

安全开发者峰会

The Evolution of Smart Motorcycles

智能摩托车进化之路

任建文 ETAS



Evolution Journey

汽车



铜缆时代(-40 years)

总线时代(-25 years)

智能时代(-20 years)

???

摩托车



铜缆时代

总线时代

智能时代

1955

1965

1975

1985

1995

2005

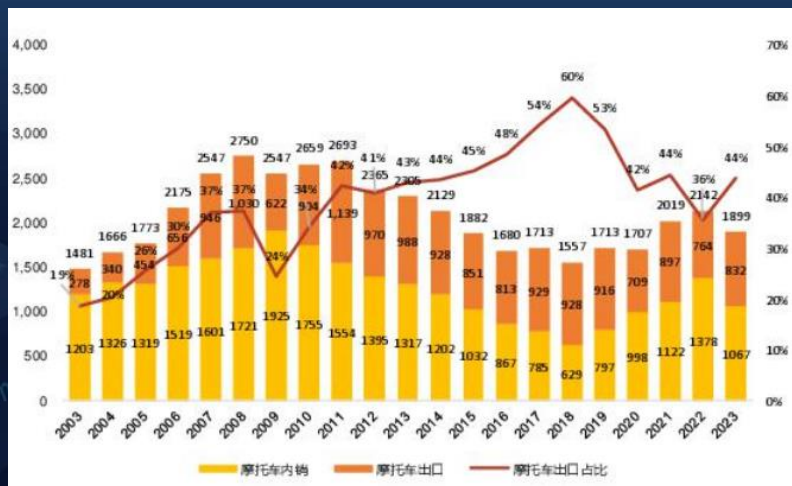
2015

2025

2035

市场巨大

根据行业数据显示，2024年，中国的摩托车市场规模预计将突破2200万辆，至2028年则有望达到2510万辆



智能化

连接性

远程信息处理：提供实时跟踪和骑行特性，例如碰撞检测。

智能手机集成：通过应用程序连接摩托车，提供导航、性能数据和远程诊断。

云连接：分析车主数据以增强车主体验和随时间改善车辆性能。

社交和社区功能

车主数据交换：应用程序使车主能够进行团体骑行、共享路线和一起规划旅行。

骑行跟踪和分享：跟踪他们的骑行并在社交媒体上分享他们的经历

远程控制和升级

远程控制：远程车辆授权、远程锁车、远程开启手把/座椅加热、远程召唤车辆

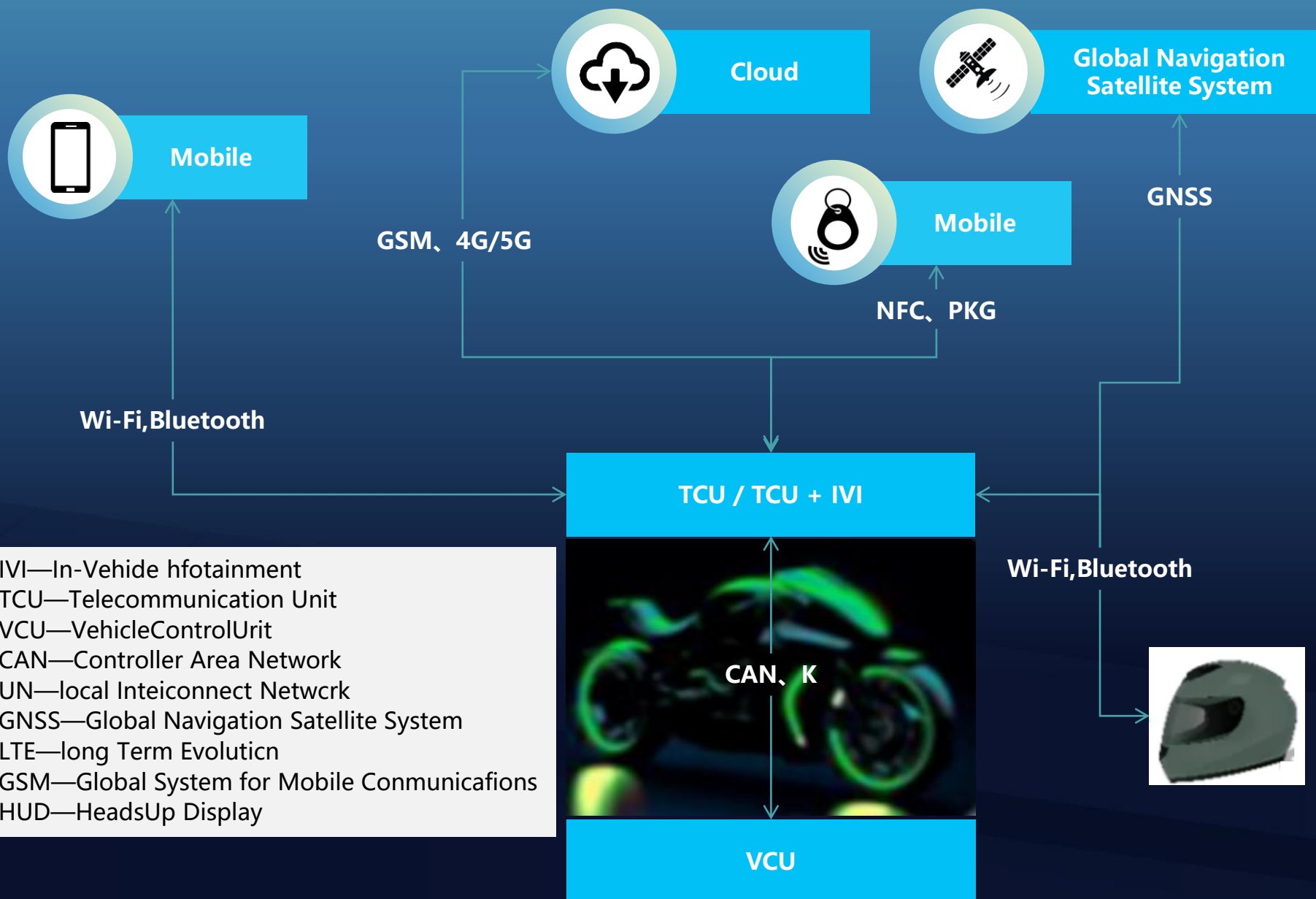
定制骑行模式：根据车主的偏好和订阅级别调整摩托车性能的软件。

AR、VR和IoT集成

智能头盔和装备：配备传感器的头盔和骑行装备，用于监测车主健康、检测碰撞并与摩托车通信。

家庭连接：与智能家居系统的集成。





- eCall+Breakdown Call & Assistance
- Alerts -Crash, Theft
- Smart Keyless Ignition
- Advanced navigation system
- Smart phone integration for
 - Navigation
 - Audio control
 - Audio Streaming
 - Calls
 - SMS
 - Media Player
- Vehicle Tracking
- Vehicle Health Management & Monitoring
- Ride statistics on mobile app
- Geo fencing
- Smart Helmets
 - Optic Mic & Headphones
 - HUD
 - Navigation, Speed, etc.
 - Calls

IVI—In-Vehicle Infotainment
 TCU—Telecommunication Unit
 VCU—Vehicle Control Unit
 CAN—Controller Area Network
 UN—local Interconnect Network
 GNSS—Global Navigation Satellite System
 LTE—Long Term Evolution
 GSM—Global System for Mobile Communications
 HUD—Heads Up Display

