



# Apollo Pilot Safety Report



# Our Vision

## Apollo Pilot愿景： 让驾驶更安全

Apollo Pilot是Apollo平台专门针对量产所设计的自动驾驶产品总称。基于大数据的不断训练，Apollo Pilot希望通过更全面的感知、更安全的驾驶规则，来降低人类驾驶员在枯燥和易错场景下的疲惫感，进一步避免人类驾驶的低级错误。Apollo Pilot旨在提升整个出行过程的安全性，让自动驾驶比人类驾驶的事故率降低一个数量级或更多。

为了实现这个愿景，短期内我们的目标是：

- 打造一个安全、可量产的自动驾驶解决方案，以提升用户在特定场景下的出行安全。
- 让主流汽车消费者更早享用到自动驾驶技术所带来的安全与便利，并逐步改善当前的驾驶环境和出行体验。

# The First L3 Automated Driving Solution in China

中国首个L3级自动驾驶产品

Apollo Pilot for Passenger Car

Apollo Pilot for Passenger Car产品定义(参考SAE-L3): 提供有驾驶员的车辆在限定场景下的自动驾驶系统; 根据系统请求, 驾驶员需做出适当的响应, 系统将会至少提前10秒钟发出请求, 以便给驾驶员保留安全响应时间。

我们这样定义这款产品, 主要是基于安全方面的考虑。现在市面上存在的“自动驾驶”产品, 都要求用户时刻保持接管能力, 并在用户未接管时发生事故后将责任甩给用户, 这样反而比用户自己驾驶的精神集中度要求更高, 更容易诱发疲劳驾驶等不安全因素。因此Apollo Pilot for Passenger Car (后续简称“APC”) 将通过对可适用场景Operational Design Domain (后续简称“ODD”) 的明确定义, 确保在ODD范围内的自动驾驶完全自适应驾驶能力, 并且在即将超出ODD边界时给用户预留至少10秒钟的接管时间, 来让用户在有需要的场景下真正享用到一个安全的自动驾驶服务。



市面上产品 (随时要求接管)

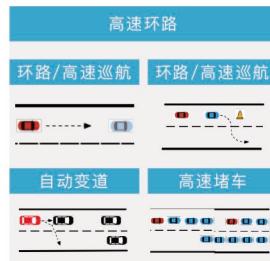


APC (给用户预留至少10秒接管时间)

# Key Functions

APC在2020年量产上市时，将优先适用这三个最高频场景

APC将在这三个场景下具有高度安全的自动驾驶安全能力：



高速自动驾驶系统：高速公路事故是致死率最高的交通事故类型之一，在中国高速单起事故死亡率为77%。为了提高高速行驶的安全性，我们设计了APC的高速自动驾驶系统。它可以在高速和城市环路上实现自动驾驶功能，将对车辆进行加速减速、车道保持和自主变道等控制，解决用户在高速上的疲劳驾驶和环境监控上的安全隐患，大幅降低高速事故率。



城市交通拥堵辅助系统：城市交通拥堵辅助系统通过堵车场景中自动驾驶系统的启用降低追尾风险，并帮助用户解决跟车注意力高度紧张带来的疲劳感，降低了潜在事故发生的风险。同时针对中国特殊的夹塞等路况做针对性训练，确保跟车的安全和舒适。



自动泊车系统：中国停车位相对空间狭小容易剐蹭，因此停车也是人类驾驶风险较高的一个场景。为此我们设计了自主泊车系统，用户可以在停车场入口让车辆自主泊车或者召唤车辆到身边，全程由APC自动驾驶，极大简化停车取车过程，不仅安全而且节约时间。

# Safety Framework

## 自动驾驶整体安全框架

为了实现我们所期望的自动驾驶安全能力，我们设计了覆盖整个自动驾驶环节的安全框架：



在这个安全框架里，我们秉持“正确的驾驶习惯是最好的安全”的理念。我们认为好的习惯胜过任何安全设计，并且会在在安全认知、安全预防、安全驾驶策略等前置环节做更多的安全引导，让用户形成正确的使用习惯。

下面我们会从安全设计和安全运行2个大方面分为7个章节进行APC的安全报告。

# Contents

## 目录

## 01 安全设计

第一次亲密接触 – 操作安全	06	融入当前社会的少数派 – 环境安全	13
1.1 HMI系统	07	2.1 环境建模系统	15
1.2 接管机制	11	2.2 EMI系统	19
		2.3 DPS系统	22
		2.4 Mobileye RSS模型	25

---

经验老到的国宾司机 – 行为安全	30	站在巨人的肩膀上 – 功能安全	41
3.1 ADS自动驾驶场景库	33	4.1 安全流程	43
3.2 DPS策略库	36	4.2 功能安全设计	44
3.3 监控和诊断系统	38	4.3 预期功能安全	46
3.4 危险应对能力	39		

## 02 安全运行

---

完整严格的质量保证 – 质量安全	47	行驶的里程越多越安全 – 安全进化	53
5.1 充分测试	48	6.1 安全问题发现机制	54
5.2 信息安全	50	6.2 OTA系统	55

