东风汽车集团有限公司技术中心
DONGFENG MOTOR CORPORATION TECHNICAL CENTER

车联网网络安全探索与实践

孙伟

深圳
2023年10月13日星期五

东风技术中心介绍—定位

“十四五”期间

成为集团共性技术与核心技术的掌控者，创新推动自主事业可持续发展

市场导向、创新驱动、自立自强、活力激发、协同高效

东风风神　东风·猛士　VOYAH 岚图　东风风行　启辰 VENUCIA

客户意识

基于市场导向，满足客户需求

服务意识

建立乙方思维，深化技术服务

支撑东风自主乘用车产品研发

成本意识

加强成本管理，加强技术转化

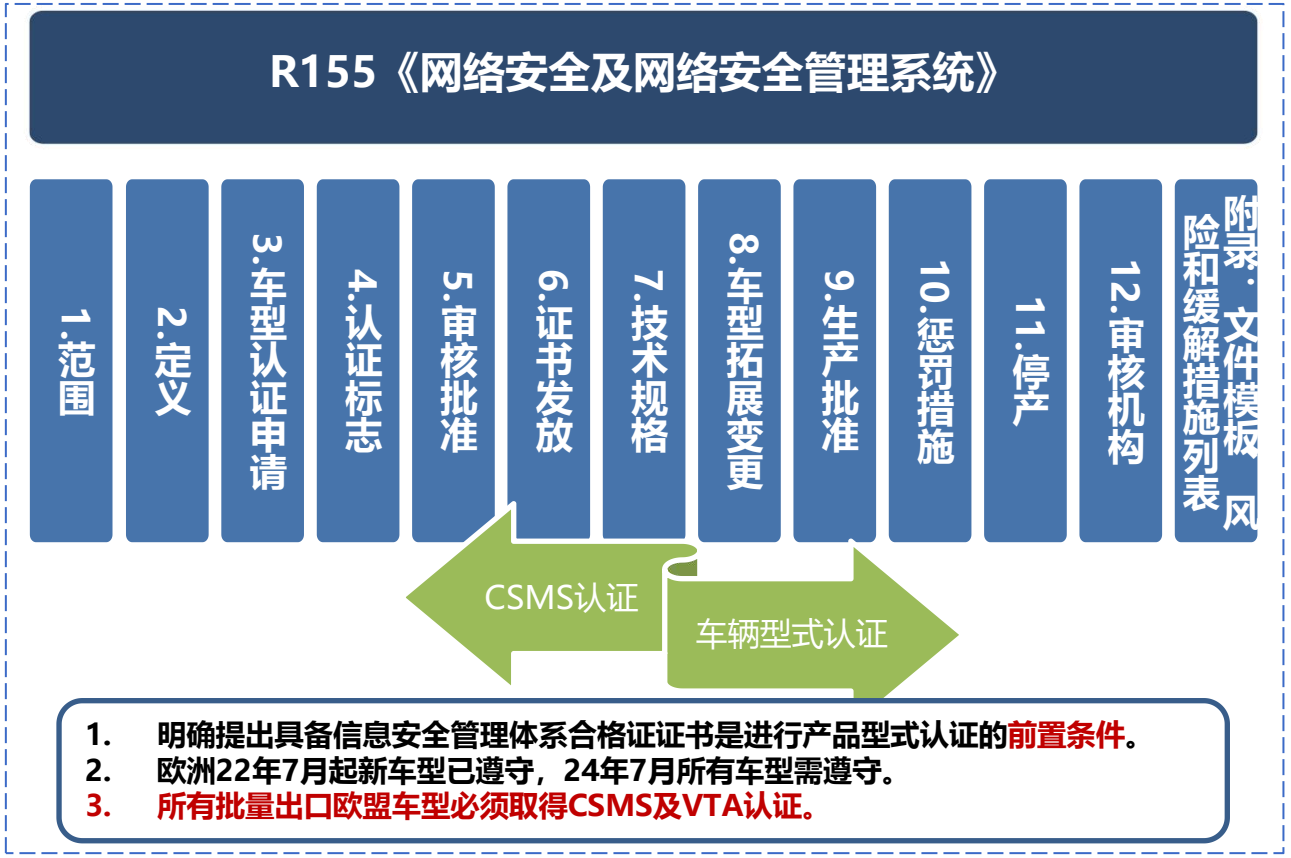
坚定自主意识

优化开发流程，掌握自主核心

产品开发 (风神/M事业)	科技创新 (集团专项)	技术推广 (研发协同)	科技孵化 (服务社会)

1 背景：国际法规—R155《网络安全及网络安全管理系统》

- 联合国世界车辆法规协调论坛（简称为UN/WP29）R155法规于2021年1月正式发布，从2022.7月开始所有新车型需要遵守。



2021.1 法规正式生效

2022.7 欧盟所有新车型需遵守（已生效）

2024.7 欧盟所有车型需遵守

1 背景： 国际法规—R155《网络安全及网络安全管理系统》

■ R155《网络安全与网络安全管理系统》将对智能汽车网络安全准入的要求划分为两部分，一是针对智能汽车车辆制造商的网络安全管理体系要求，二是针对车辆产品的网络安全能力要求。

CSMS 要求

适用范围

适用于M类（乘用车）、N类（载货车）、至少有一个电控单元的O类车（挂车）以及具备L3以上自动驾驶功能的L6和L7类车辆。

制造商所具备的信息安全管理系统是否涵盖**开发**、**生产**、**后生产**阶段。

- 组织内部信息安全管理流程；
- 风险和威胁类型的识别流程；
- 评估、分类、处理已识别风险的流程；
- 确认风险已有效管理的流程；
- 车辆信息安全测试的流程；
- 监视、检测、识别、响应网络威胁和漏洞的流程；
- 分析已发生的攻击事件的流程等