杜*迪或成为国内最大的“共享”机车品牌



带无钥匙启动的杜*迪



安全挑战



物理接触

更容易被盗窃：如果未受到保护，IVI（车载信息娱乐系统）系统容易暴露，成为盗窃的易攻击目标。



网络安全威胁

黑客攻击和恶意软件：连接系统（如信息娱乐和导航系统）可能成为黑客的目标。

远程控制漏洞：可能被利用来控制或禁用摩托车。

数据泄露：连接系统收集的個人和车辆数据可能被泄露。



隐私问题

位置跟踪：未经授权的跟踪车主通过连接系统的运动。

数据挖掘：未经车主同意，收集和滥用来自连接设备个人数据。



基础设施脆弱性

充电安全：对于电动两轮车，确保充电过程免受篡改和未经授权使用的安安全。

网络安全：保护摩托车与云服务之间的通信。

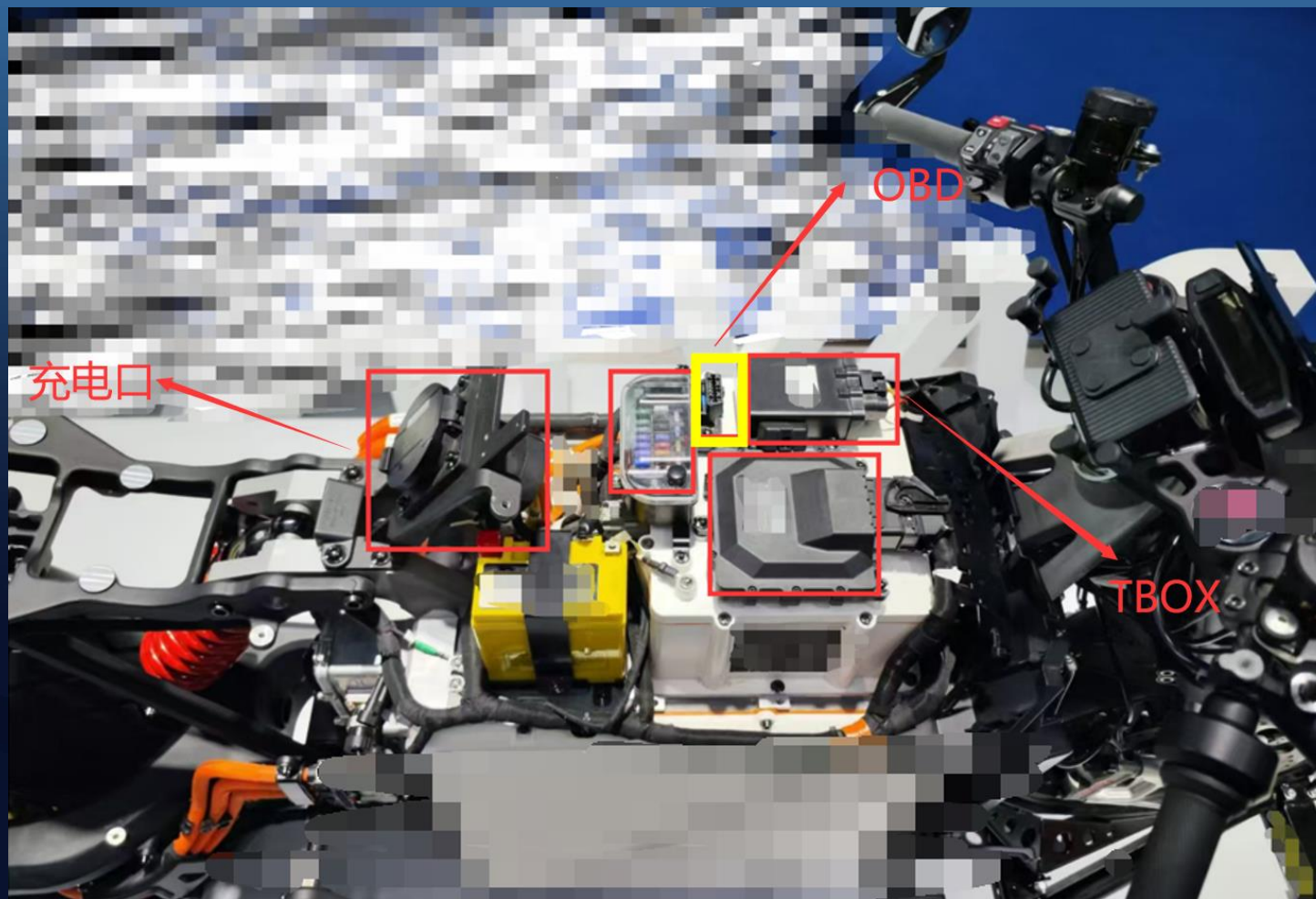


IoT设备安全

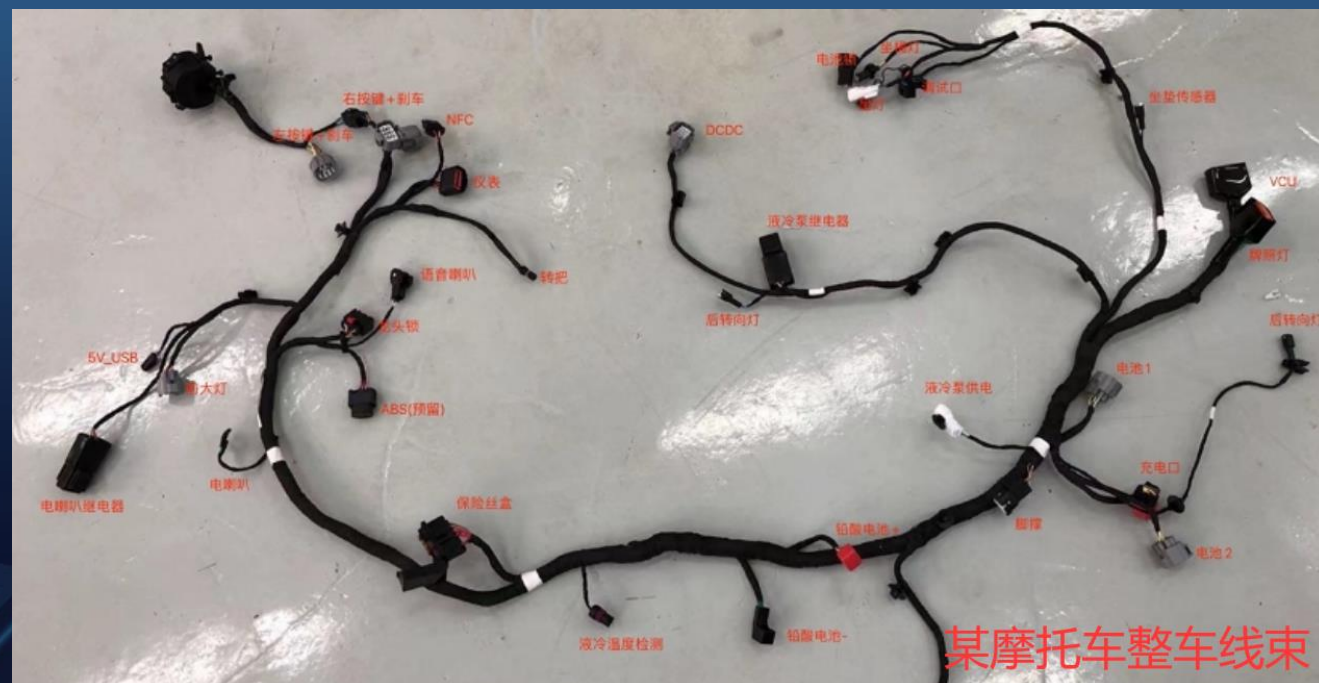
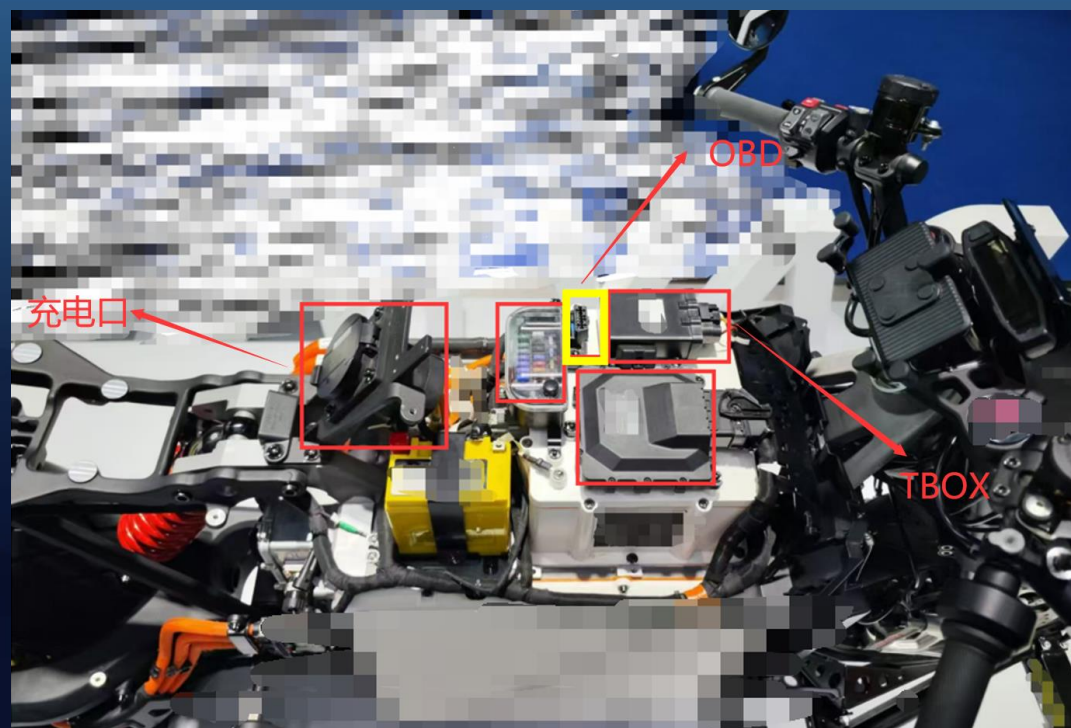
智能头盔和装备：保护连接头盔和骑行装备的安全，防止未经授权的访问和数据泄露。



