2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

# 整车电子电器架构演变推动车联网信息安全的发展

汪向阳
重庆长安汽车股份有限公司智能化研究院
副总工程师

# CONTENTS

一 PART ONE
整车电子电器架构发展趋势

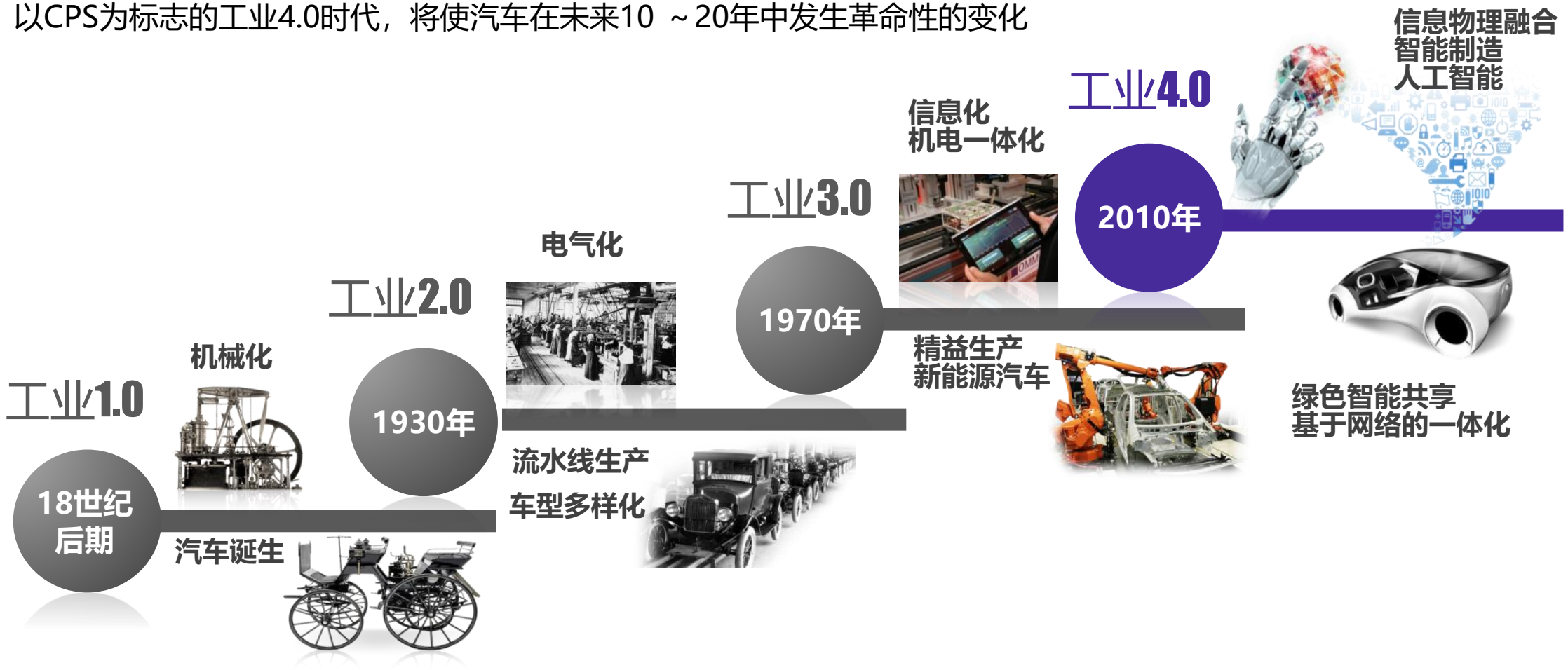
二 PART TWO
智能网联汽车信息安全存在的风险与挑战

三 PART THREE
智能网联汽车信息安全建议方案

# 一、整车电子电器架构发展趋势

## 1. 人工智能等新技术驱动汽车产业进入4.0时代

- 从工业1.0的机械化、2.0的电气化到3.0的机电一体化，汽车工业每次都发生了重大变革
- 以CPS为标志的工业4.0时代，将使汽车在未来10 ~20年中发生革命性的变化



## 2. 智能网联带来交通系统的深刻变革

- **交通安全**：交通事故率可降低 95%；
- **交通效率**：车联网技术可提高道路通行效率10%，CACC系统大规模应用将会进一步提高交通效率；
- **节能减排**：协同式交通系统可提高自车燃油经济性20%-30%，高速公路编队行驶可降低油耗10%-15%；
- **产业带动**：智能网联汽车产业将会拉动机械、电子、通信、互联网等相关产业快速发展；
- **交通出行及商业模式的改变**：减轻驾驶负担，娱乐，车辆共享，便捷出行。

