到第六名，总占比约9%，车载网络未做安全隔离问题由第五名下降到第七名，总占比约7%
    - 图
      - 

- Upstream Security
  - 2020年《汽车网络安全报告》
    - 自2016年至2020年1月，汽车网络安全事件的数量增长了605%，仅2019一年就增长了一倍以上
      - 82%涉及短程和远程攻击
      - 在过去十年中，前三大攻击媒介
        - 无钥匙进入系统（30%）
        - 后端服务器（27%）

        - 移动应用程序（13%）
    - 安全事件造成的后果
        - 汽车盗窃/入侵（31%）
        - 对汽车系统的控制（27%）
        - 数据/隐私泄露（23%）

攻击角度

对于汽车，有各种角度可以利用和攻击。



其中：

- 常规性安全风险
    - APP
    - 云平台
- 其他
    - 零部件
        - T-BOX
            - 固件逆向，攻击者通过逆向分析 T-BOX 固件，获取加密算法和密钥，解密通信协议，重放篡改指令
            - 利用调试口访问无身份校验漏洞，通过焊接的方式连接调试线，车载T-BOX可深度读取汽车Can总线数据和私有协议，从硬件层获取shell，导致信息泄露问题
            - 固件后门：TBox的固件刷写功能是由IVI提供，在TBox刷入固件首先要在整体升级包中分离出TBox的固件包，并将后门文件写入到固件包中
            - 网络劫持：TBox通常会支持2G/3G/4G，所以基于GSM或LTE的伪基站都可以劫持TBox的网络连接，劫持T-BOX会话，通过伪造协议实施对车身控制域、汽车动力总成域等的远程控制
        - IVI
            - 硬件调试接口：观察主板的MCU型号及引脚信息，可以通过焊接连接调试线，从硬件层获取shell
            - 通过内置浏览器访问恶意页面，安装任意应用程序
            - 拒绝服务攻击:利用恶意程序大量耗费系统内存，使其无法正常提供服务
            - 刷入后门：如果获取了刷写系统固件的权限，可以直接将后门程序通过刷写固件的方式写入系统中，如开机启动脚本、dropbear、msf后门等
    - OTA风险
        - 升级包中间人攻击：OTA升级功能，测试过程中可以通过拦截或者抓取流量包，修改后重新发送

        - 欺骗攻击，同第一个类似，类似于伪造升级包发送给车端
    - 无线电测试风险
        - 这个类似于常规的无线电测试，指对汽车智能无线钥匙、蓝牙、WIFI、GPS和胎压监测单元等车载无线电组件进行的渗透包括但不限于干扰测试
            - 一般包括信号屏蔽、信号篡改、中间人攻击、蓝牙劫持、蓝牙嗅探、信号截取、重放攻击等技术手段
    - CAN风险
        - CAN报文重放
            - 利用录制的CAN报文进行重放，在未接触并操作车辆实际物理操作界面的情况下，实现对车辆的相关控制与操作
        - CAN 模糊测试
            - 利用CAN报文模糊测试并暴力破解数据位控制指令，通过得到的数据位控制指令进行车辆控制及操作
            - 攻击类型
                - 报文过滤绕过：CAN总线会针对TBox发送的报文进行过滤操作，通常是基于CAN ID及CAN Data的头部字节，测试时可以针对相关字段进行模糊测试
                - 绕过状态检查：CAN总线中的ECU在执行指令之前会进行状态检查，如车辆是否在行驶中档位设置等，绕过检查并执行恶意报文会产生更大的破坏，漏洞也更严重
                - 拒绝服务：测试工具通过随机生成大量数据，将数据发送给车辆，可以通过发送大量伪造报文来进行拒绝服务攻击

攻击手法

- 攻击手法
    - 传统的攻击手法
    - 新的
        - 利用超声波的 海豚音 攻击
        - 利用照片以及马路标识线的AI攻击
- 攻击进入车辆方式

- 。

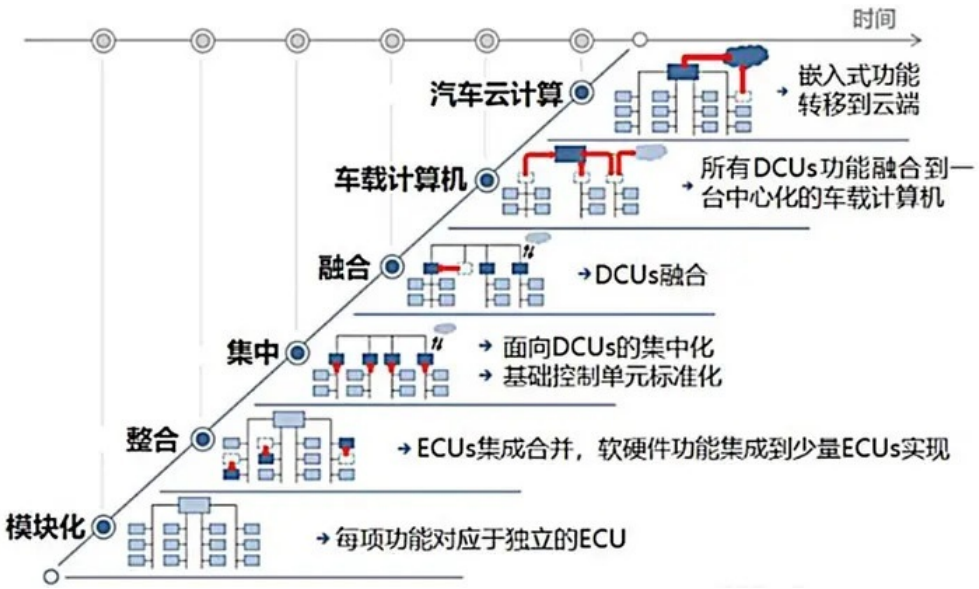
安全事件

- 汽车安全事件
  - 正向=汽车安全
    - Enev利用机器学习算法，对汽车控制器局域网络（CAN， controller area network）总线数据进行特征提取，实现对汽车驾驶员的身份识别，证明了用户隐私存在被泄露的风险
    - 腾讯科恩安全实验室研究员远程入侵了特斯拉汽车的网关、车身控制模块（BCM）和自动驾驶控制单元，证明了汽车中存在很多安全隐患
    - Zeng等使用便携式GPS欺骗器实现了非法篡改车辆的GPS路线，严重威胁了车载GPS安全
    - Miller等在DEFCON会议中指出，ICV中存在大量可被利用的攻击面，如远程无钥匙进入（RKE，remote keyless entry）、蓝牙、Wi-Fi、车载资讯系统、互联网、APP等，都有可能使用户隐私泄露，甚至导致车辆被远程控制
  - 逆向=汽车破解=汽车攻击
    - 特斯拉
      - 2015年，黑客就曾入侵了特斯拉Model S的车载系统，导致其在行驶过程中突然熄火
      - 2017年，来自360公司和腾讯公司的安全技术人员分别展示了如何“无钥匙”远程进入特斯拉的车载系统和电网系统
      - 通过使用一种名为Worley的噪音（Worley噪声能够模拟石头，水或其他噪音的纹理）生成函数，通过加补丁的方式生成所需的对抗样本图片，可以启动特斯拉的自动雨刮器
      - 2020年，全球更是发生了多起特斯拉App宕机事件，致使手机无法与车辆进行链接，车主处于“盲开”状态，甚至有些车主被锁在车中
    - Jeep
      - 自由光
        - 2015年7月，两位著名白帽黑客查理·米勒以及克里斯·瓦拉塞克曾入侵了一辆Jeep自由光的Uconnect车载系统，通过软件远程向该系统发送指令，启动了车上的各种功能
    - 日产
      - 2016年，日产汽车不得不关闭其专为Leaf系列开发的应用程序Nissan Connected EV，因为他们发现，黑客可以侵入汽车系统，控制电池操作等功能，以耗尽电池
    - 其他
      - 奥迪、保时捷、宾利和兰博基尼等大众旗下品牌的Megamos Crypto防护系统也都被黑客攻破过
      - 黑客获取智能汽车的T-Box通讯模块后，即可通过通讯模块接入车厂私有网络，进而攻击车厂内网导致TSP沦陷
      - 在道路上贴上对抗样本贴纸，则能误导自动驾驶系统，使车辆行驶到对面的车道造成逆行
      - 数字车钥匙漏洞也让汽车安全存在更多隐患
- 2020年汽车安全事件

- 。

基础知识

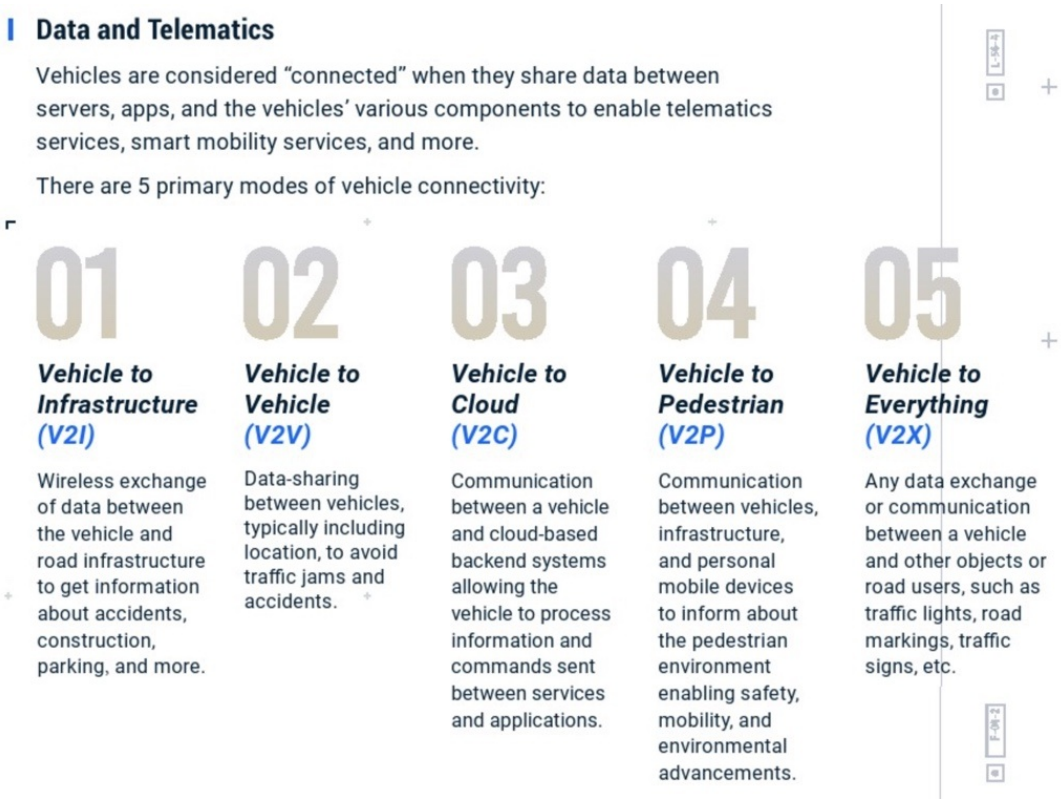
汽车电子电气架构

- 汽车的 `电子电气架构` = `Electronic Architecture`
  - 历史
    - 最早由德尔福（全球最大汽车线束系统制造厂商）提出
  - 演化
    - 

