课件目录

- 第一章：认识无人驾驶系统
- 第二章：无人驾驶系统的定位方法以及传感器的应用
- 第三章：深度学习和无人驾驶视觉感知
- 第四章：迁移学习和强化学习在无人驾驶中的应用
- 第五章：无人驾驶的规划
- 第六章：车辆模型和高级控制
- **第七章：无人驾驶的平台介绍和系统安全**
- 第八章: 多智能体无人系统

参考资料：

《第一本无人驾驶技术书》（刘少山等）

《视觉SLAM14讲从理论到实践》（高翔）

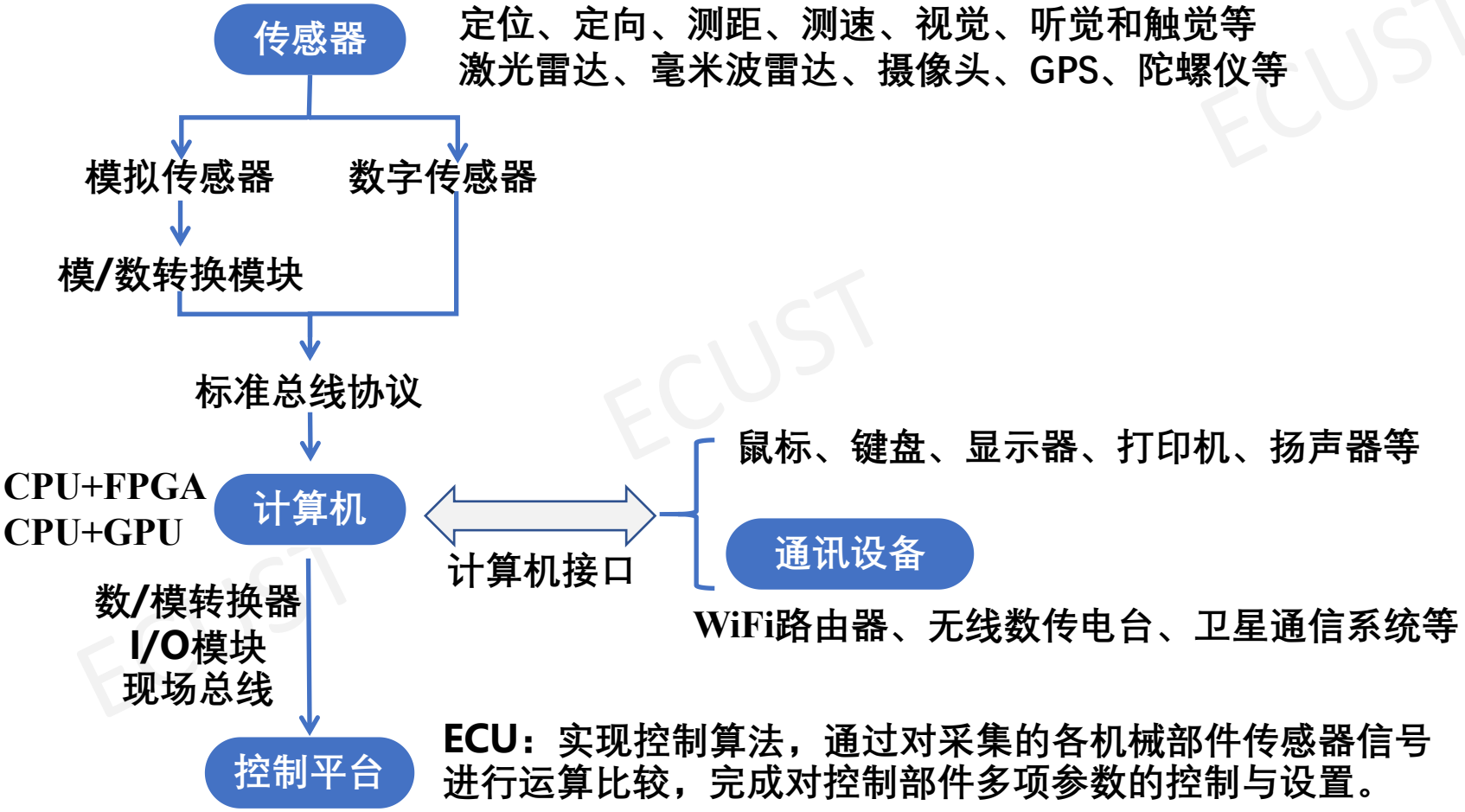
《机器视觉技术在安全辅助驾驶中的应用》中文版（泉田良辅 ）

第七章：无人驾驶的平台介绍和系统安全

本章目录 CONTENT

无人驾驶：复杂系统

硬件平台



7.1 传感器平台

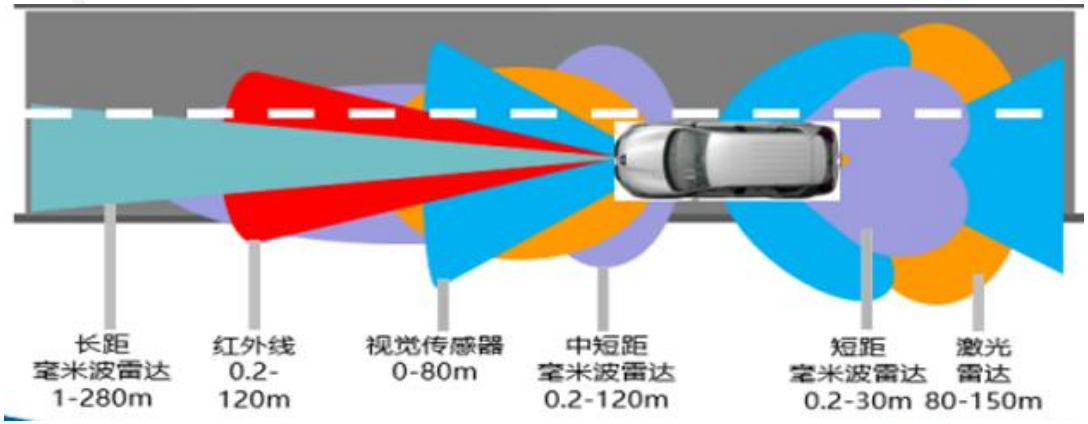
现有的车载传感器包括超声波雷达、激光雷达、毫米波雷达、车载摄像头、红外探头等。

主流的无人驾驶传感平台以**激光雷达和车载摄像头为主**，并呈现**多传感器融合**发展的趋势。

各个传感器之间借助各自所长相互融合、功能互补、互为备份、互为辅助。

	激光雷达	毫米波雷达	摄像头	GPS/IMU
远距离测量能力	优	优	优	优
分辨率	良	优	优	优
低误报率	良	优	一般	优
温度适应性	优	优	优	优
不良天气适应性	较差	优	较差	优
灰尘/潮湿适应性	较差	优	较差	较差
低成本硬件	较差	优	优	良
低成本信号处理	较差	优	较差	良

各种车载传感器的性能对比



各种传感器在无人驾驶中的应用

7.1 传感器平台

一. 激光雷达

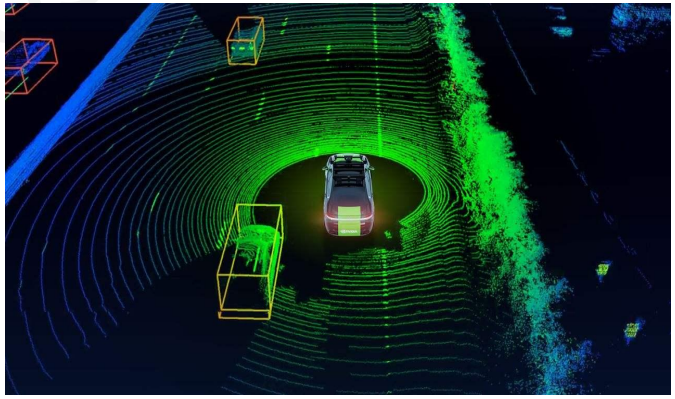
工作原理：利用**可见和近红外光波（**多为 950nm 波段附近的红外光）发射、反射和接收来探测物体。

作用：可以探测白天或黑夜下的特定物体与车之间的距离。由于反射度的不同，也可以区分开车道线和路面，但是无法探测被遮挡的物体、光束无法达到的物体，在雨雪雾天气下性能较差。

在无人驾驶中的核心作用：

（1）3D建模进行环境感知。

（2）SLAM 加强定位。



激光雷达演示图

7.1 传感器平台

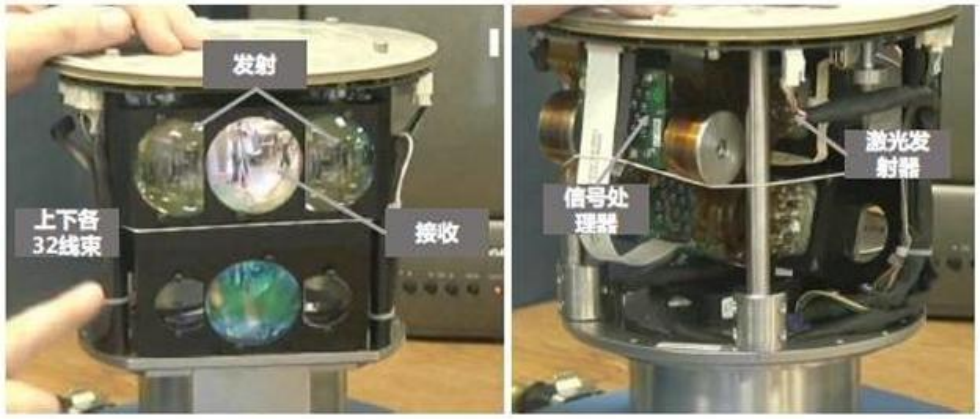
一. 激光雷达——分类与产品

- **单线激光雷达**的应用在国内已经相对较广（如扫地机器人），可以获取 2D 数据，但无法识别目标的高度信息。
- **多线激光雷达**则可以识别 2.5D 甚至是 3D 数据，在精度上会比单线雷达高很多。

随着线数的提升，其识别的数据点也随之增加，所要处理的数据量也非常巨大。

- **Velodyne HDL-32E** 传感器每秒能扫描70万个数据点。
- 百度无人车和 Google 无人车配备的 **Velodyne HDL-64E** 每秒能产生的数据点高达130万。

Velodyne HDL-64E 的内部结构如图，主要由上下两部分组成。



Velodyne HDL-64E激光雷达结构示意图

7.1 传感器平台

一. 激光雷达——分类与产品

激光雷达激光发射器线束越多，每秒采集的云点就越多，造价就更加昂贵。

目前，Velodyne 公司已经开发出了相对便宜的 HDL-32E 和 HDL-16E。其中 HDL-16E 是由16束激光取代64束激光，支持360度无盲区扫描，牺牲一定的数据规模云点，每秒钟只提供30万个数据点。

	HDL-64	HDL-32	VLP-16
价格	8万美元左右	2万美元	7999美元
激光束	64	32	16
扫描范围	120米	100米	100米
精度	正负2厘米	正负2厘米	正负2厘米
数据频率	1.3M 像素/秒	700,000像素/秒	300,000像素/秒
角度（垂直/水平）	26.8° /360°	40° /360°	30° /360°
功率	60W	12 W	8 W

Velodyne激光雷达详细数据

7.1 传感器平台

一. 激光雷达

降低激光雷达价格的解决办法：

1） 采用低线数雷达配合其他传感器，但需搭配拥有极高计算能力系统的无人车；

2）采用固态激光雷达。固态激光雷达无需旋转部件，采用电子设备替代。

激光雷达

固态激光雷达优点：体积更小，方便集成在车身内部，系统可靠性提高，成本也可大幅降低。

行业对固态雷达的出现仍处观望态度，主要因为：

1）对成本是否能有如此大幅下降抱有疑问；

2）激光特性在大雾等天气仍然并不适用。

7.1 传感器平台

一. 激光雷达——应用

- Google 和百度的无人驾驶试验车均采用了 Velodyne 的64线激光雷达；
- 福特的混动版蒙迪欧安装了 Velodyne 的32线激光雷达，第三代自动驾驶车辆 Fusion Hybrid 配置了2台 Velodyne 的混合固态激光雷达；
- 日产 LEAF 搭载了6个 Ibeo 的4线激光雷达，测试了其高级驾驶辅助系统；
- 奥迪的无人驾驶汽车 A7 Piloted Driving 采用了 Ibeo 和 Valeo 合作的 Scala 混合固态激光雷达；
- 德尔福无人驾驶汽车配备了4台由 Quanergy 研发的固态激光雷达；
- 大众的一款半自动驾驶汽车搭载了 Scala，该激光雷达隐藏在保险杠内，用于取代毫米波雷达做 AEB 的测距模块。