**驾驶去人化**

**出行共享化**

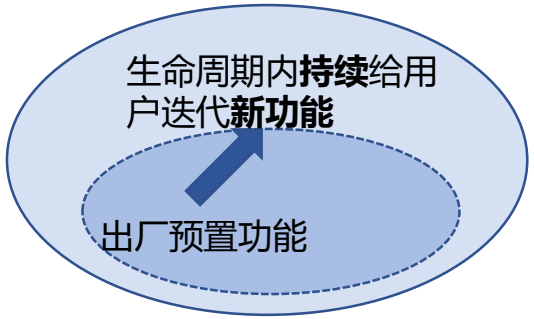

**产业生态化**

# 一、整车电子电器架构发展趋势

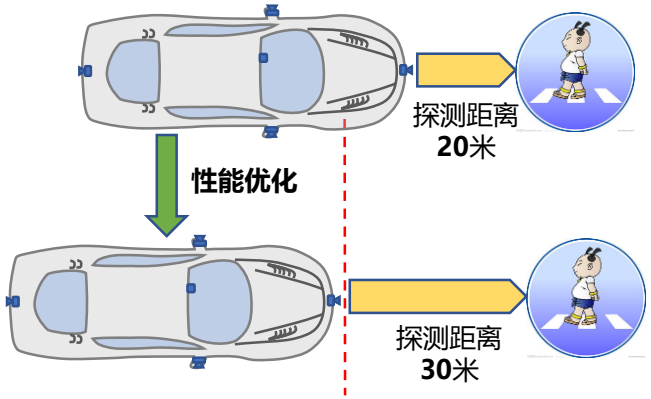
## 3. 智能网联汽车的变革

- 当前汽车已从功能车向智能车的转变，功能不断更新、性能持续升级、迭代频率持续提高，已成为对智能车的基本要求

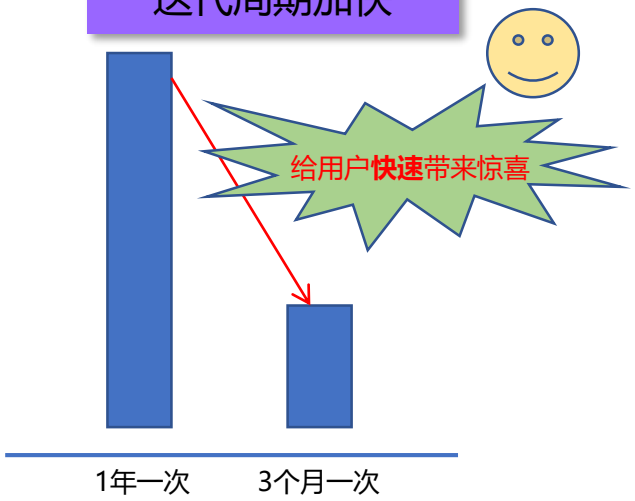
### 功能持续更新




### 性能不断提升




### 迭代周期加快




*特斯拉软件迭代应用案例*

**软件迭代增加180度行车记录仪功能**

特斯拉更新行车记录仪功能，启用 3 颗摄像头实现 180 度无死角拍摄

2019年3月，特斯拉更新行车记录仪功能。

亮点：
三个摄像头一起工作，记录了超过 180 度的路面信息。车辆可记录前方、左后侧和右后侧的探碰的情况。如果车主用后置摄像头充当后视镜，这相当于 360 度无死角拍摄了。

注意事项：
实际录制出来之后会保存成三个视频文件，视频是将主将三个画面剪辑在一起之后的画面。

**软件迭代提升自动紧急制动性能**

特斯拉Autopolit软件升级，自动紧急制动技术提升

2017年10月，特斯拉发布最新软件升级包，为搭载Autopilot 2.5的车辆提供全速自动紧急制动功能，其他功能也有相应的提升。

此外
搭载Autopilot 2.5的车辆：紧急制动所适用的最大车速由早前的50 mph增至90 mph。
搭载 Autopilot 2.0的车辆也提供了类似的功能，但车速限制在28 mph

**软件迭代提升低温续航里程**

特斯拉升级电池预热功能，在严寒中提升行驶里程

2017年12月，特斯拉发布了 2017.50 版汽车软件更新，如果电动汽车接通电源，特斯拉车主就能够通过手机 APP 激活电动汽车中的“电池预热”功能。

当车外面的温度低到接近零度时，特斯拉 APP就会出现橙色警告按键，可以让电池先加热，以保障出行有全部的动力。预热过程要提前1小时开始，并且特斯拉建议，最好插电预热，以减少耗电。