车联网

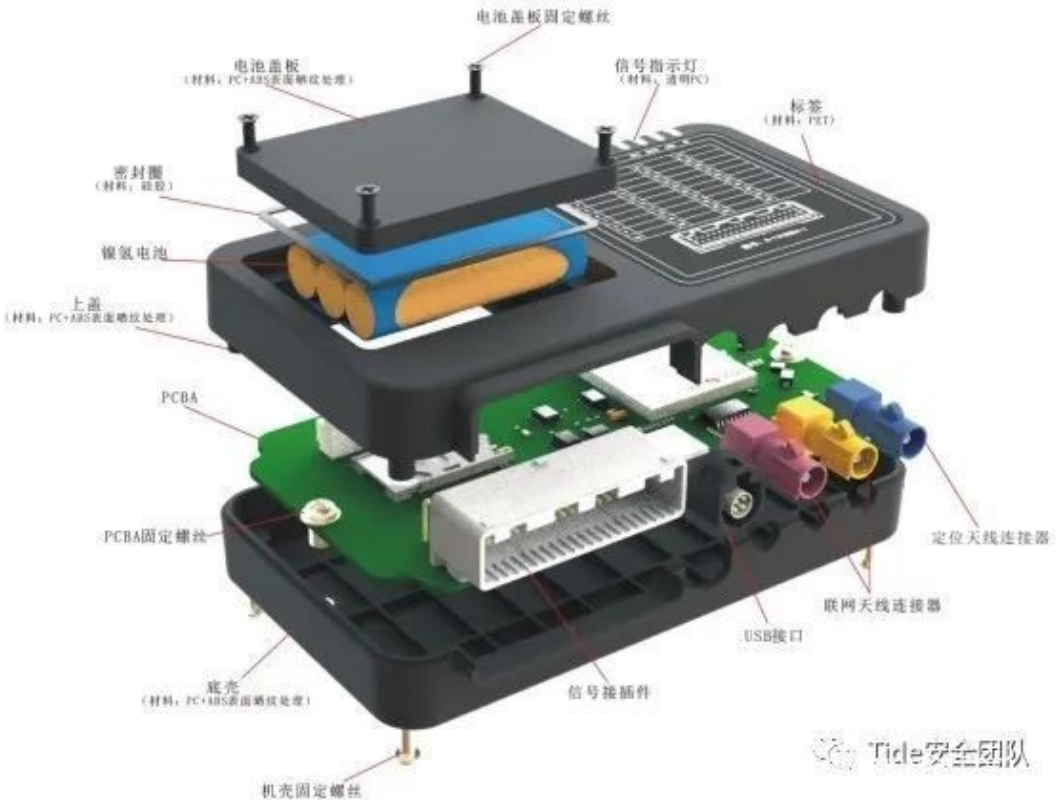
V2X

- V2X
  - 概述
    - V2X技术使车辆与周围环境（其他车辆、基础设施或行人）之间进行通信，主要应用就是提高道路安全性
    - 要实现V2X技术 （包括采用IEEE802.11p 的互联汽车技术）的愿景，车辆必须能够信任来自周围环境的信息
  - 图
    - 
    - 
  - 产品和方案
    - Autotalks解决方案
      - 汽车网络安全 | 汽车安全系统 | 互联汽车安全 | Autotalks (auto-talks.com)
  - 相关技术和概念
    - 概览



- 包括
  - `V2I` = `Vehicle to Infrastrucure`
  - `V2V` = `Vehicle to Vehicle`
  - `V2C` = `Vehicle to Cloud`
  - `V2P` = `Vehicle to Pedestrian`
  - `V2X` = `Vehicle to Everthing`

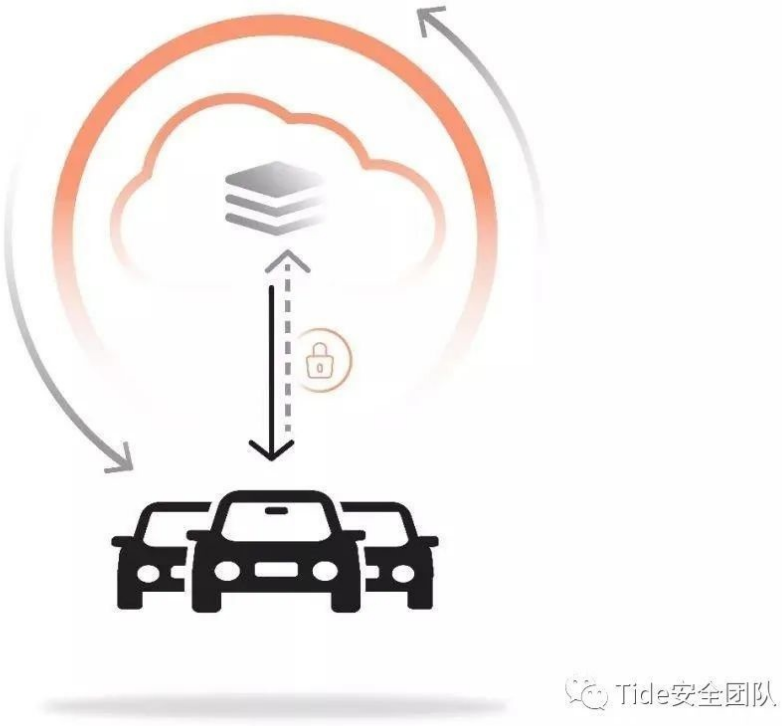
T-Box

- `T-BOX` = `Telematics BOX` = `远程信息处理器`
  - 组件：包含OBD、MCU/CPU、FLASH、SENSOR、GPS、3G/4G、WiFi/蓝牙等模块
  - 作用：用于车与车联网服务平台之间通信
    - 对内：与车载 CAN 总线相连，实现指令和信息的传递
    - 对外：通过云平台与手机/PC 端实现互联，车内外信息交互的纽带其主要功能是为汽车提供网络连接
  - 用途
    - T-B0X可实现车辆远程控制、远程查询、安防服务等功能
      - 举例
        - 远程控制车门、车窗、空调等开启
        - 远程车辆定位、查询车况信息;车辆异动报警紧急救援求助等
  - 举例
    - 某T-BOX厂家产品
    - 

  - 注意
    - T-B0X 为人们生活提供了越来越多的便利和安全保障，同时也为汽车带来了更多的信息安全隐患

OTA

- `OTA` = `Over The Air` = 无线更新
  - 是什么：一项基于短消息机制的远程更新技术
    - 即终端通过无线或蜂窝网络的接口与服务器连接来实现对本地设备数据的更新
      - 具体是指通过服务器、移动通信网络和终端等的网络连接
        - 最终实现终端内存储数据的更新，进而改善终端的功能和服务作用
  - 对比：传统更新设备的固件，都是要通过有线网络和接口去更新的。而OTA无线更新，和有线比，更加方便。
  - 用途
    - 给汽车中的软件(模块、系统、固件)通过OTA更新



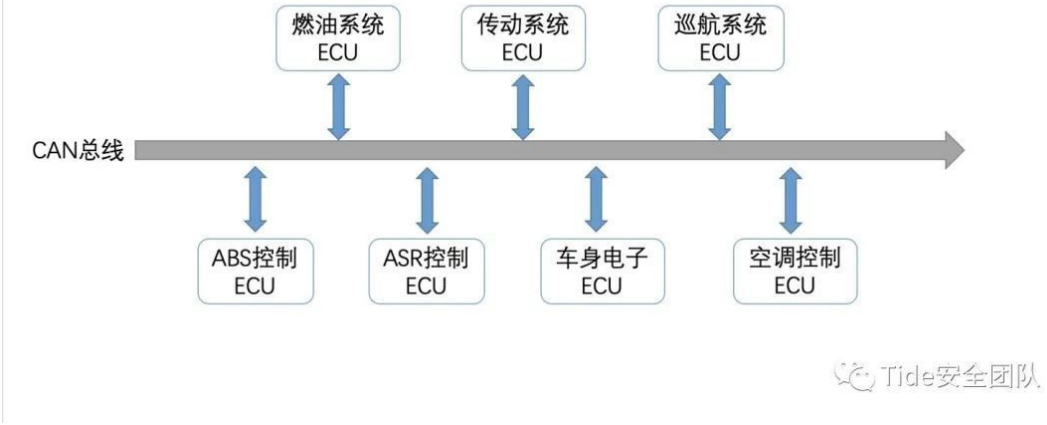
汽车OTA升级

- 两种方式
  - 对比
    - 

  - `FOTA` = `Firmware OTA` = 固件在线升级
    - 适用：多数核心和基础的ECU
    - 指的是给一个设备、ECU 闪存下载完整的固件镜像，或者修补现有固件、更新闪存，用户也可以通过特定的刷新程序进行 FOTA 升级，影响的是动力系统、电池管理系统等
  - `SOTA` = `Software OTA` = 软件在线升级
    - 适用：少数非核心ECU
    - 那些看上去离使用者更近的应用程序和地图OTA，都属于 `SOTA` 的范畴，如应用程序（App）、车载地图、人机交互界面等功能

