标准化驱动-共建汽车网络安全开发生态

UAES-谢晓超

2025.5.12

介绍内容

我们是谁

遇到的问题&解决思路

标准化设计实例

标准化驱动-共建汽车网络安全开发生态

我们是谁

1995年7月13日，签订联合汽车电子合资合同与章程

联合汽车电子有限公司

49%
中联汽车电子有限公司

罗伯特·博世有限公司
41%

10% 博世（中国）投资有限公司

1995-1998

公司成立

- 1995公司成立
- 发动机管理系统（EMS）开始生产，上海成立技术中心

1998-2008

稳步前进

- EMS业务稳步发展
- 2007年国内第一个自主研发EMS电子控制器M7.8.0批产

2008-2012

业务扩展

- 拓展EMS业务，汽油直喷系统投产
- 布局新业务领域：变速箱控制(TC)、电力驱动(EH）和车身电子(BE)

2012-2017

高速发展

- 各业务板块蓬勃发展：EH, BE, EMS, TC
- 2013年销售额突破100亿，2016年销售额突破200亿

2017-2021

转型成长

- 拓展新能源、智能网联、数据服务等业务
- 发布汽车服务品牌“U行·天下”，USP

2021-至今

突破进取

- 加快推进：热管理系统、电控悬架、智能传感器、软件与服务业务
- 发布新愿景“科技驾驭未来出行”
- 2022年销售额突破309亿元，2024年销售额突破416亿元

发动机管理系统

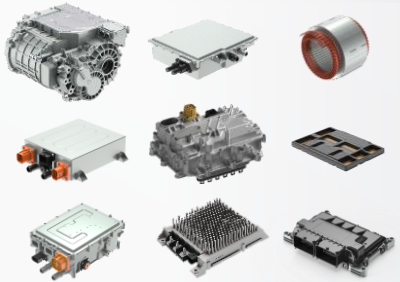
- 电子控制器
- 燃油喷射系统
- 供油与空气管理系统
- 传感器与点火线圈
- 两轮车与运动车辆