# 4. 商业模式转变

- 传统制造企业的竞争异常激烈，传统整车厂的盈利模式空间越来越小，逐渐从制造型企业向服务型企业转型，并通过生态、大数据、OTA等实现服务变现

**过去 ：硬件盈利**

**整车销售**

**未来 ：服务盈利**


## 生态

- 智慧交通、智慧城市
- 智能家居
- 会员服务
- 驾乘服务（智慧推荐）

## 大数据

- 数据变现（保险、广告、服务业）
- 售后诊断
- 出行及共享服务

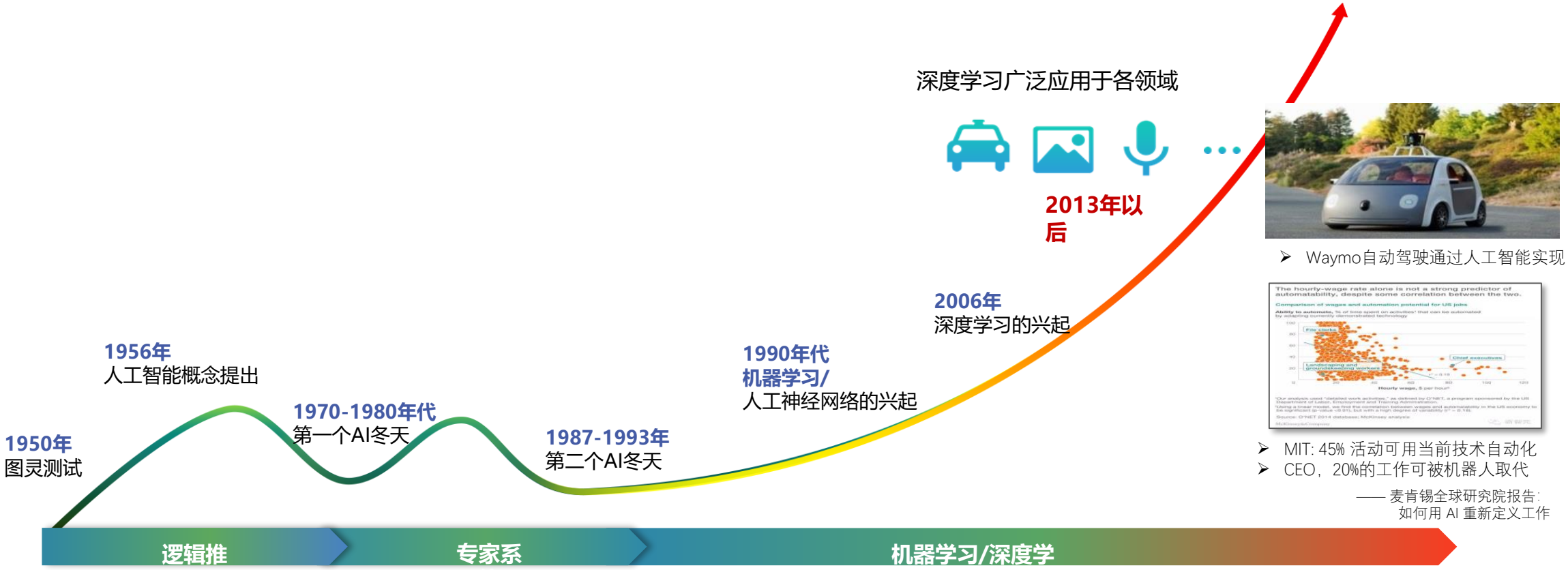
## OTA

- 自动驾驶硬件出厂，软件付费打开
- 付费升级迭代

**服务市场转型升级**

# 5.发展趋势1—人工智能与汽车深度融合

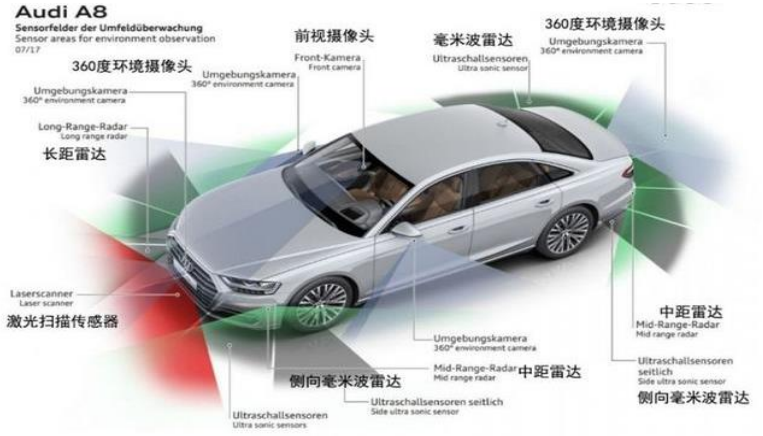
- 技术进步是核心推动力，**人工智能、5G、物联网等前沿技术对未来全球经济产生重要的影响**，在汽车领域，通过人工智能与汽车的深度融合，加速推动智能网联汽车的发展。



# 一、整车电子电器架构发展趋势

## 5.发展趋势2—低速特定场景下的L3/L4级聚焦量产

### 奥迪：全球首台量产L3

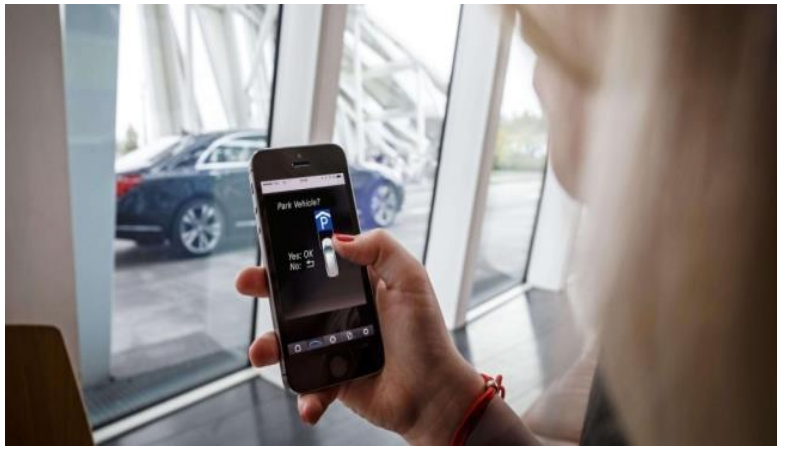



- 2018年正式推出量产的L3级自动驾驶车型奥迪A8，这是世界范围内第一台**量产的L3级自动驾驶汽车。**
- 基于**域控制器**的L3量产提供了智能网联汽车的基础平台

### 特斯拉：量产且持续升级


- 特斯拉推出Autopilot 2.0，并**持续升级**，成为广泛使用的自驾量产车辆。其Model3 架构更进一步推动车辆E/E变革
- 通用推出SuperCruise, 国内各大自主品牌纷纷制定2020左右的**L3量产计划**

### 博世：代客泊车




- 2018年9月，戴姆勒和博世合作研发的自动代客泊车技术在中国首次亮相。
- 通过人工发出的信号，传递到行车电脑，车辆已能够实现自动寻找并停车入库的功能。
- 车主无需等待，只需要操作APP，剩下的行驶工作全部交给车辆自行处理。

# 一、整车电子电器架构发展趋势

## 5.发展趋势3—智能网联汽车下的5G/V2X及云计算应用时代即将到来

### 华为、大唐LTE-V芯片与模组


- **华为、大唐**等厂商已经推出各自的LTE-V2X商用通信芯片或模组，同时支持PC5口和Uu口双模通信；
- **星云互联、东软、千方**等终端厂商纷纷推出各自的终端设备，支持多种品牌LTE-V2X通信芯片。

### 高通全新C-V2X芯片


- 针对**汽车领域5G**应用，高通推出Snapdragon方案，为汽车带来信息娱乐与Telematic服务；
- 高通推出9150 C-V2X[2]芯片，**兼容LTE和5G**，预计2019年下半年量产。

### C-V2X应用示范


- **无锡：**全球首个城市级V2X示范，170平方公里，约240个路口，40余项交通管理信息，支持12大类、20余个交通出行应用场景；
- **上海：**全球首例V2X三跨测试，底层采用3GPP R14直接通信技术，上层采用我国网络层和应用层技术规范，充分展示我国V2X标准的成熟度。

# 一、整车电子电器架构发展趋势

## 5. 发展趋势4—智能网联汽车下的新型安全问题成为聚焦点

### 功能安全+预期功能安全+信息安全


1. **功能安全**：减少失效引起的危害；
2. **预期功能安全**：减少感知或决策控制不符合（功能或设计）预期引起的危害；
3. **信息安全**：建设网联安全防护体系，抵御和减轻网络攻击引起的危害。

### 英伟达：功能安全架构

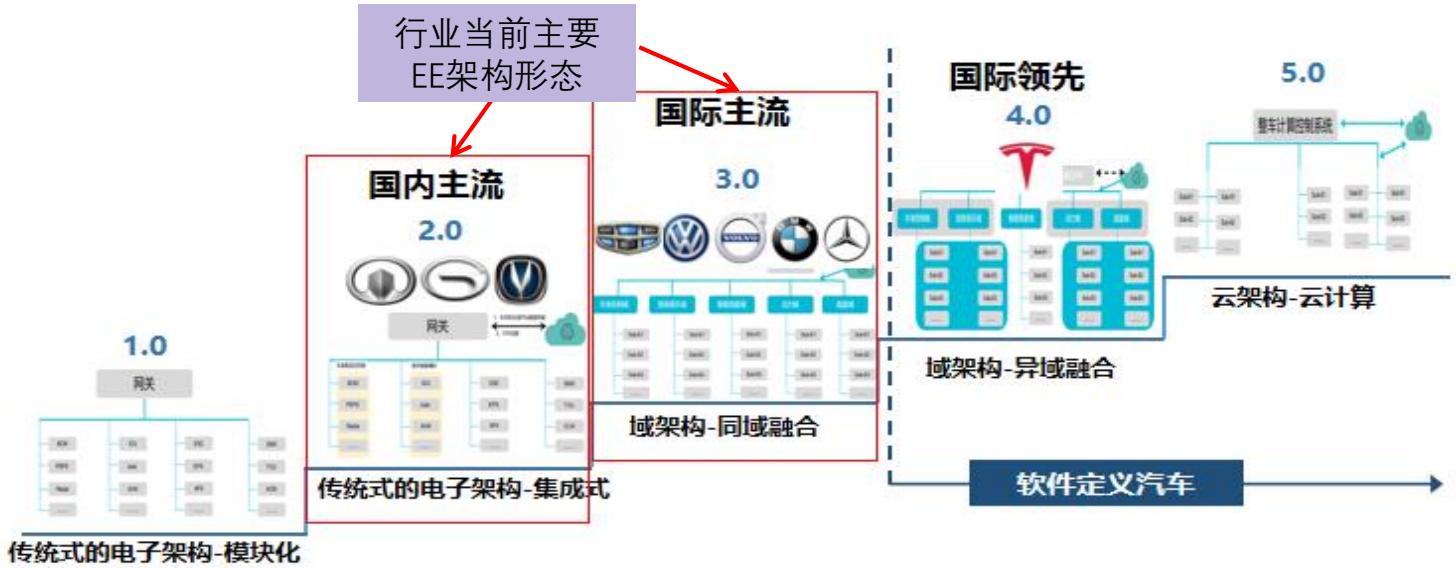
●NVIDIADRIVE的功能安全架构（functional safety architecture），该平台可操纵冗余及多样化的功用，提升车辆运转的安全性，**符合ISO26262**等国际标准。