总线

CAN

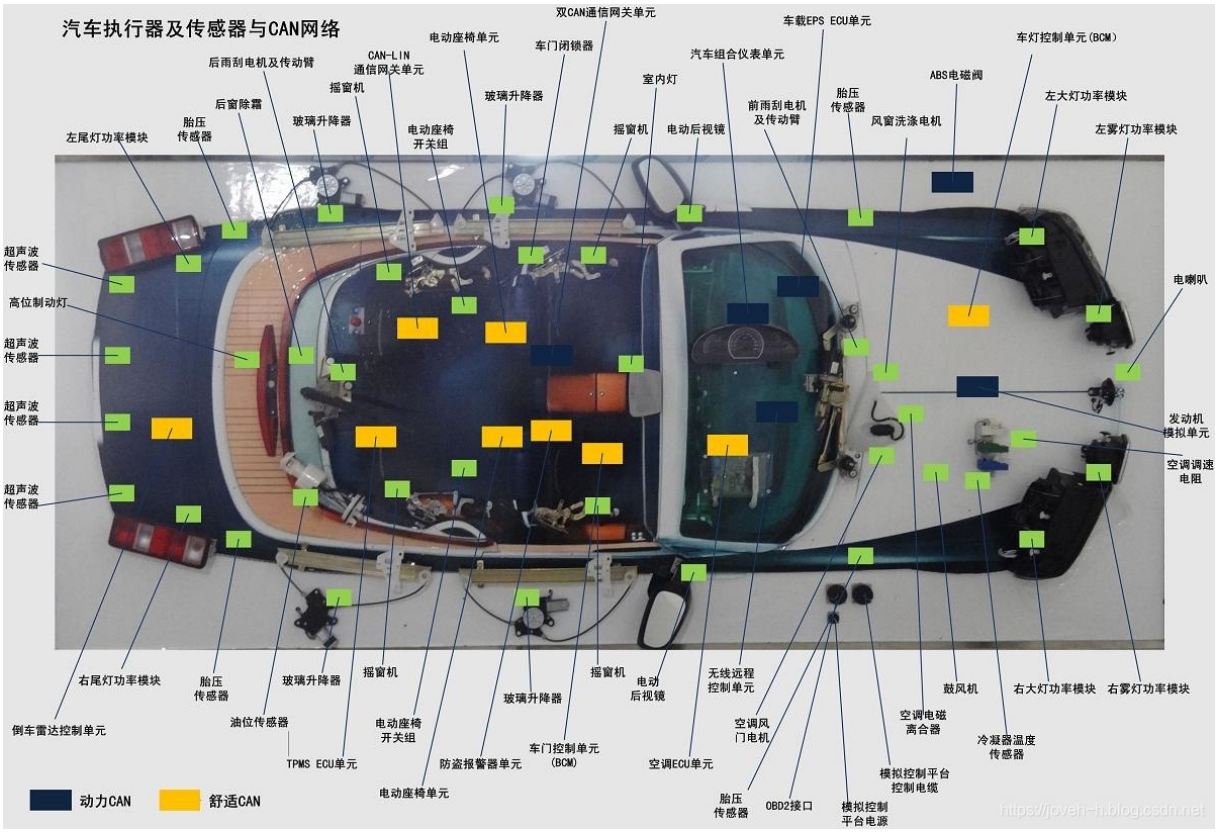
- `CAN` = `Controller Area Network` = 控制器局域网
  - == `CAN总线` = `Controller Area Network Bus`
  - 是什么：一种能够实现分布式实时控制的串行通信网络
  - 优点：传输速度最高到1Mbps，通信距离最远到10km，无损位仲裁机制，多主结构
  - 概述：由以研发和生产汽车电子产品著称的德国BOSCH公司开发的，并最终成为国际标准 `ISO 11898` ，是国际上应用广泛的现场总线之一
  - 用途：是制造厂中连接现场设备（传感器、执行器、控制器等）、面向广播的串行总线系统，最初开发用于汽车工业，后来也应用于工业自动化
  - 现状：CAN有很多优秀的特点，使得它能够被广泛的应用
  - 举例
    - 汽车内的CAN总线
    - 

FlexRay

- `FlexRay`
  - 是什么：汽车领域的网络通信（总线）协议
  - 谁开发的：FlexRay联合会
    - 核心成员
      - Freescale Semiconductor
      - Robert Bosch GmbH
      - NXP Semiconductors
      - BMW AG
      - Volkswagen AG
      - Daimler AG
      - General Motors
  - 目的：用于管理汽车中的计算资源
    - 希望比 `CAN` 和 `TTP` 速度更快更可靠
  - 优点
    - 速度更快 = 传输速率更高
    - 更可靠
    - 容错率更高
  - 缺点：成本更高=更贵
  - 发展历史
    - 2009年，FlexRay联合会，已解散
      - 但FlexRay的协议标准已成为ISO标准：`ISO 17458-1` 到 `ISO 17458-5`
  - 内部机制
    - 基于时间循环内操作，被拆分成静态或动态的时间段segment，用于基于事件触发或基于时间触发的通讯

模块

车辆中有多个模块：

- 

下面就来详细介绍具体模块。

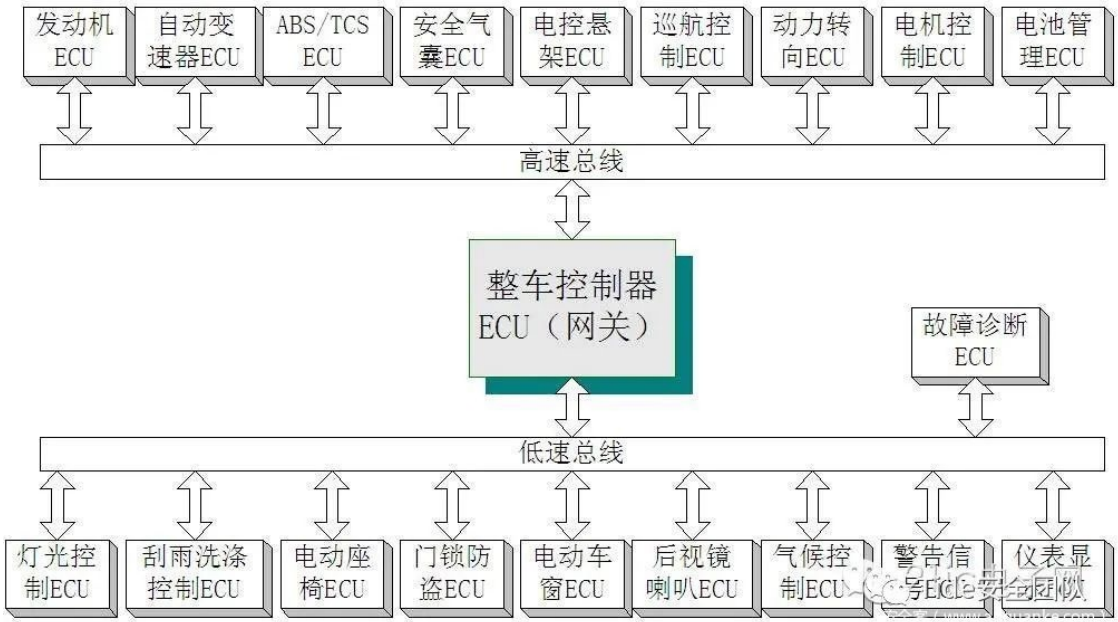
IVI

- `IVI` = `In-Vehicle Infotainment` = 车载信息娱乐系统
  - 概述：该部分是车主可以直观接触到的部分，车内中控屏，音响，空调，甚至仪表盘都可以连接到IVI中
  - 发展历史
    - 第一代：IVI提供控制空调，查看里程/燃油，提示手刹/车门于车辆本身直接相关的功能，其实现方式是通过IVI中的CAN芯片向CAN总线或LIN总线发送特定指令实现
    - 第二代：IVI中在功能上更加内聚，其主要负责处理与用户的直接交互（通过触摸屏或车载中控台）和WIFI，FM，GPS等信号的处理
      - 第二代IVI中自身只实现UI，多媒体等功能，而运营商网络上网功能及与下发控车指令（这里的控车指令是指用户在车内控制空调，车座等）的功能则已交到Tbox处理，这使IVI功能更集中
  - 图
    - 

ECU

- `ECU` = `Electronic Control Unit` = `电子控制器单元`
  - 别称：汽车的 `行车电脑`
  - 用途：控制汽车的行驶状态以及实现其各种功能
  - 原理：主要是利用各种传感器、总线的数据采集与交换，来判断车辆状态以及司机的意图并通过执行器来操控汽车
  - 图
    - 

  - 分类
    - 根据功能分
      - 传统燃油车：电控单元主要存在于汽车的三大件上
        - `EMS` = `发动机管理系统` ： 通过控制进气、喷油、点火实现发动机动力性、经济性、排放等性能的均衡，整车的扭矩解析功能集成在于EMS
        - `TCU` = `变速箱控制单元` ： 通过电磁阀控制油压，实现离合器自动接合或者分离，在合适的时机完成档位切换，提高车辆的动力性、经济性、平顺性
        - `EPS` = `电动助力转向` ： 通过电机辅助驾驶员进行转向，降低驾驶难度
        - `ESC` = `车身稳定控制` ： 集合了TCS、ABS、ESC等功能，通过控制轮端制动力实现车辆的稳定行驶
        - `MRC` = `主动悬挂系统` ： 控制电磁阀调节悬挂系统高度或阻尼，提高车辆行驶稳定性、舒适性
      - 新能源车：由于动力系统的变化，电控单元有所变化和增加（这里以混动车为例）
        - `VCU` = `整车控制器` ： 吸收了传统车上的扭矩解析功能，在加上混动车特有的能量管理、高压管理等等功能，形成一个整车控制的枢纽，协调各控制单元配合工作
        - `TCU` = `混动变速箱` ： 混动变速箱相比于传统变速箱，结构有所变化，往往会集成1个或2个电机，实现串联、并联或功率分流模式，主要通过电机、离合器的配合工作，实现模式的切换
        - `BMS` = `电池管理系统` ： 主要包括状态监控、高低压控制、充放电控制、SOC估算、电池均衡等功能，实现电池安全高效运行
        - `DCU` = `电机控制器` ： 通过控制逆变器的输出电流，实现电机扭矩的精确稳定控制
        - `OBC` = `交流充电机` ： 将220V交流电经过整流变成直流，再经过DCDC变换后给电池充电
        - `Ibooster` = `电动助力制动` ： 新能源汽车为了尽可能多的实现能量回收，开发了电动助力制动系统，辅助驾驶员进行制动助力，也能在小范围内实现制动解耦，提高能量回收效率
  - 架构图