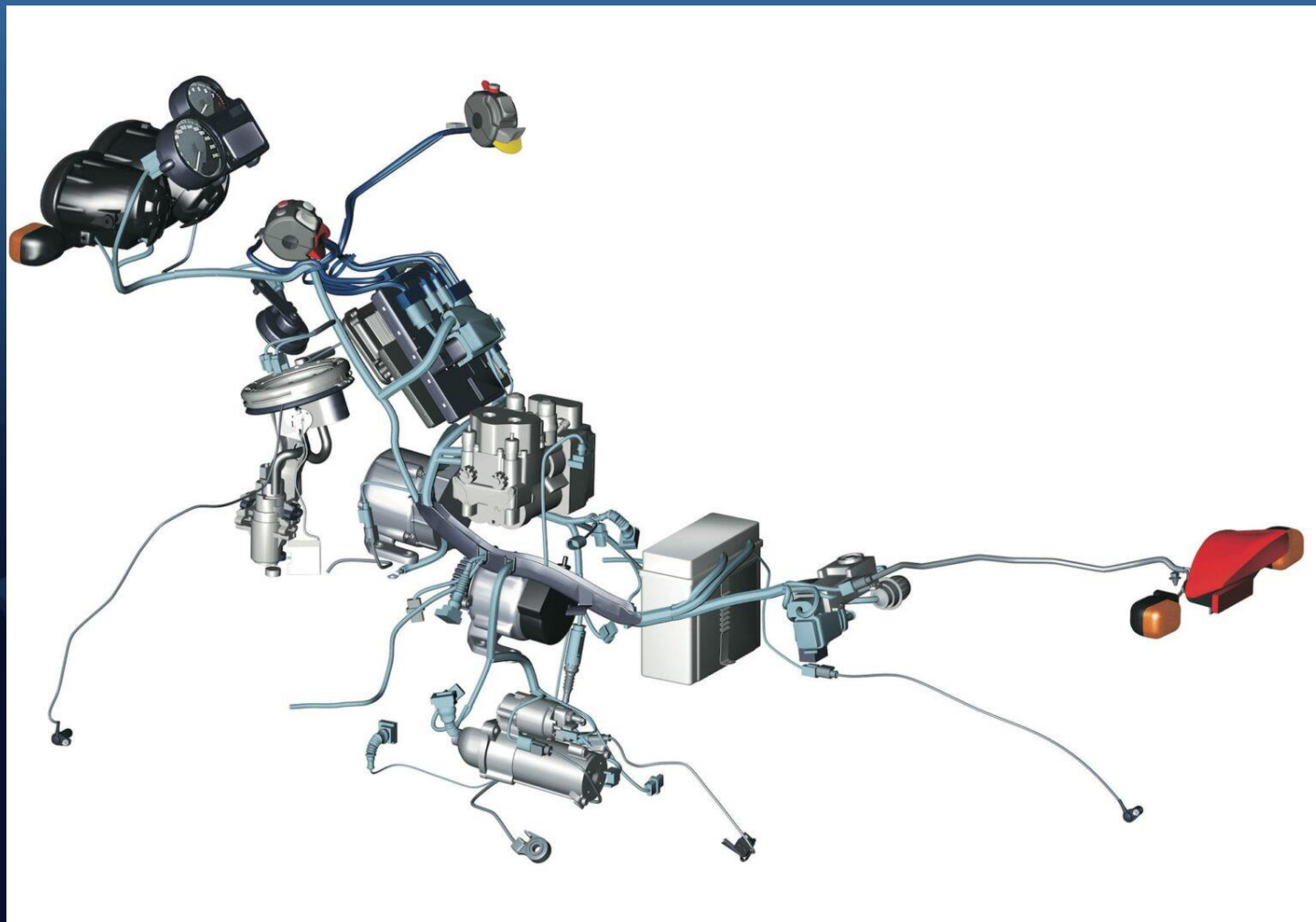
车辆内部



车辆内部通信



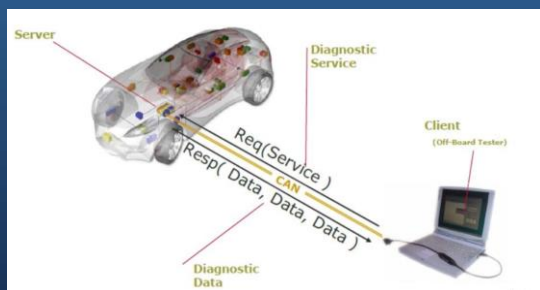
车辆内部通信



2004年的R1200系列是第一个使用CAN总线架构的宝马摩托车



车辆内部通信



汽车诊断是指通过使用专业设备和软件，对汽车系统进行检测和分析的过程，目的是识别和排除故障。

诊断可以
干什么

车辆监测

故障排查

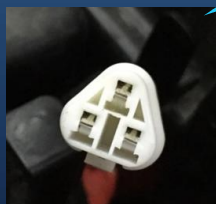
车辆配置

ECU刷写