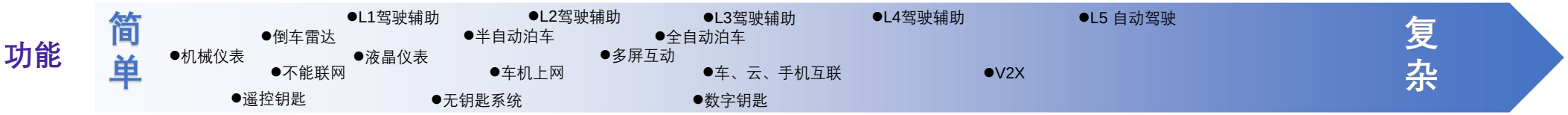
### 博世：IDPS防护系统

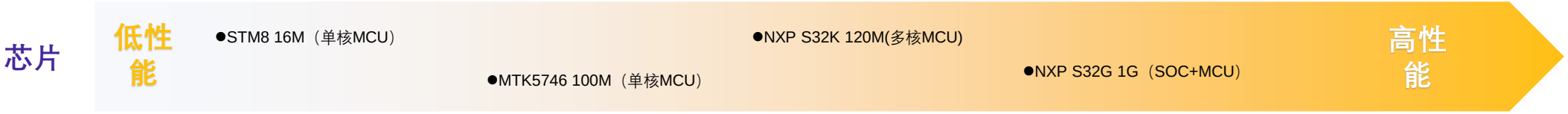
●博世旗下子公司Escrypt开发了IDPS**入侵检测和防御**系统，对网联车所遭遇的潜在威胁进行识别并进行分析，从而快速采取有效措施来保护个人车辆甚至整个车队。