---

承担社会责任和事故处理机制 – 机制安全	57
7.1 法律法规建设	58
7.2 保障机制建设	59
7.3 黑匣子和远程协助	60

# Chapter 1

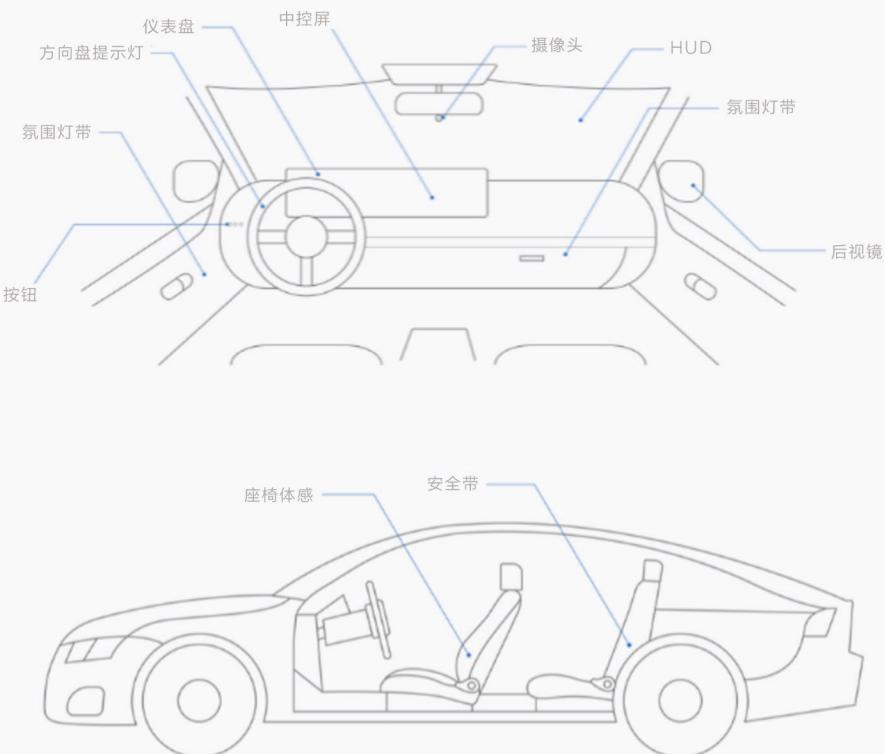
# Operational Safety

## 第一次亲密接触—操作安全

APC计划于2020年在中国的多家车厂的主流经济车型上大规模上市，这将会是很多用户第一次接触到L3级别的自动驾驶。为了帮助用户更好的和自动驾驶系统进行配合，我们将确保用户能够非常明确了解自动驾驶的行为能力和边界，知道什么情况下使用自动驾驶可以帮助自己，什么情况下车辆会请求驾驶员接管，什么环境下启用自动驾驶会存在安全风险，在自动驾驶的过程不能做哪些可能影响自己安全的危险行为如睡觉等，通过安全的操作，APC自动驾驶将真正帮助到用户，这也是我们认为能实现自动驾驶最安全有效的途径。

## Section 1.1 HMI（人机交互）系统

伴随着自动驾驶的到来，许多传统人机交互方式将被替换，语音交互、人脸识别等更多高科技的交互模式会被引入，机器与人类的交互方式将变得越来越自然。更自然的人机交互意味着更高效直接的沟通，在与复杂系统，如自动驾驶汽车合作时这些变化是有正向收益的。对于APC，我们定义一辆自动驾驶汽车HMI的核心理念是“自然，安全”。APC的HMI由共享全画面屏、环绕氛围灯、智能方向盘和体感座椅等组成，多感官提示将为驾驶员带来更沉浸的交互体验。



中控上的共享全面屏将是乘客们获取系统信息的主要媒介。为了保障乘客安全，除车辆基本信息区外，共享全面屏上还将在突出位置显示自动驾驶重要提示和警示通知等。除屏幕外，环绕氛围灯将根据自动驾驶系统状态通过颜色变化给乘客带来更全面的视觉交互，保证不错过任何重要信息。声音上的互动设计也体现出了“自然”这一理念。在系统状态变换时，乘客将收听到必要的语音提示。不仅如此，驾驶员还可通过语言与系统直接互动，完成状态查询，状态切换等操作，与传统人机交互相比极大缓解了乘客注意力过度分散等问题。在视觉与听觉的刺激之外，APC的HMI系统还将触觉交互融入进来，在必要条件下智能方向盘和座椅将通过震动等方式确保接管安全提示及时的传达给乘客。

- A 危险警示灯
- B 灯光状态区
- C 速度显示区
- D 危险警示灯2
- E 自定义显示区
- F 基本信息区
- G 自定驾驶状态区
- H 自动驾驶消息通知



- H 虚拟道路场景显示
- I 基本信息区2
- J 自定义显示区2
- K 自动驾驶状态+设置
- L 自动驾驶重要提示
- M 道路实景展示区



用户在接触自动驾驶HMI时将会经历两个阶段：探索期和成熟期

探索期：自动驾驶系统是一套精密的系统，此类系统普遍对用户操作规范有较高要求。APC的产品使用手册中涵盖了用户想要了解的产品信息，然而仅仅寄希望于用户对手册的阅读和掌握是不安全的。为了确保用户准确理解自动驾驶系统，在初次接触自动驾驶时Apollo Pilot会以多种形式向用户传递重要信息。举个例子，HMI系统会提前推送小贴士，将自动驾驶的核心信息（开启、接管、限制、警示信号源等）自然的教育给用户，让懒得看说明书的用户逐步的充分认知自动驾驶系统。同时APC会默认使用偏保守的驾驶策略，让用户首先建立对自动驾驶的安全信任感，直到用户熟悉后去自行调整设置成更合适自己的驾驶策略。