TCU

- `TCU` = `Transmission Control Unit` =（自动） `变速箱控制单元`
  - 作用：通过电磁阀控制油压，实现离合器自动接合或者分离，在合适的时机完成档位切换，提高车辆的动力性、经济性、平顺性
    - 根据行车数据进行车速、驾驶者动力请求等数据选择档位、匹配变速箱输入输出两端的转速，实现快速、平顺、稳定的档位切换，既能让车辆行驶更平稳舒适又安全，还能降低变速箱损耗、提升系统寿命
  - 重要性： `TCU` 之于 `燃油车` ，重要性不亚于， `VCU` 之于 `纯电车`
  - 举例
    - 博世为宝马某车型设计的TCU模块
    - 

  - 背景知识
    - 燃油车的变速箱形式
      - `AT` 变速箱
      - `双离合` 变速箱
      - `CVT` 变速箱

VCU

- `VCU` = `Vehicle Control Unit` = `整车控制单元`
  - 对于纯电动车：必备单元，相当于整车的大脑
  - 作用
    - 采集电机控制系统信号、踏板信号及其他部件信号，根据驾驶员的驾驶意图综合分析并作出响应判断，同时监控下层的各部件控制器的动作，对汽车的正常行驶、电池能量的制动回馈、网络管理、故障诊断与处理、车辆状态监控等功能起着关键作用
  - 举例
    - 博世VCU模块
    - 

ESP

- `ESP` = `Electronic Stability Program` =车身 `电子稳定程序`
  - 作用：根据轮胎滑移率、车速、车身所受加速度、车身横摆角变化率等数据，在恰当的时机对单个车轮施加恰到好处的制动力矩，通过控制车轮来调整车身姿态，大大降低车辆失控的概率

IPB

- `IPB` = `Integrated Power Brake` =智能 `集成制动系统`
  - 作用和效果：相当于： `ESP` 和 `iBooster` 制动系统的集合体
    - 对于采用这种系统的车辆来说，没有了 `IPB` 就相当于连刹车都丢了，更遑论 `ESP`

车载网关

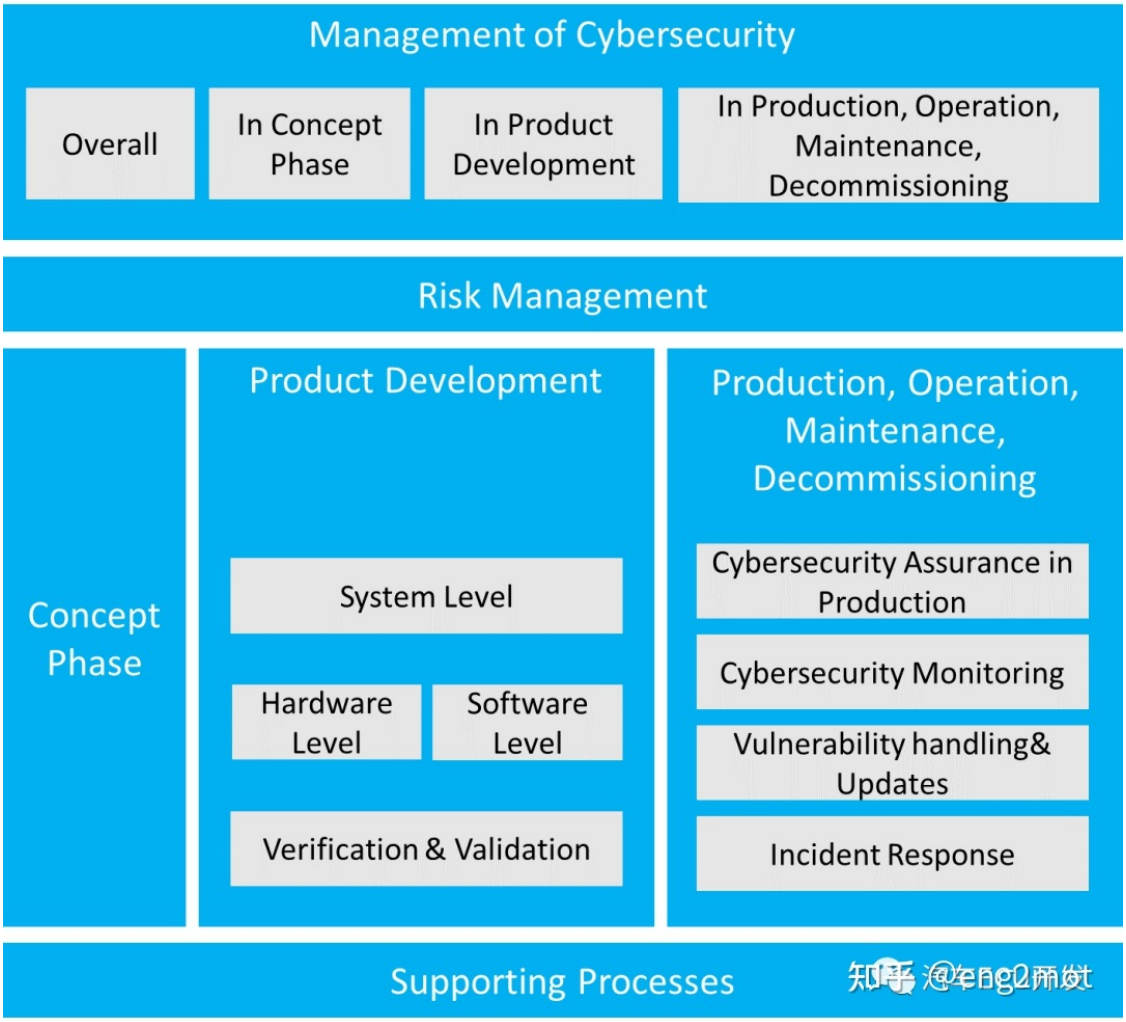
- `车载网关`
  - 概述
    - 车载网关为各网段ECU提供报文路由转发服务,与车内所有ECU均有数据交互，有些网关还承担OTA升级的主刷控制器功能
    - 车载网关通过不同网络间的物理隔离和不同通信协议间的转换，在各个共享通信数据的功能域
      - 如动力总成域、底盘和安全域、车身控制域、信息娱乐域、远程信息处理域、ADAS域之间进行信息交互
        - `ADAS = Advanced Driving Assistance System = 高级驾驶辅助系统`
  - 汽车网关是整车电子电器架构的核心部件，可通过 `CAN` 协议与车内其它ECU进行交互，是车内网络的数据交互枢纽

标准

WP.29

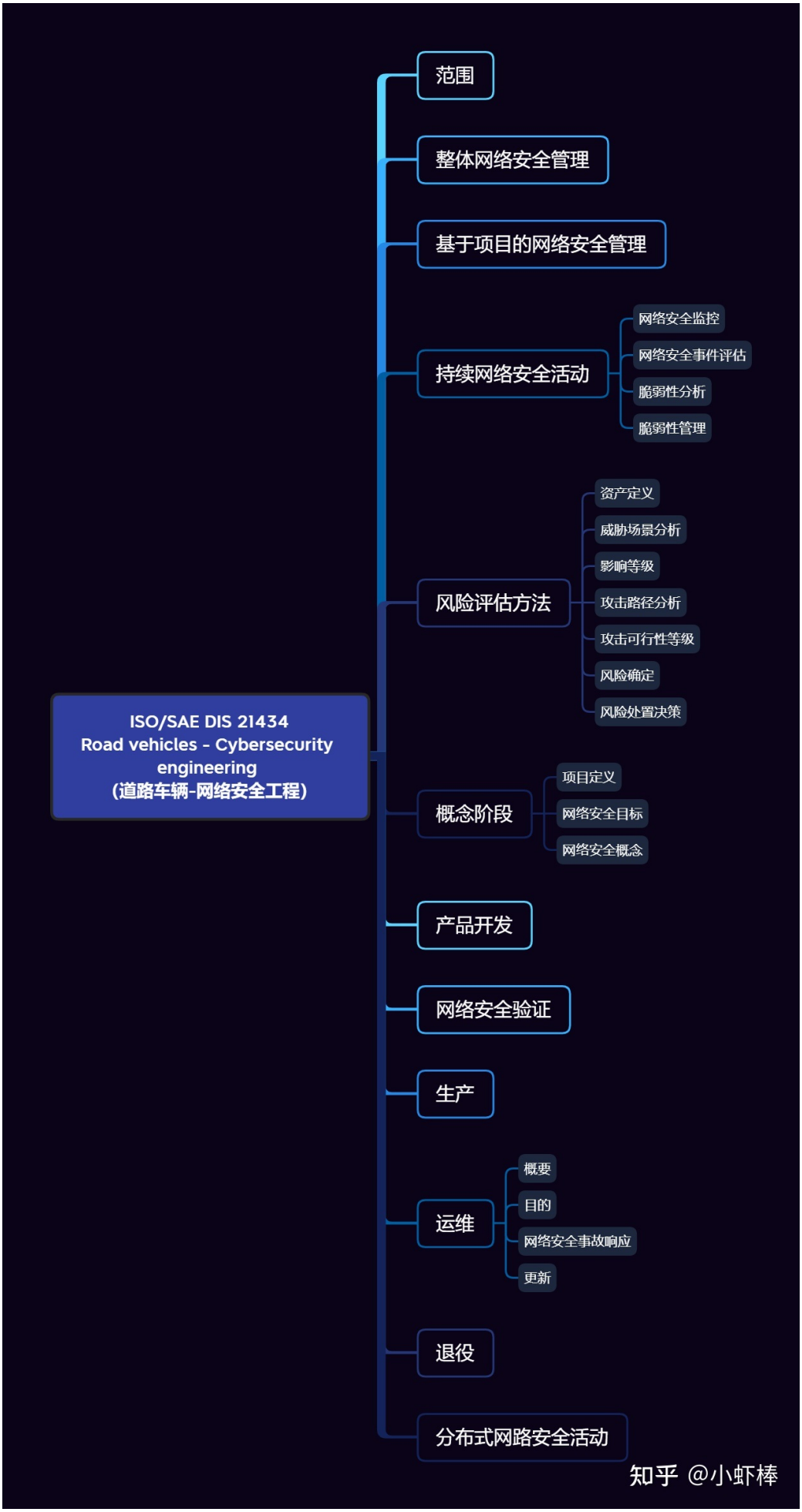
- `WP.29` = `UNECE WP.29 TF-CS/OTA` = `UNECE WP.29`
  - `UNECE` = 联合国世界车辆法规协调论坛
  - 新法规要求
    - 车辆制造商只有获得网络安全管理体系（CSMS）认证的情况下，才可以进行车辆型式认证和市场准入