# 6. 整车电子电器架构发展趋势

- 功能复杂度逐渐增加的需要，芯片算力不断增强的支撑，功能逻辑集中化成为了必然趋势，驱动着整车电子电气架构由分布式→域→中央的方向进行发展演变。



# CONTENTS

一 PART ONE
整车电子电器架构发展趋势

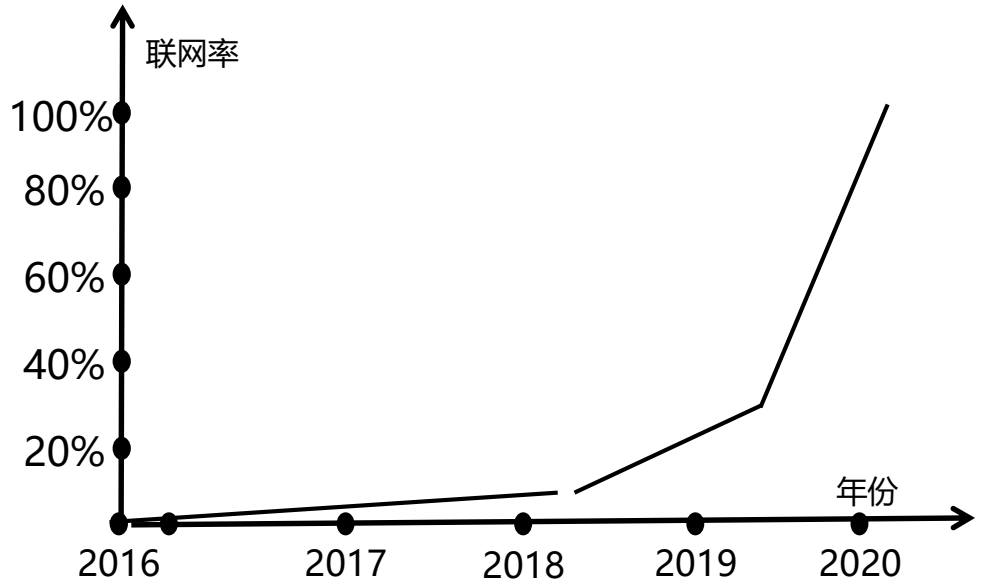
二 PART TWO
智能网联汽车信息安全存在的风险与挑战

三 PART THREE
智能网联汽车信息安全建议方案

# 1. 汽车联网率持续增加，使得大规模的攻击成为可能

■ 新车网联率迅速提高，2020年多家**知名品牌联网汽车将达到100%**，网联汽车的剧增，使大规模的攻击成为可能。

**车联网在2020年会出现井喷式增长**

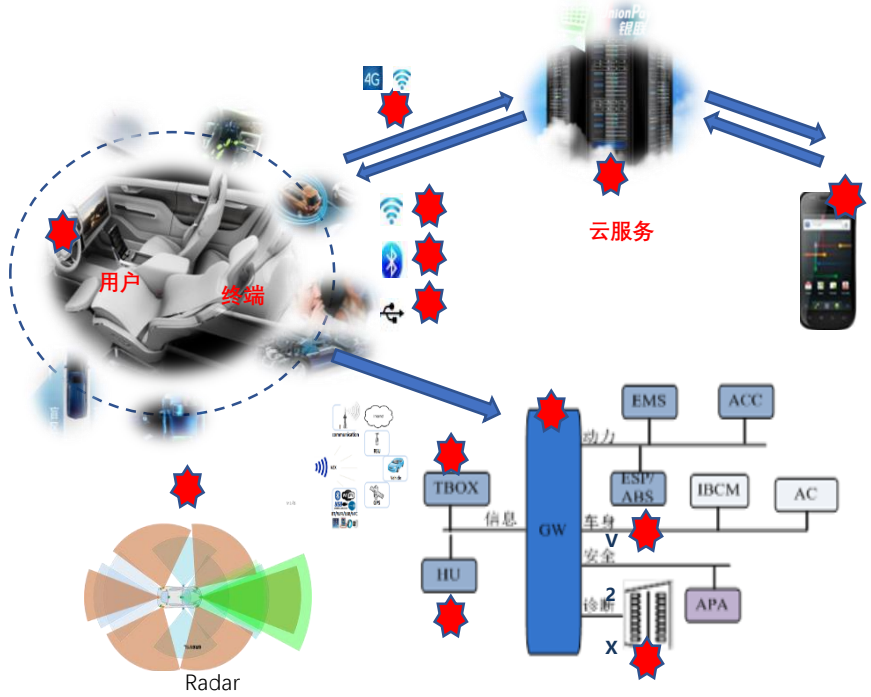



**新车联网率将达到100%**

| 企业 | 当前搭载率 | 2020搭载率 |
|---|---|---|
| 上汽荣威 | 20%-30% | 100% |
| 长城 | 20%-30% | 100% |
| 吉利 | 20%-30% | 80%/75% |
| 蔚来 | 20%-30% | 100% |
| 小鹏汽车 | 30%-40% | 100% |
| 理想汽车 | 30%-40% | 100% |
| 长安汽车 | 25%-30% | 100% |

# 2. 网联汽车新功能越丰富安全风险越大

- 随着汽车智能化技术的快速发展，智能网联汽车通过**3G/4G、蓝牙、WIFI、V2X、射频、USB、OBD-II**等途径**对外互联的应用场景、智能驾驶等新技术**越来越多，智能网联汽车面临的信息安全威胁越来越大，一旦发生重大信息安全事件，会影响到公共安全，对车企造成巨大的经济损失，名誉损失，对用户造成生命、财产损失。




| 风险项 | 风险点 | 可能导致的危害 |
|---|---|---|
| TSP（服务器） | 数据窃取、伪冒<br>劫持、仿冒 | 后台被攻破，大量信息泄漏，批量车被非法控制，大批车辆召回，企业名誉、财务遭受重大损失 |
| 车载终端 | 物理窃取、系统漏洞、软件仿冒、通讯劫持、仿冒 | 车辆被非法锁定，勒索车主，车辆召回 |
| 网络通信 | 4G、WIFI 仿冒<br>CANFD、ETH | 非法远程控制车辆，车辆、财务损失 |
| 用户信息 | 敏感信息、权限认证、<br>用户授权、支付 | 用户隐私信息泄漏，用户维权 |
| 新技术 | 智能驾驶、V2X、Radar | 车辆失控，造成人员伤亡、车辆损失、经济损失 |