变速箱控制系统

- 变速箱控制器
- 变速箱电磁阀
- 电子模块
- 智能电机控制器

电动化

- 电桥、电机、定转子
- 逆变器、逆变砖、功率模块
- 车载充配电单元、高压直流转换器、48V直流转换器
- 电池管理系统

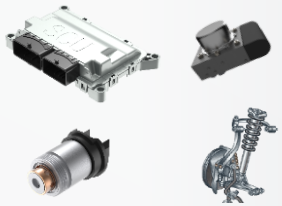


先进网联

- 车身控制
- 区域控制
- 网关及车载计算平台
- 数字钥匙系统
- 电网管理

电控悬架

- 电控悬架控制器
- 智能空簧供气模块
- 悬架电磁阀
- 整车垂向运动控制算法



智能传感器

- 电流传感器
- 高度传感器
- 加速度传感器
- 门把手传感器
- NFC传感器

热管理

- 制冷剂回路集成模块
- 冷却液回路集成模块
- 双回路集成模块
- 热管理控制器
- 多通阀、膨胀阀

软件与服务

- 联电软件平台：提供标准SOA服务组件和快易用开发工具
- U行·天下：云端动力监控，预测能量管理，用车画像，智慧匹配，数字钥匙…

USP 开发者平台

U行·天下

经营业绩 | 客户分布

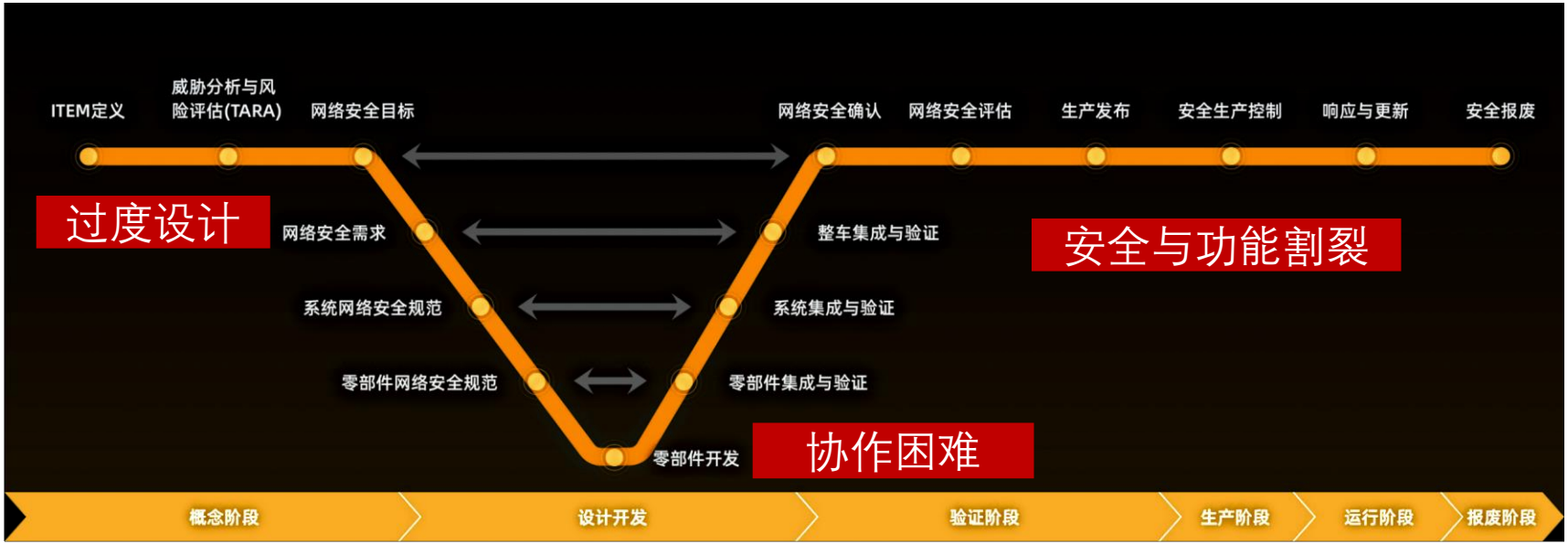
一汽-大众 FAW-VOLKSWAGEN
上汽大众 SAIC VOLKSWAGEN
大众安徽 VOLKSWAGEN ANHUI
BMW
VOLVO
神龙汽车有限公司
mazda
NISSAN
广汽丰田
广汽 HONDA
东风 HONDA
一汽丰田
上汽通用五菱 SGMW
上汽通用汽车 SAIC-GM
JAGUAR
LAND ROVER
Ford

BYD 比亚迪汽车
GEELY
长城汽车
中国一汽 FAW GROUP
SAIC
长安汽车 CHANGAN AUTO
CHERY
广汽集团 GAC GROUP
BAIC 北京汽车
JAC 江淮汽车
DFM