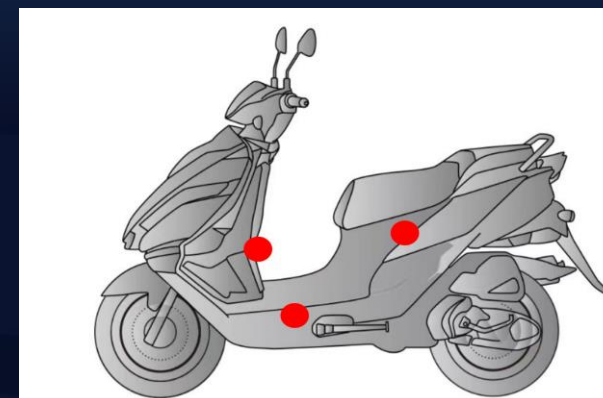
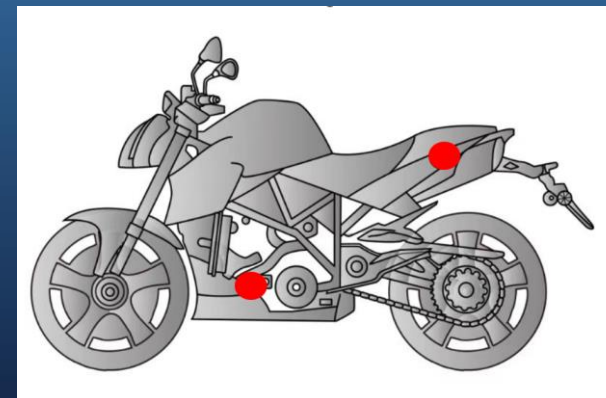
车辆内部通信

诊断口类型

K线 (KDS)



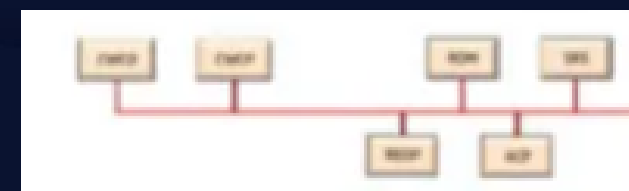
诊断口位置



更容易的接入方式



架构 ?



摩托车架构

网关？



极少部分车型有网关

常见漏洞

系统安全



WIFI、BT



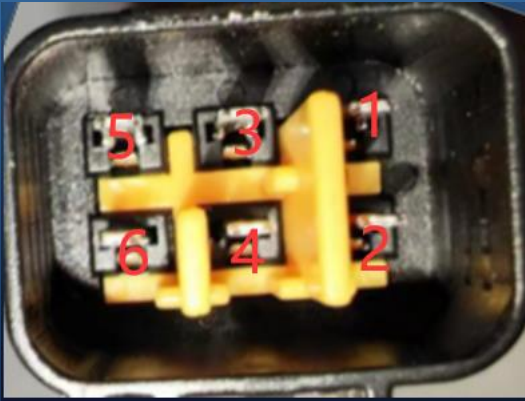
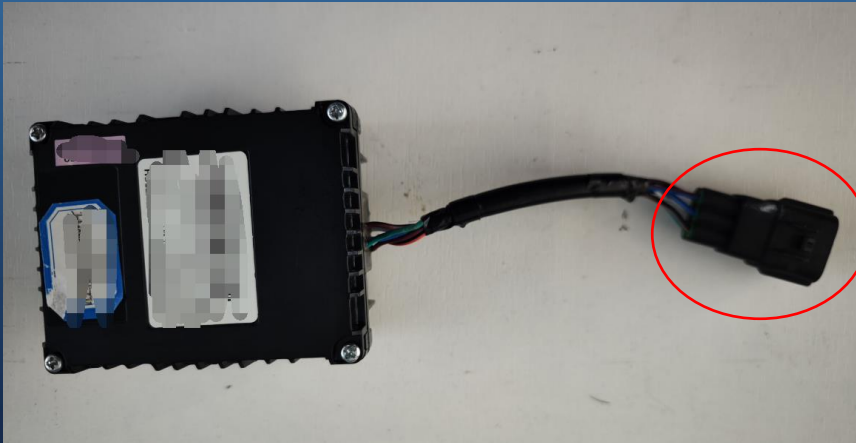
配套装备