制造商需证明对其**供应商**、**服务商**以及**子公司**实施了信息安全相关的管控措施

CSMS合格证 是智能网联汽车进入欧洲市场的首要通行证

车辆型式认证（VTA）技术要求

◆ 有效CSMS证书

◆ 识别和管理供应链的风险

◆ 识别车辆关键元素，并且进行详尽的风险评估，并适当处理/管理已识别的风险，并采取削减措施

◆ 应针对识别的风险采取缓解措施

◆ 应确保存储或执行的售后软件、服务应用和数据的安全

◆ 应在型式认证之前，开展充分的测试

◆ 车辆制造商应针对待型式认证的车辆类型**采取以下措施**：

① 发现并防止网络攻击

② 支持在检测与车辆类型有关的威胁、漏洞和攻击方面的监测能力

③ 提供数据取证能力，以分析尝试或已成功的攻击

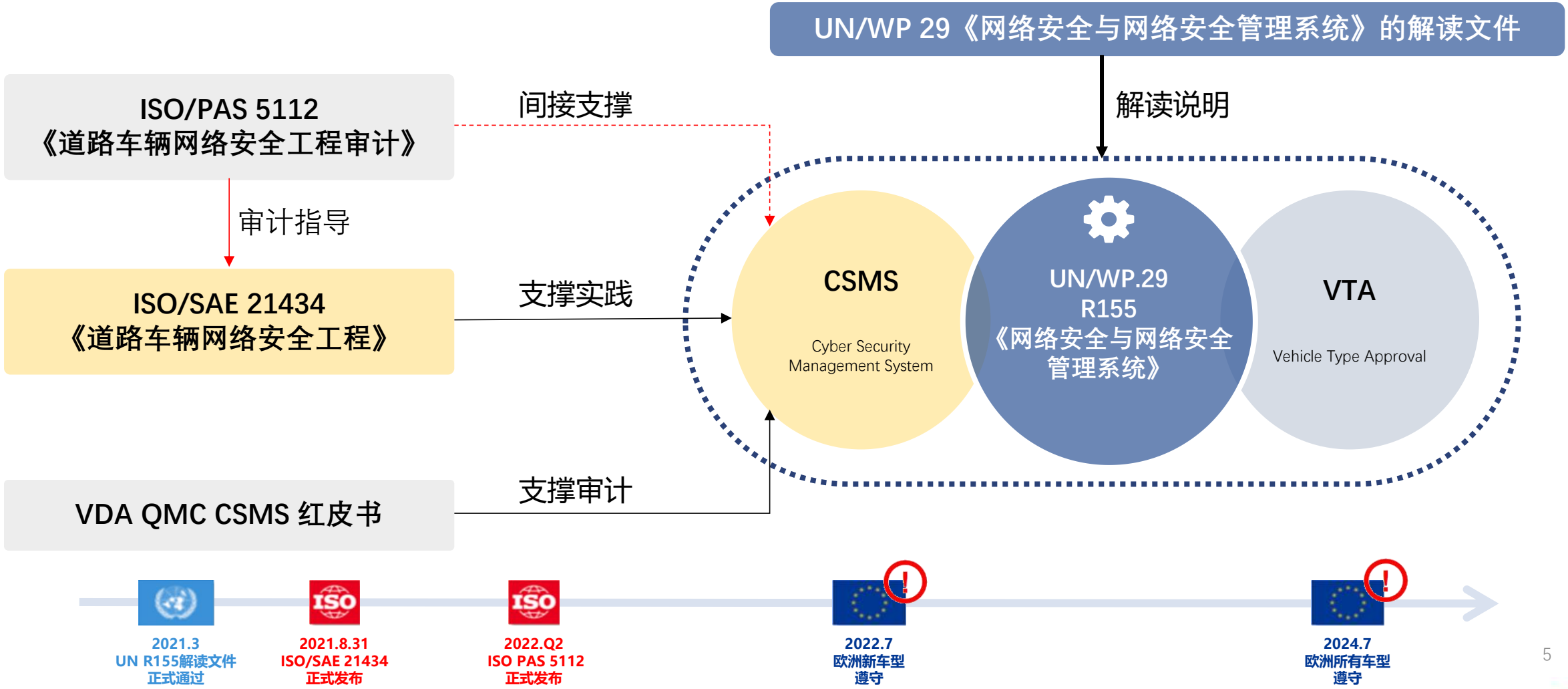
◆ 密码算法

——使用公认密码算法

获得CSMS合格证后，可由制造商或授权代表提出**型式认证申请**。

1 背景：国际法规及标准关系

- UN/WP 29 R155法规《网络安全与网络安全管理系统》是全球第一个汽车网络安全强制法规，与之相关联的文件包括：ISO/SAE 21434、ISO PAS 5112、解读文件以及VDA红皮书细则。



1 背景：国内法规

■ 为更好做好国内国际法规的协调，2021年，《汽车整车信息安全技术要求》调整为强制标准。

序号	标准名	项目号	进度
1	《汽车信息安全通用技术要求》	GB/T 40861-2021	发布，2022.05.01实施
2	《电动汽车远程信息服务与管理系统信息安全技术要求及试验方法》	GB/T 40855-2021	发布，2022.05.01实施
3	《车载信息交互系统信息安全技术要求及试验方法》	GB/T 40856-2021	发布，2022.05.01实施
4	《汽车网关信息安全技术要求及试验方法》	GB/T 40857-2021	发布，2022.05.01实施
5	《电动汽车充电系统信息安全技术要求》	GB/T	发布
6	《汽车软件升级通用技术要求》	GB	已于2022.6.23日公开征求意见
7	《汽车诊断（OBD）接口信息安全技术要求》	GB/T	下达计划
8	《汽车信息安全应急响应管理指南》	GB/T	下达计划
9	《道路车辆 信息安全工程》（ISO 21434国际标准转）	GB/T	提交立项
10	《汽车整车信息安全技术要求》	**GB**	**正在进行意见征集和完善中.....**
11	《汽车电子控制单元（ECU）信息安全防护技术要求研究》	GB/T	完成预研
12	《ISO 24089: 道路车辆——软件升级工程》《汽车信息安全风险评估规范》	GB/T	完成预研
13	《车载计算平台标准化需求研究》	研究项目	完成预研
14	《智能网联汽车 数字证书应用技术要求研究》	研究项目	完成预研
15	《智能网联汽车 商用密码应用技术要求研究》	研究项目	完成预研

1 背景：政策监管

■ 2021年开始，各部委连续出台网络安全、数据安全相关标准政策，开启了网络安全强监管时代，与标准同步推进。

- **2021年8月12日 工业和信息化部发布《关于加强智能网联汽车生产企业及产品准入管理的意见》**
- **2022-04-15 工业和信息化部装备工业发展中心 《关于开展汽车软件在线升级备案的通知》**
- **2022-04-08 工业和信息化部等五部委 《关于进一步加强新能源汽车企业安全体系建设的指导意见》**
- **2022-04-01 市场监管总局等五部委 《关于试行汽车安全沙盒监管制度的通告》**
- **2022-03-07 工业和信息化部 《车联网网络安全和数据安全标准体系建设指南》**
- 2022-01-04 国家发展和改革委员会 《网络安全审查办法》
- 2021-02-17 工业和信息化部 《关于做好工业领域数据安全管理试点工作的通知》
- 2021-11-14 国家互联网信息办公室 《网络数据安全管理条例（征求意见稿）》
- 2021-09-30 工业和信息化部 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》
- **2021-09-16 工业和信息化部 《关于加强车联网网络安全和数据安全工作的通知》**
- 2021-08-20 《中华人民共和国个人信息保护法》
- **2021-08-20 国家互联网信息办公室 《汽车数据安全管理若干规定（试行）》**
- **2021-08-12 工业和信息化部 《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》**
- 2021-07-13 工业和信息化部、国家互联网信息办公室、公安部 《 网络产品安全漏洞管理规定》
- 2021-06-10 《中华人民共和国数据安全法》
- 2021-06-04 市场监管总局 《关于汽车远程升级(OTA)技术召回备案的补充通知》
- 2021-05-12 国家互联网信息办公室 《汽车数据安全管理若干规定（征求意见稿）》