蔚来
理想
mi
SERES 赛力斯汽车
FORTHING 东风风行
岚图 VOYAH
AVATR
ZEEKR
SPOTLIGHT
AION 埃安

——遇到的问题——

遇到的问题 | 总览

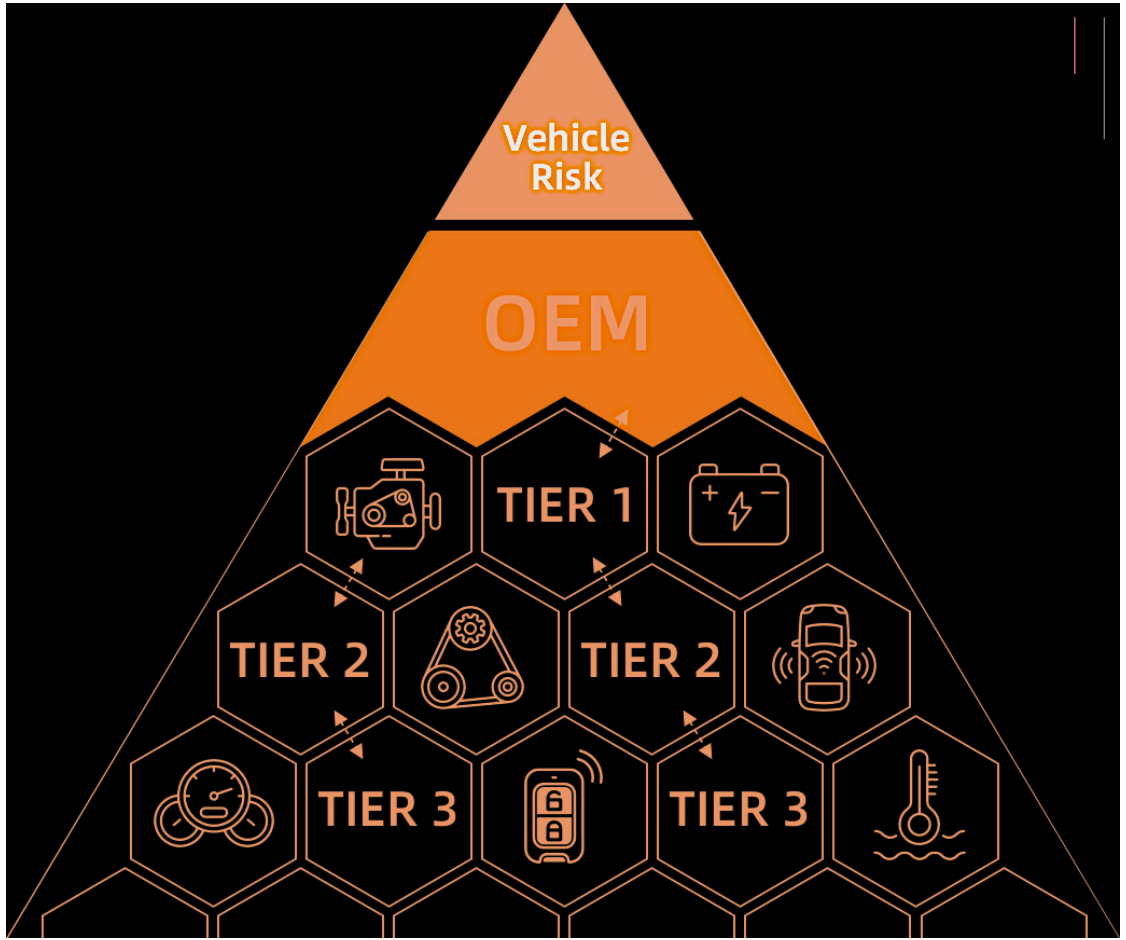


挑战1:过度设计

- **多层加密的边际效益递减**
- **硬件安全模块的滥用**
- **通信防护的过度设计**

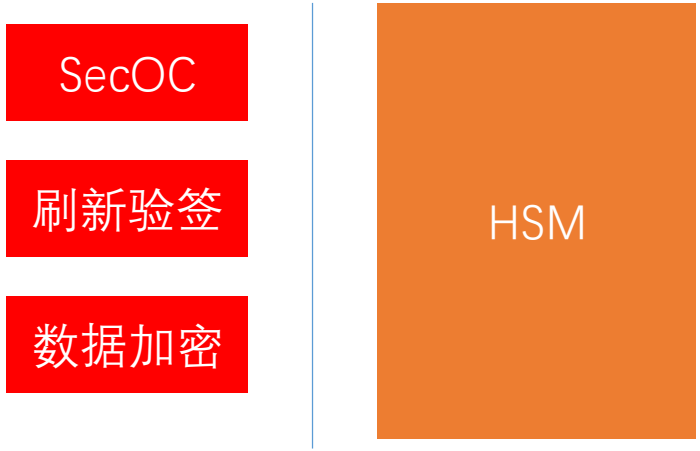
挑战2:协作困难

- **主机厂、供应商之间协同**
- **企业内不同组织间协同**
- **设计 & 开发工具间协同**



挑战3:安全与功能的设计割裂

- **需求定义阶段的“信息孤岛”**
- **开发流程中的“并行脱节”**
- **技术架构的割裂：安全功能长期作为“外挂模块”导致资源抢占**



解决思路

Baseline需求

静态-风险分析结果

Baseline设计

整车架构

安全需求

功能需求

硬件架构