目标：建立信任，提供安全感

主动反馈，易见性、一致性、易懂、随时帮助，随时接管

成熟期：减少第一阶段的新手提示，加强更多的预先信息提示（路况、路型）和ODD边界（道路范围、天气光照、切入和变道、跟车等）教育提示。基于百度高精数据服务平台Intelligent Map的预先感知和交通大数据的生态感知，APC可以做到精准的预先提示，实时感知的输出将通过HMI传递给用户，帮助用户更好的掌控系统和建立自动驾驶信任感。



目标：轻松自在、享受驾驶

## Section 1.2 接管机制

受限于目前的硬件计算能力，当前阶段的APC还只能在经过大量训练和测试的限定操作环境(ODD)内自动驾驶，因此在超出ODD边界时需要用户接管。

我们在设计接管系统时，不仅考虑在需要的时候用户如何安全的实现接管，更多的考虑是如何让用户使用起来尽量不会不断的在需要接管和不需要接管的状态之间切换，而是由系统进行大量的自动处理，包括实时的监控、诊断、暂时的降级运行等，目标是在自动驾驶场景下的95%以上的时间里，都不会对用户做接管准备的强制要求，真正做到用户安全放松的驾驶体验。

在能够预判的超出ODD边界情况下，比如逐渐变大的中雨到大雨天气、距离驶出高速还有1公里、前方车辆回传告知断路修路等常见的情况会覆盖到大部分超出ODD边界的需要接管情景，我们会预先多次提醒用户，给用户预留出从容的接管时间，保证安全。

在遇到非预判类的超出ODD接管时，我们的系统将会自动进行安全操作，包括减速刹车到安全区域、在当前车道安全刹停、以及保证安全的紧急AEB制动。在停车后，会通过双闪、喇叭、自动联系客服中心、警务中心等措施来保证车上人员安全。

另外，为了实际践行我们的安全愿景，APC还专门设计了“特别关怀安全停车”功能，当自动驾驶系统遇到人员状态异常时，例如驾驶员因为睡着或者突发身体原因对预留的10秒时间的接管请求一直无响应，APC在保证安全刹停之外，如果检测到环境和车辆状态都允许，会主动超越系统对自己的仅需保证10秒安全的义务，一直持续的自动行驶寻找可停泊的安全区域例如临时停车岛或者足够宽敞的应急车道停下来，尽自己的最大努力保证车上人员的安全。



## Chapter 2

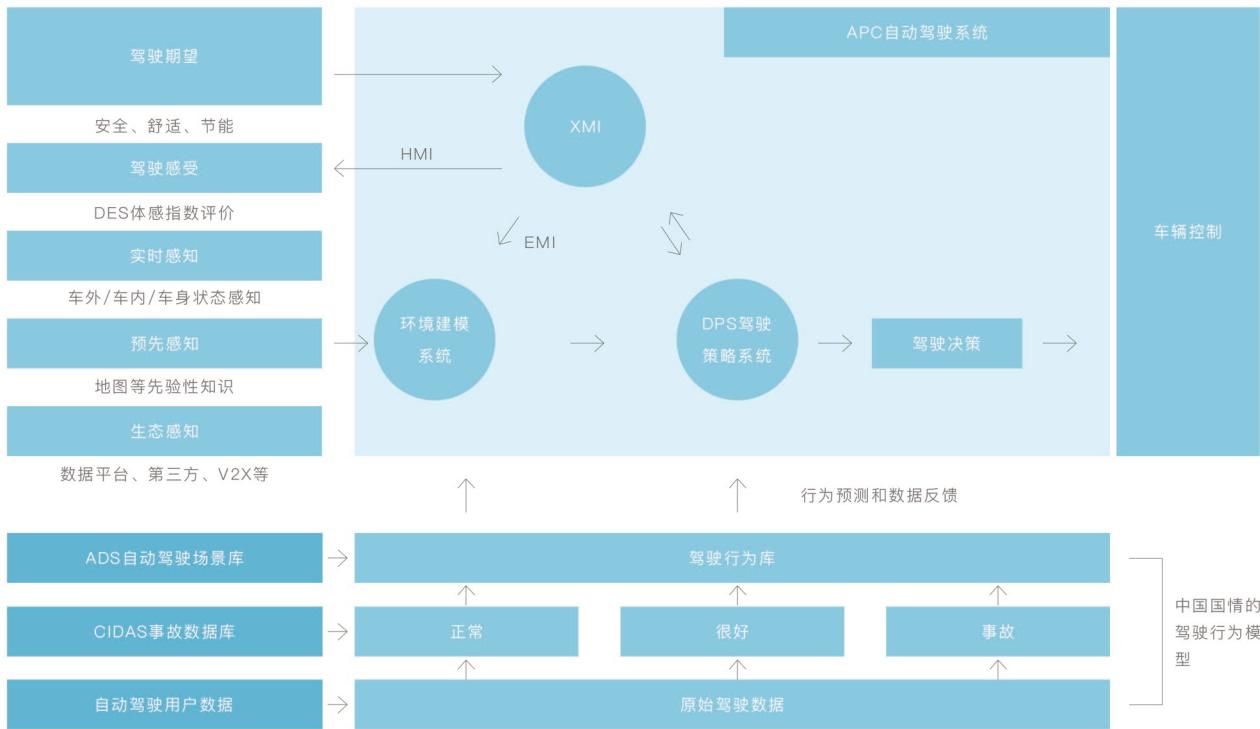
# Environmental Safety

## 融入当前环境的少数派 —环境安全

在2020年搭载了Apollo Pilot的自动驾驶车辆开始上路运行之后，自动驾驶车辆相对数量庞大的人类驾驶车辆，还是一个少数派，只有让自动驾驶车辆自然融入到这个现实的车辆行驶环境中，而不是表现的象一个异类，才能做到真正的自动驾驶车辆和人类驾驶车辆的双重安全。