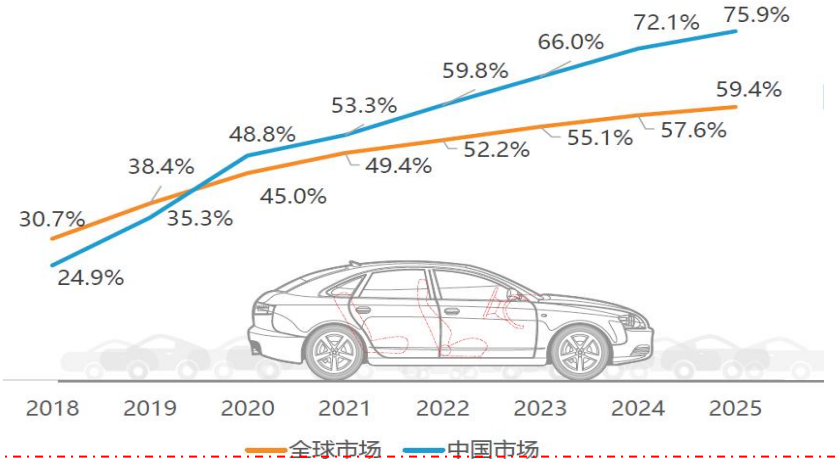
汽车领域

法律法规

1 市场和用户的应用场景变化带来新需求

■ 智能网联汽车在市场占有率逐步走高，泛Z世代成为购车主力，车联网作为彰显个性与提升体验的重要载体，需要车企在保障服务的同时提供更安全的信息技术保障。

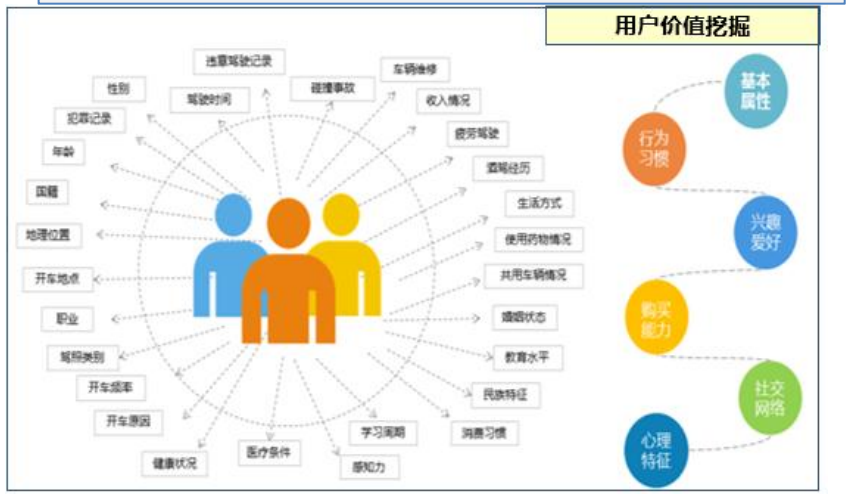
■ 全球&中国智能网联汽车渗透率情况



智能服务场景

■ 端+云支持网联应用

■ 用户连接



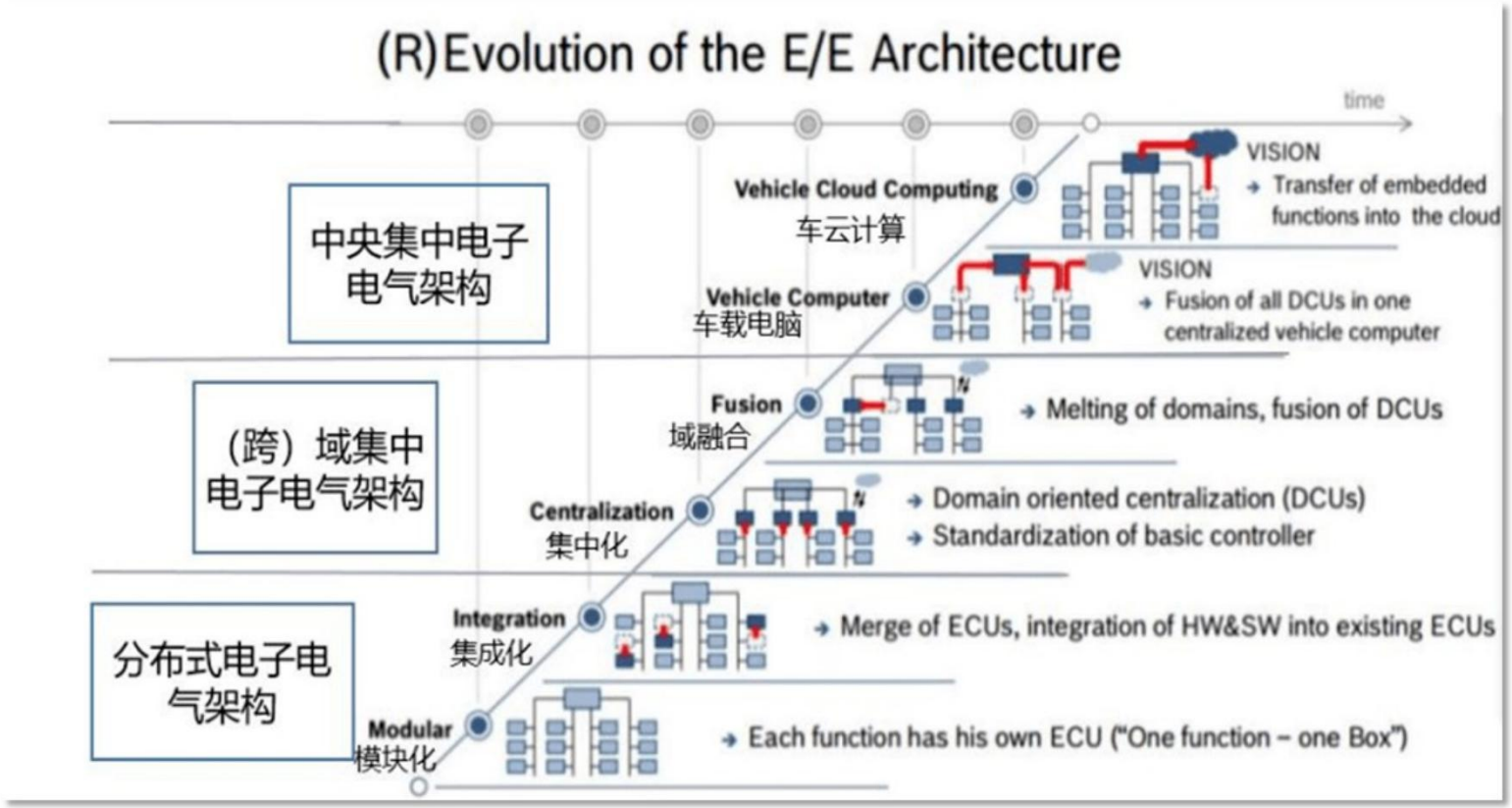
■ 未来消费主体需求

■ Z世代的消费特性

1 车联网网络安全成为一个车企必须面对的课题

- 随着汽车智能化、网联化趋势的进度加快，汽车整车EEA架构同步发生快速迭代，从域集中式电子电气架构向中央集中电器电气架构演变、车云一体化趋势越来越清晰。
- 新架构下，如何更好的保障信息安全成为一个必须解决的关键技术问题。

✓ **车云一体架构**



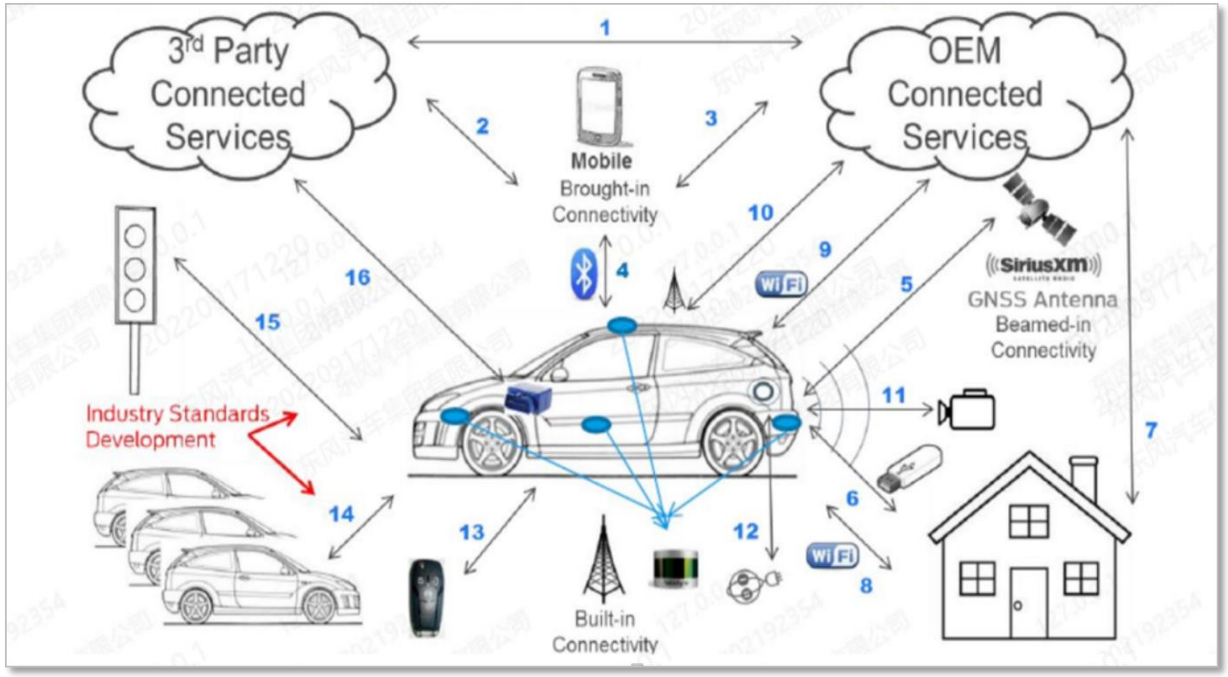
来源：BOSCH

EEA四个关键技术

- ✓ 车云计算平台
- ✓ 面向服务的SOA
- ✓ 功能安全
- ✓ 信息安全

1 越来越多的连接带来便利也带来更多风险入口

- 丰富的对外连接和丰富的应用服务；也将车辆置于车路云协同一体的总体环境，越来越多的对外交互端口，带来新的网络安全风险入口。



1. 车企服务平台与第三方服务平台的交互。
2. 第三方服务平台与手机的交互。
3. 车企服务平台与手机的交互。
4. 手机通过蓝牙与车辆的交互。（娱乐蓝牙或蓝牙钥匙的主动车控、被动车控和自动车控等功能）
5. 车辆接入全球导航卫星系统的定位信号。
6. 车辆通过 USB 接口与外界的交互。（通过 USB 刷写程序或播放外部文件）
7. 车企服务平台与智能家居的交互。（驾驶员通过车辆远程控制家中智能家居）
8. 车辆通过 Wifi 网络与智能家居的交互。
9. 车辆通过 Wifi 网络与车企服务平台的交互。
10. 车辆通过蜂窝网络与车企服务平台的交互。
11. 车辆通过摄像头设备与外界的交互。
12. 车辆通过充电口与外界设备的交互。
13. 车辆通过 RKE(Remote Keyless Entry 遥控门锁)或 PKE(无钥匙汽车门禁系统)与车辆钥匙的交互。
14. 车辆与车辆的交互。（V2V 场景下）
15. 车辆与路端设备的交互。（V2R 场景下）
16. 车辆通过诊断口与第三方服务平台的交互。（诊断场景下）
    车辆通过雷达与外界的交互。