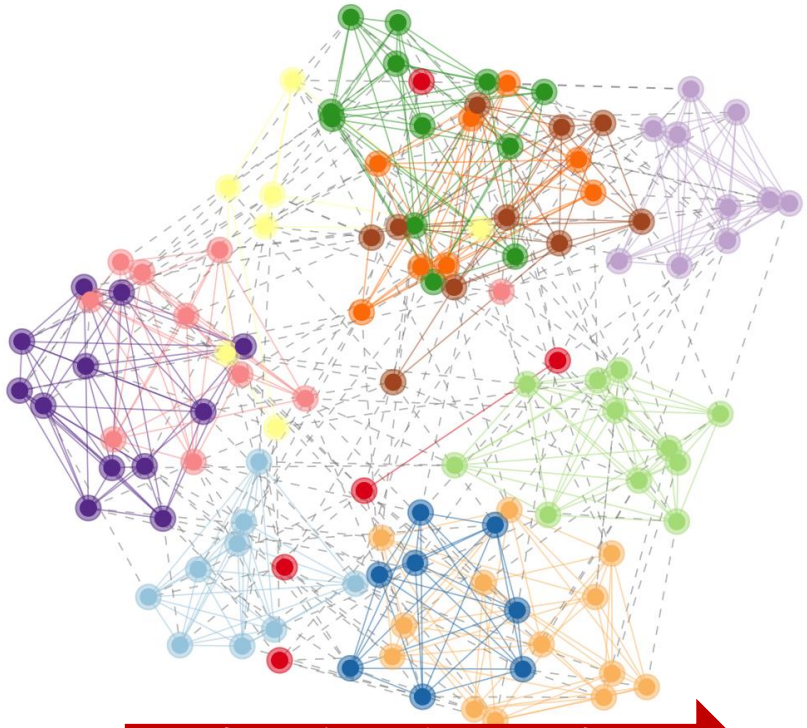
软件架构

攻击路径

功能测试

…

输入



输出

网络安全计划

TARA分析报告

网络安全需求

网络安全设计规范

网络安全漏洞

整车级信息安全验证

系统级信息安全验证

…

动态-轻量化模型建模

解决思路 | 统一架构

安全架构1.0
模块化

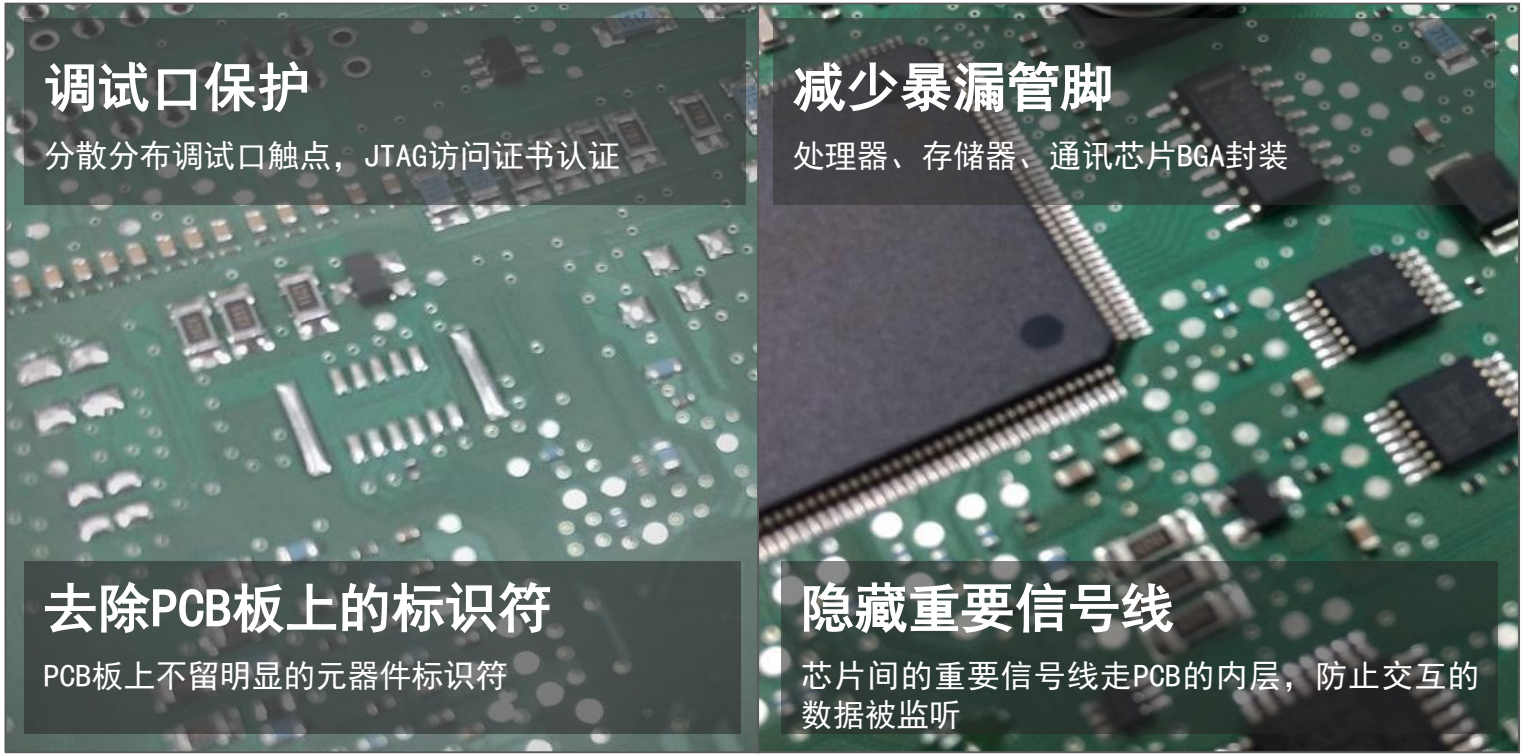
安全架构2.0
服务化

安全架构3.0
配置化

标准化
设计实例

PCB加固
增加攻击者信息收集难度

- PCB加固
- 调试口锁定
- 安全刷新功能
- 安全启动功能
- 安全认证
- 车内安全通讯
- 防火墙
- 车内TLS



调试口保护
分散分布调试口触点，JTAG访问证书认证

减少暴漏管脚
处理器、存储器、通讯芯片BGA封装

去除PCB板上的标识符
PCB板上不留明显的元器件标识符

隐藏重要信号线
芯片间的重要信号线走PCB的内层，防止交互的数据被监听

调试口访问控制
给芯片加上“门锁”