这个融入表现在两方面，一方面是自动驾驶车辆自身的行为要表现的适应现实驾车环境，另一方面是能让人类驾驶员对自动驾驶车辆的行为做出很好的掌握和预判，这样才能保证双方的安全。

为了达到这个目标，我们设计了三大系统，来保证自动驾驶车辆能对自身所处的静态环境和动态有清晰明确的认知，能和环境进行输入输出的双向交互，并有基于实时环境信息的全面的可解释的驾驶行为规则。



## Section 2.1

# 环境建模系统

要做到“融入环境”，自动驾驶车辆自身需要先理解周边环境来作出合理的驾驶行为。为了在复杂的环境中进行非常安全的汽车驾驶的工作，我们设计了环境建模模块。环境建模通过对多种感知和识别技术的融合，让汽车能够清晰的对当所行驶的环境有一个完整准确的认知。环境模型的输入可以简单被分为三大类，分别是实时感知、预先感知、和生态感知。



为了尽可能全面的做到实时感知，在我们的量产方案中配置了光学、声学、惯导等多种传感器。其中，9个视觉高清摄像头分布在车身外部，以实现360度全方位监控。在前向我们一共安置了3种焦距的视觉传感器，用来感知不同车距上的障碍和车道信息。此外，车内还配置了1个驾驶员监控摄像头，它将在自动驾驶的行为安全中发挥重要作用。

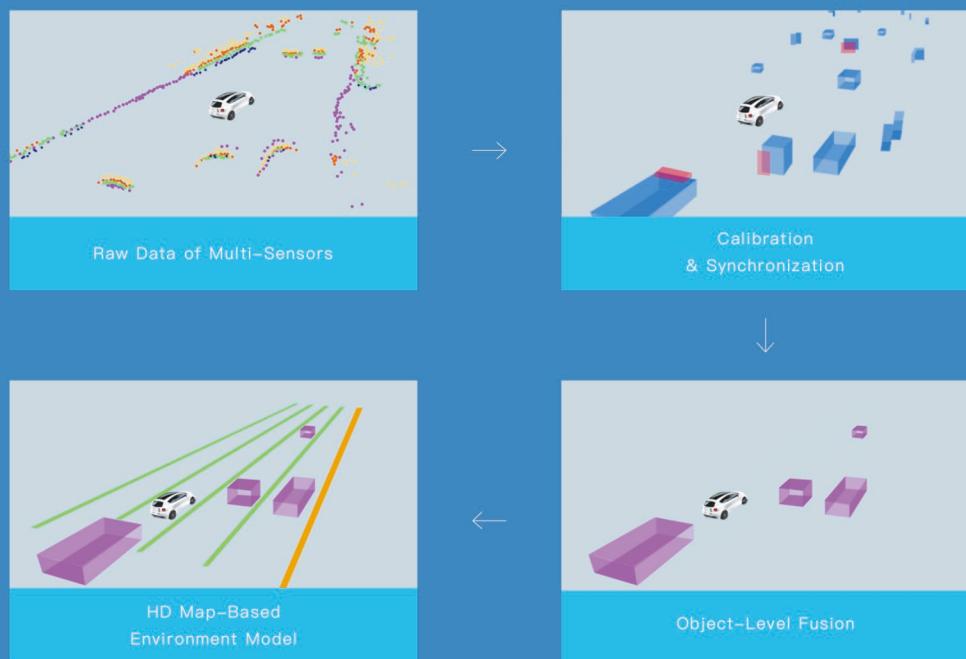
除视觉传感器外，4个毫米波雷达分别以超过10Hz的频率实时检测前向、侧前向和后向物体的运动状态。与视觉传感器相比，毫米波雷达可以提供更精确的物体位置和速度信息，完成传感器性能间的互补。相较于这两种传感器，超声波雷达已经在汽车量产方案中普及，APC应用了12个超声波传感器全向监听5米范围内物体的靠近，做到避让或刹车。

这三类传感器搭配惯导定位等硬件组成了APC的实时传感器系统。

我们选择量产方案的传感器布局时主要基于两个角度考虑。第一是安全需求，我们通过对市面上正在售卖的比较典型的某两个“自动驾驶”车辆的对比测试以及考虑到APC所设计的比这两个产品更多更复杂的使用场景和功能，采用了更加全面的360度的实时传感器方案。

举例来说，相比这两辆车我们增加了后向的长距毫米波雷达，以及前向的两个毫米波角雷达，来配合做视觉识别的摄像头，更加完善的解决目前他们在中国道路上表现较差易出事故的两个典型场景：车辆变道和车辆切入的安全性。

第二个考虑是实际的量产安全要求，比如现在很多自动驾驶DEMO车辆上使用的激光雷达型号，还达不到车规级的安全要求，并不能做到用于主流量产车型上给广大普通用户使用。而我们选用的自动驾驶硬件均为成熟可靠的达到ASIL-D安全认证标准的型号。