车辆的网联化、功能的软件化、车辆的智能化将车辆信息安全防护边界扩大的同时；车辆终端的计算机化也将IT中信息安全特点引入到车辆。

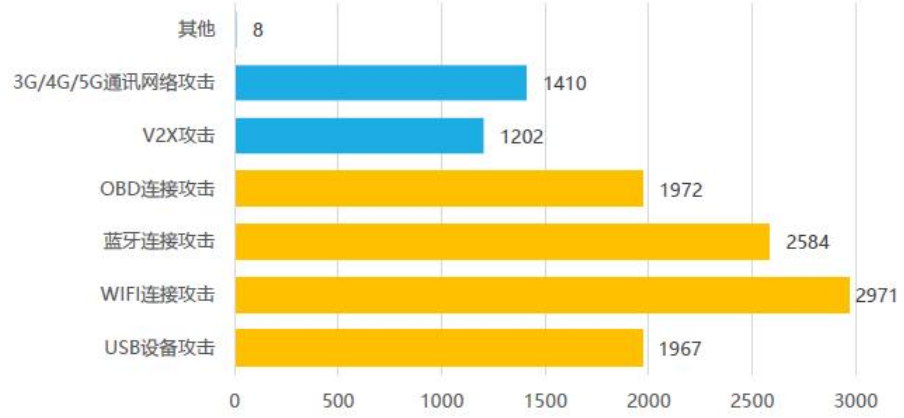
1 用户对信息安全的认识和关注度越来越高

信息安全调研

图表 70 信息安全调研-消费者最担心的使用场景

Source：车云研究院

图表 71 信息安全调研-消费者最担心的攻击载体



Source：车云研究院

被动安全 → 主动安全 → 信息安全

图表 22 汽车安全概念演进

	被动安全	主动安全	信息安全
防护目的	事故发生后，最大程度减轻人身伤害	利用智能科技实现预防及防止交通事故的发生	保障汽车软硬件系统、数据的可靠性和安全
应对场景	交通事故发生后	交通事故发生前	车联网及自动驾驶所有场景
发展阶段	1970 年后	2000 年后	2010 年后

Source：专家观点，车云研究院整理

功能安全 → 功能安全 + 预期功能安全+信息安全

图表 24 汽车信息安全的变化

	过去主要的安全挑战	新增的安全挑战
安全边界	功能安全	功能安全+信息安全
安全目标	行车环境及电子电气的稳定性	信息网络攻击下的汽车可靠性与稳定性
适用范围	人主导驾驶下的安全需求	人机共存下的汽车安全需求
适用标准	ISO26262等	J3061，ISO21434等

Sources：全国信息安全标准化技术委员会，北京航空航天大学，梆梆安全

01 智能网联汽车面临的网络安全挑战

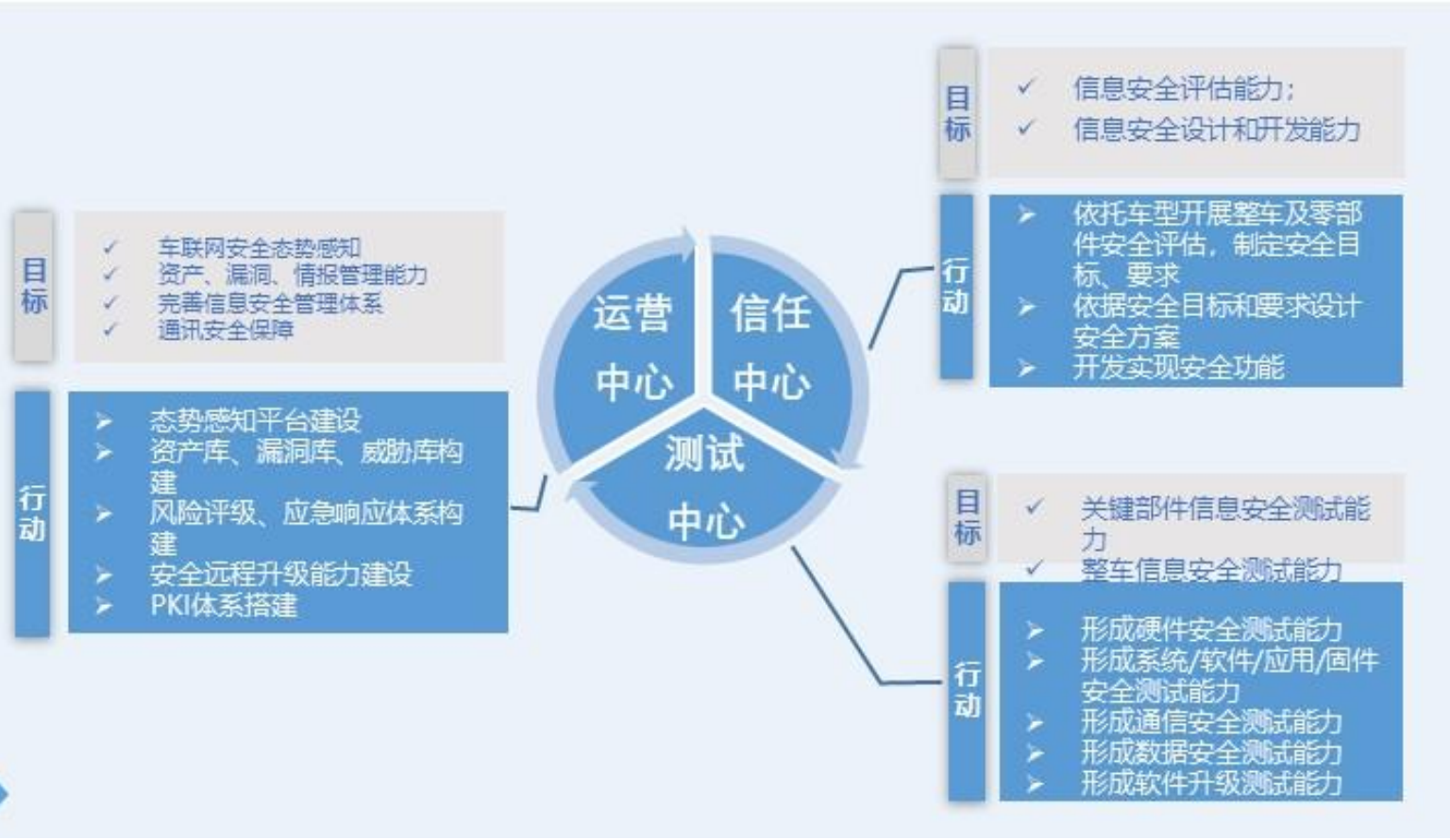
02 东风在车辆网络安全中的探索实践

03 总结及思考

2 东风在车辆网络安全实践—总体目标

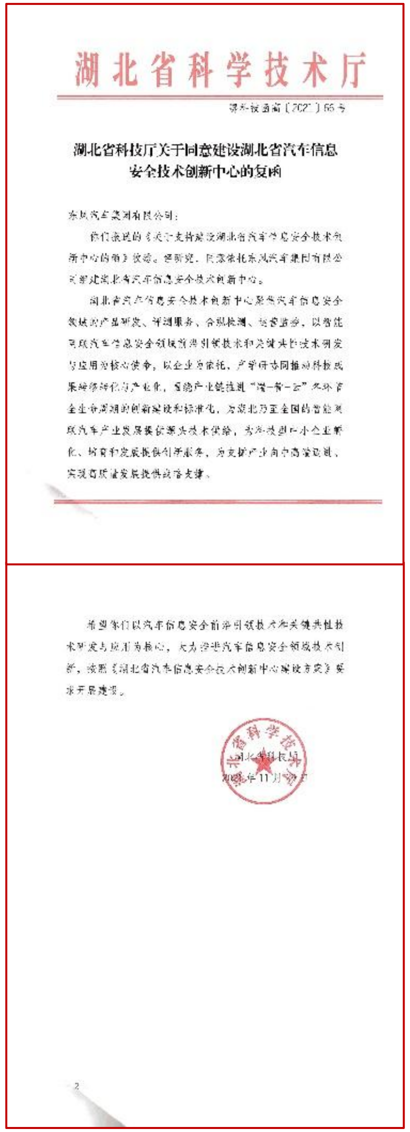
- 为了打造让客户放心的、安全可靠产品，东风汽车公司技术中心成立专门的车联网信息安全团队开展信息安全工作
- 提出总体目标： 建立信息安全体系、建设安全信任中心、安全测试中心、安全运营中心