# CONTENTS

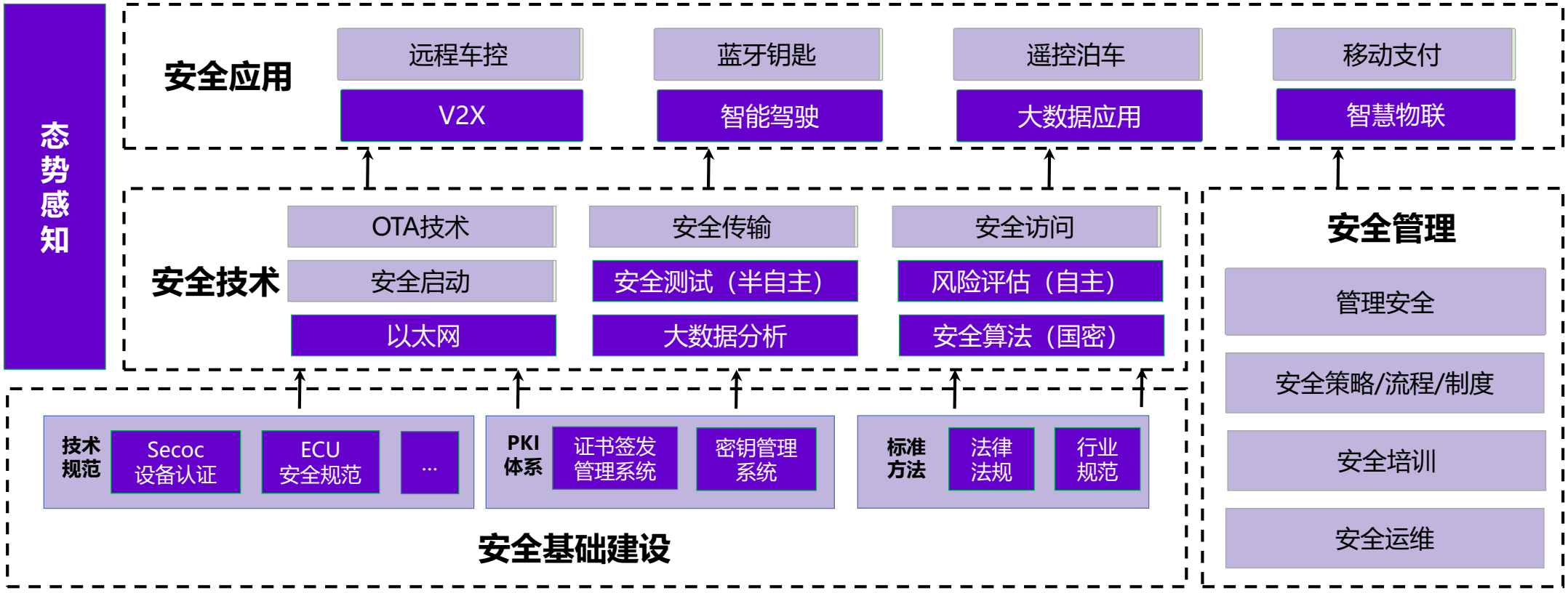
一 PART ONE
整车电子电器架构发展趋势

二 PART TWO
智能网联汽车信息安全存在的风险与挑战

三 PART THREE
智能网联汽车信息安全建议方案

# 1. 车联网信息安全框架

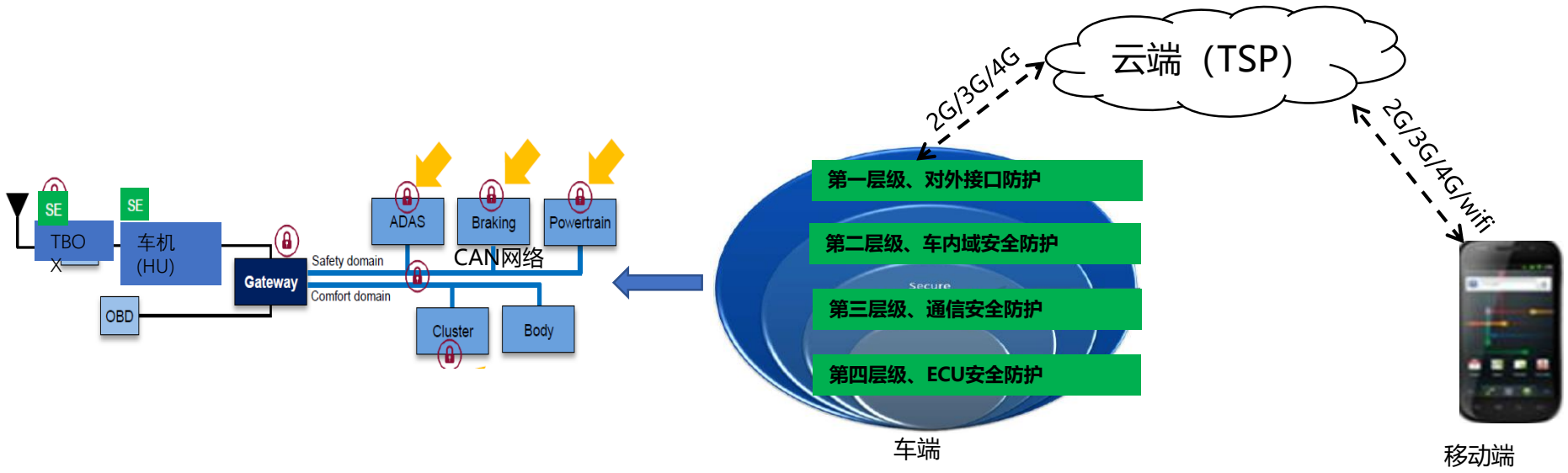
■ 从**安全基础建设、安全技术、安全管理、态势感知**等方面开展信息安全工作以支持各**安全应用**。



# 2. 信息安全方案整体设计思路

■ 车联网业务涉及云端、管端、车端、移动端，信息安全工作从车联网业务出发，保障**云端、管端、车端、移动端**的安全性。

- **云端安全：**通过风险分析、上线前安全测试、上线后定期漏扫、基线检查以及等保测评全面保护云端安全。
- **管端安全：**采用标准的安全通信协议（HTTPS\TLS1.2），保护云端到车端、云端到移动端的通信安全。
- **车端安全：**从需求分析、安全设计、安全测试、安全运营开展工作，通过纵深防御体系，安全基础保障体系保护车端安全。
- **移动端安全：**从开发前、开发过程中、上线运行及应用运维四方面保障移动APP安全。



# 2.1 云端安全

## 1、云端安全设计

基于云端安全风险分析，从**物理安全、业务安全、基础安全、安全运维、安全管理**方面持续提升服务器的安全防护，避免批量信息安全事件的发生。


**物理安全**：保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。

**业务安全**：通过应用加固、应用漏洞扫描、密码、证书安全管理等措施保障业务应用安全、业务数据安全。

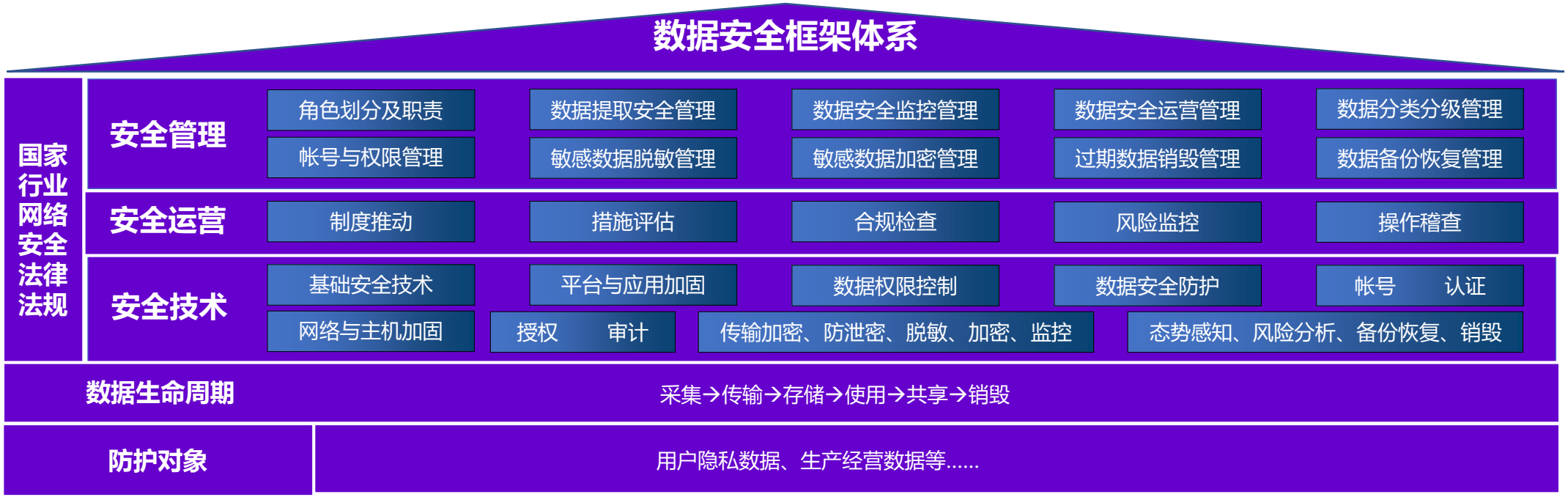
**基础安全**：包括服务器出口/入口网络安全防护、服务器主机安全防护、第三方安全服务支持等。