7.1 传感器平台

一. 激光雷达——制造现况

国外

- **Velodyne** 成立于1983年。美国举办的世界无人车挑战赛获得第一名和第二名的高校卡耐基梅隆大学和斯坦福大学，使用的就是 Velodyne 的激光雷达。
- **Ibeo** 是无人驾驶激光雷达供应商，成立于1998年， 2010年和法雷奥合作开始量产可用于汽车的产品 Scala。
- **Quanergy** 成立于2012 年，造出了全球第一款固态激光雷达，搭载在奔驰E上。

国内

- 激光雷达研发的企业主要有北醒光子、思岚科技、镭神智能、速腾聚创、禾赛科技。
- **北醒光子**目前的产品有三大系列：单线环境雷达 、多线长距雷达和固态雷达系列。
- **镭神智能**成立于2015年，提供中远距离脉冲测距激光雷达等产品及解决方案。
- **速腾聚创**宣布完成其混合固态的16线激光雷达研发。

二. 毫米波雷达

工作原理：通过**发射无线电信号（毫米波波段的电磁波）并接收反射信号**来测定汽车车身周围的物理环境信息（如汽车与其他物体之间的相对距离、相对速度、角度、运动方向等），然后根据所探知的物体信息进行目标追踪和识别分类，进而结合车身动态信息进行数据融合，完成合理决策，减少事故发生几率。

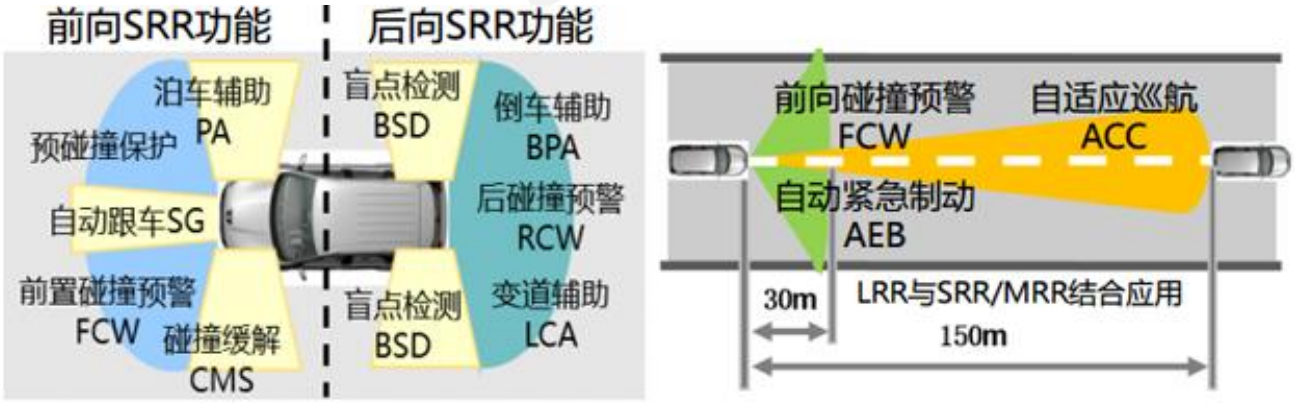
毫米波雷达

二. 毫米波雷达

优点：

毫米波雷达的工作频段为 30～300GHz 毫米波，毫米波的波长为波长为 1～10mm，介于厘米波和光波之间，因此毫米波兼有**微波制导**和**光电制导**的优点。

雷达可以检测30-100米远的物体。同时，毫米波雷达不受天气状况限制，穿透雾、烟、灰尘的能力强。具有全天候、全天时的工作特性，且探测距离远，探测精度高，被广泛应用于车载距离探测。



毫米波雷达应用范围原理示意

二. 毫米波雷达

缺点：

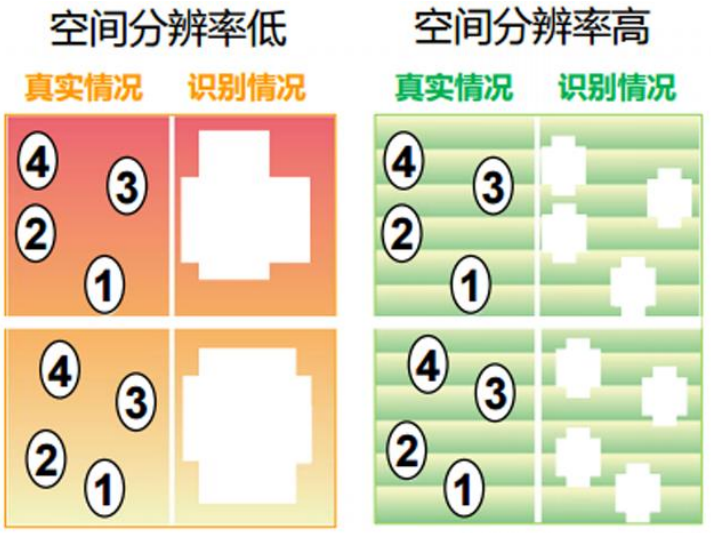
- 相比激光雷达，毫米波雷达精度低、可视范围的角度也偏小。
- 传输的是电磁波信号，因此它无法检测上过漆的木头或是塑料。
- 对金属表面非常敏感。
- 在大桥和隧道里的效果同样不佳。

二. 毫米波雷达——分类

毫米波雷达的主流可用频段为**24GHz 和 77GHz**，分别应用于中短距和中长距测量，如图。

相比于 24GHz，77GHz 毫米波雷达物体分辨准确度可提高2-4倍，测速和测距精确度提高3-5倍，能检测行人和自行车；且设备体积更小，更便于在车辆上安装和部署。

长距离雷达的侦测范围更广，可适配开行速度更快的车辆，但是相应地探测精度下降，因此更适用于 ACC 自适应巡航这类的应用。



中距和短距雷达空间分辨率对比

	LRR 长距离雷达	SRR/MRR短距离雷达
分类	窄带雷达	宽带雷达
覆盖距离(米)	280	30/120
车速上限Km/h	250	150
精度	0.5M	厘米级
主要应用范围	ACC自适应巡航	车辆环境监测

中长距和短距雷达参数对比

二. 毫米波雷达——分类

为完全实现 ADAS 各项功能一般需要**“1长+4中短”**5个毫米波雷达。

目前全新奥迪 A4 采用的就是 “1长+4短”5个毫米波雷达的配置。

下图是奔驰的 S 级车型，采用的是7个毫米波雷达（1长+6短）。

毫米波雷达在无人驾驶中的使用

二. 毫米波雷达——分类

电磁波频率越高，距离和速度的检测解析度越高，因此**频段发展趋势是逐渐由 24GHz 向 77GHz 过渡**的。

- 1997年，欧洲电讯标准学会确认 76-77GHz 作为防撞雷达专用频道。
- 2005年，原信息产业部发布《微功率（短距离）无线电设备的技术要求》将 77GHz 划分给车辆测距雷达。
- 2012年，工信部进一步将 24GHz 划分给短距车载雷达业务。
- 2015年，日内瓦世界无线电通信大会将 77.5-78.0GHz 频段划分给无线电定位业务，以支持短距离高分辨率车载雷达的发展，从而使 76-81GHz 都可用于车载雷达，为全球车载毫米波雷达的频率统一指明了方向。
- 至此之后，最终车载毫米波雷达将会统一于 77GHz 频段（76-81GHz），该频段带宽更大、 功率水平更高、探测距离更远。

二. 毫米波雷达——制造现况

全球汽车毫米波雷达主要供应商为传统汽车电子优势企业，如博世、大陆、Hella、富士通天、电装、德尔福、Autoliv、法雷奥等传统优势企业。

博世：长距离毫米波雷达，主要用于 ACC 系统；最新产品 LRR4 可以探测250米外的车辆，是目前探测距离最远的毫米波雷达；主力产品为 24GHz 毫米波雷达。

Hella：在 24GHz-ISM 领域客户范围最广，24GHz 雷达传感器出货量达650万片，市场占有率全球第一。

富士通天和电装主要占据日本市场。富士通天、松下和电装是未来 79GHz 雷达市场领域的强者。

二. 毫米波雷达——制造现况

在雷达数据处理芯片领域，主要采用的是**恩智浦**（NXP）MR2001多通道 77GHZ 雷达收发器芯片组；以及**意行半导体**24GHz 射频前端 MMIC 套片产品。

2016年NXP推出了目前全世界最小（7.5×7.5mm）的单晶片 77GHz 高解析度 RFCMOS IC 雷达晶片。该款车用雷达晶片的超小尺寸使其可以近乎隐形地安装在汽车的任意位置，且其功耗比传统雷达晶片产品低 40%。

	长距		中距		短距	
厂商	型号	性能参数	型号	性能参数	型号	性能参数
BOSCH	远距 LRR4	76-77GHz 前向 250m	中距 MRR	76-77GHz 前向 160m/42° 后向 80m /150°		
continental	长距 ARS410	76-77GHz 前向 170m			SRR320	24-25GHz
	长距 ARS430	76-77GHz 前向 250m				
HELLA					短距离雷达 SRR	24GHz 前向距离 0.75-70m 视角 165°
Delphi			中距 ESR2.5	76-77GHz 前向 174m		
Denso	长距离雷达 LRR	76-77GHz 前向距离 205m 视角 36°				
Autoliv					短距离雷达 SRR 25GHz	超宽带 24GHz 窄带 77GHz 多模式雷达

各个主要厂商的主要毫米波雷达产品

三. 摄像头

原理:

采集图像进行处理，将图片转换为二维数据；进行模式识别，通过图像匹配进行识别；依据物体的运动模式或使用双目定位，以估算目标物体与本车的相对距离和相对速度。

优点:

摄像头最为接近人眼获取周围环境信息的工作模式，可以通过较小的数据量获得最为全面的信息，摄像头技术成熟，成本较低。

局限性:

- 基于视觉的解决方案受光线、天气影响大；
- 物体识别基于机器学习资料库，需要的训练样本大，训练周期长，也难以识别非标准障碍物；
- 广角摄像头的边缘畸变，得到的距离准确度较低。

三. 摄像头

	应用场景
单目	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
后视	AP
立体（双目）	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
环视	AP, SVC

摄像头的应用场景

（1）**单目摄像头：**一般安装在前挡风玻璃上部，用于探测车辆前方环境，识别道路、车辆、行人等。单目视觉方案的技术难点在于模型机器学习的智能程度或者模式识别的精度；

（2）**后视摄像头：**一般安装在车尾，用于探测车辆后方环境，技术难点在于如何适应不同的恶劣环境；

三. 摄像头

	应用场景
单目	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
后视	AP
立体（双目）	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
环视	AP, SVC

摄像头的应用场景

（3）**立体（双目）摄像头：**依靠两个平行布置的摄像头产生的“**视差**”，找到同一个物体所有的点，依赖三角测距，算出摄像头与前方障碍物距离。使用这种方案，需要两个摄像头有**较高的同步率和采样率**，因此技术难点在于**双目标定**及**双目定位**。

相比单目，双目的解决方案没有识别率的限制，无需先识别可直接进行测量；直接利用视差计算距离精度更高；无需维护样本数据库。但因为检测原理上的差异，双目视觉方案在距离测算上相比单目以及毫米波雷达、激光雷达，其硬件成本和计算量级的加倍。