序号	类别	总体目标
1	安全信任中心	基于产品硬件可信环境和车联网信任平台的正向安全设计开发能力
2	安全测试中心	面向“端管云”整体车联网系统的产品合规性测试和攻防渗透测试能力
3	安全运营中心	面向车联网漏洞库的信息安全管理体系和态势感知运营能力
4	信息安全体系	构建车辆全生命周期的信息安全管理体系CSMS



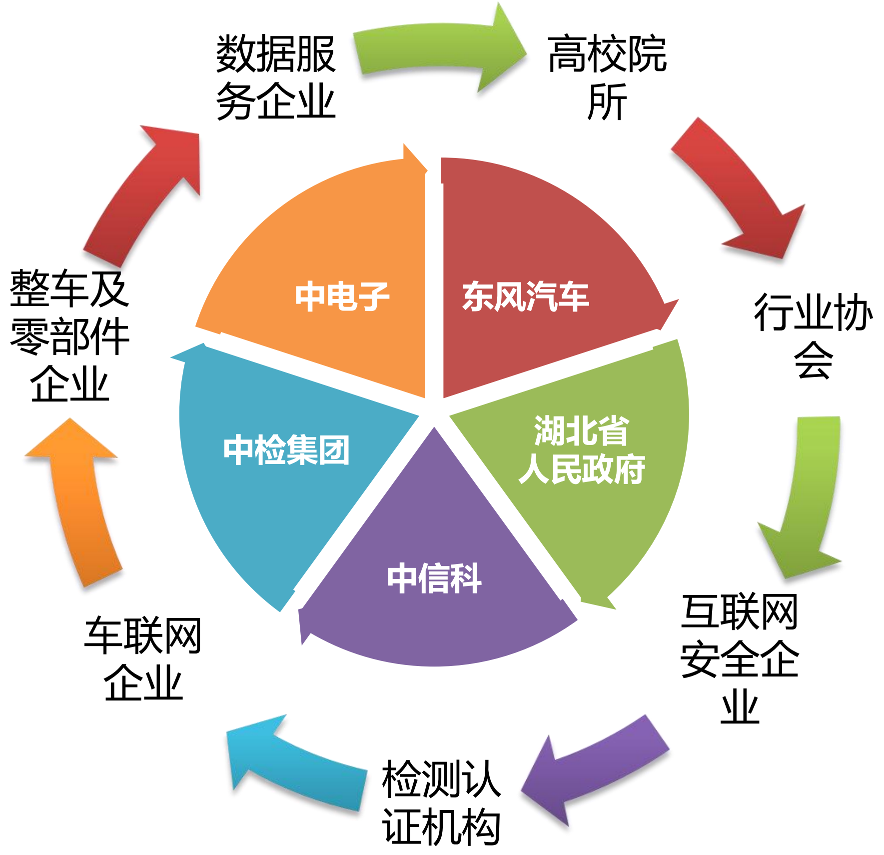
2 东风在车辆网络安全实践—共建湖北省车联网信息安全创新中心

■ 同时在省相关部门支撑下，东风牵头与相关单位一起创建湖北省车联网信息安全创新中心，共同推进技术落地。



湖北省科学技术厅

湖北省科技厅关于同意建设湖北省汽车信息安全技术创新中心的复函



角色定位

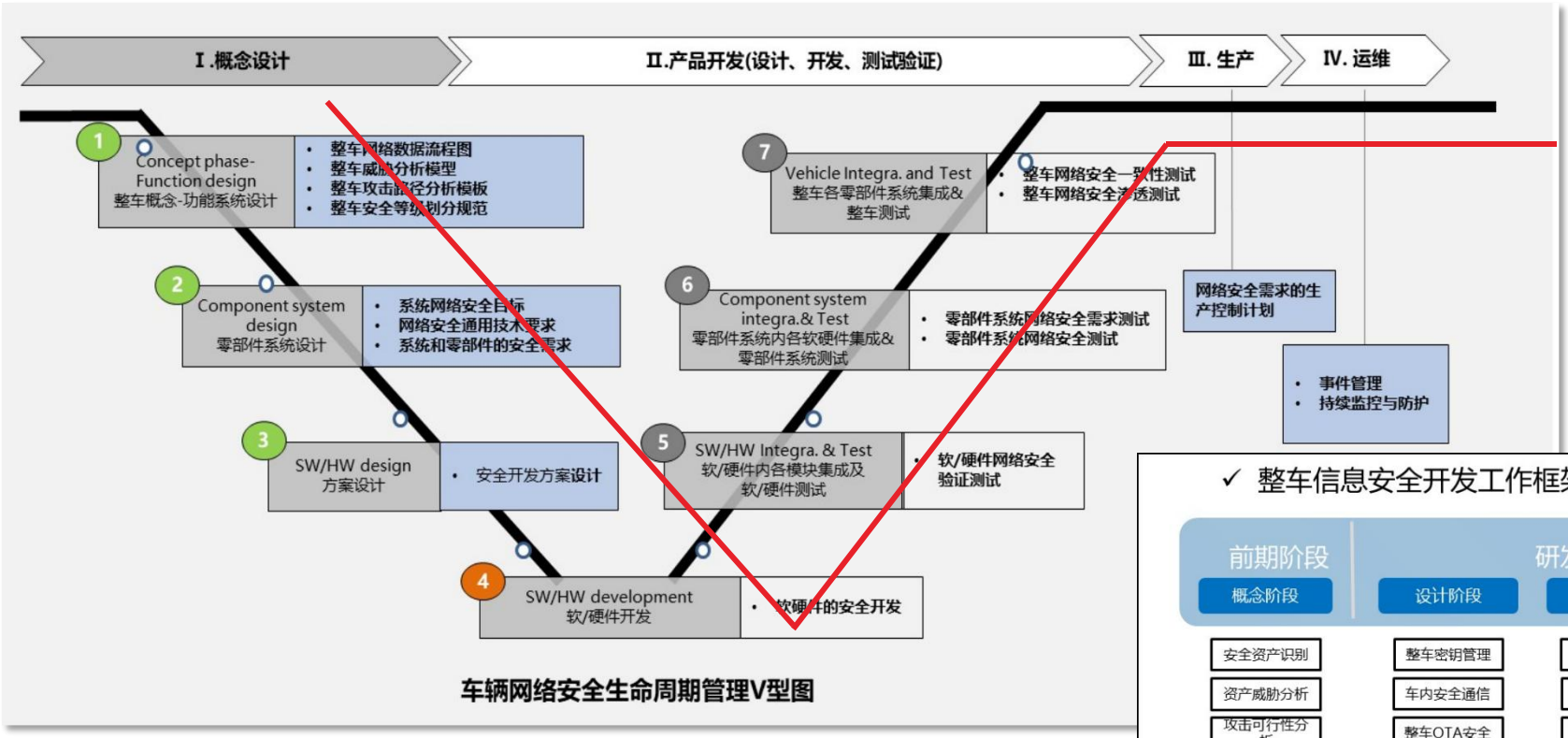
- **东风汽车**：核心载体、验证支持和应用对象，安全软硬件产品、汽车安全电子电气架构、车联网身份认证与安全态势感知、安全数据源
- **中检集团**：第三方权威的安全合规检证机构、车联网身份认证和安全运行监控服务平台
- **中信科、中电子**：提供安全通讯产品和技术保障、安全数据运行，建设并协助运营汽车安全数据中心
- **高校院所**：安全核心技术策源地，创新技术人才，技术成果转化、技术服务支持
- **地方政府**：政策经费支持、跨行业协同、国家科研平台