- PCB加固
- 调试口锁定
- 安全刷新功能
- 安全启动功能
- 安全认证
- 车内安全通讯
- 防火墙
- 车内TLS

典型安全威胁

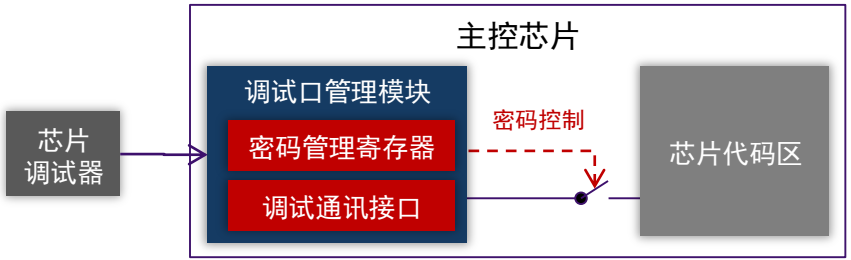
❑ **控制器固件提取**

➢ 通过控制器芯片调试口，提取出程序代码，进行二进制代码逆向，以获取核心数据和程序工作逻辑

安全防护措施

❑ **芯片调试口锁定**

➢ 设置访问密码，限制通过调试器提取软件代码的功能



安全刷新功能介绍
校验刷新包的合法性

- PCB加固
- 调试口锁定
- 安全刷新功能
- 安全启动功能
- 安全认证
- 车内安全通讯
- 防火墙
- 车内TLS

典型安全威胁

❑ **篡改程序代码**

➢ 篡改程序代码，再通过软件刷新手段更新控制器中的程序，达到改变控制器工作逻辑的功能

```
if (Security_Activated == True)
{
    Execute Security_Authentication;
    ……
}
```