三. 摄像头

	应用场景
单目	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
后视	AP
立体（双目）	ACC, LDW,LKA,FCW,AEB,TSR,AP,PDS,DMS
环视	AP, SVC

摄像头的应用场景

（4）**环视摄像头：**一般至少包括四个摄像头，分别安装在车辆前、后、左、右侧，实现360°环境感知，难点在于畸变还原与对接，如右图所示。

无人车中各摄像头传感器的方位设置

三. 摄像头

根据不同 ADAS 功能的需要，摄像头的安装位置也有不同，如右表。实现自动驾驶时全套 ADAS 功能将**安装6个以上**摄像头。

安装部位	摄像头类型	应用场景
前视	单目、双目	FCW、LDW、TSR、ACC、PCW
环视	广角	全景泊车、LDW
后视	广角	后视泊车辅助
侧视	广角	盲眼检测、替代后视镜
内置	广角	闭眼提醒

按功能需求的摄像头划分

各种无人驾驶应用摄像头

- 前视摄像头：采用55度左右的镜头来得到较远的有效距离（单目和双目）。
- 环视：广角摄像头，通常在车四周装备四个进行图像拼接实现全景图，通过辅助算法可实现道路线感知。

三. 摄像头

安装部位	摄像头类型	应用场景
前视	单目、双目	FCW、LDW、TSR、ACC、PCW
环视	广角	全景泊车、LDW
后视	广角	后视泊车辅助
侧视	广角	盲眼检测、替代后视镜
内置	广角	闭眼提醒

按功能需求的摄像头划分

- 后视：采用广角或者鱼眼镜头，主要为**倒车后视**使用。
- 侧视：两个广角摄像头，完成**盲点检测**等工作，也可代替后视镜。
- 内置：广角镜头，安装在车内后视镜处，完成在行驶过程中对驾驶员的**闭眼提醒**。

三. 摄像头

首要特性是快速，在高速行驶场合，系统必须能记录关键驾驶状况、评估这种状况并实时启动相应措施。为避免两次图像信息获取间隔期间自动驾驶的距离过长，要求相机具有**最慢不低于30帧/秒的影像捕捉速率。**

在功能上，车载摄像头需要在复杂的运动路况环境下都都能保证采集到稳定的数据。具体如下：

高动态	在较暗环境以及明暗差异较大下仍能实现识别
中低像素	降低计算处理负担，目前30-120万像素已经满足要求
角度要求	环视和后视一般采用135度以上的广角镜头，前置摄像头对视距要求更大，一般采用55度的范围

三. 摄像头

相比工业级与生活级摄像头，车载类型在安全级别上要求更高，尤其是对与前置ADAS的镜头安全等级要求更高。主要体现在：

温度要求	车载摄像头温度范围在-40~80℃
防磁抗振	汽车启动时会产生极高的电磁脉，车载摄像头必须具备极高的防磁抗震的可靠性
较长的寿命	车载摄像头的寿命至少要在8-10年以上才能满足要求

三. 摄像头

国内行业龙头优势地位明显，如**舜宇光学车载后视镜头**出货量目前居全球第1位，全球市场占有率达30%左右，客户遍及欧美、日韩和国内。具体的型号包括有：4005、4408、4009、4017、4017、4034、4043、4044等。以4005与4043为例，其规格参数见表。

型号	ELF(mm)	HFOV(°)	Max Image Circle	Resolution
4005	1.02	138	1/4" (Φ5.0)	VGA
4043	1.1	187	H1/4"(Φ4.0)	MEGA

舜宇光学4005、4043视觉传感器规格参数

四. GPS/IMU

GPS 的路径反射：导致获得的 GPS 定位信息很容易产生几米的误差。

GPS 的更新频率低：车辆快速行驶时很难给出精准的实时定位。

GPS通常辅助以惯性传感器（IMU）用来增强定位的精度

IMU 是检测加速度与旋转运动的高频传感器，但也有**偏差积累与噪音**等问题影响结果。

使用**基于卡尔曼滤波的传感器融合**技术，融合 GPS 与 IMU 数据

- 实现导航设备之间优势互补，增强系统适应动态的能力，并使整个系统获得优于局部系统的精度；
- 提高了空间和时间的覆盖范围，从而实现真正意义上的连续导航。

四. GPS/IMU

GPS/IMU 组合的优势：

1) 系统精度的提高

2) 系统抗干扰能力的增强

3) 导航信息的补全

- IMU 惯性器件的标定技术由于加速度计、陀螺仪等惯性器件本身存在缺陷，会产生一些器件误差，如标度因数误差等。
- 对 IMU 进行集成的时候，各个器件之间的非正交安装会引起交叉耦合误差。

通过**器件标定**来加以补偿

四. GPS/IMU

GPS/IMU 的主要制造商包括：NovAtel、Leica、CSI Wireless 以及 Thales Navigation。

NovAtel 提出了 SPAN 技术。SPAN 集合了 GPS 定位的绝对精度与 IMU 陀螺和加速计测量的稳定性。

基于 SPAN 技术，NovAtel 有以下两款主要的 GPS/IMU 产品：

NovAtel SPAN-CPT一体式组合导航系统　NovAtel SPAN-FSAS分式组合导航系统

四. GPS/IMU

SPAN-CPT 采用 NovAtel 自主的专业级的高精度 GPS 板卡与德国的 iMAR 公司制造的光纤陀螺 IMU。其解算精度在不同的模式下可适用于不同的定位需求。

SPAN-FSAS 也采用德国 iMAR 公司高精度、闭环技术的 IMU，其陀螺偏差小于0.75度/小时和加速计偏差小于1mg，配合目前 NovAtel 的 FlexPak6™ 或 ProPak6™ 集成了组合导航解算。

NovAtel SPAN-CPT一体式组合导航系统

NovAtel SPAN-FSAS分式组合导航系统

五. V2X通信传感系统

V2X 是车联网通信机制的总称。V2X通信系统可以看作是一个超级传感器，它提供了比其他车载传感器都高得多的感知能力和可靠性。

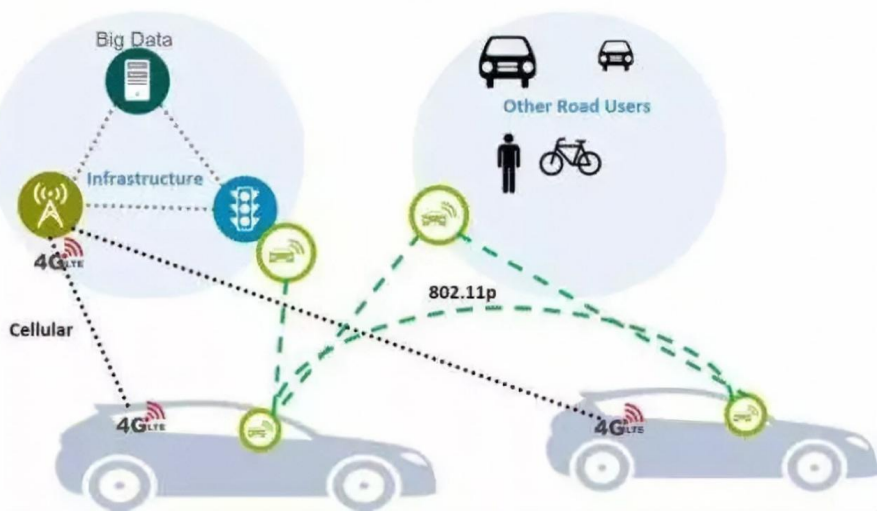
V2X是无人驾驶必要技术和智慧交通的重要一环。通过 V2X可以获得实时路况、道路信息、行人信息等一系列交通信息，从而带来远距离环境信号。

- V2X
  - V2V (Vehicle toVehicle，车车通信)
  - V2I (Vehicle to Instruction，车路通信)
  - V2P (Vehicle to Pedestrian，车人通信)

五. V2X通信传感系统

V2X是一种**网状网络**，网络中的**节点** (汽车、智能交通灯等)可以发射、捕获并转发信号，车辆可以获取周围环境的未知参数及附近车辆的运行状态。

V2V通信技术首次由福特公司在2014年6月3日发布，如图所示。



V2X通信辅助下的行车状况示意图

五. V2X通信传感系统——V2X通信优势

V2X通信传感系统优势

1）**覆盖面更广：**300~500米的通信范围，不仅是前方障碍物，身旁和身后的建筑物、车辆都会互相连接，大大拓展了驾驶员的视野范围。

2）**有效避免盲区：**由于所有物体都接入互联网，每个物体都会有单独的信号显示，因此即便是视野受阻，通过实时发送的信号可以显示视野范围内看不到的物体状态。

3）**对于隐私信息的安全保护性更好：**系统将采用5.9GHz频段进行专项通信，相比传统通信技术更能确保安全性和私密性。

五. V2X通信传感系统——V2X通信的国内外发展进展

1）国外V2X的进展

目前这套V2V协议由通用、福特、克莱斯勒等厂商联合研发，除了美国汽车三巨头，丰田、日产、现代、起亚、大众、奔驰、马自达、斯巴鲁、菲亚特等车企也在协议名单内。

2016年12月14日，美国交通部发布了V2V的新法规，法规强制要求新生产的轻型汽车安装V2V通信装置。

美国交通部的新规中要求V2V装置的**通信距离达到300米，并且是360度覆盖**，远超摄像头的探测能力，其感知信息属于**结构化信息**，不存在误报的可能。

根据美国家公路交通安全管理局(NHTSA)的研究，利用V2X技术，可以减少80%的非伤亡事故，但这一切是以100%的覆盖率为前提的。

五. V2X通信传感系统——V2X通信的国内外发展进展

2）中国V2X的进展

2019年，发改委发布了**《智能网联汽车创新发展战略（征求意见稿）》**，指出2020年中国的大城市高速路要达到90%覆盖C-V2X，2025年实现人、车、路、云的高度协调。5G-V2X要满足ICV要求。

工信部国标委也发表了**《国家车联网产业标准体系建设指南》**，明确要求LTE-V2X作为广域和中短程智能网联汽车关键技术。

工信部也发布了**《车联网(智能网联汽车)产业发展行动计划》**，明确了到2020 年实现LTE-V2X在部分城市主要道路和高速公路覆盖，开展5G-V2X示范应用，车联网用户渗透率达到30%以上。

五. V2X通信传感系统——V2X通信的国内外发展进展

2）中国V2X的进展

为了满足在商业应用上的高可靠性，越来越多的车企意识到在增强车辆能力的同时，需要将道路从**“对人友好”改造为“对车友好”**，从 2015年开始，中国所有的无人驾驶示范园区都在规划部署**路侧系统（V2I）**。随着5G的时间表日渐清晰，更大范围的部署也让人非常期待。5G 的核心推动力来自物联网，而汽车可能是其中最大的单一应用。

目前，多个地图供应商正在积极准备用于无人驾驶的**实时高精地图**，以克服静态高精地图无法适应道路变化的难题，但之前受无线带宽限制，很难达到实用，而5G可提供高达10Gbit/s 以上的峰值速率，以及 1ms 的低延时性能，以满足这样的需求。

7.1 传感器平台

传感器小结

传感器	成　本	优　势	劣　势	功　能
激光雷达	8000 美元以上	扫描周围环境得到精确环境信息	成本高，大雾、雨雪天气效果差，无法图像识别	周边环境 3D 建模
毫米波雷达	300~500 美元	不受天气影响，测量精度高，距离范围广	无法识别道路指示牌，无法识别行人	无法应用视觉识别要求较高功能
摄像头	35~50 美元	成本比较低，通过算法可以实现各种功能	极端恶劣环境下会失效，难以测距，距离较近，算法要求高	能实现大多数 ADAS 功能，测距功能难以实现
V2X	150~200 美元	不受距离现实，V2X 成本较低，深度融合智能系统	精度较低，技术协议仍在讨论中，普及难度大	利用通信协议，感知实时路况，道路信息和行人信息
红外传感器	600~2000 美元	夜视效果极佳	成本较高，技术仍由国外垄断	夜视
超声波传感器	15~20 美元	成本低	探测距离较近，应用局限大	侧方超车提醒、倒车提醒