2 东风在车辆网络安全中的探索实践—整车网络安全方案架构

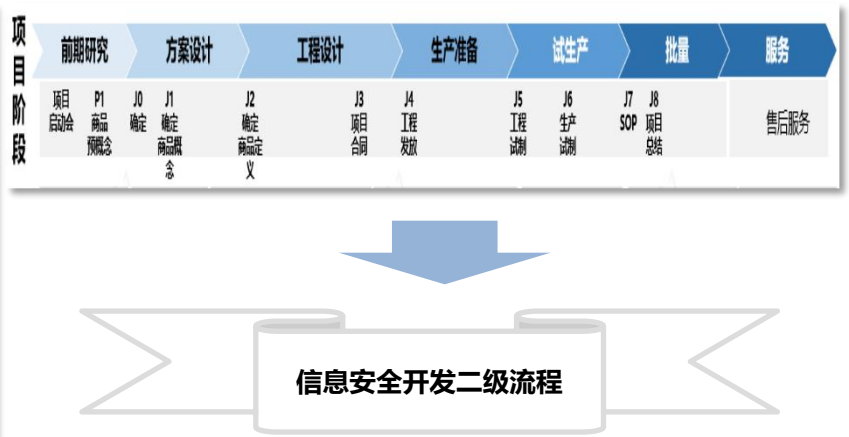
✓ 从云管端的总体环境中，建立整车信息安全纵深防御体系，从***云端安全防护***、整车的***对外接入系统安全、车内网络安全***和***零部件安全***进行信息安全方案设计。

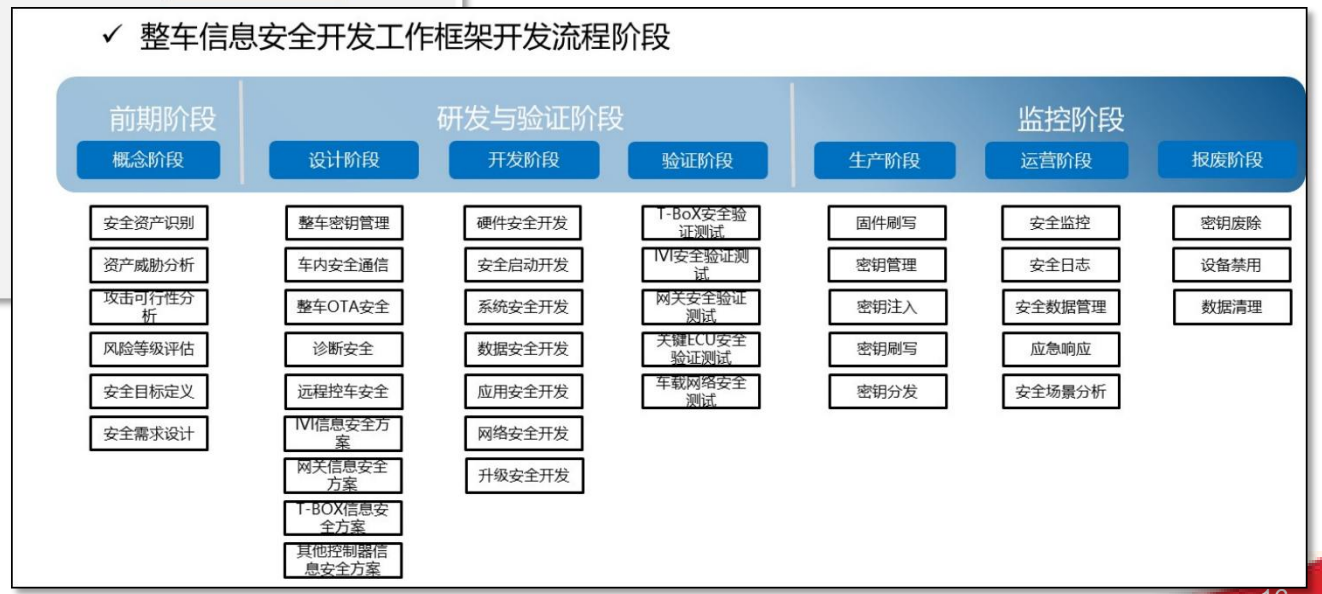
2 东风在车辆网络安全中的探索实践—体系建设、流程融合

参照《ISO21434 道路车辆网络安全工程》的要求，结合车型开发流程，形成整车开发二级流程；推进网络安全开发工作应与零部件&车型开发同步。



车辆网络安全生命周期管理V型图

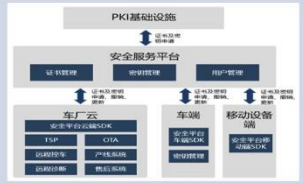
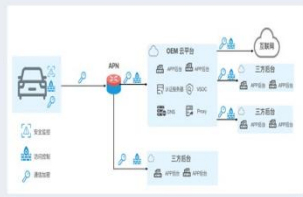


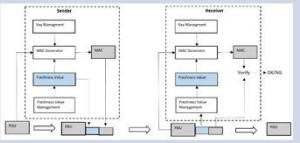
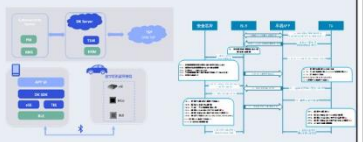


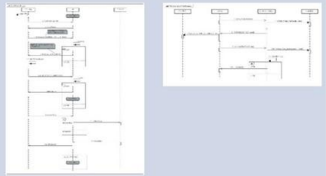
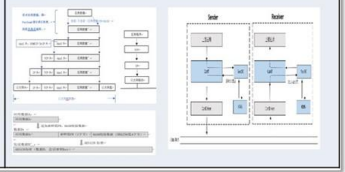
推进ISO21434道路车辆网络安全工程与企业产品开发流程融合、衔接

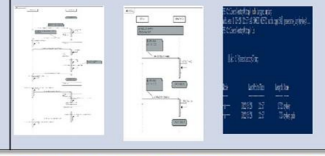
2 东风在车辆网络安全中的探索实践—整车及关键零部件信息安全方案简述

✓ 针对前面的网络安全方案，通过深入沟通、结合业务系统特点，提出针对性的网络安全方案，实现系统的安全可靠；同时围绕零部件开展安全组件设计，从基础上保证安全的实现。

序号	方案名称	方案简述	方案架构
1	整车密钥证书部署及管理方案	◘ 依托安全服务平台完成高安全等级可动态管理的的密钥管理流程设计，支撑安全机制的实现。 （1）满足安全升级、车云安全通信、远程控车、远程诊断、数字钥匙、应用安全认证、控制器安全启动等9大场景。 （2）支持后续业务场景持续扩展。	
2	车云认证信息安全方案	◘ 应用成熟的身份认证、数据加解密等技术，完成保证车云通信数据的安全可信设计。 （1）DNS通信：DNS Over TLS方案加密通信 （2）HTTP通信：HTTP+TLS1.2以上安全信道 （3）TCP通信：TCP+TLS加密通信	

序号	方案名称	方案简述	方案架构
3	整车升级安全方案	◘ 依据合规和渗透2个维度完成云管端OTA安全方案设计，并制定高于合规基线的本地升级数据传输方案设计： （1）云端安全等级保护及升级包完整性校验 （2）CAN通信采用SecCO防护 （3）USB/UART分发：FV+MAC通信防护	
4	蓝牙钥匙安全方案	◘ 制定蓝牙钥匙云管端架构下的业务认证、传输、加固方案： （1）基于安全服务平台完成端管云之间安全会话通道的建立及通信身份的双向认证设计。 （2）基于车端和手机端的硬件安全环境完成控车业务的重放攻击和篡改攻击设计。 （3）应用行业加固技术对相关软件进行混淆校验及完整保护设计。	端管云双向认证　控车业务安全交互 

序号	方案名称	方案简述	方案架构
5	诊断信息安全方案	◘ 诊断仪接入认证安全方案： （1）EOL与网关间：工厂模式认证豁免 （2）CANoe与网关间：X509证书单向验签认证 （3）诊断仪与网关间：X509证书单向验签认证 2. 27 Service诊断安全方案： sha256+AES128安全访问算法增强 ……	通用诊断认证　27服务加固 
6	车内安全通信信息安全方案	◘ 开展支持车内以太网、. CANFD、CAN的安全通信方案设计. （1）覆盖SOMEIP，DoIP，HTTP，TCP/IP协议的AES128（应用数据+新鲜值+HASH校验）加密通信 （2）CAN/CANFD通信安全方案 引入SecOC组件：PDU数据+FV+MAC 的CAN通信，保证数据的真实性，完整性校验。	以太网加密　SecOC 