将关键字节从 01改成00，对应的程序逻辑从True 变成 False，则跳过了安全认证

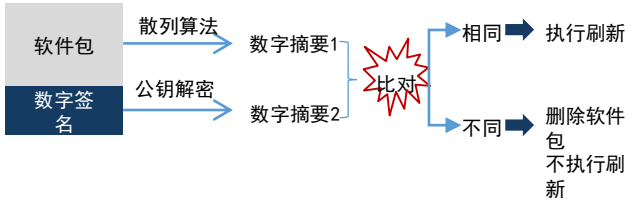
红框为配置字 Security_Activated 的值

- 01 代表 True，执行 Security_Authentication
- 00 代表 False，不执行

安全防护措施

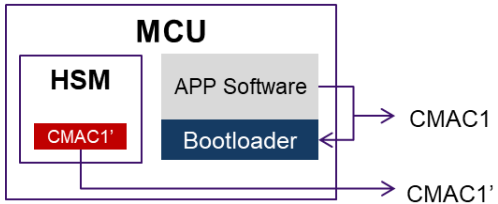
❑ **安全刷新校验**

➢ 利用非对称算法和数字签名机制，实施程序代码的保护，在刷新程序时进行合法性和完整性校验　　e.g. 非对称加密 + 散列算法…



安全启动功能介绍
校验启动固件的合法性

- PCB加固
- 调试口锁定
- 安全刷新功能
- 安全启动功能
- 安全认证
- 车内安全通讯
- 防火墙
- 车内TLS



HSM中的CMAC值是在成功刷新Host核之后，通过调用HSM的接口进行计算得到，用于计算CMAC值的密钥原生在HSM中，在芯片出厂时就已自带，永远不会离开芯片本身，无法被修改，而且每颗芯片都不同。

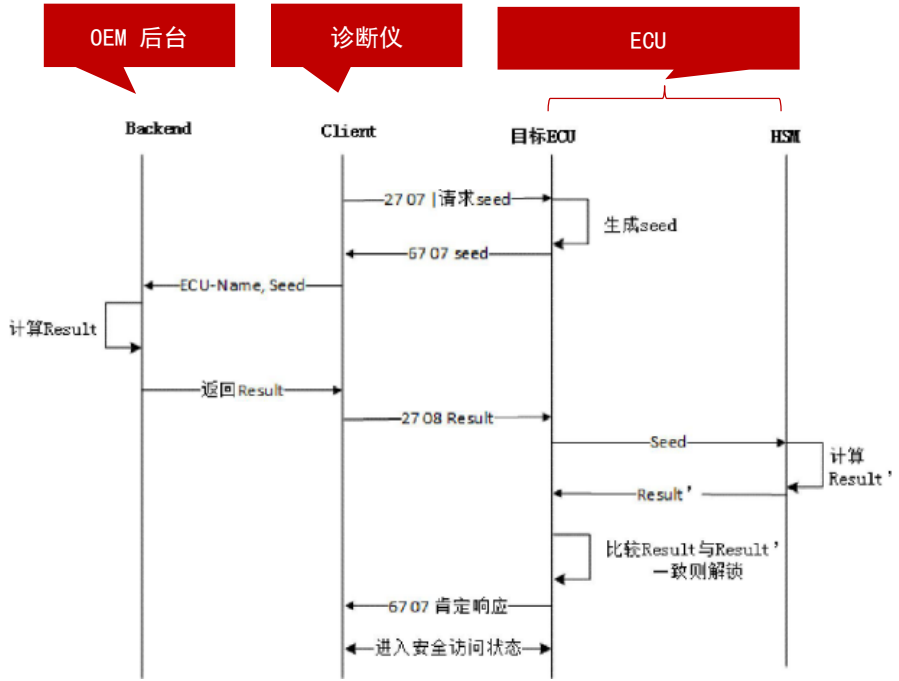
Step1： Bootloader加载APP Software时，调用HSM API接口计算得CMAC1