各种传感器的比较

第七章：无人驾驶的平台介绍和系统安全

本章目录 CONTENT

7.2 计算平台

当硬件传感器接收到环境信息后，数据会被导入计算平台，由不同的芯片进行运算。计算平台的设计直接影响到无人驾驶系统的实时性以及鲁棒性。本节将深入了解无人驾驶计算平台。

- 了解无人驾驶计算平台的要点
- 了解芯片制造商将如何解决这些问题

7.2 计算平台

L4级无人驾驶平台实例

该计算平台由两计算盒组成。每个计算盒配备了一颗英特尔至强 E5 处理器（12核）、四到八颗 NVIDIA K80 GPU加速器。

CPU 运算峰值速度可达400帧/秒，消耗 400W 的功率。每个 GPU 运算峰值速度可达8Tops/s，同时消耗 300W 的功率。整个系统能够提供 64.5 TOP/S 的峰值运算能力，其功率需求为 3000W。

计算盒与车辆上安装的**十二个高精度摄像头**相连接，以完成实时的物体检测和目标跟踪任务。车辆顶部还安装有**一个激光雷达装置**以完成车辆定位及避障功能。

为了保证可靠性，两个计算盒执行完全相同的任务。在最坏的情况下两个计算盒都在计算峰值运行，将产生超过5000瓦的功耗并急聚大量的热量，**散热问题**不容忽视。此外，每个计算盒的**成本**预计为2至3万美元。

现有计算解决方案

现有的针对无人驾驶的计算解决方案：

- 基于 GPU 的计算解决方案
- 基于 DSP 的解决方案
- 基于 FPGA 的解决方案
- 基于 ASIC 的解决方案

7.2 计算平台

现有计算解决方案——基于 GPU 的计算解决方案

GPU在浮点运算、并行计算等方面能够提供数十倍至上百倍的CPU性能。利用GPU运行机器学习模型，在云端进行分类和检测，其相对于CPU耗费的时间大幅缩短，占用的数据中心的基础设施更少，能够支持10~100倍的应用吞吐量。

凭借强大的计算能力，在机器学习快速发展的推动下，目前GPU在深度学习芯片市场非常受欢迎，很多汽车生产商也在使用GPU作为传感器芯片发展无人车。

凭借具备识别、标记功能的图像处理器，在人工智能还未全面兴起之前，NVIDIA就先一步掌控了这一时机。2019年，NVIDIA发布了**DRIVE AGX系列**计算平台，针对无人驾驶作业进行加速。

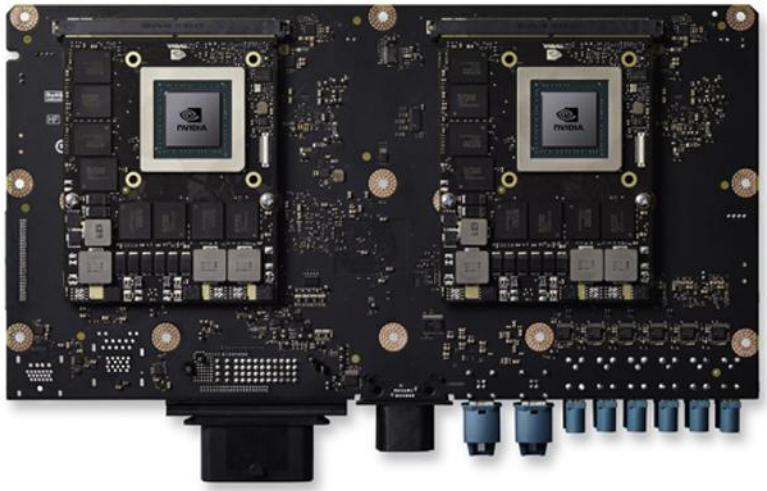
7.2 计算平台

现有计算解决方案——基于 GPU 的计算解决方案

NVIDIA 的 PX 平台是目前领先的基于 GPU 的无人驾驶解决方案。

每个 PX2 由两个 Tegra SoC 和两个 Pascal GPU 图形处理器组成。为了提供高吞吐量，每个 Tegra SOC 使用 PCI-E Gen 2x4总线与 Pascal GPU 直接相连，其总带宽为 4 GB/s。

两个 CPU-GPU 集群通过千兆以太网相连，数据传输速度可达70 Gigabit/s。借助于优化的 I/O 架构与深度神经网络的硬件加速，每个 PX2 能够每秒执行24兆次深度学习计算。



NVIDIA PX2平台芯片示意图

7.2 计算平台

现有计算解决方案——基于 DSP 的解决方案

DSP (Digital Singnal Processor) 以数字信号处理大量数据。

DSP采用的是**哈佛设计**，允许取出指令和执行指令完全重叠，并进行译码，这大大提高了微处理器的速度。

DSP允许在程序空间和数据空间之间进行传输，因为增加了器件的灵活性。它不仅具有可编程性，而且其实时运行速度可达每秒数以千万条复杂指令程序，远远超过通用微处理器。

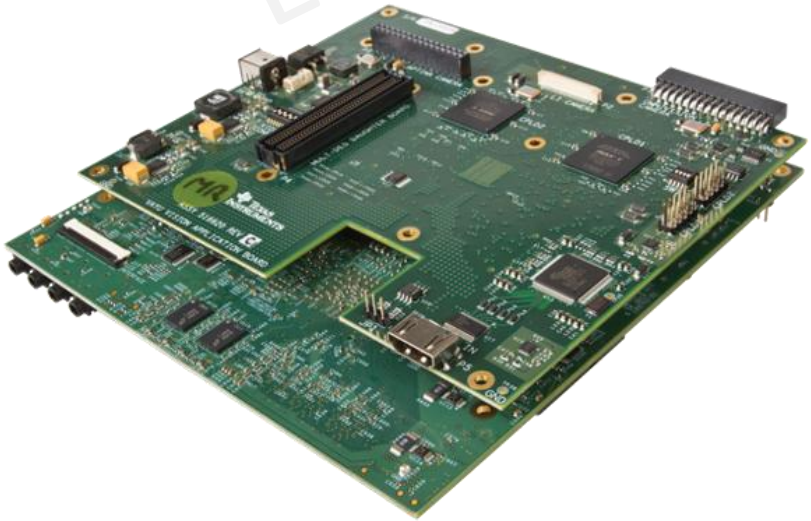
运算能力很强，速度很快，体积很小，而且采用软件编程具有高度的灵活性。

7.2 计算平台

现有计算解决方案——基于 DSP 的解决方案

德州仪器的TDA2x SoC 拥有两个浮点 DSP 内核 C66x 和四个专为视觉处理设计的完全可编程的视觉加速器。相比 ARM Cortex-15 处理器，视觉加速器可提供八倍的视觉处理加速且功耗更低。

类似设计有 CEVA XM4，专门面向计算视觉任务中的视频流分析计算。实时3D深度图和点云数据(Point Cloud)生成，用于目标识别和语义环境认知(context awareness)的深度学习和神经网络算法，用于图像增强的计算图像学功能，包括变焦、图像稳定、降噪和低照度增强功能。



TDA2 SoC芯片示意图

现有计算解决方案——基于 FPGA 的解决方案

FPGA硬件配置灵活，具有低能耗、高性能及可编程等特性，十分适合感知计算，FPGA相比 GPU价格便宜。在能源受限的情况下，FPGA相对于CPU 与GPU有明显的性能与能耗优势。

感知算法不断发展意味着感知处理器需要不断更新，FPGA具有硬件**可升级、可迭代**的优势。

随着FPGA与传感器结合方案的快速普及，视觉、语音、深度学习的算法在FPGA上进一步优化，FPGA极有可能逐渐取代GPU 与CPU成为无人车、机器人等感知领域上的主要芯片。

现有计算解决方案——基于 FPGA 的解决方案

百度大脑——FPGA版百度大脑

在百度的深度学习应用中，FPGA相比相同性能水平的硬件系统消耗能率更低，将其安装在刀片式服务器上，可以完全由主板上的 PCIExpress 总线供电，并且使用FPGA可以将一个计算得到的结果直接反馈到下一个，不需要临时保存在主存储器，所以存储带宽要求也在相应降低。

现有计算解决方案——基于 FPGA 的解决方案

Altera 公司的 Cyclone V SoC 是一个基于 FPGA 的无人驾驶解决方案。Altera 公司的 FPGA 专为传感器融合提供优化。

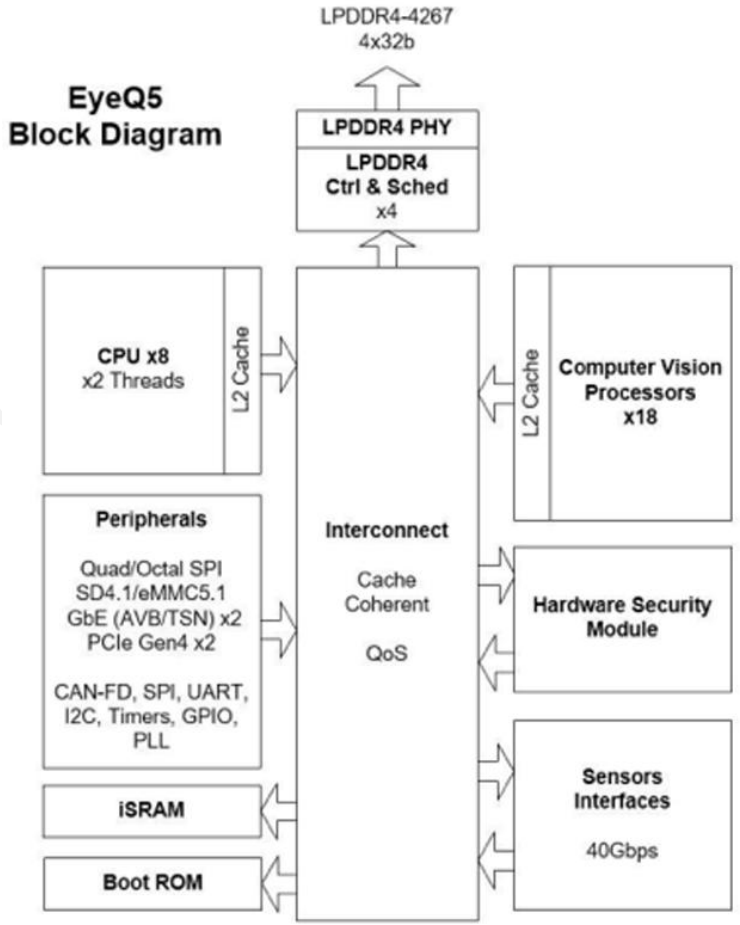
类似的产品有 Zynq 专为无人驾驶设计的 Ultra ScaleMP SoC。当运行卷积神经网络计算任务时，Ultra ScaleMP SoC 运算效能为14帧/秒/瓦，优于 NVIDIA Tesla K40 GPU 可达的4帧/秒/瓦。

Altera Cyclone V SoC 芯片示意图

现有计算解决方案——基于 ASIC 的解决方案

Mobileye 是一家基于 ASIC 的无人驾驶解决方案提供商。其 Eyeq5 SOC 装备有四种异构的全编程加速器，分别对专有的算法进行了优化。

Eyeq5 SOC 同时实现了两个 PCI-E 端口以支持多处理器间通信。这种加速器架构尝试为每一个计算任务适配最合适的计算单元，硬件资源的多样性使应用程序能够节省计算时间并提高计算效能。



MobilEye EyeQ5

第七章：无人驾驶的平台介绍和系统安全

本章目录 CONTENT

7.3 控制平台

控制平台是无人车的核心部件，控制着车辆的各种控制系统：

ABS-汽车防抱死制动系统、ASR-汽车驱动防滑转系统；

ESP-汽车电子稳定程序、SBC-电子感应制动控制系统；

EBD-电子制动力分配、BAS-辅助制动系统；

SRS-安全气囊 、 EAT-电控自动变速器；

CVT-无级变速器、CCS-巡航控制系统；

ECS-电子控制悬架、EPS-电控动力转向系统。

控制平台主要包括了电子控制单元 ECU 与通信总线两大部分：

- **ECU** 主要实现控制算法
- **通信总线**主要实现ECU以及机械部件间的通信功能

7.3 控制平台

电子控制单元 ECU

ECU（Electronic Control Unit）**电子控制单元（车载电脑）**。发动机工作时，ECU 采集各传感器的信号，进行运算，并将运算的结果转变为控制信号，控制被控对象的工作。