ISO/SAE 21434

- `ISO/SAE 21434` = `ISO 21434`
  - 是什么：一个安全标准=安全规范
  - 领域：汽车行业
  - 一句话概述：`ISO/SAE 21434` 是 `SAE` 和 `ISO` 共同制定的第一个汽车行业的网络安全标准
  - 背景
    - 当前OEM无法保证车辆在连接网络后不会带来不可预知的风险，因为没有安全性的衡量标准，在开发软件/固件的过程中也没有遵循任何标准，确保车辆的安全性
    - 汽车领域对网络安全的需求是定义可以在整个供应链中使用的通用语言或术语。为了应对汽车行业中的网络安全挑战，现已提出ISO / SAE 21434，以在汽车领域内建立共同点
    - `ISO/SAE 21434` 是一个单一标准，适用于车辆中任何与外部网络相连的系统或者组件
  - 架构
    - 

  - 最新状态：ISO/SAE21434标准最终版已于2020年完成
  - 内容
    - 概述
      - 规定了道路车辆，其组件以及整个工程(如概念、设计和开发)、生产、运行、维护等过程中的网络安全风险管理要求
        - 像ISO26262管理功能安全要求一样
        - 目的：管理道路车辆电气和电子系统的网络安全威胁
      - 全面规定了道路车辆及其部件和接口的网络安全要求
        - 详细描述了如何根据网络安全问题实现网络安全管理目标

- 图
  -

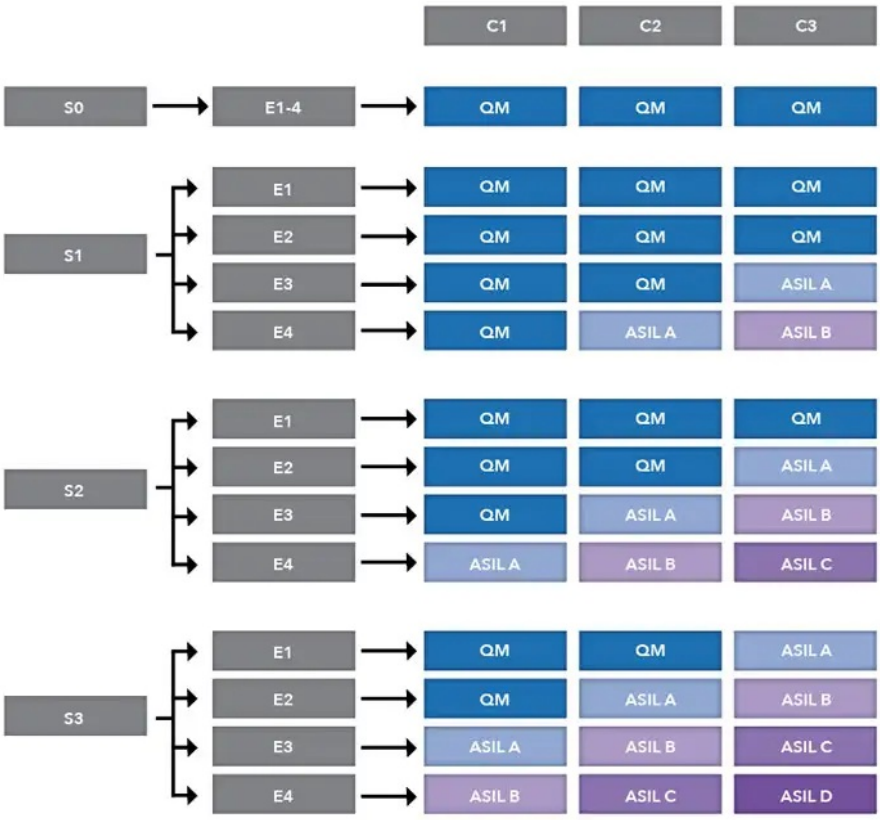

ISO/SAE DIS 21434
Road vehicles - Cybersecurity engineering
(道路车辆-网络安全工程)
范围
整体网络安全管理
基于项目的网络安全管理
持续网络安全活动
网络安全监控
网络安全事件评估
脆弱性分析
脆弱性管理
风险评估方法
资产定义
威胁场景分析
影响等级
攻击路径分析
攻击可行性等级
风险确定
风险处置决策
概念阶段
项目定义
网络安全目标
网络安全概念
产品开发
网络安全验证
生产
运维
概要
目的
网络安全事故响应
更新
退役
分布式网路安全活动
知乎 @小虾棒

    - 细节
        - 主要从15个方面对车辆的网络安全进行了阐述
            - 其中5-7章：从宏观上介绍车辆网络安全的总体要求
                - 整体网络安全管理
                - 基于项目的网络安全管理
                - 持续网络安全活动
            - 后续的7个章节：按照产品全生命周期的顺序，定义了从风险评估、概念开发、验证到生产、运维、退役等各阶段对于车辆网络安全的要求
            - 最后一章：“分布式网络安全活动”主要介绍当前车辆分布式合作开发的背景下，对于资产识别，要求报价，责任分布等方面的网络安全要求
        - 每个章节都是从“概要、目的、输入、要求和建议、工作产品”5个角度进行叙述
    - 评价
        - ISO/SAE 21434 被看作一项业界共识，是目前网络安全方面监管和认证机构的重要参考文件

ISO 26262

- `ISO 26262`
  - 是什么：汽车领域中的一个功能安全标准 `functional safety standard`
  - 重点：`Road vehicles – functional safety` = 道路车辆的功能安全 =简称： `功能安全`
  - 来源：衍生自 `IEC 61508`
  - 用于：汽车中的电子或电气设备，包括辅助驾驶、动力、车辆动态控制系统等
  - 目的
    - 提供车用产品安全生命周期（管理、开发、生产、运行、维修、退役），并在各个阶段可以订制需要的活动
    - 包括整个开发过程的机能安全层面（包括需求规格、设计、实现、整合、验证、确认及组态等活动）
    - 提供针对车用，以风险为基础的风险确认方式（ `ASIL` = 车辆安全完整性等级 ）
    - 用ASIL来确认，若要达到可接受的残余风险，应该要满足哪些安全需求
    - 提供验证和确认方式的需求，以确保已达到足够，且可以接受的安全性
  - `ISO 26262` 的主要部分
    - `ISO 26262:2011` 是10个部分
      - Part 1: Vocabulary
      - Part 2: Management of functional safety
      - Part 3: Concept phase
      - Part 4: Product development at the system level
      - Part 5: Product development at the hardware level
      - Part 6: Product development at the software level
      - Part 7: Production and operation
      - Part 8: Supporting processes
      - Part 9: ASIL-oriented and safety-oriented analysis
      - Part 10: Guideline on the safety standard
    - `ISO 26262:2018` 是12个部分
      - Part 1: Vocabulary
      - Part 2: Management of functional safety
      - Part 3: Concept phase
      - Part 4: Product development at the system level
      - Part 5: Product development at the hardware level
      - Part 6: Product development at the software level
      - Part 7: Production, operation, service and decommissioning
      - Part 8: Supporting processes
      - Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analysis
      - Part 10: Guidelines on ISO 26262
      - Part 11: Guidelines on application of ISO 26262 to semiconductors
      - Part 12: Adaptation of ISO 26262 for motorcycles
  - 核心模块： `ASIL`
    - `ASIL` = `Automotive Safety Integrity Level` = 汽车安全集成度等级
      - 定义了软件开发的安全方面的需求
      - 不同维度
        - 包括
          - Severity
            - S0: No injuries
            - S1: Light to moderate injuries
            - S2: Severe to life-threatening (survival probable) injuries
            - S3: Life-threatening (survival uncertain) to fatal injuries.
          - Exposure
            - E0: Incredibly unlikely
            - E1: Very low probability (injury could happen only in rare operating conditions)

        - E2: Low probability
        - E3: Medium probability
        - E4: High probability (injury could happen under most operating conditions)
    - Controllability
        - C0: Controllable in general
        - C1: Simply controllable
        - C2: Normally controllable (most drivers could act to prevent injury)
        - C3: Difficult to control or uncontrollable
- 概述



SAE J3061

- `SAE J3061` = `网络物理车辆系统网络安全指南` = `信息物理汽车系统网络安全指南` = `Cyber Security Guidebook for Cyber-Physical Vehicle Systems`
  - 概述：车辆网络安全的指南。该标准于 2016 年 1 月发布，在 128 页上描述了在整个生命周期内（从开发到退役/刮取）保护产品的框架，并通过大量引用其他项目，概述网络安全方法
    - 首部针对汽车网络安全而制定的指导性文件
  - 目的和作用
    - 这份指导文件提供了一个网络安全流程的框架和指导，以帮助企业识别和评估网络安全威胁，同时定义了一个完整的开发生命周期过程框架，便于在每个组织的开发过程中对其进行定制和使用，从而将网络安全从概念阶段到生产，运营，服务和最终退出市场的阶段，都整合到现有物理车辆系统的整个开发生命周期过程中
  - 要点
    - 流程模型的基石，组织（公司）可以自行适应。
    - 介绍一些方法和工具，以验证车辆使用的技术系统
    - 网络安全的基本原则
    - 制定进一步标准的基础，在公布后列入 `ISO/SAE 21434`
  - 说明
    - 有些方法来源于 `ISO 26262` 的 `功能安全道路车辆` （功能安全），一般来说，有许多参考这个标准

方案

- 汽车安全方案
  - 毕马威+ESCRYPT
    - 优势和经验
      - `毕马威`：`信息安全审计`
      - `ESCRYPT`：`汽车安全工程`
    - CSMS解决方案
      - `PROOF = Product Security Organization Framework = 产品安全组织框架`
        - 将网络安全要求集成到企业管理和汽车工程之中，PROOF将有助于企业有效集中资源，快速制定和实施满足业务发展并且行业合规的CSMS体系和流程，建立并形成涵盖企业端和产品端的网络安全持续改进能力
        - 白皮书：汽车网络安全白皮书 (assets.kpmg)
          - https://assets.kpmg/content/dam/kpmg/cn/pdf/zh/2020/12/automotive-cyber-security-whitepaper.pdf