序号	方案名称	方案简述	方案架构
7	外部设备接入认证方案	◘ 根据各控制器的接入设备及接入端口制定了如下方案： 1.UART口：预置密钥HASH，进行中断拦截和密码认证 2.USB口：X509证书签名验签+AES128加密通信 3.JTAG口：CANoe使能控制/系统端口使能设定 4.ADB认证：公私钥认证 ……	USB加密　JTAG关闭　ADB认证 

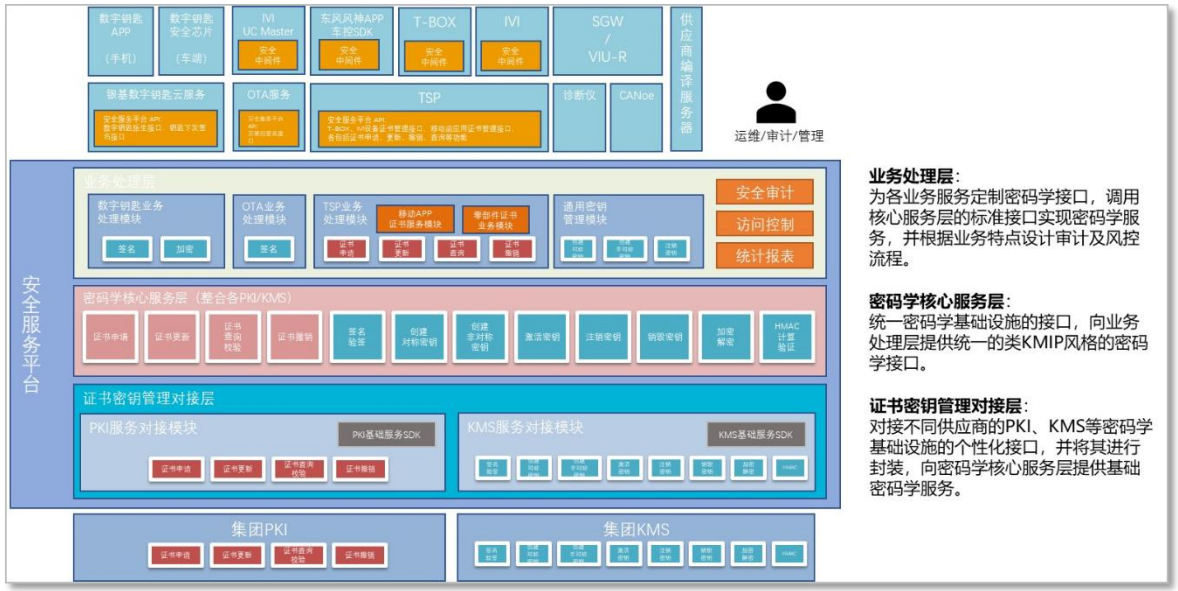
控制器安全架构示例

2 东风在车辆网络安全中的探索实践—安全基础服务基础能力解耦的尝试

✓ 密码学基础设施是推进车联网安全工作中引入的重要资源，如何将这一块能力掌握并利用好，形成企业自己的密码学基础设施应用规范和方法，通过项目我们做了一定的尝试。

序号	场景名称	场景简介
1	远程控车	车端（T-BOX）、移动端、与云端TSP服务基于HTTPS协议进行可信安全通信
2	OTA安全升级	车端（IVI / UC Master）与云端OTA服务基于HTTPS协议进行可信安全通信 使用PKI证书体系对OTA安装包文件的机密性、完整性、可用性进行保障
3	OBD安全诊断	诊断设备基于X509证书的身份认证与车端CAN网关进行加密通信
4	远程安全诊断	车端（IVI）、移动端、与云端TSP服务基于HTTPS协议进行可信安全通信
5	安全启动	基于eFuse、Bootloader等技术实现IVI、VIUL/R等设备的安全启动
6	数字钥匙	实现汽车与作为数字钥匙载体的手机APP之间的安全通信机制
7	车内安全通信	基于SecOC方式实现车内ECU的安全CAN通信（控车指令、诊断指令等）
8	应用签名	使用东风PKI证书体系管控IVI中的应用签名
9	车云通信	车端（IVI）、移动端、与云端TSP服务基于HTTPS协议进行可信安全通信

安全设施需求基本业务场景



- 更多元的选择密码学基础设施；
- 更自主的应用开发能力和规范；
- 更完整的密码学安全审计记录；
- ……

2 东风在车辆网络安全中的探索实践—VSOC 车云一体融合的构思

✓ VSOC建设要打破云端和车端隔离的现状，构建车端、云端一体融合的态势感知平台，进一步构建围绕云管端的安全评估体系和方法，更多从全局和业务角度考虑VSOC的构思，让VSOC 走出纯技术思维，让更多业务能够看懂，看到全局。

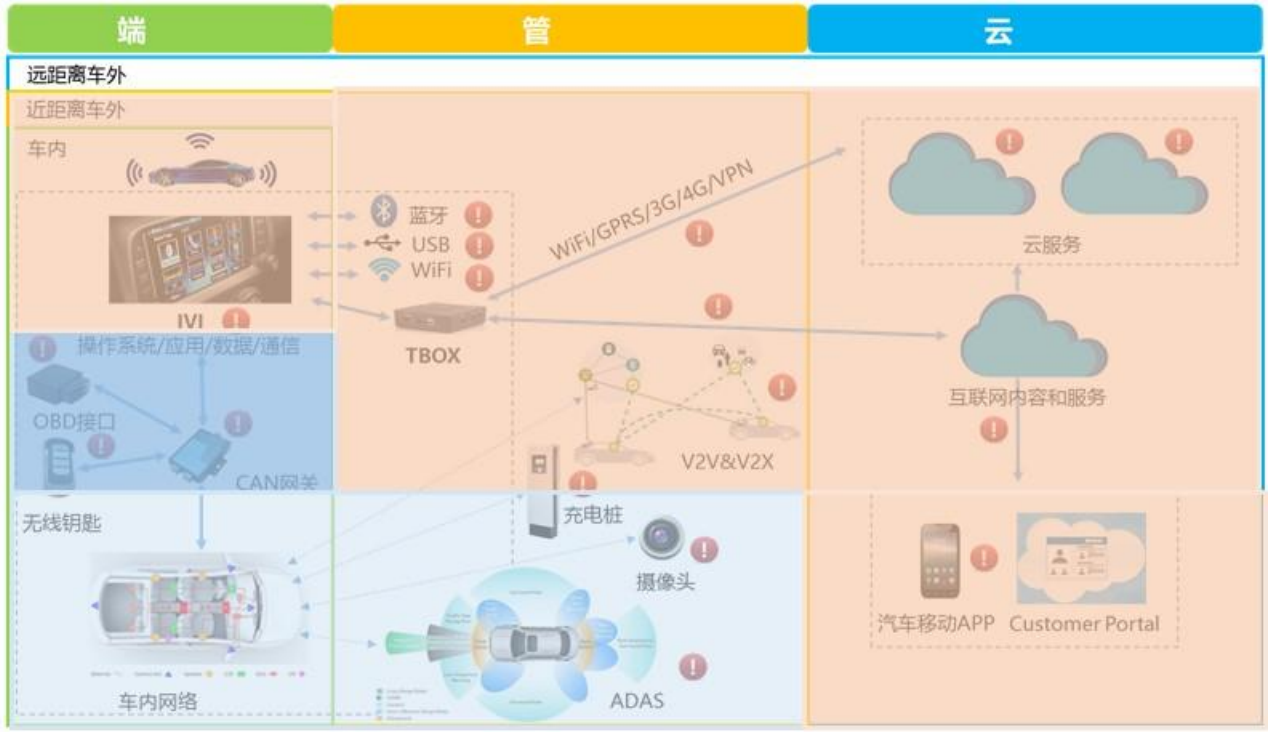
- 网络异常检测
- 屏蔽利用已知漏洞所发动的网络攻击
- 预警信息及本地安全日志