**安全运维**：包括7x24小时运维，定期安全审计、渗透测试、基线检查，以及发生安全事件的应急响应。

# 2.1 云端安全

## 2、大数据安全

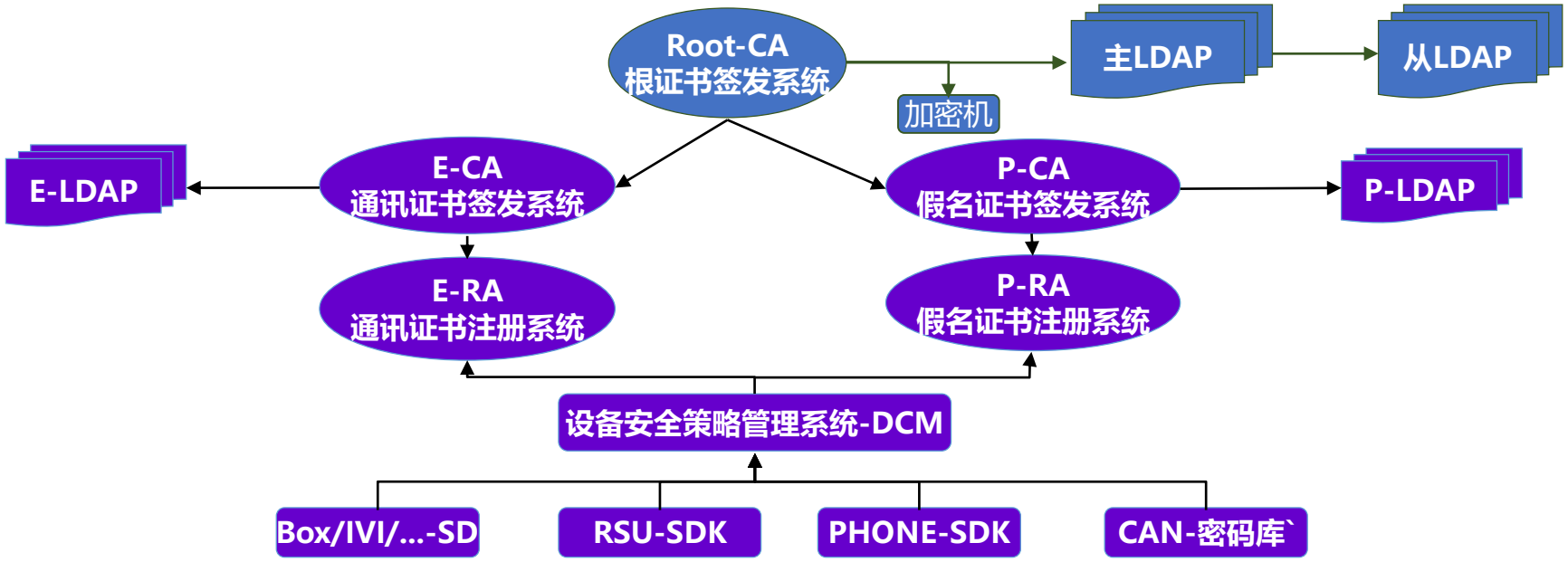
依据《网络安全法》《网络安全等级保护基本要求》《大数据服务安全能力要求》《数据安全能力成熟度模型》《大数据安全管理指南》等国家法律法规及标准，需要从**安全技术**、**安全管理**、**安全运营**三方面开展工作，保护车联网数据全生命周期安全。



# 2.1 云端安全

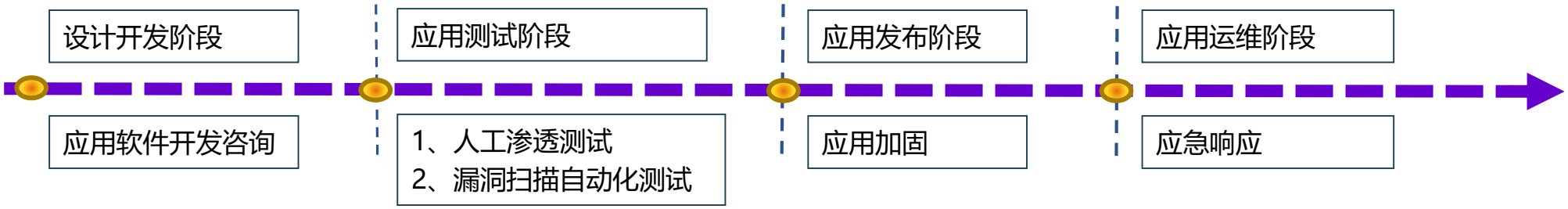
### 3、云端安全业务—V2X

为实现车联网终端之间的**安全认证和安全通信**，需使用基于公钥证书的PKI机制确保终端间的安全认证和安全通信,通过**数字签名和加密**等技术手段实现车联网终端之间消息的安全通信。为此，需要建立一套完整的管理系统，实现证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，确保V2X的安全。



# 2.2 移动端安全

- **从设计开发、应用测试、应用发布，以及上线后的应用运维对移动端APP进行全生命周期的安全保障工作，避免重大信息安全事件的发生。**




| 设计开发（安全措施） | | 应用测试 | 应用运维 |
|---|---|---|---|
| APP软件应用安全 | 组件安全、客户端程序安全（安装包签名、应用完整性校验、代码安全、逆向保护、程序可被任意调试、程序数据任意备份、资源文件保护） | 1.人工渗透测试<br>2.漏洞扫描自动化测试 | 应急响应 |
| 软件数据安全 | （Log）敏感信息检测）、SharedPreferences敏感信息检测<br>、SharedPreferences加密检测、SQLite敏感信息检测、SQLite加密检测 | | |
| 运行环境安全 | Root环境检测、网络环境检测、Ptrace注入检测、代码hook检测、调试器检测、APP多开检测、网络代理检测 | | |
| 网络通信安全 | 关键参数加密、开放端口检测、网络切换保护、网络通信加密、安全退出检测 | | |
| 安全管理 | 密码修改策略、账号锁定策略、验证码有效性、登录信息模糊处理、界面切换保护、账号登录限制策略、密码复杂度策略、键盘记录保护 | | |