Step2： HSM比对CMAC1和预存的CMAC1’的一致性，决定跳转与否

安全认证功能介绍
对外部节点进行身份认证

- PCB加固
- 调试口锁定
- 安全刷新功能
- 安全启动功能
- 安全认证
- 车内安全通讯
- 防火墙
- 车内TLS

诊断安全认证



其它安全认证

挑战-应答：IMMO，PEPS，RKE…

车内安全通讯功能介绍
关键信号认证

安全存储功能

调试口锁定

安全刷新功能

安全启动功能

安全认证

车内安全通讯

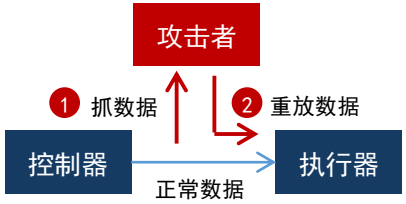
防火墙

车内TLS

典型安全威胁

❑ 信号重放

➢ 抓取交互数据并重放，若接收方未做校验，则误以为来自合法发送方



Line	Description	ArbI...	DataBytes
30950	HS CAN $2FC	2FC	0A 00 00 00 00 00 40 69
30951	SAS_Status	E0	F0 41 15 E0 21 CC 00 00
30952	HS CAN $84	84	FF 00 00 78 40 94 DF 9E
30953	EMS_EngineRPM	85	9E 00 14 D2 79 60 00 F0
30954	HS CAN $1B2	1B2	00 00 06 3F 00 00 00 00
30955	HS CAN $1A3	1A3	FF 18 28 18 00 00 0D 3D
30956	HS CAN $1A6	1A6	00 FF 00 00 7F 00 00 00
30957	HS CAN $1A7	1A7	00 7F 00 00 7F 00 00 00
30958	ACU_ChimeTelltaleReq	380	12 BC D6 00 00 00 00 00
30959	HS CAN $2B1	2B1	22 01 00 00 00 00 00 00