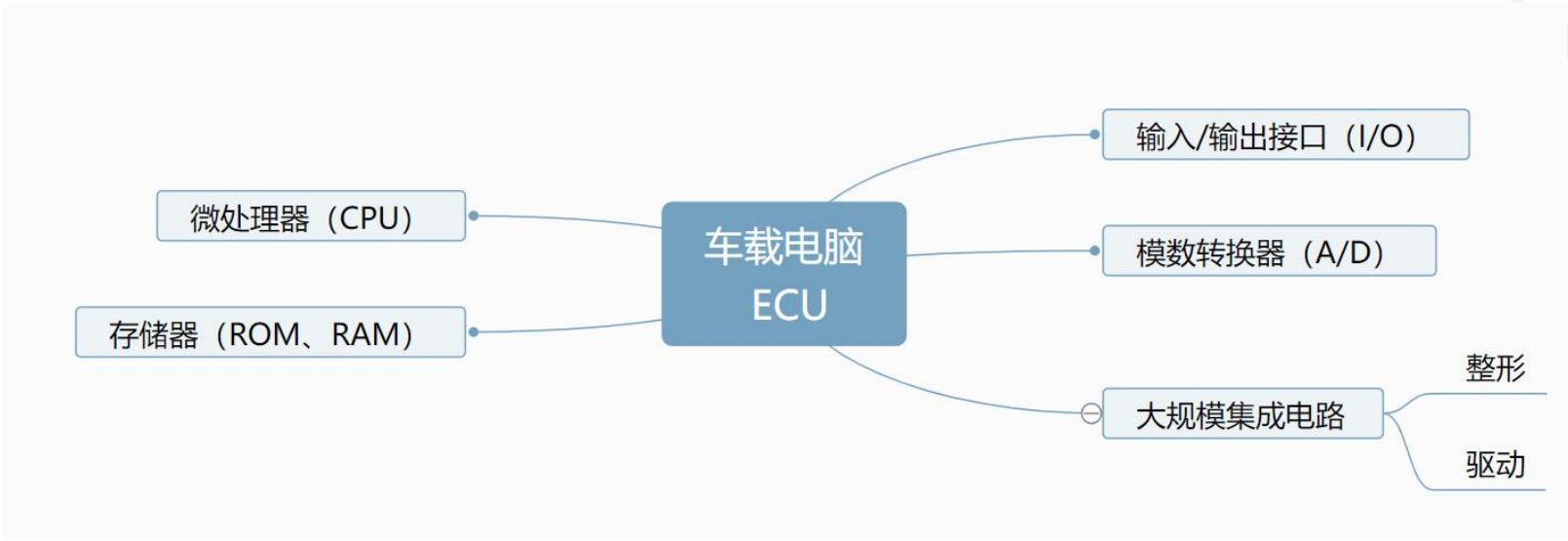
它还有故障自诊断和保护功能。存储器也会不停地记录行驶中的数据，成为 ECU 的学习程序，为适应驾驶习惯提供最佳的控制状态，称为**自适应程序**。

在高级轿车上，有不止一只 ECU。ECU 损坏率非常小。

电压工作范围：6.5-16V； 工作电流：0.015-0.1A；
工作温度：-40~80℃；能承受 1000Hz 以下的振动。

7.3 控制平台

电子控制单元 ECU



存储器 ROM 中储存的是一套固定的程序，该程序是经过精确计算和大量实验取的数据为基础。固有程序在发动机工作时，不断地与采集来的各传感器的信号进行比较和计算，然后输出指令，以控制发动机的点火、空燃比、怠速、废气再循环等多项参数的设置，判断是否需要改变喷油量、点火时间、气门开度的大小等 。

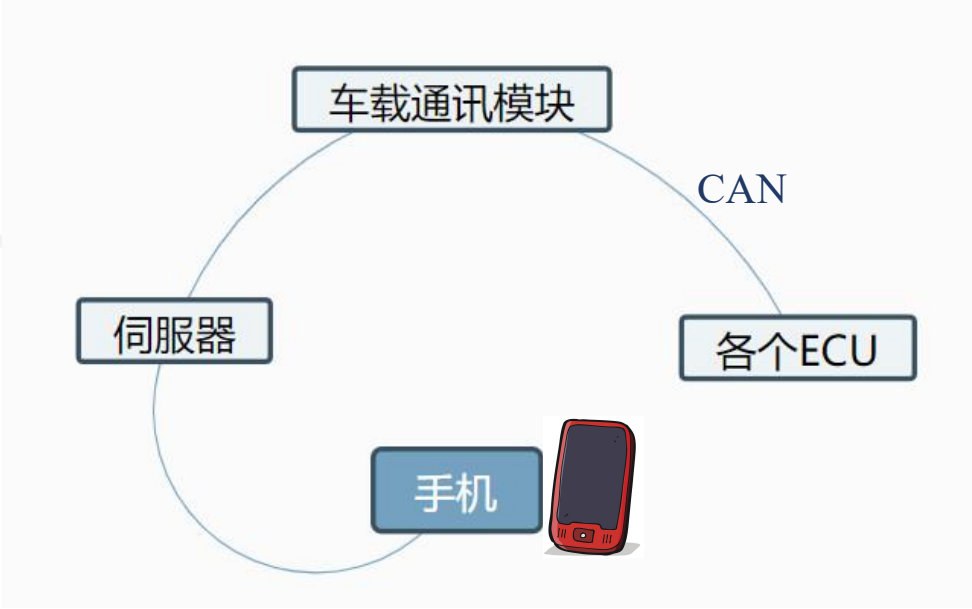
7.3 控制平台

电子控制单元 ECU

随着轿车电子化自动化的提高，ECU 将会日益增多，目前高端汽车在总计100多个 ECU 系统中包含多达200个微处理器。这数百个 ECU，在汽车内部组成了一个区域网。

要让所有的这些 ECU 之间相互配合，就需要采用一种称为**多路复用通信网络协议**进行信息传递，**控制器区域网（Controllers Area Network，CAN）总线**是其中之一。

借助 CAN 协议，汽车内部的数百个 ECU 可以组建一个区域网，有效地解决线路信息传递所带来的复杂化问题。通用、沃尔沃、特斯拉等车型支持**远程控制**。



电子控制单元 ECU

汽车工业还研发出了很多其他协议，比如 **LIN 协议**。相比 CAN，LIN 的带宽要更小，承载的数据量更少，但同时成本也更低，适合应用于一些简单的 ECU 中。

随着技术进步，汽车内部的数据量暴增。更高级的通讯协议问世了，比如 MOST、FlexRay、乙太网等。

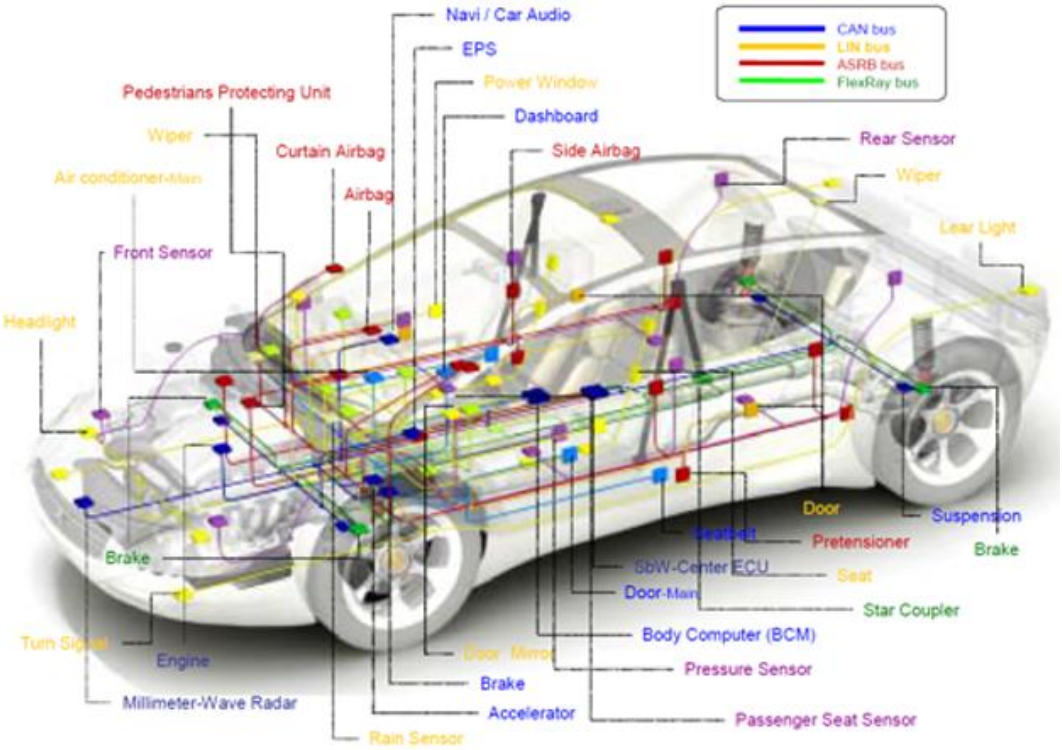
- **MOST** 是一种**高速多媒体传输接口**，专门为汽车内部的一些高码率音频、视频提供传输。
- **FlexRay** 也是一种**高速协议**，但不仅限于多媒体传输。在自动驾驶的奥迪 A7 中，位于后备箱的车载 CPU（奥迪称之为 zFAS）模组，就是依靠 FlexRay 协议来读取前置摄像头捕捉的数据。

7.3 控制平台

通信总线

为了满足各电子系统的实时性要求，要对汽车数据实行共享，因而需要汽车通信总线。

目前，车用总线技术被美国汽车工程师协会 SAE 下属的汽车网络委员会按照协议特性分为 A、B、C、D 四类。



车用通信总线

7.3 控制平台

通信总线

A类总线面向传感器或执行器管理的**低速网络**，它的位传输速率通常小于20Kb/s。A类总线以**LIN**(Local Interconnect Network，本地互联网)规范为代表，主要用于车内分布式电控系统，尤其是面向智能传感器或执行器的数字化通信场合。

B类总线面向独立控制模块间信息共享的**中速网络**，位速一般在10~125 Kb/s。B类总线以**CAN**(Controller Area Network，控制器局域网络)为代表。1993年，ISO正式颁布了道路交通运输工具——数字信息交换——高速通信控制器局域网(CAN)国际标准(ISO11898-1)。

7.3 控制平台

通信总线

C类总线面向闭环实时控制的**多路传输高速网络**，位速率多在125Kb/s~1Mb/s。C类总线主要用于车上动力系统中对通信的实时性要求比较高的场合，主要服务于动力传递系统。

D类总线面向多媒体设备、高速数据流传输的**高性能网络**，位速率一般在2Mb/s 以上，主要用于CD等播放机和液晶显示设备。

低速(IDB-C为代表)、高速(IDB-M为代表)和无线(Bluetooth为代表)