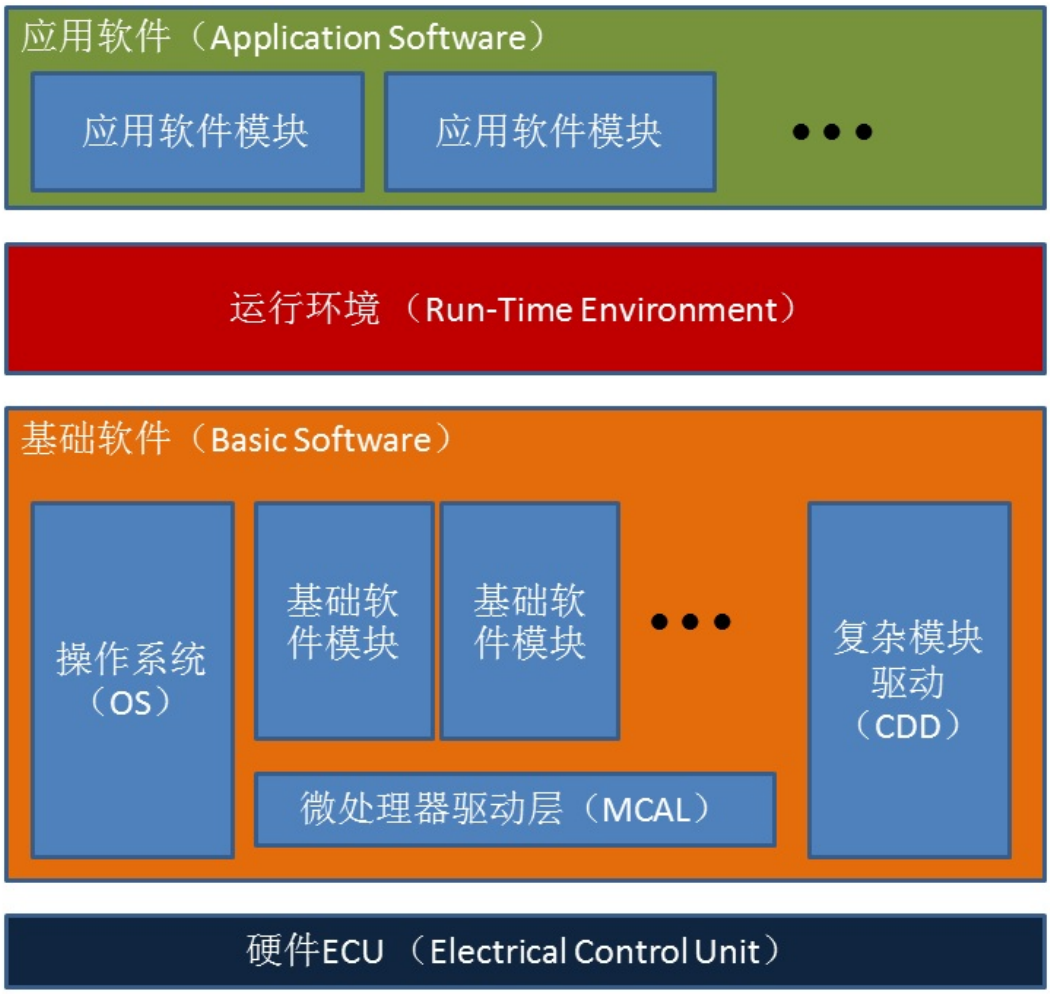
相关

此处整理和汽车安全相关的其他方面的内容。

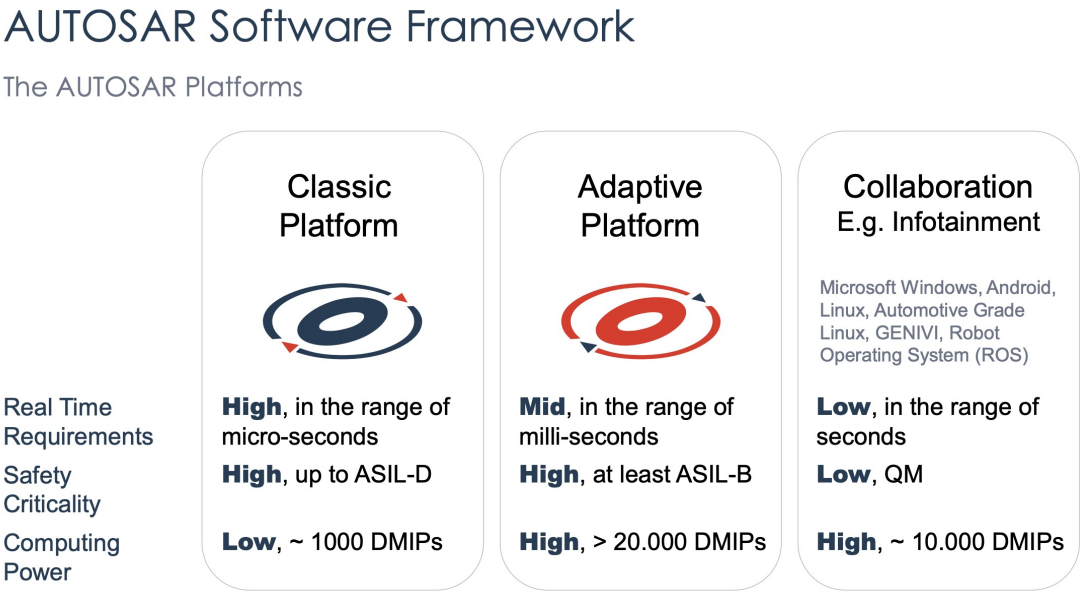
AutoSar

- `AutoSar`
  - = `AUTOSAR` = `AUTomotive Open System ARchitecture` = 汽车开放系统架构
  - 概述：由全球汽车制造商、零部件供应商及其他电子、半导体和软件系统公司建立，目的是为了降低汽车控制软件的开发风险，提高软件复用度
    - AUTOSAR联盟自2003年成立以来，成员队伍不断壮大，基本上涵盖了世界各大著名整车厂、零部件供应商、半导体公司及软件工具开发商。近年来也有越来越多的中国企业例如华为、百度、长城汽车等加入联盟
  - AUTOSAR联盟成员