- 全网安全运营态势图
- 安全数据管理
- 安全运营场景分析
- 安全监控决策

3.东风在车辆网络安全中的探索实践—与车型配置配套的差异化方案

- ✓ 用配置化思维来考虑车型的安全方案落地：针对不同车型，要充分考虑不同车型成本、卖点、用户群体的特点，将网络安全定义选装化，可以针对不同的车辆配置进行不同的安全方案选择，同时未来结合OTA方案，可以按需个性化进行网络安全选装升级。

序号	名称	T-Box/OBU	IVI	CGW	HAD	BDC	PDCU	BMS
1	可信环境-安全芯片（硬件形式）	✓	✓	✓	✓	✓	✓	✓
	可信环境-软件模块（软件形式）	✓	✓	—	✓	—	—	—
2	数据安全	✓	✓	✓	✓	—	—	—
3	操作系统加固	✓	✓	—	—	—	—	—
4	固件防护	✓	✓	✓	✓	✓	✓	✓
5	应用程序加固	—	✓	—	—	—	—	—
6	TBOX/IVI资源访问控制	✓	✓	—	—	—	—	—
7	系统漏洞修复	✓	✓	—	✓	—	—	—
8	总线安全通信（板内总线）	✓	✓	✓	—	—	—	—
9	总线安全通信（车内总线）	✓	✓	✓	✓	✓	✓	✓
10	OBD接入认证	—	—	✓	—	—	—	—
11	近场安全通信-数字钥匙	—	✓	—	—	—	—	—
12	近场安全通信-V2X	✓	—	—	—	—	—	—
13	OTA升级检验	✓	✓	✓	✓	✓	✓	✓
14	车云安全通信	✓	✓	—	—	—	—	—
15	入侵检测防御（网关）	—	—	✓	—	—	—	—
16	入侵检测防御（T-BOX/OBU）	✓	—	—	—	—	—	—
17	入侵检测防御（IVI）	—	✓	—	—	—	—	—



2 东风在车辆网络安全中的探索实践—网络安全与成本的平衡考虑

✓ 如何做好安全方案与开发成本的平衡是车型网络安全开发中必须面对的课题，怎么处理?

ECU识别分类

序号 NO.	控制器名称 Part Name
1	Tbox
2	IVI
3	VIUL
4	HAD
5	PDCU
6	BMS
7	VIUR

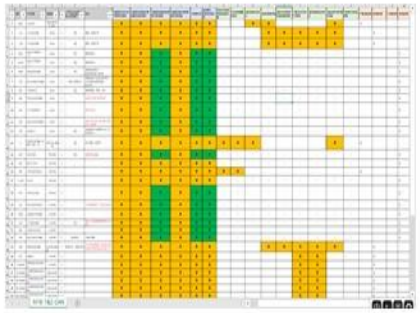
•Critical Level-ECU：（3个）

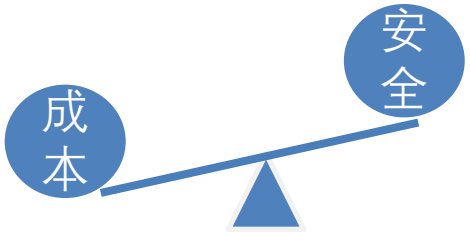
•Tbox\IVI\VIUL

•High Level -ECU：（4个）

•HAD\PDCU\BMS\VIUR

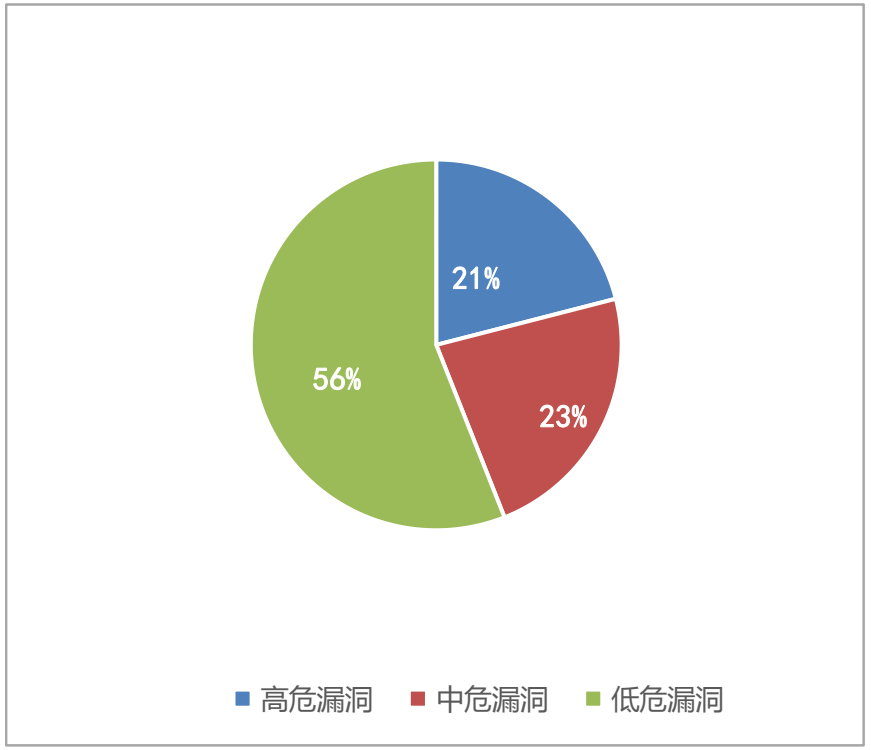
• Low Level-ECU：（37个）





合规

抓重点短板
抓关键节点
抓关键部件

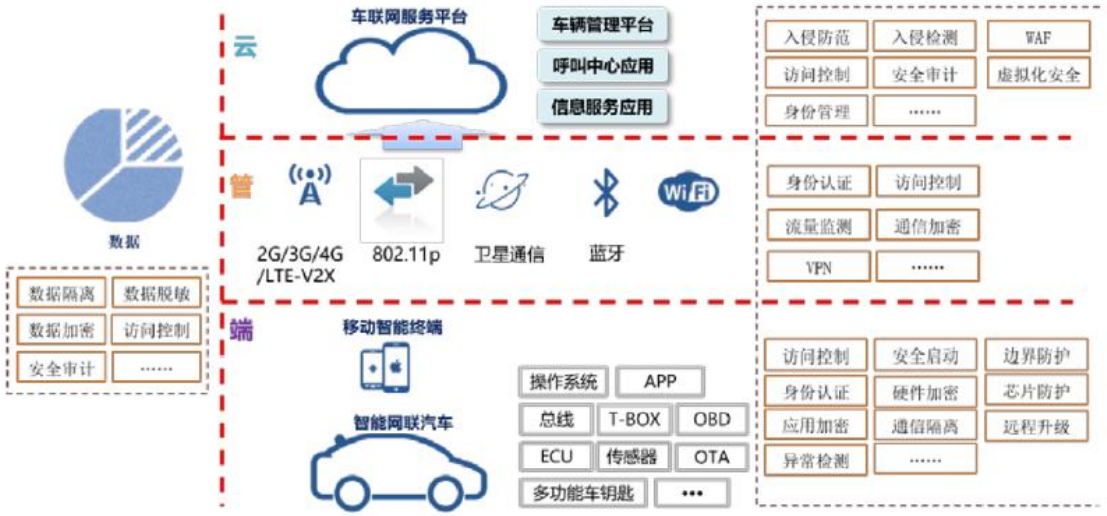


◆整车中已存在百余个ECU，但高危漏洞仅存在于21%的ECU中

◆在成本可控的情况下，遵循“二八原则”，重点防护高危漏洞ECU

4 总结与思考

✓ 思考一：攻击点众多，攻易守难，信息安全建设需要全局思维



✓ 思考二：动态防护，持续迭代更新

✓ 思考三：安全是一种能力，已经从一个可选项变成汽车产品的必要机能，成本的平衡、信息安全保障水平的定义都是面临的问题，主机厂最终要靠我们自己实现自主可控。

✓ 思考四：一个新的领域，技术标准和体系的建立尤其重要，需要大家共同努力不断完善标准规范、推动行业共同的进步。

人才缺　　成本高　　攻点多　　评测难

创造·快乐

CREATE SMILE

感 谢 聆 听

责任意识 现场意识 用户意识 专业意识 成本意识