除了目前大家直接能看到的车上的实时的传感器外，APC的自动驾驶方案还用到了另外两种在业界最先进也是代表自动驾驶技术未来方向的感知系统，我们把他叫做预先感知系统和生态感知系统。

预先感知系统的表现形式是高精地图。通过事先采集的达到厘米级别精度的高精地图，APC可以让自动驾驶汽车“看”得更远，远超目前实时感知系统几百米的感知范围，这样就可以在自动驾驶的过程中极大的增加安全性。举个例子，通过高精地图，我们可以预先知道在我们当前行驶的道路的1公里外会有一个右侧的并入匝道，是一个多车道大流量的高速入口，那么自动驾驶系统就可以预先的切换到最内侧道路行驶，并且在通过匝道之前做好其他车辆切入的准备工作比如进行适当的降速等操作来最大降低出事故的概率。

再比如当我们在城市环路上行驶时，经常会遇到车道线磨损比较严重的路段，在这种路段单纯依靠实时感知的自动驾驶系统，会造成车辆的行驶过程中需要不断实时调整会发生抖动等不舒适的体感和事故风险，但是有了高精地图的预先采集信息，结合实时感知的信息融合在一起，我们就可以建立一个非常稳定可靠的行驶区域模型，从而实现稳定安全的自动驾驶。

最后一类是生态感知，也是百度构建Apollo自动驾驶平台所能发挥的核心价值。

自动驾驶系统是机器构成的系统，他和人类开车的时候有很多不一致的地方。举个简单的例子，人类在开车时，遇到高速上前方一辆车都没有的时候，视野开阔，会觉得是最安全的时候，可以把车速提升到很高的速度。

然而对自动驾驶系统来说，这个场景的安全性反而比前方跟随一辆汽车开起来安全性要低，因为在跟车模式下，前方车辆对自动驾驶系统来说就是一个延伸出的传感器，它可以帮助自动驾驶系统把感知范围再向前延伸几百米范围，这就是生态感知的力量。

APC会通过百度Apollo平台的强大生态能力感知到当前道路更远范围的实时状况，从而让驾驶更加安全。提前通过百度地图和百度Apollo数亿的日活用户的实时数据回传进行依法脱敏后的大数据挖掘，我们就可以对当前路况、安全性做级别上的判断，采用不同的驾驶策略来保证安全。

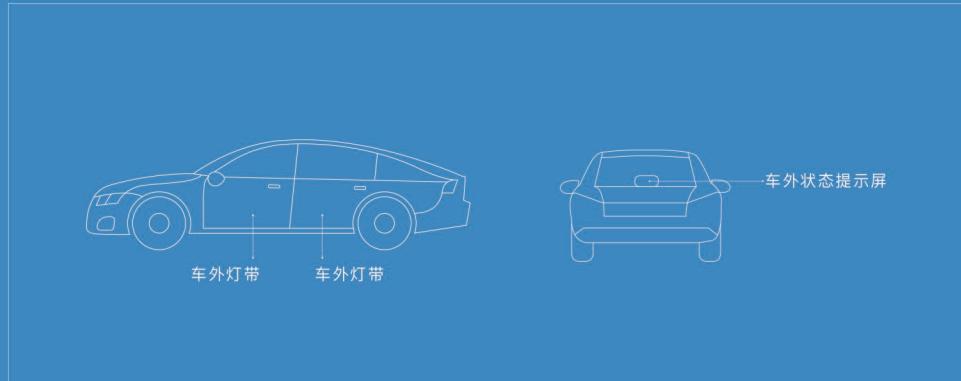
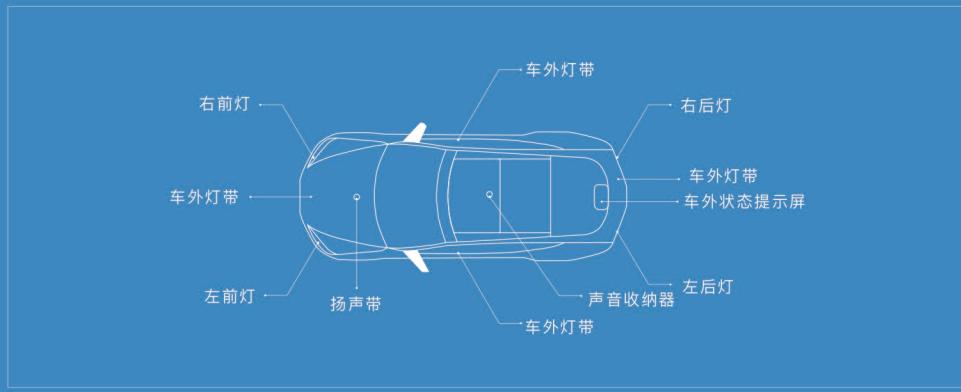
例如，如果前方1公里处多辆车通过时都出现减速情况，那么APC在获取到此信息后就可以作出适当的预判，预先调整自己的安全行驶速度。

这套生态系统也会体现在高精地图上，来实现高精地图的分钟级更新，例如当一个路段出现了道路维修封闭一个车道，我们的高精地图系统就会在1分钟内做出实时更新，通过OTA下发到后续的车辆，来让后续车辆提前避开以提升安全性。

## Section 2.2 EMI系统

我们认为仅靠和驾驶员进行人机交互的HMI系统，是不足以适应自动驾驶的全部需求的，自动驾驶系统还需要包含一套和环境进行输入和输出的接口，我们称之为EMI。EMI和HMI综合起来形成完整的XMI自动驾驶交互系统。