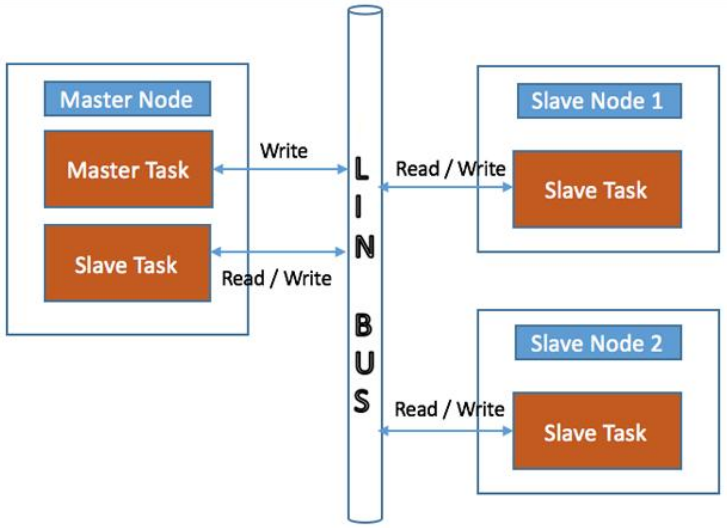
- 局部互联协议 LIN
- 控制器局域网 CAN
- 高速容错网络协议 FlexRay

通信总线——局部互联协议 LIN

局部互联协议 LIN：面向汽车低端分布式应用的低成本低速串行通信总线。

目标：为现有汽车网络提供辅助功能，在不需要 CAN 总线的带宽和多功能的场合使用，降低成本。

节省成本原因：（1）采用单线传输（2）硅片中硬件或软件的低实现成本（3）无需在从属节点中使用石英或陶瓷谐振器



LIN总线信息交换示意图

模式：单个主控制器多个从设备。

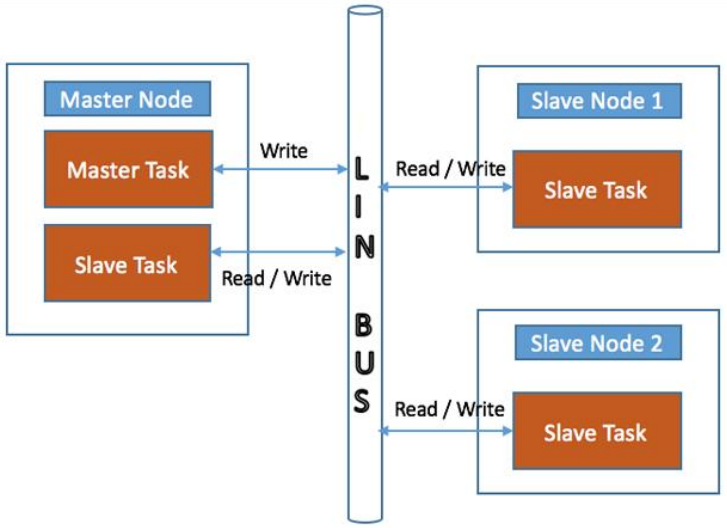
主要应用：电动门窗、座椅调节、灯光照明等控制。以门窗控制为例，在车门上有门锁、车窗玻璃开关、车窗升降电机、操作按钮等。

通过CAN 网关，LIN网络还可以和汽车其他系统进行信息交换。

通信总线——局部互联协议 LIN

局部互联协议 LIN：含**一个宿主节点**（Master）和一个或**多个从属节点**（Slave）。所有节点都包含一个被分解为发送和接收任务的从属通讯任务，而宿主节点还包含一个附加的宿主发送任务。实时LIN中通讯总是由宿主任务发起的。

- 宿主节点发送一个包含同步中断、同步字节和消息识别码的**消息报头**。
- 从属任务在收到和过滤识别码后被激活并开始**消息响应**的传输。
- 报头和响应部分组成一个消息帧。



LIN总线信息交换示意图

主机节点的主机任务发起通讯，确定当前通讯内容，发送帧头并为报文帧分配帧通道。 → 总线上的从机节点接收帧头之后，判断是否做出响应、做出何种响应。

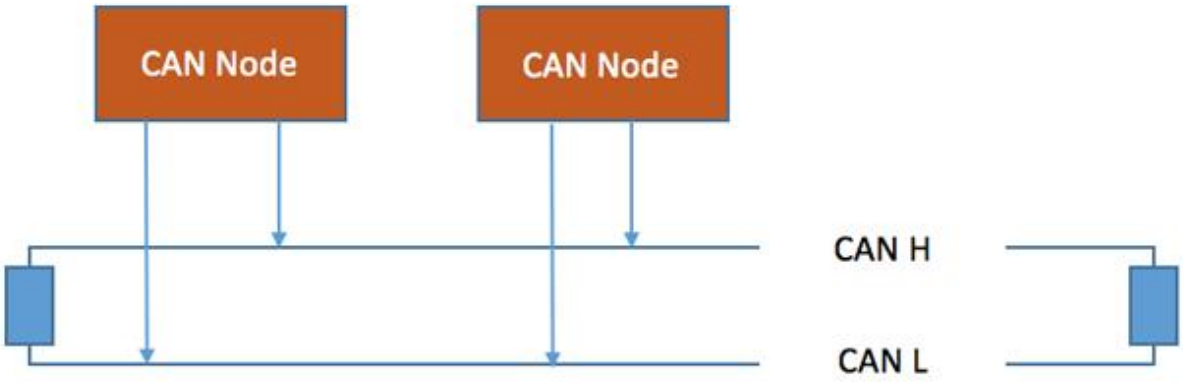
LIN可实现多种数据传输模式，且一个报文帧可以同时被多个节点接收利用

通信总线——控制器局域网 CAN

CAN 总线：占据当前汽车总线网络市场的主导地位，是德国博世公司在20世纪80年代初为了解决现代汽车中众多的控制与测试仪器之间的数据交换问题而开发的一种串行数据通讯协议。

特性：短帧数据结构、非破坏性总线性仲裁技术及灵活的通讯方式适应了汽车的实时性和可靠性要求。

分类：高速 CAN 最高速度为 1Mbps（C 类总线），低速 CAN 为250Kbps（B 类总线）

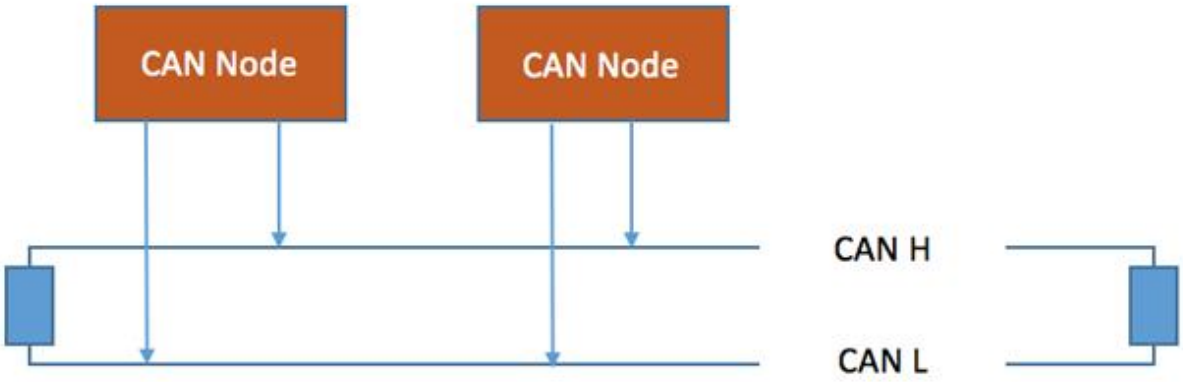


CAN总线结构图

通信总线——控制器局域网 CAN

- CAN 总线一般为**线型结构**，所有节点并联在总线上。
- CAN 总线是采用 **CSMA/CA机制**。

各节点会一直监听总线，发现总线空闲时便开始发送数据。当多个节点同时发送数据时，会通过一套**仲裁机制**竞争总线。每个节点会先发送数据的 ID，ID 越小表示优先级越大，优先级大的会自动覆盖小的 ID。当节点发现自己发送的 ID 被覆盖掉时，便自动停止发送。优先级最高的消息获得总线使用权，开始发送数据。当高优先级的数据包发送完后，各节点便又尝试竞争总线。



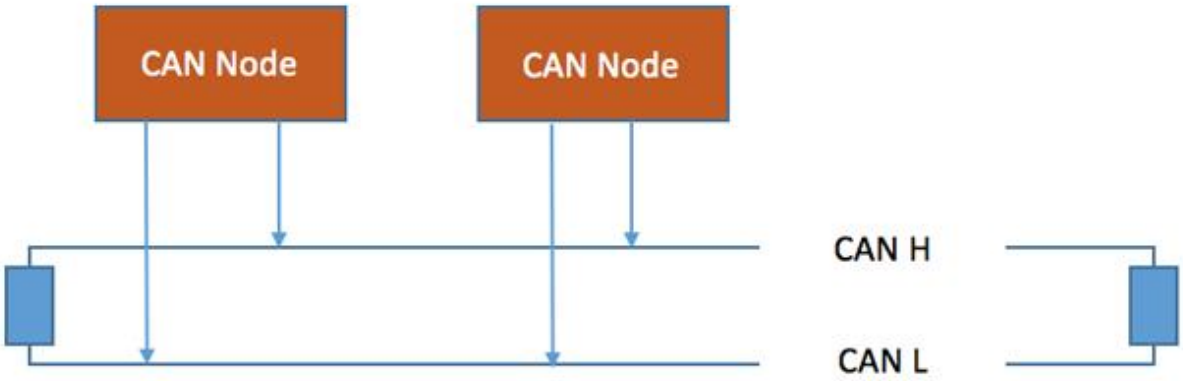
CAN总线结构图

通信总线——控制器局域网 CAN

优势：能最大程度的利用总线。

弊端：有时效延迟，优先级越低的数据包，可能需要等待的时间越长。

数据出错时：节点发现当前发送的数据有误时，会发送错误帧告知总线上的所有节点。发送错误数据的节点会重发。每个节点都有一个错误计数器。当一个节点总是发送或接收错误超过一定次数时，会自动退出总线。



CAN总线结构图

通信总线——高速容错网络协议 FlexRay

FlexRay 总线数据收发采取时间触发和事件触发的方式。

时间触发通信：网络中的各个节点都预先知道彼此将要进行通信的时间，接收器提前知道报文到达的时间，报文在总线上的时间可以预测出来。

优点：FlexRay 协议可以确保即便行车环境恶劣多变，干扰了系统传输，能将信息延迟和抖动降至最低，尽可能保持传输的同步与可预测。

两种周期通信方法： TDMA（Time Division Multiple Access）和 FTDMA（Flexible Time Division Multiple Access）

FlexRay 将一个通信周期分为静态部分、动态部分、网络空闲时间。

静态部分使用 TDMA 方法，每个节点会均匀分配时间片，每个节点只有在属于自己的时间片里面才能发送消息，即使某个节点当前无消息可发，该时间片依然会保留。

动态部分使用 FTDMA 方法，会轮流问询每个节点有没有消息要发，有就发，没有就跳过。

通信总线——高速容错网络协议 FlexRay

静态部分用于发送需要经常性发送的重要性高的数据

动态部分用于发送使用频率不确定、相对不重要的数据

当 FlexRay 总线通信过程中出现数据错误时，该周期里接收到的所有数据都会被丢弃掉，但没有重发机制。所有节点会继续进行下一个周期的通信。FlexRay 同样也有错误计数器，当一个节点发送接收错误过多时会被踢出总线。