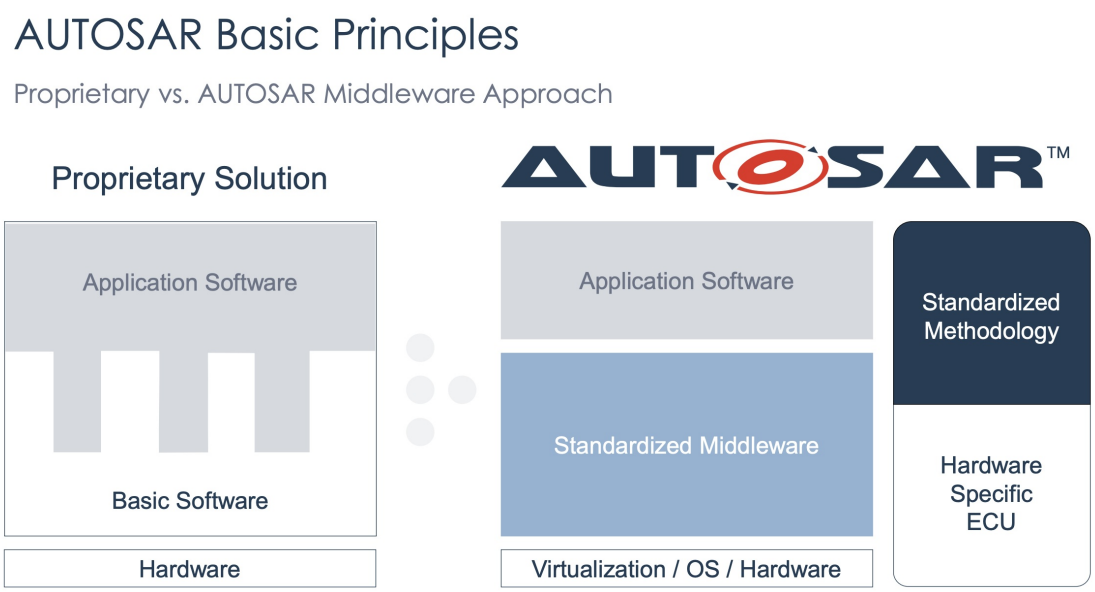
    -
  - AutoSar软件架构



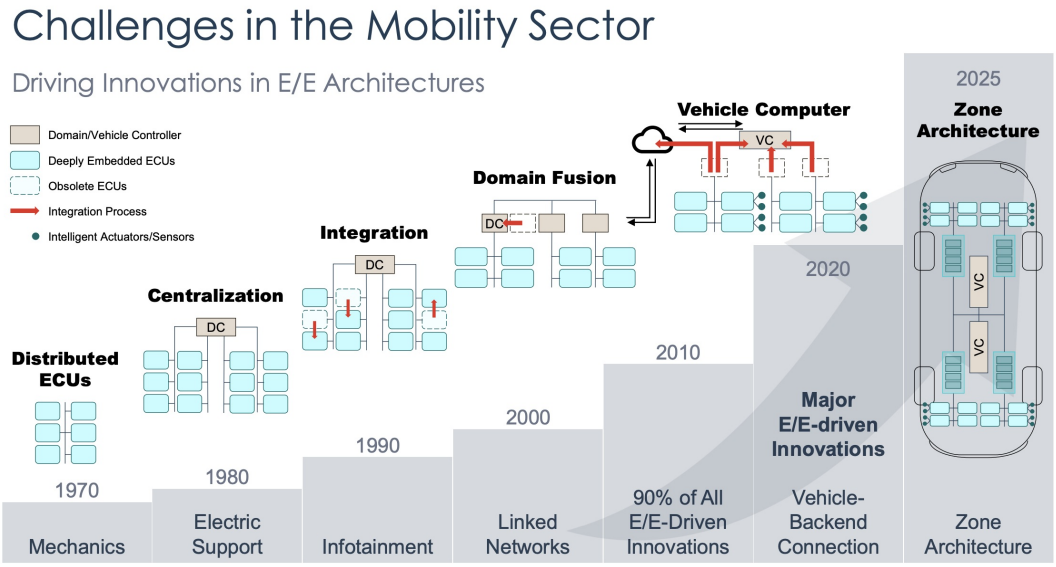
- AutoSar软件框架



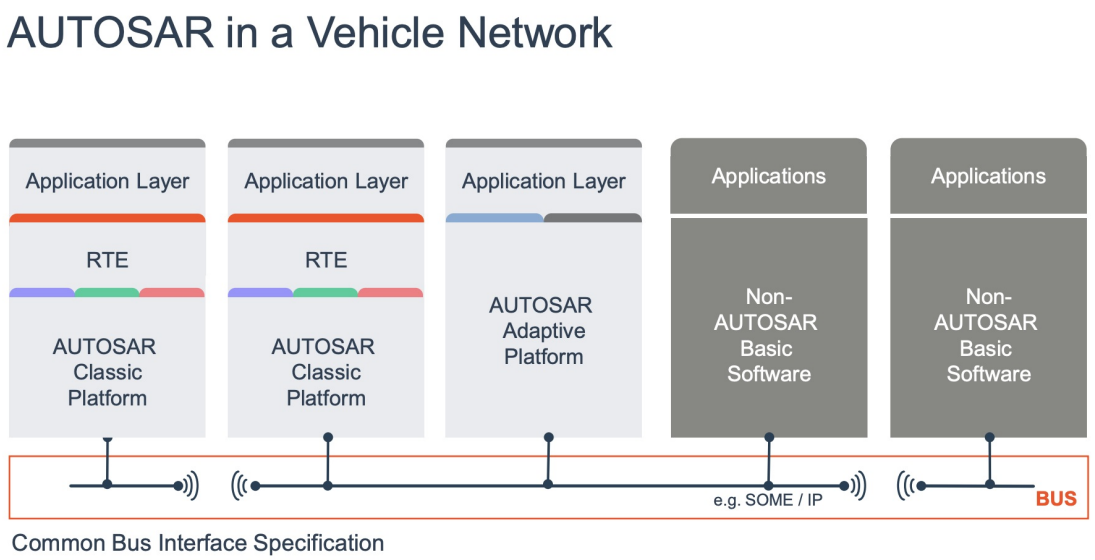
- 和传统方法对比=AutoSar的基本原则



- 背景
  - 汽车电子电器架构发展趋势



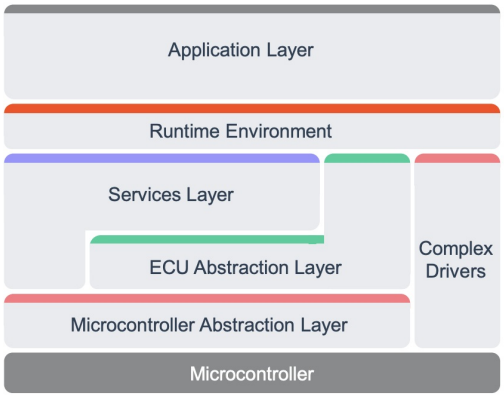
- AutoSar在车辆网络架构的作用



- AutoSar的平台

- 经典平台 = Classic Platform

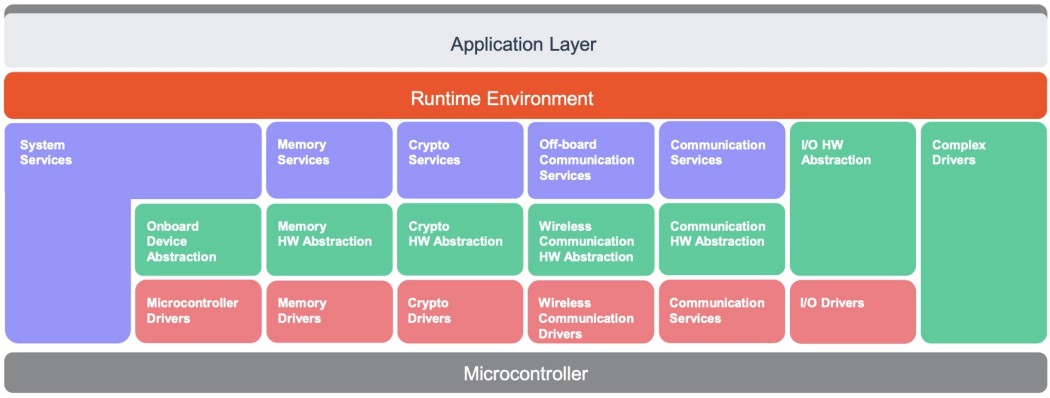
AUTOSAR Classic Platform
Layered Software Architecture (1/2)



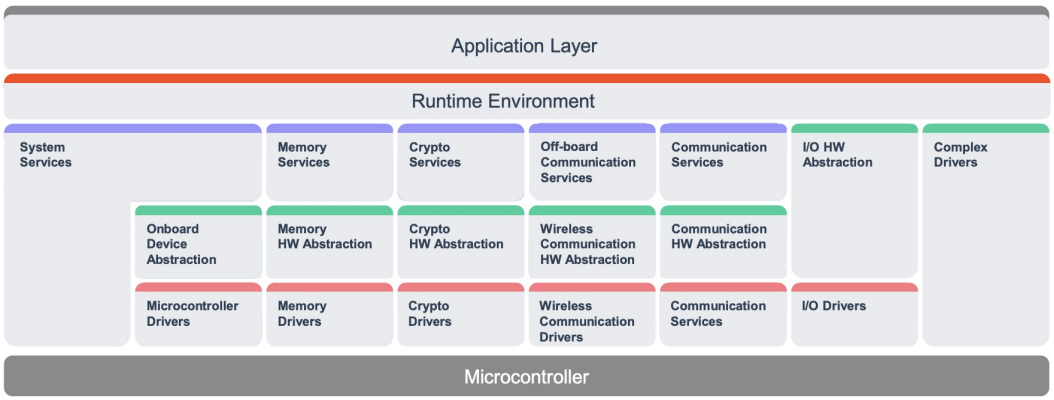
The layered architecture of the classic platform basically supports

- Hardware abstraction
- Scheduling of runnables and tasks (OS)
- Communication between applications on the same hardware and over the network
- Diagnosis and diagnostic services
- Safety- and
- Security Services

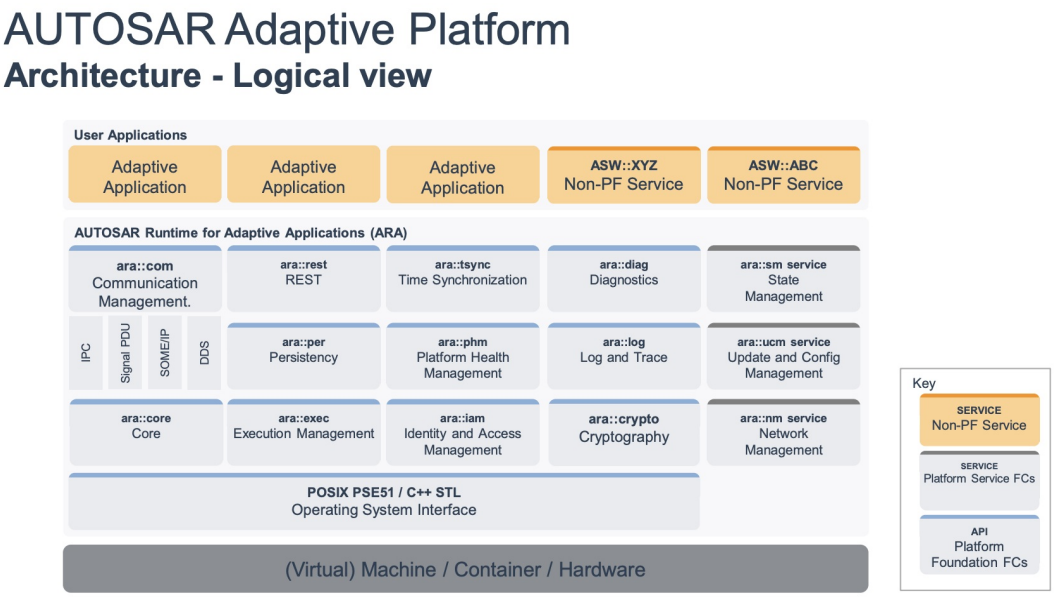
AUTOSAR Classic Platform
Layered Software Architecture (2/2)



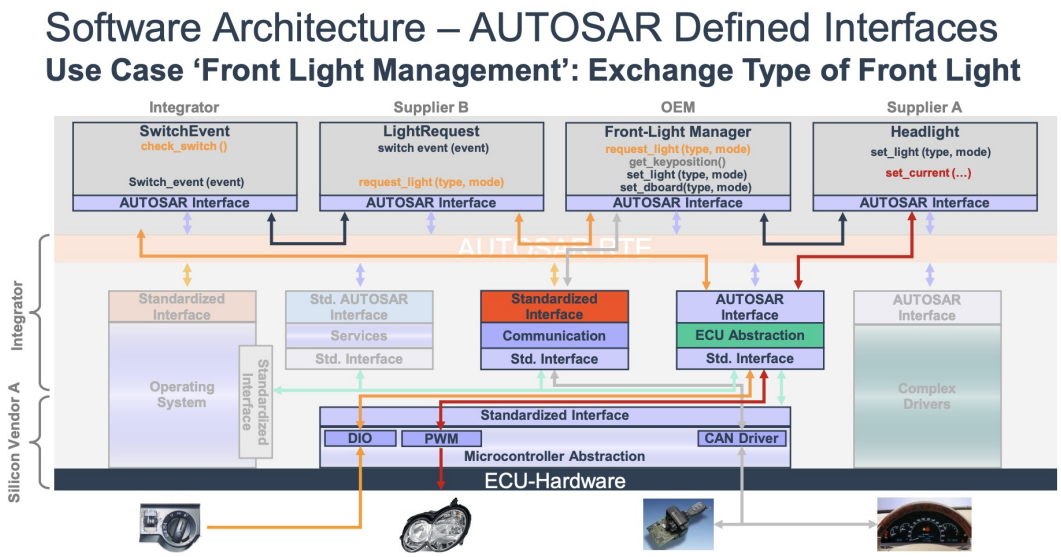
AUTOSAR Classic Platform
Layered Software Architecture (2/2)