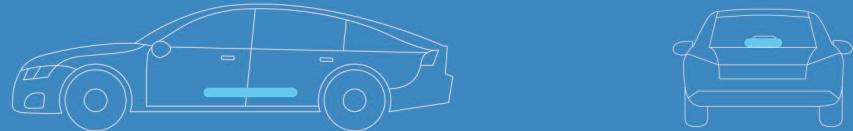
EMI系统将影响驾驶行为的环境交互作为输入以确保自身车辆行驶安全。人类驾驶员在行驶过程中会用双闪、远光灯、鸣笛等“车辆语言”与其他车辆沟通，这些行为往往传递着重要的信息。

例如，双闪意味着“我出现了一些问题，请离我远一点”，而鸣笛意味着“你干扰到我了，请根据我的动作及时调整”。对于自动驾驶汽车来说，如果无法准确捕捉并理解环境交互是十分危险的。

据此，我们设计了APC的EMI系统，它将通过全向摄像机和麦克风阵列来完成对环境交互信息的收集工作。原始输入信息在被捕捉后将通过算法转换为语义化信息，为后续的决策模块提供安全保证。

除此之外，EMI系统还将主动输出与环境的交互行为来降低潜在风险。除车辆自备的灯光、喇叭，我们在车辆外围又加装了车外灯带、扬声器、状态显示屏等互动设备，强化车辆与环境的交互能力。

除了类似人类驾驶员的远光灯、双闪等操作，车外视觉效果将随着自动驾驶的状态变化而变化。此举的目的是保证其他车辆对自动驾驶车辆行为有一个合理预期，做到“自身安全保证”和“他人安全保证”的双保险。



自动驾驶开启后车外灯光：  
左右车门有蓝色灯光状态显示，车后有文字+灯光状态显示。



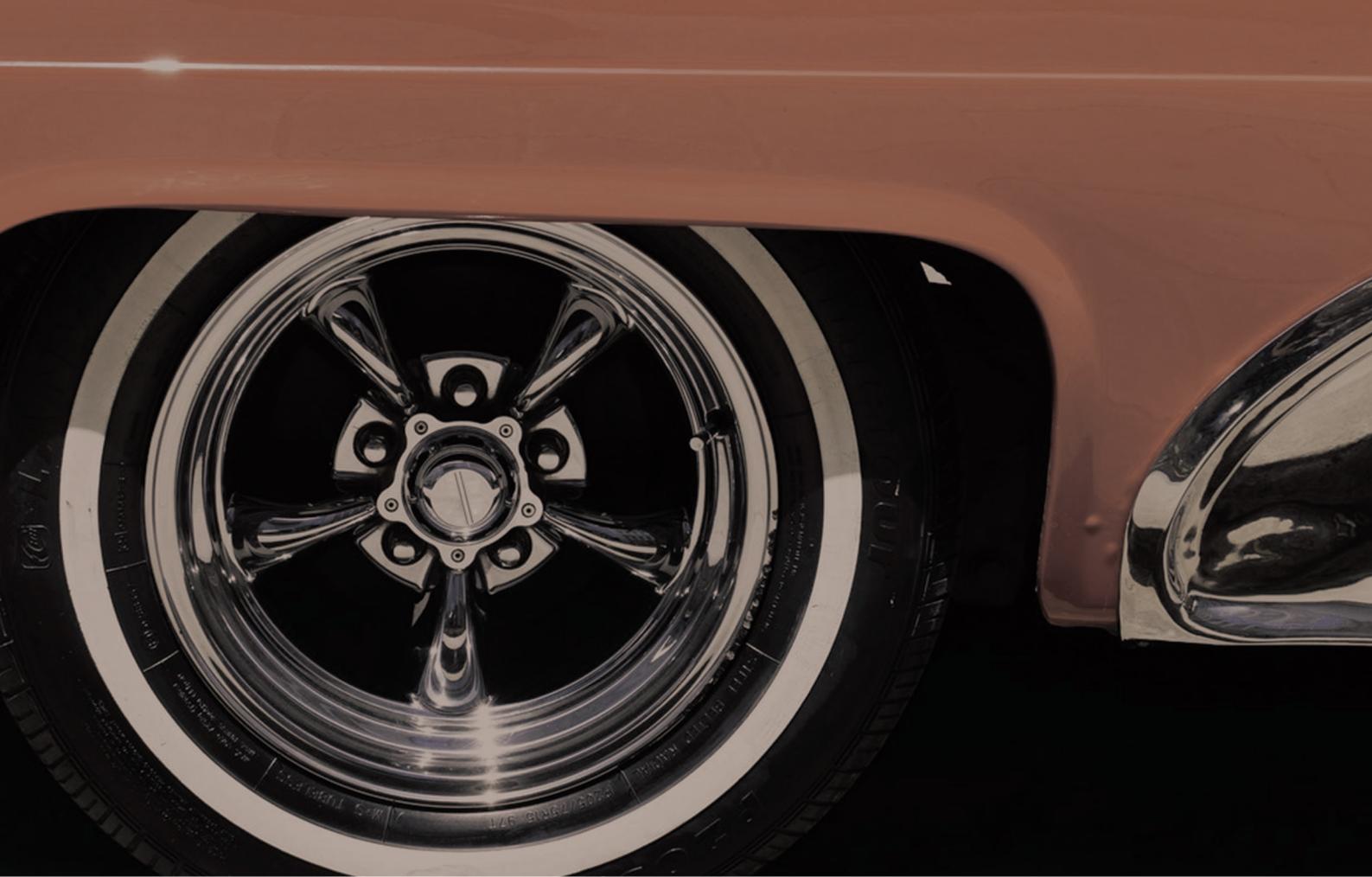
紧急制动时车外灯光+声音：  
车后灯光屏文字提示，打开双闪，发出连续警示音。

## Section 2.3 DPS系统

通过对环境的清晰认知，以及具备和环境交互的手段后，APC解决了融入环境的两个前置条件，那么车辆如何能真正的融入当前环境，做一个符合当前驾驶要求的好司机，DPS（Driving PolicySystem）系统将重点要解决这个问题。