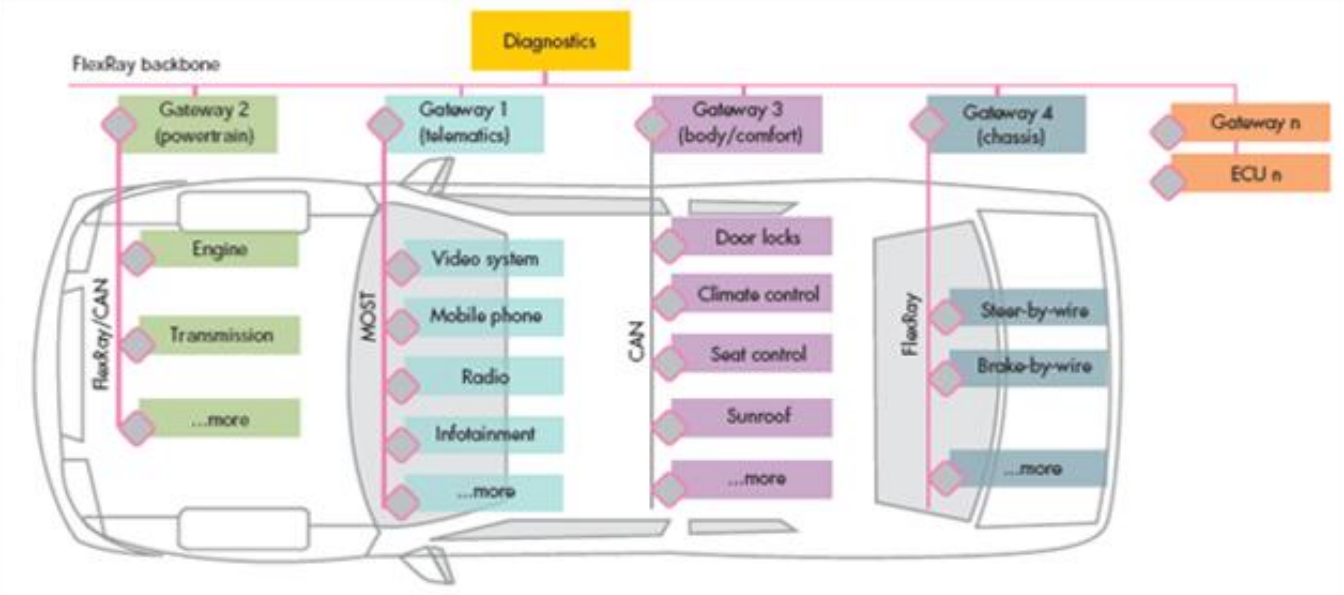
具有高速、可靠及安全的特点

- FlexRay 具备的冗余通信能力可实现通过硬件完全复制网络配置，并进行进度监测。
- FlexRay 同时提供灵活的配置，可支持各种拓扑，如总线、星型和混合拓扑。
- FlexRay 本身不能确保系统安全，但具备大量功能，可以支持以安全为导向的系统的设计。

通信总线——高速容错网络协议 FlexRay

宝马公司在07款 X5 系列车型的电子控制减震器系统中首次应用了 FlexRay 技术。

采用基于飞思卡尔的微控制器和恩智浦的收发器，可以监视有关车辆速度、纵向和横向加速度、方向盘角度、车身和轮胎加速度及行驶高度的数据，实现了更好的乘坐舒适性以及驾驶时的安全性和高速响应性，此外还将施加给轮胎的负荷变动以及底盘的振动均减至最小。



FlexRay总线分布图

第七章：无人驾驶的平台介绍和系统安全

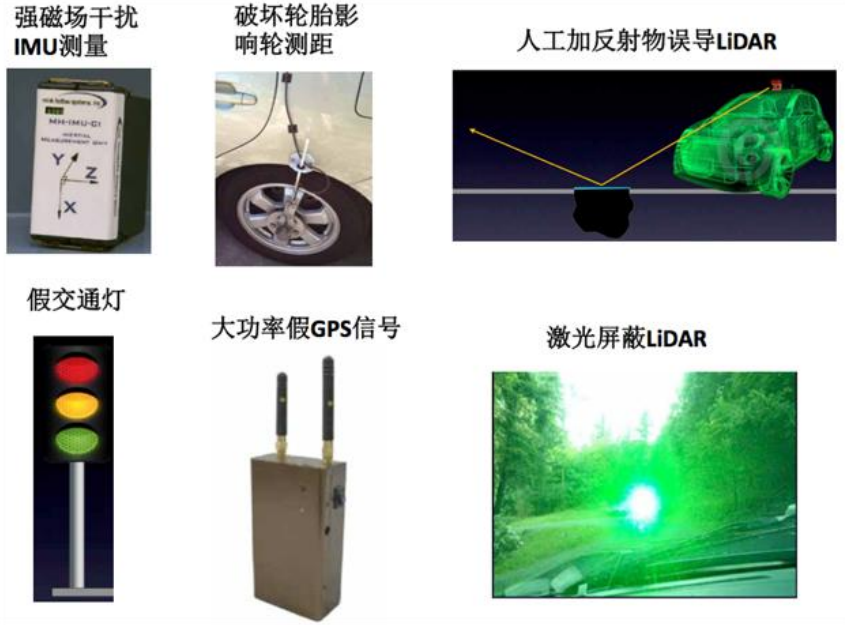
本章目录 CONTENT

无人驾驶系统安全

- 首先，针对**传感器**的攻击不需要进入无人驾驶系统内部，这种外部攻击法技术门槛相当低，既简单又直接。
- 第二，如果进入**无人驾驶操作系统**，黑客可以造成系统崩溃导致停车，也可以窃取车辆敏感信息。
- 第三，如果进入**无人驾驶控制系统**，黑客可以直接操控机械部件，劫持无人车去伤人，是极其危险的。
- 第四，车联网连接不同的无人车，以及中央云平台系统，劫持**车联网通信系统**也可以造成无人车间的沟通混乱。

7.4 无人驾驶传感器的安全

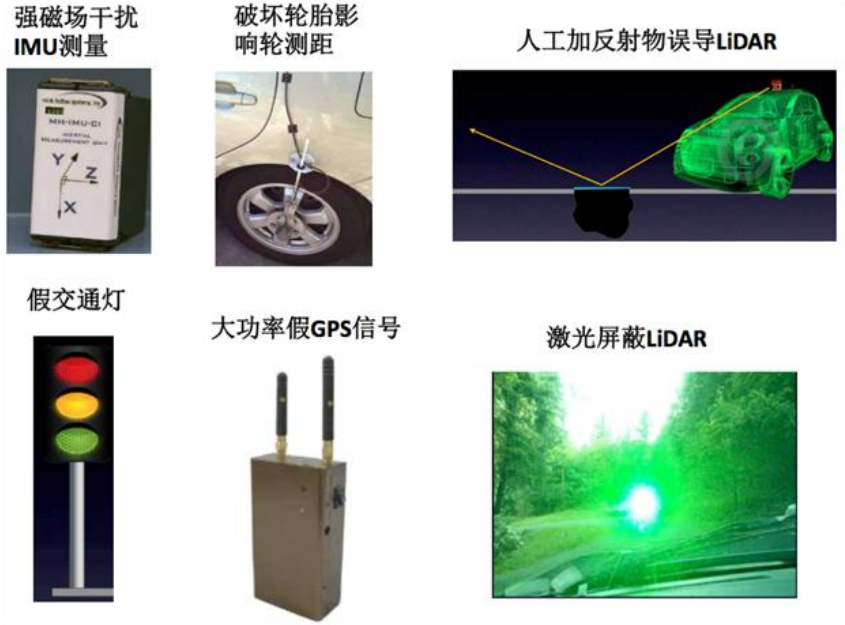
- **惯性传感器 IMU：** IMU辅助无人驾驶定位，但 IMU 对磁场很敏感，如果使用强磁场干扰 IMU，就有可能影响 IMU 的测量。
- **GPS：**如果在无人车附近设置大功率假 GPS 信号，就可以覆盖原来的真 GPS 信号，从而误导无人车定位。
- **轮测距技术：**辅助无人车定位，轮测距是通过测量轮子的转速乘与轮子的周长进行测距，如果黑客破坏了轮子，这个定位辅助技术也会受影响。



针对传感器的攻击示意图

7.4 无人驾驶传感器的安全

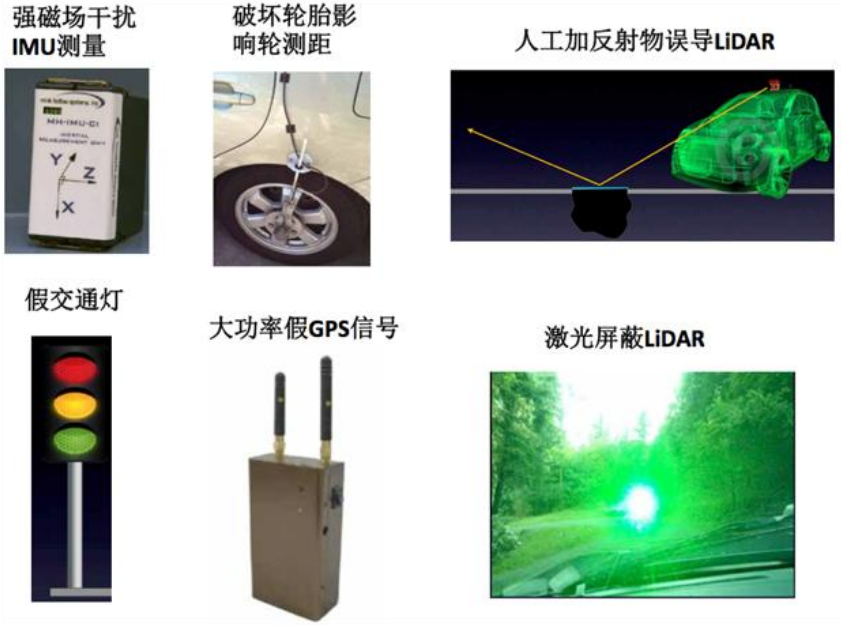
- **激光雷达：**无人车依赖于激光雷达数据与高精地图的匹配进行定位。但激光雷达也可以轻易地被干扰。（1）激光雷达是通过测量激光反射时间来计算深度的。如果在无人车周围放置**强反光物**，比如镜子，那么激光雷达的测量就会被干扰，返回错误信息。（2）如果黑客使用**激光照射**激光雷达，测量也会受干扰。（3）无人车会不断下载更新的高精地图，如果黑客把下载的**地图调包**，也会造成定位失效。



针对传感器的攻击示意图

7.4 无人驾驶传感器的安全

- **计算机视觉：**可以辅助无人车完成许多感知的任务。在交通灯识别的场景中，无人车上的摄像机如果检测到红灯，就会停下来。如果检测到行人，也会停下以免发生意外。黑客可以轻易地在路上放置假的红绿灯以及假的行人，迫使无人车停车并对其进行攻击。



针对传感器的攻击示意图

7.4 无人驾驶传感器的安全

既然每个传感器都可以轻易被攻击，如何保证无人车安全?

使用多传感器融合技术互相纠正。攻击单个传感器很容易，但是如果同时攻击所有传感器难度相当大。当无人车发现不同传感器的数据相互间不一致，就知道自己可能正在被攻击。

例如，无人车检查到交通灯，但是高精地图在此处并未标注有交通灯，那么就很可能是被攻击了。又例如 GPS 系统与激光雷达系统定位的位置极不一致，无人车也很可能是被攻击了。

第七章：无人驾驶的平台介绍和系统安全

本章目录 CONTENT

7.5 无人驾驶操作系统的安全

ROS 本身安全性有一定问题，总结有以下两种攻击方法：

（1）其中一个 **ROS 节点被劫持**，然后不断地进行分配内存，导致其系统内存消耗殆尽，造成系统 OOM 而开始关闭不同的 ROS 节点进程，造成整个无人驾驶系统崩溃。

原因：ROS 节点本身是一个进程，可以无节制分配资源导致崩溃，另一个原因是 ROS 节点可以访问磁盘以及网络资源，并无很好的隔离机制。

解决方案：可以使用**容器技术（Linux containers，LXC）**来管理每一个 ROS 节点进程，限制每一个节点可供使用的资源数。并采用**沙盒的方式**以确保节点的运行独立，这样以来可最大限度地防止资源泄露。

7.5 无人驾驶操作系统的安全

（2）**ROS 的话题（topic）或服务（service）被劫持**，导致 ROS 节点之间传递的信息被伪造，从而导致无人驾驶系统的异常行为。

原因：通信的信息没有被加密，以至于攻击者可以轻易得知通信内容。

解决方案：目前业界有不少对 ROS 节点间通信的加密尝试，比如使用 DES 加密算法。

缺点：在通信的信息量十分小的时候，加密与否对性能影响不大。但随着信息量变大，加密时间相对信息量成几何级增长。另外，由于 ROS 通信系统的设计缺陷，加密时间也与接收信息的节点数量有直接关系。当接受信息的节点数量增长时，加密时间也随之增长。