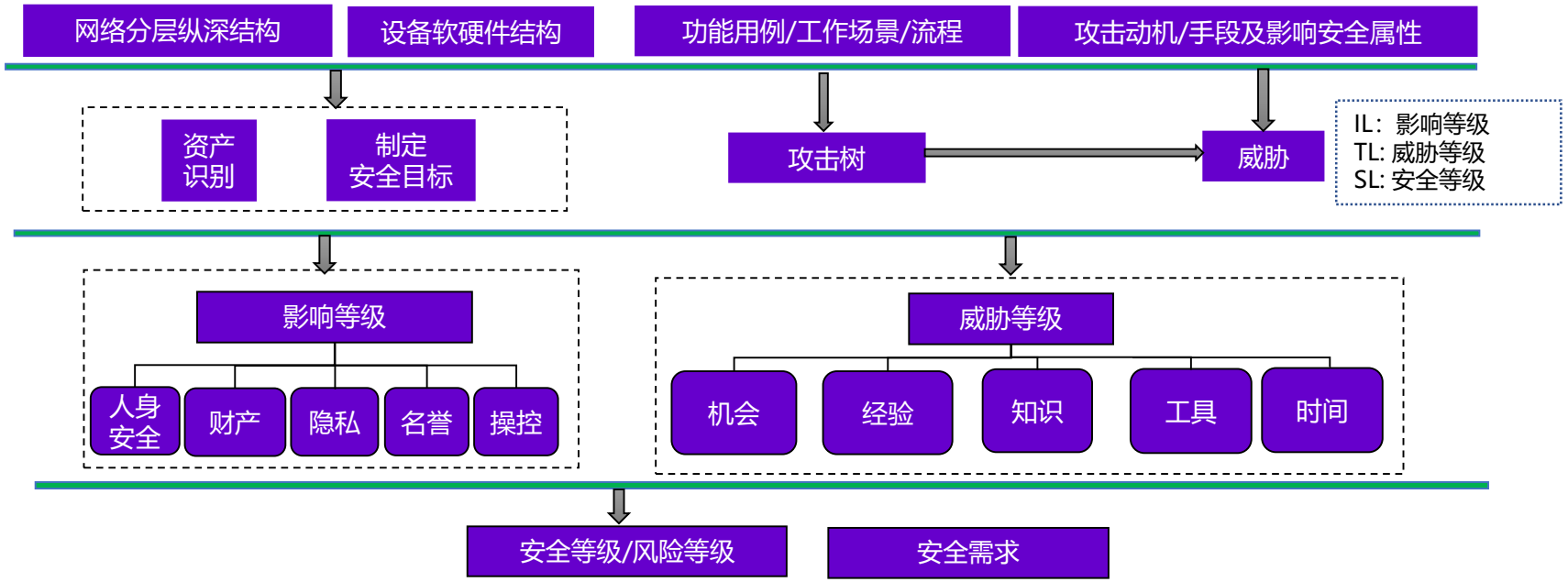
# 2.3 车端安全

■ **从需求分析、安全设计、安全测试、安全运营等方面对整车进行全生命周期安全防护。**

**1、安全需求分析**

1）以**J3061\ISO27005**为依据，对**整车及OTA、数字钥匙、自动驾驶等**关重的安全功能开展风险分析工作。

2）针对车型项目中的**新功能、新特性**开展风险分析工作，通过资产识别、安全目标制定、攻击树分析、风险评估后制定安全需求。



# 2.3 车端安全

■ **从需求分析、安全设计、安全测试、安全运营等方面对整车进行全生命周期安全防护。**

**2、车端安全设计**

基于**整车信息安全风险分析**结果，以**纵深防御**为建设思路，以**安全基础保障体系**为技术支撑开展车端安全设计工作。


建立**整车四层级纵深防御体系**，逐层开展信息安全工作：

**第一层级：**保障TBOX\HU等与外界互联设备硬件安全、系统安全、数据安全、安全启动、安全升级、安全传输；

**第二层级：**对连接各域的网关增加硬件安全、安全启动、入侵检测、数据安全等特性，保障跨域数据安全访问；

**第三层级：**对蓝牙钥匙等重要功能采用端对端消息认证机制，实现数据的身份合法性验证及防重放；

**第四层级：**根据安全应用对各ECU制定安全要求，如安全启动、硬件安全、数据安全等。

# 2.3 车端安全

■ **从需求分析、安全设计、安全测试、安全运营等方面对整车进行全生命周期安全防护。**

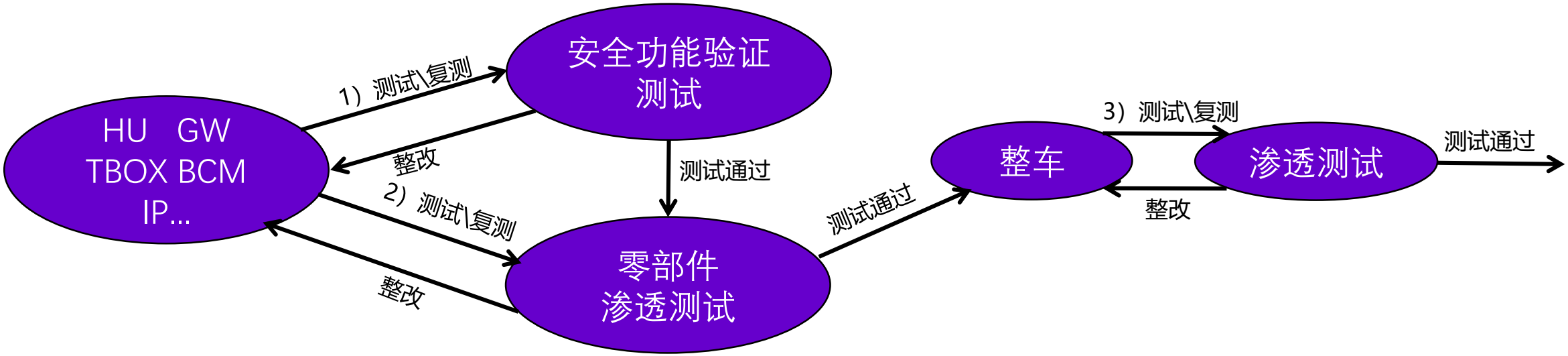
**3、车端安全测试**

车端安全测试按**被测对象**可分为**零部件安全测试、整车安全测试**；**按测试方法**可分为**安全功能测试、渗透测试，测试流程如下：**

**1）功能验证测试：**在车型项目测试阶段，对零部件安全功能验证测试工作，针对测试不通过项进行整改，直至测试通过；

**2）渗透测试：**功能验证测试通过后，提交至第三方进行渗透测试，针对测试不通过项进行整改，直至测试通过；

**3）整车渗透测试：**零部件渗透测试通过后，对整车进行渗透测试，对测试不通过项进行整改，直至测试通过，不存在高、中危风险。



# 2.4 安全运营

■ **建设车端、移动端、云端一体化安全事件态势感知平台，具备风险提前感知、应急响应能力。**

**1. 车　端：**对报文ID、周期等进行异常检测；对DOS、非法注入等攻击事件进行记录，将安全事件通过4G上传云端；

**2.移动端：**对运行环境进行监控，当发现恶意程序、内存攻击工具、恶意 APP 列表、不当或威胁APP 的行为，将异常情况上传到云端；

**3.服务端：**对用户流量威胁分析，对恶意代码上传、口令爆破、敏感文件恶意扫描、漏洞扫描等攻击行为和系统漏洞进行拦截并预警；

**4.应急响应：**云端将（车、移动）端、云端安全事件进行导入分析，可视化呈现，通过**应急响应**下发安全策略，修复漏洞，形成闭环。

# 2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

# THANKS

全球网络安全 倾听北京声音