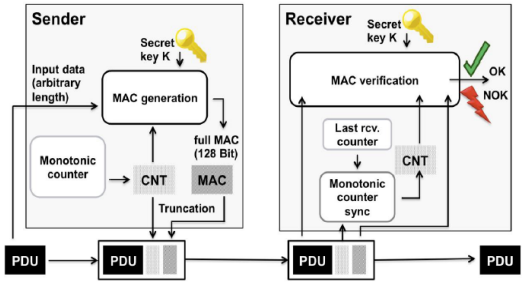
被抓取的交互数据

安全防护措施

❑ SecOC

➢ 增加单向增加的消息计数值，以标识报文唯一性，接收方对其进行校验，确保新收到的计数值大于以前的计数值

➢ 基于对称加密算法，对消息数据和计数值计算对应的消息验证码，以确保消息不被篡改



防火墙功能介绍

对非法的数据包进行过滤

典型安全威胁

❑ **恶意数据攻击**

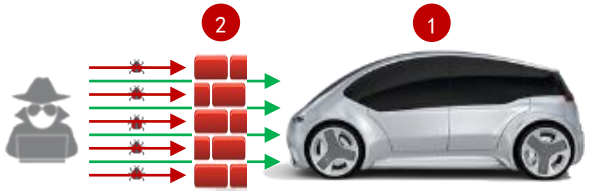
- 发送恶意数据请求给目标
- 短时间内发送海量数据给目标，导致目标瘫痪

攻击者发送恶意数据，试图破解目标系统，或抢占合法用户的访问通道，甚至可使服务器超载运行并且瘫痪

安全防护措施

❑ **防火墙流量清洗**

➢ 设置一个异常流量的检测器，对恶意流量进行清洗过滤



1. 配置流量过滤规则
2. 数据过滤

车内TLS
基于PSK的轻量认证

安全存储功能

调试口锁定

安全刷新功能

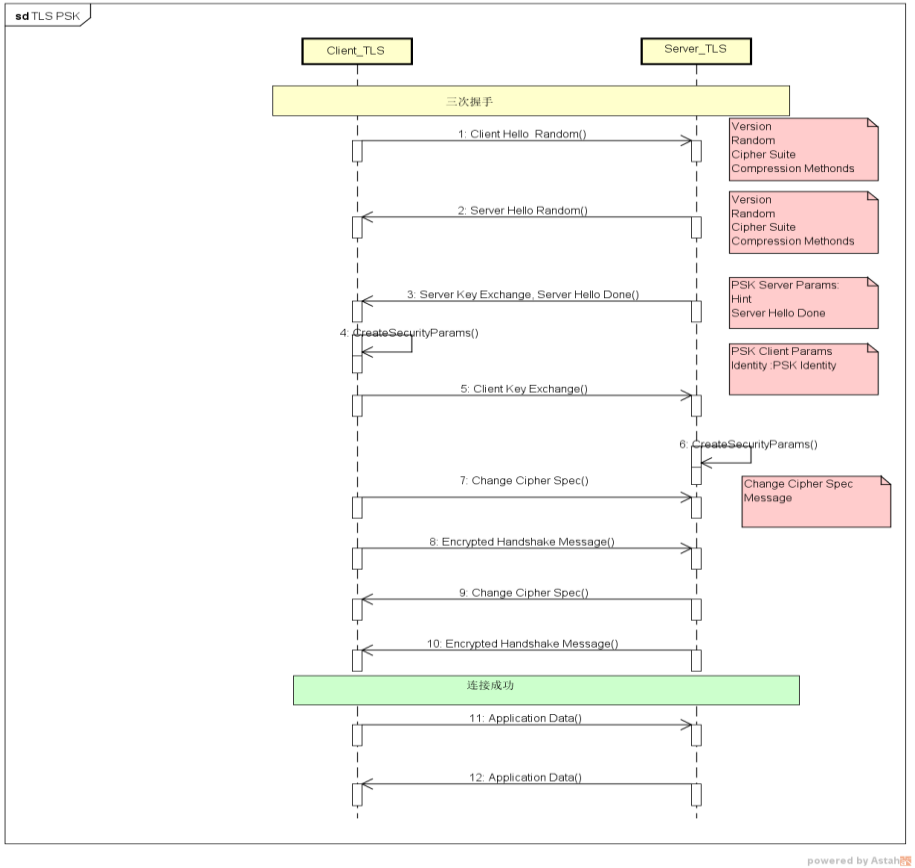
安全启动功能

安全认证

车内安全通讯

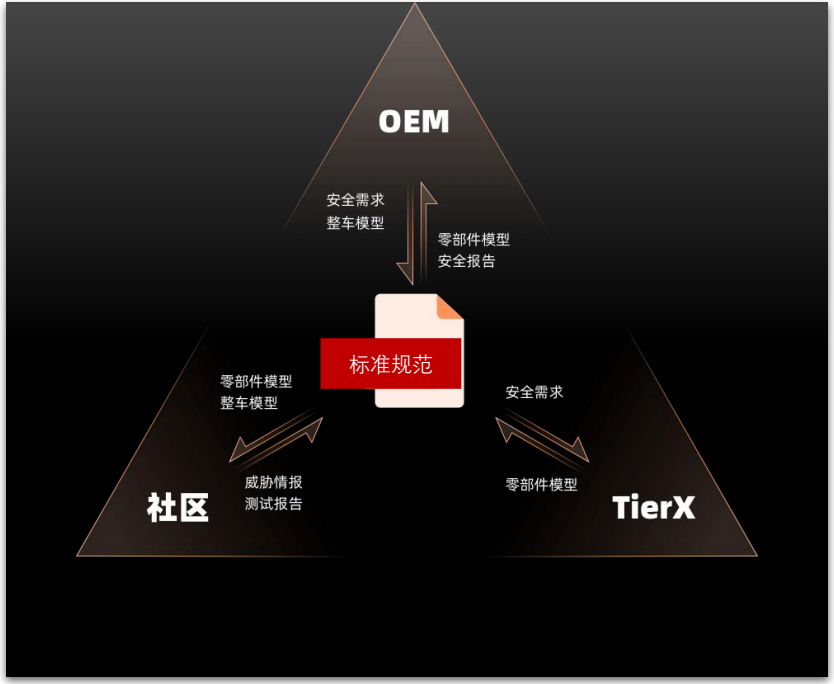
防火墙

车内TLS



——标准化驱动——

- **标准化生态协同的“底层语言”**
- **标准化赋能技术创新**
- **从“合规驱动”到“价值共创”**
- **避免“过度标准化”抑制创新、造成浪费**



UAES 科技驾驭未来出行
PASSION TO SHAPE MOBILITY

Thanks !