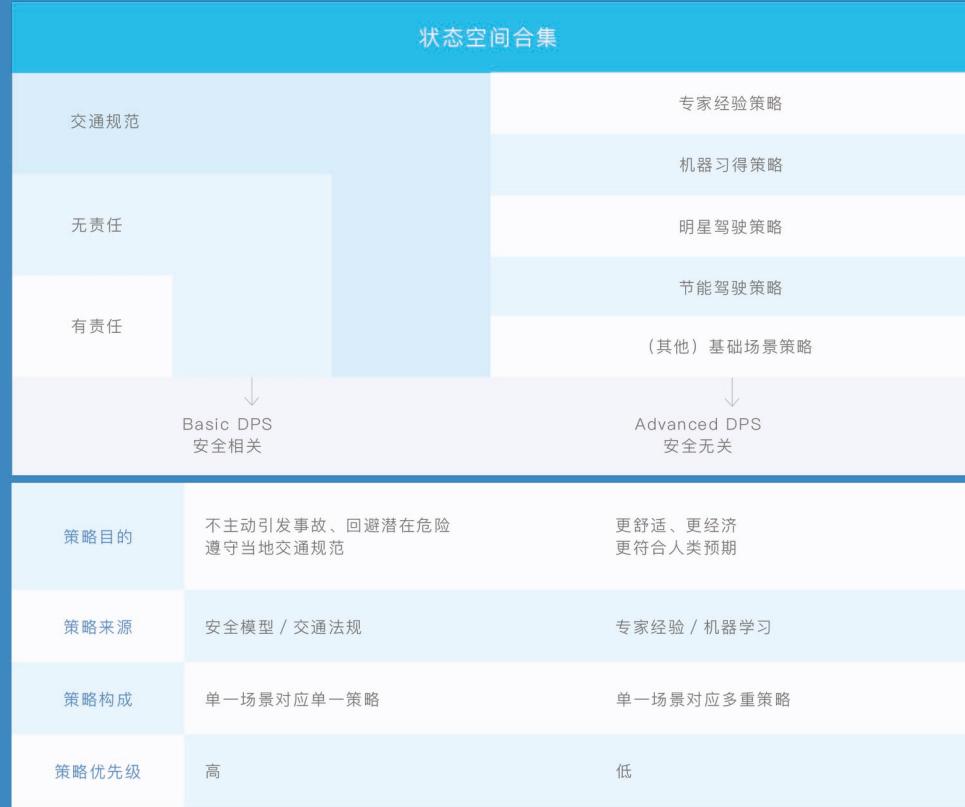
众所周知，在AI时代，科技公司使用机器训练和学习的方法，来培养具有足够人工智能的机器，比如被广泛报道的围棋机器人AlphaGo，经过大量的自我对战学习训练，对阵人类棋手的时候可以下出来很多人类暂时无法解释的不符合之前围棋运动总结出来的规律的妙招。

虽然我们认为这是AI训练和进化的一个理想的方向，但是考虑到自动驾驶车辆在目前的驾驶环境中还是少数派，完全由AI决定的不可解释的驾驶行为，即使能做到很安全，在现阶段也是存在监管和法律问题的。因此，DPS系统在设计的时候，就希望达到两个目标：全面性和可解释性，从而能让大众和政府监管机构对自动驾驶车辆在社会上运行的安全担忧得到解决。



全面性是指在任意组合出的确定环境状态下，自动驾驶车辆所对应的驾驶策略都是完全覆盖到的，确定的，可以查询的。这样就可以把整个DPS策略拿出来给大众和监管部门进行安全审核，来保证自动驾驶车辆的策略是安全透明的。

可解释性是指每一条策略，都是有来源，比如来自于交通法规对最小安全距离的保持要求，比如来自于交通法规的路权优先和避让规定，比如来自于CIDAS的某个真实事故的反推安全要求等。



整个DPS的设计框架如上图，分为影响驾驶安全的Basic DPS和不影响驾驶安全的Advanced DPS两部分。在Advanced DPS部分，我们会引入更多的机器学习的模式，来总结更多人类优秀驾驶员经验，形成更多可解释的更安全的驾驶策略。

## Section 2.4 MOBILEYE RSS模型

自动驾驶业界非常知名的Mobileye公司于2018年发布了自动驾驶责任敏感安全模型“Responsibility-Sensitive Safety”(RSS)，百度Apollo自动驾驶团队在和Mobileye团队进行深入交流和研究后，非常认同RSS在自动驾驶中的作用和价值，将会融合应用在APC的安全模型中，并将和Mobileye团队一起继续深入研究和打造适用于中国驾驶环境的安全模型和驾驶策略，在Apollo平台中进行开放，帮助Apollo自动驾驶的开发者们提升产品方案安全性。