第七章：无人驾驶的平台介绍和系统安全

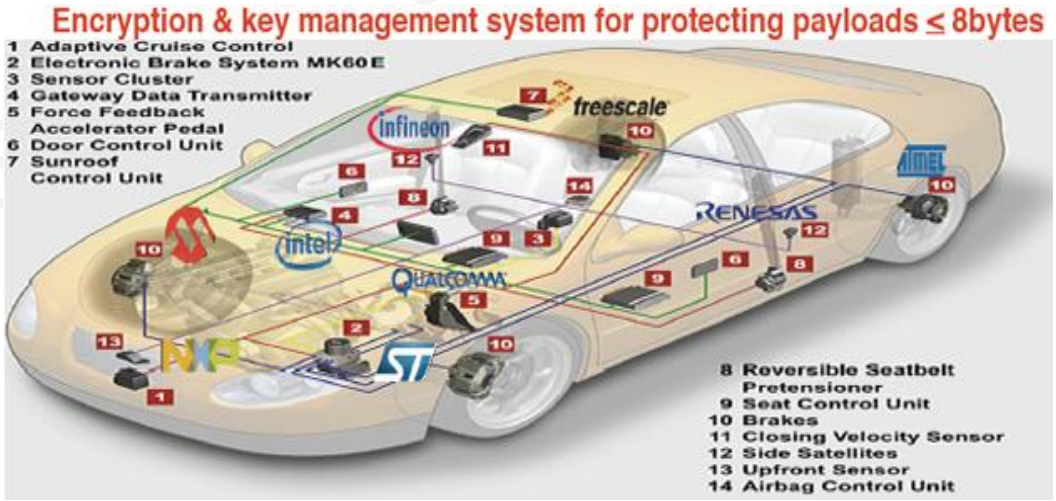
本章目录 CONTENT

7.6 无人驾驶控制系统的安全

车辆的CAN**总线**连接着车内的所有机械以及电子控制部件，是车辆的中枢神经。

CAN 总线特点：布线简单、典型总线型结构、可最大限度节约布线与维护成本、稳定可靠、实时、抗干扰能力强、传输距离远等。

CAN 总线采用**差分信号**传输，通常情况下只需要两根信号线（CAN-H 和 CAN-L）就可以进行正常的通信。在干扰比较强的场合，还需要用到屏蔽地即CAN-G（主要功能是屏蔽干扰信号）。



CAN总线安全

7.6 无人驾驶控制系统的安全

黑客进入 CAN 的攻击方式包括以下几点。

（1）**OBD-II 入侵：**OBD-II 端口主要用于检测车辆状态，通常在车辆进行检修时，技术人员会使用每个车厂开发的检测软件接入 OBD-II 端口并对汽车进行检测。由于 OBD-II 连接到 CAN 总线，只要黑客取得检测软件，便能轻易截取车辆信息。

（2）**电动车充电器入侵：**电动车的充电装置在充电时会与外部充电桩通信，而且电动车的充电装置会连接 CAN 总线，这就给了黑客们通过外部充电桩入侵 CAN 系统的机会。

（3）**车载 CD 机入侵：**攻击代码编码到音乐 CD 中，当用户播放 CD 时，恶意攻击代码便会通过 CD 播放机侵入 CAN 总线，从而可以取得总线控制以及盗取车辆核心信息。

（4）**蓝牙入侵：**用户可以通过蓝牙给 CAN 发送信息以及从 CAN 读取信息，这也给黑客们攻击的窗口。除了取得车主手机的控制权，黑客们也可以使用蓝牙进行远程攻击。

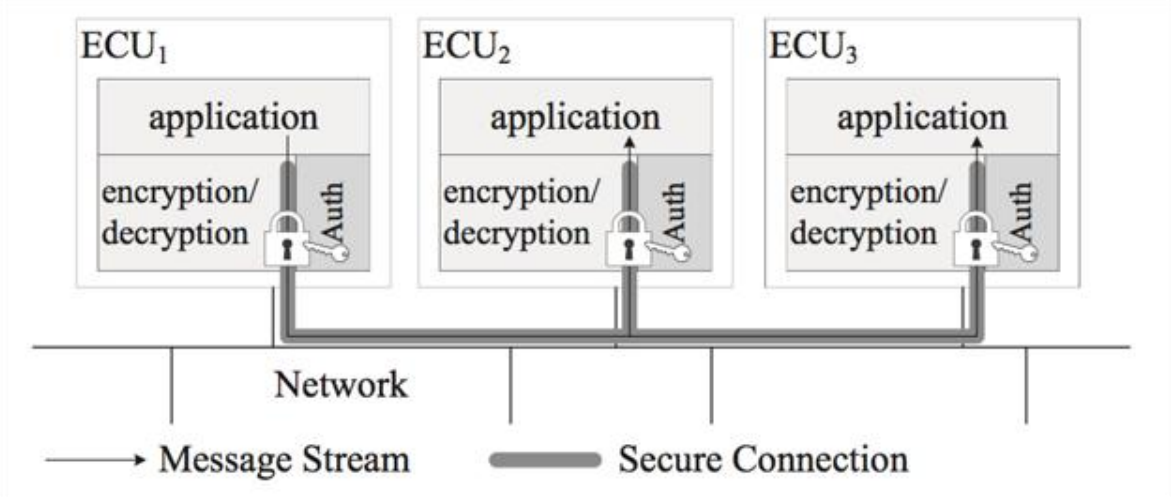
（5）**TPMS 入侵：**TPMS 是车轮压力管理系统。黑客先把攻击代码放置在车辆 TPMS ECU中，当 TPMS 检测到某个胎压值的时候，恶意代码便会被激活，从而对车辆进行攻击。

7.6 无人驾驶控制系统的安全

解决方法：对 ECU 接收的信息进行**加密验证**，以保证信息是由可信的 ECU，而不是由黑客发出。

使用加密验证可以选择**对称**或者**非对称密码**。对称密码的计算量小但是需要通信双方预先知道密码。非对称密码无需预先知道密码，但是计算量大。

由于大部分车的 ECU 计算能力与内存有限，现在通用做法是使用对称密码加密，然后密钥在生产过程中被写入 ECU。



*ECU*安全加密系统组成

7.6 无人驾驶控制系统的安全

为了解决这个问题，学术界和业界也提出了几种解决方案：

- TLS 安全协议沿用非对称密码的算法对通信双方进行验证。
- Kerberos 是一个通用的基于对称密码算法的验证平台。
- TESLA 安全协议提出了使用对称密码机制去模拟非对称密码的做法，从而达到既安全又能降低计算量的目的。
- LASAN 安全协议使用两步验证的机制实时让通信双方交换密钥，然后使用对称密码的算法对信息进行验证。

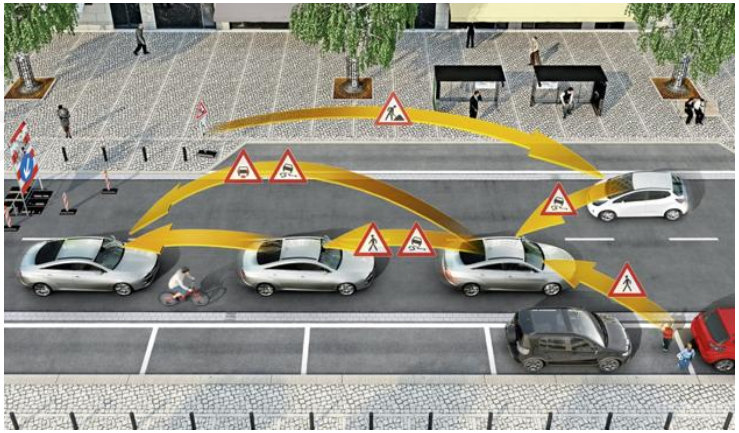
第七章：无人驾驶的平台介绍和系统安全

本章目录 CONTENT

7.7 车联网通信系统的安全性

当无人车上路后，它会成为车联网的一部分，**V2X** 是车联网通信机制的总称。V2X 是泛指各种车辆通讯的情景，包括 **V2V 车车通讯、V2I 车路通讯、V2P 车与路人通讯**等。通过 V2X 车辆可以获得实时路况、道路、行人等一系列交通信息，从而带来远距离环境信号。

比如 V2V，最普遍的应用场景是在城市街道、高速公路，车辆之间可以相互通信，发送数据，实现信息的共享。



车联网V2X系统示意图

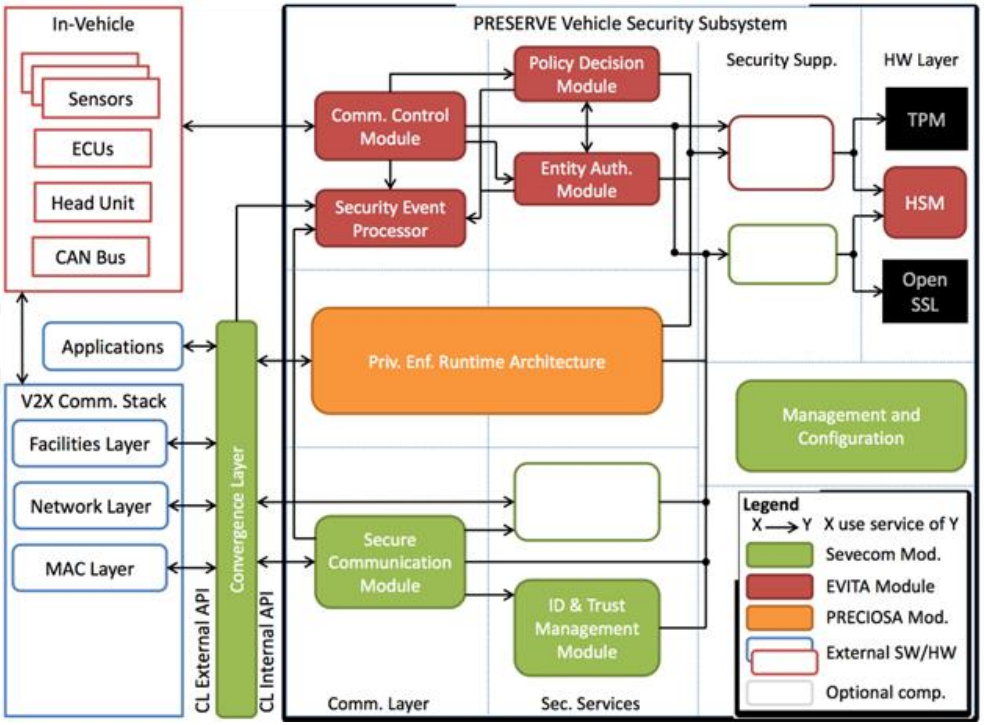
将车辆的时速、相对位置、刹车、直行还是拐弯等数据提前提供给周围车辆

7.7 车联网通信系统的安全性

（1）确认消息来自合法的发送设备，这个需要通过**验证安全证书**来保证。

（2）确认消息传输过程中没有被修改，这个需要接受信息后计算**信息的完整性。**

为了实现 V2X 的安全，欧盟发起了 V2X **安全研究项目 PRESERVE** 并在项目中提出了符合 V2X 安全标准的硬件、软件，以及安全证书架构。



PRESERVE系统架构图

7.7 车联网通信系统的安全性

安全研究项目 PRESERVE

（1）**硬件：**在每个车辆中存储了大量密钥，如果使用普通的 Flash 与 RAM，密钥会被轻易盗取。另外，使用加密解密技术会对计算资源消耗极大。为了解决这些问题，PRESEVER 提出了设计**安全存储硬件**，以及使用 **ASIC 硬件加速加解密。**

（2）**软件：**在安全硬件上，PRESEVER 提供了**一整套开源软件栈提供安全通信。**这套软件栈提供了加密解密的软件库、电子证书认证库、与受信任的证书颁发机构的安全通信库等。

（3）**安全证书：**为了确保信息来源于可信设备，可以使用**受信任的证书颁发机构**来提供安全证书与密钥。

谢谢！

THANK YOU FOR LISTENING