PKE



案例 某车TBOX

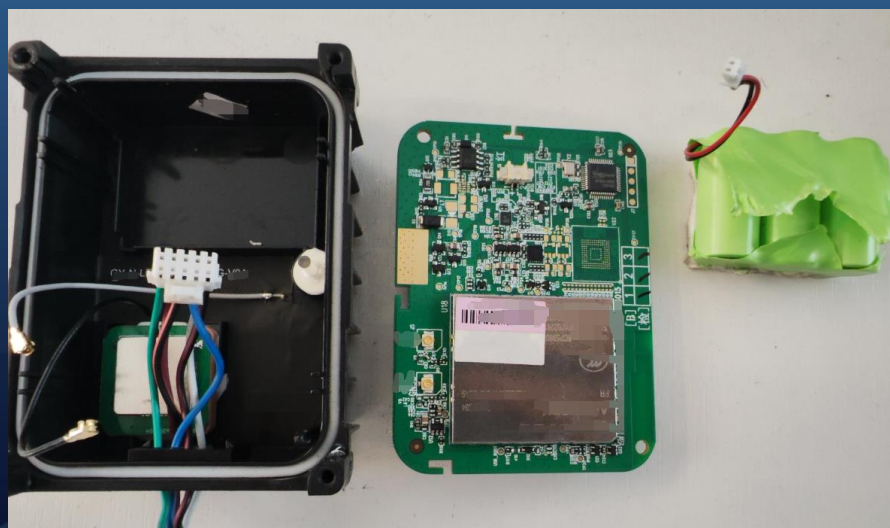


物理外壳

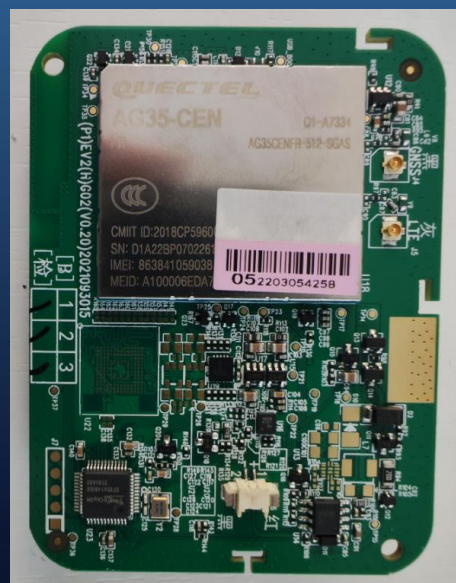


序号	定义
1	VBAT
2	KL.15
3	CAN_H
4	CAN_L
5	KLINE
6	GND

案例 某车TBOX



拆开



PCB



CTF

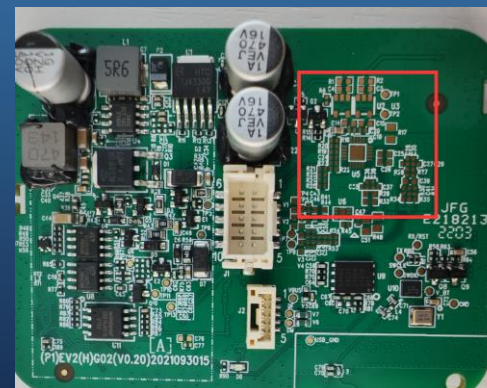
案例 某车TBOX

通信模组 : QUECTEL AG35-CEN
MCU: KF32A
FLASH: W25Q16JVSSIQ

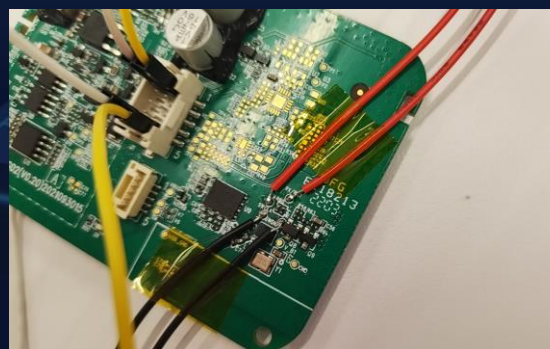
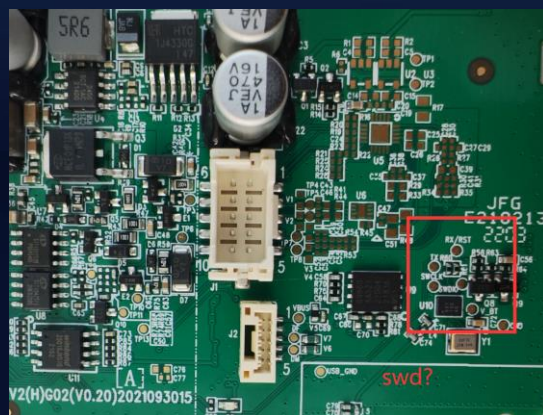


案例 某车TBOX

试引脚



提固件



案例 某车TBOX

//处理CAN数据

```
handleCanData(JSONObject canData) {  
    try {  
        int canId = canData.getString("canId");  
        String content = canData.getString("content");  
        int count = canData.getInt("count");  
        int times = canData.getInt("times");  
        for (int i = 0; i < times; i++) {  
            for (int j = 0; j < count; j++) {  
                an(canId, content);  
            }  
        }  
    }  
}
```