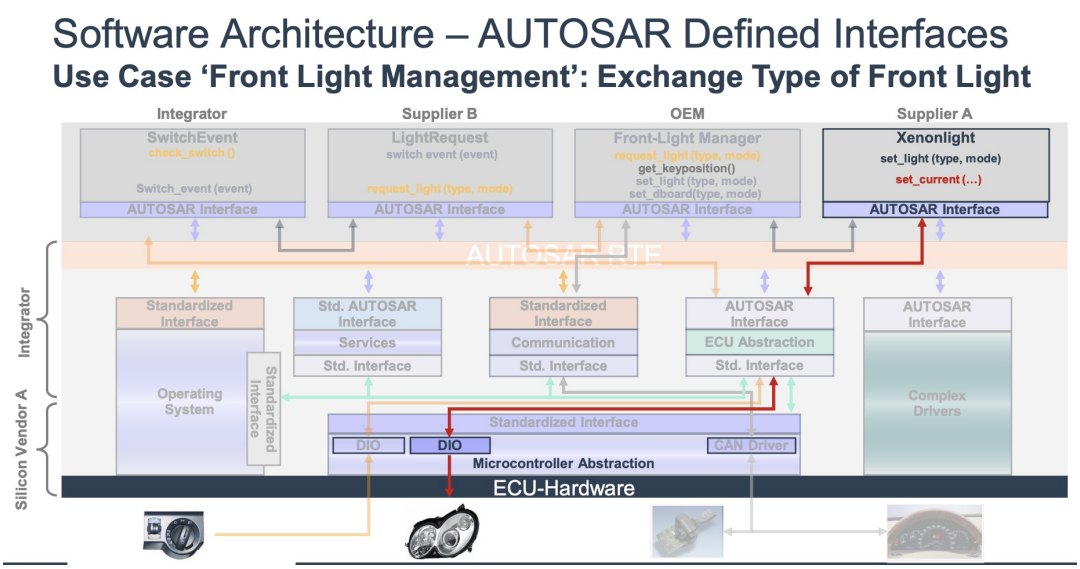


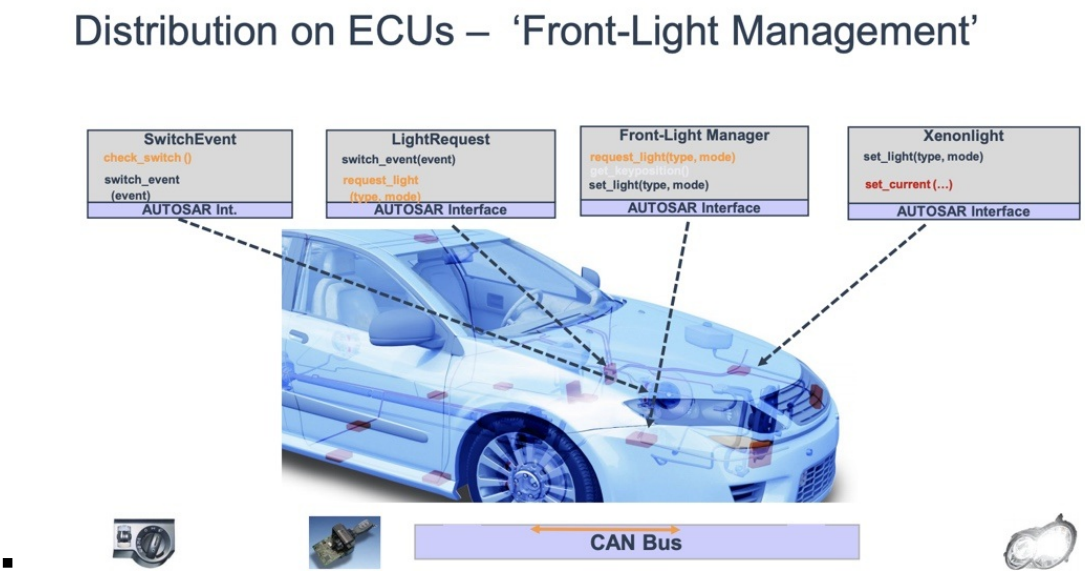
- 自适应平台 = Adaptive Platform

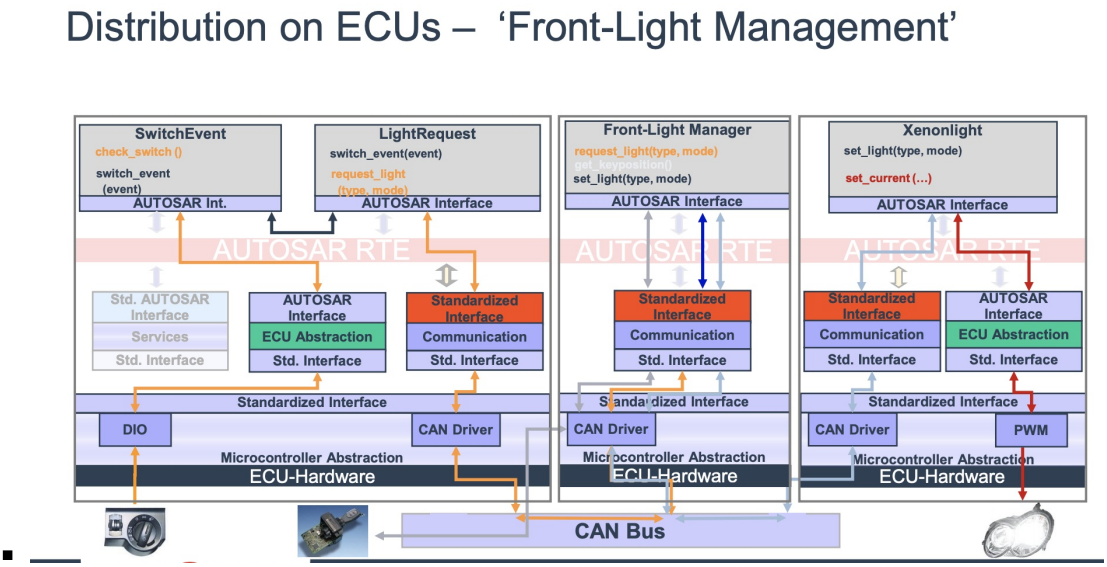


- 举例
  - Front Light Management









NHTSA

- `NHTSA` = `National Highway Traffic Safety Administration` =（美国） `国家公路交通安全管理局`
  - 官网
    - NHTSA | National Highway Traffic Safety Administration
      - https://www.nhtsa.gov/
  - Logo
    - 

  - 概述
    - `NHTSA` 是美国运输部下的一个执行机构，成立于美国华盛顿特区，其宗旨是“保护生命、防止伤害，减少车辆撞击
      - Save lives, prevent injuries, reduce vehicle-related crashes
  - 主要工作
    - 编写和执行机动车辆相关的安全性、防盗、燃油经济标准相关标准，关于燃油经济业务是依照 `CAFE` 来制定
      - `CAFE` = `Corporate Average Fuel Economy` = `统合平均燃料效能标准`
    - 给汽车制造商和进口商发放授权
    - 管理允许或栏截进口车辆、汽车安全性零件
    - 掌管车辆识别号码
    - 开发用于安全测试的仿真人偶，和进行安全测试
    - 提供车辆保费相关讯息
    - 统计分析部门（National Center for Statistics and Analysis）制作和更新相关资料
      - 其中的 `FARS` = `Fatality Analysis Reporting System` = `事故报告分析系统` 的分析数据，被全世界相关研究所关广泛引用

附录

下面列出相关参考资料。

参考资料

- 【整理】汽车网络安全
- 信息安全
-
- 汽车黑客揭秘：我是如何通过逆向API接口黑掉宝马i3的
- 初识智能网联汽车安全 - 安全客，安全资讯平台
- 『智能设备』-看雪安全论坛
- [翻译]对宝马车载apps协议的逆向分析研究-『智能设备』-看雪安全论坛
- BMW Connected Apps Protocol
- 车联网信息安全技术专家 | 江苏智能网联汽车创新中心有限公司 | LinkedIn
- FlexRay - Wikipedia
- AUTOSAR - Wikipedia
- AUTOSAR介绍 - 知乎
- About - AUTOSAR
- AUTOSAR_EXP_Introduction_Part1
- AUTOSAR_EXP_Introduction_Part2
- National Highway Traffic Safety Administration - Wikipedia
- 美国国家公路交通安全管理局 - 维基百科，自由的百科全书
- SAE J3061 - 维基百科，免费百科全书
- Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061_201601
- SAE J3061<信息物理汽车系统网络安全指南>解读（一）搜狐汽车搜狐网
- ISO26262_百度百科
- ISO 26262 - 维基百科，自由的百科全书
- ISO 26262 - Wikipedia
- ISO - ISO 26262-1:2018 - Road vehicles — Functional safety — Part 1: Vocabulary
- ISO26262 - 知乎
- What Is ISO 26262? Overview + ASIL | Perforce
- 网络隐患堵在智能汽车起跑线上-新华网 (xinhuanet.com)
- 汽车网络安全白皮书 - 毕马威中国 (home.kpmg)
- 汽车网络安全白皮书 (assets.kpmg)
- 汽车网络安全 | 汽车安全系统 | 互联汽车安全 | Autotalks (auto-talks.com)
- 汽车网络安全事件4年增长605%，国内首个智能汽车网络靶场落地深圳_36氪 (36kr.com)
- 360的《2019 智能网联汽车信息安全年度报告》
- 浅谈ISO/SAE 21434汽车网络安全标准（一）概述 - 知乎 (zhihu.com)
- ISO/SAE 21434网络安全标准概述 - 知乎 (zhihu.com)
- 五菱在海南大会的所展示的芯片和换电
- 博世中国高管相约“跳楼”背后，马来西亚芯片厂如何影响汽车业？ (qq.com)
- OTA是点金石，还是遮羞布？_懂车帝
- CAN笔记（1） CAN简介_氢键H-H-CSDN博客
- 移动终端/消费类电子/汽车电子等相关总线的协议分析和测试工具概述（2） - 极术社区 - 连接 AIoT 开发者与生态服务
- 兼容功能安全和信息安全的车载网络解决方案是否存在？ - 知乎 (zhihu.com)
- [原创]智能硬件入门-智能设备-看雪论坛-安全社区|安全招聘|bbs.pediy.com
- 网络安全的学习路线是怎么样的？ - 知乎 (zhihu.com)
- CIVC王羽：《汽车自动驾驶技术路线图》 信息安全技术 - 安全内参 | 决策者的网络安全知识库
-