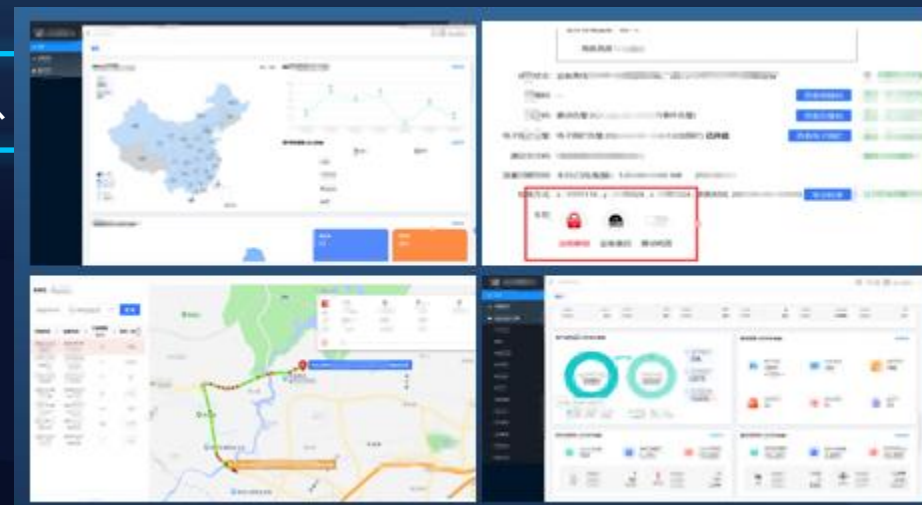
//发送CAN数据到服务器

```
sendDataToServer(Session session, JSONObject canData) {  
    if (session != null && session.isOpen()) {  
        try {  
            session.getBasicRemote().sendText(canData.toString());  
        }  
    }  
}
```

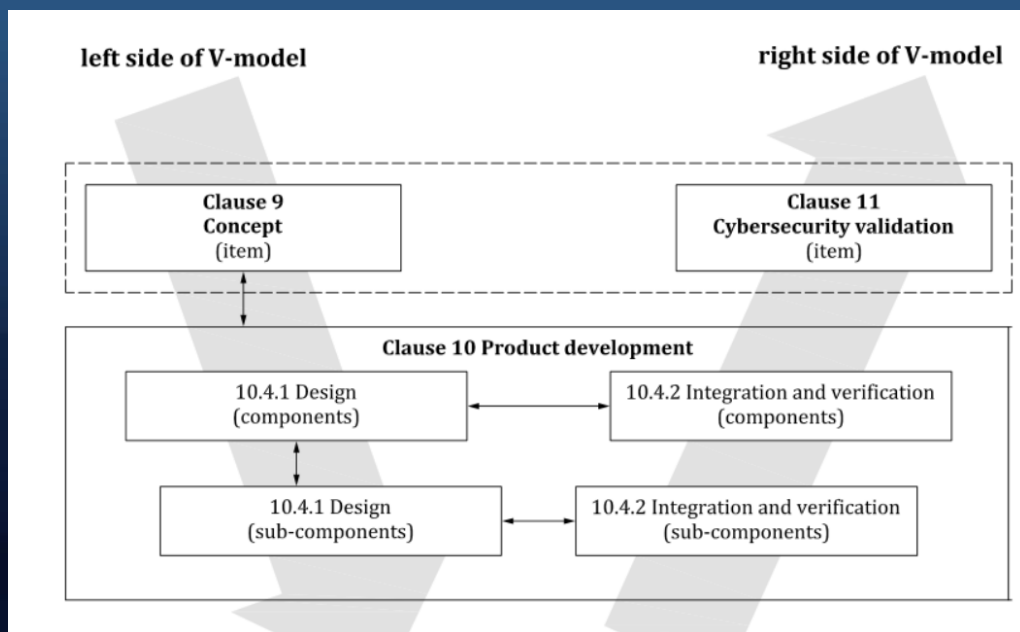
```
{  
    "deviceNum": "",  
    "canId": "123",  
    "content": "10 23",  
    "count": 1,  
    "times": 200  
}
```

deviceNum ?

案例 某车TBOX



路在何方

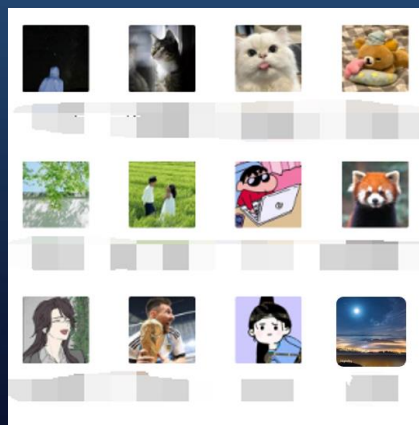


构建全面的网络安全标准体系

加强车辆网络安全架构设计

把握好网络安全基线

致谢



Thanks