### RSS模型简介

自动驾驶汽车的部署存在一项独特的挑战：用于决策的DPS技术基于人工智能。这种技术针对系统典型行为而优化，在你想要系统模仿典型行为（即人类行为）时，是非常不错的。但同时也意味着，非典型的边缘案例往往被优化或者过滤掉了。

归根结底，人工智能本质上是概率性，这意味着有出错的可能。那么我们如何才能避免受到此类概率性错误的影响？如果使用的方法会使得行为过度保守，将导致自动驾驶汽车难以应对复杂的交通环境。



## 责任敏感安全模型——危险情况

责任敏感安全(RSS)模型能为自动驾驶汽车提供可验证的安全决策。RSS像是一个自动驾驶汽车人工智能决策功能的“安全密封”，确保一直到行动为止的所有阶段始终都只能做出“安全”决策，如图所示。



责任敏感安全模型分两部分运行，第一部分是定义“危险情况”，我们将在这节中对此进行探讨，因为这与环境感知模型有关。第二部分是定义“适当响应”，换句话说，即遇到危险情况时的正确行为，我们将在下面对此进行探讨。

如果自动驾驶汽车与另一个物体之间的纵向与横向距离均不安全，那么自动驾驶汽车便处于危险情况之中。

例如，假设有一个简单的场景，其中只有两辆汽车——前车 $cf$ 和后车 $cr$ ，速度分别为 $v_f$ 和 $v_r$ ，响应时间（决策时间）为 $\rho$ ，最大加速以及最小和最大制动参数已知，则两车之间最小安全距离为：

$$d_{\min} = \left[ v_r \rho + \frac{1}{2} a_{\max, \text{accel}} \rho^2 + \frac{(v_r + \rho a_{\max, \text{accel}})^2}{2 a_{\min, \text{brake}}} - \frac{v_f^2}{2 a_{\max, \text{brake}}} \right]_+$$

这意味着，如果 $cr$ 是自动驾驶汽车，只要与前车保持这一距离，那就总能避免追尾。这样，我们始终都能对人工智能决策引擎提议的行动进行测试，以确保行动不会将自动驾驶汽车置于危险情况。

责任敏感安全模型针对各种各样的驾驶场景定义了公式，百度和Mobileye将开展合作，确保各种场景均能正确反映中国独特的驾驶风格。

如前所述，责任敏感安全模型是一种为自动驾驶汽车决策提供安全保证的正式模型，通过定义等式定义出了危险情况。接下来，自动驾驶汽车的目标就是避免进入危险情况。责任敏感安全模型定义了“适当响应”，这是避免进入危险情况的关键，并且还定义了危险情况强加于自动驾驶汽车时要采取的行动。





#### 责任敏感安全模型——适当响应

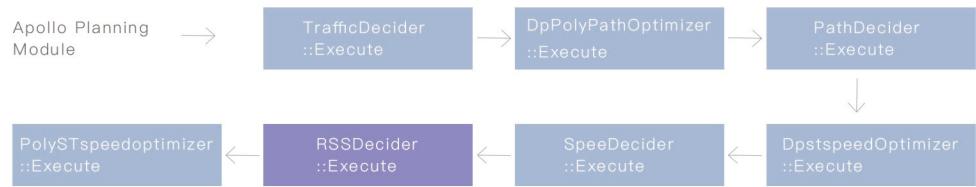
例如，在前例中，在cf减速，将要打破公式计算出的最小距离时，对于cr来说，“适当响应”就是减速，以保持安全跟车距离。

对于更复杂的场景，如进行变道切入，适当响应行为可能需要结合横向与纵向减速。

归根结底，此类“适当响应”是优秀的人类驾驶员都知道的常识。通常不是严格的交通规则，而是人们已经掌握的常识造就出最安全的驾驶员。

RSS只是将此类常识性优良驾驶实践形式化为可正式验证的模型，该模型通过逻辑上可证明的规则确保自动驾驶汽车能始终做出安全的决策，并且将会竭尽所能地避免卷入其他物体导致的不安全情况。

由于RSS是环境策略和行为策略的结合，因此从架构上来说，其实施必须在路径规划决策（Path Decider）之后，但在提议路径执行之前。将“安全密封”（RSS）从策略规划功能（DPS）中分离出来的一大好处是，目前DPS提议的安全行动空间将会扩展，因为这样人工智能决策算法中就可以不再把安全作为加分项而使用。这意味着，DPS将能自由地规划更多的行动，可确保做出安全但又果断的驾驶行为——这在中国独特的驾驶情况中非常重要。由RSS提供终极安全保护，因此DPS可以规划出安全却果断的行动。



这样，我们成功地将RSS整合进了Apollo项目和Apollo Drive解决方案，将确保在最复杂驾驶情况中保持最高等级的果断性，同时凭借RSS提供的正规模型保护，安全性也不会打折。

# Chapter 3

## Behavior Safety

培养一个面面俱到的老司机  
—行为安全

我们通常把一个有很长驾车里程经验，见识过多种路况，长期安全行车从不出事故的有经验的司机叫做国宾级老司机；自动驾驶系统也和人类司机一样，是通过不断的学习和训练从一个新司机进化到老司机的。



### 驾考

驾驶学员需要在驾校学习驾驶的法律法规，熟悉驾驶车辆及简单的驾驶操作，并通过驾驶规范的道路测试。



### 实习

实习期的驾驶员往往会请熟练司机来指导和训练。通过这一阶段的真实道路场景学习，驾驶员才具备独自驾驶上路的基本能力。



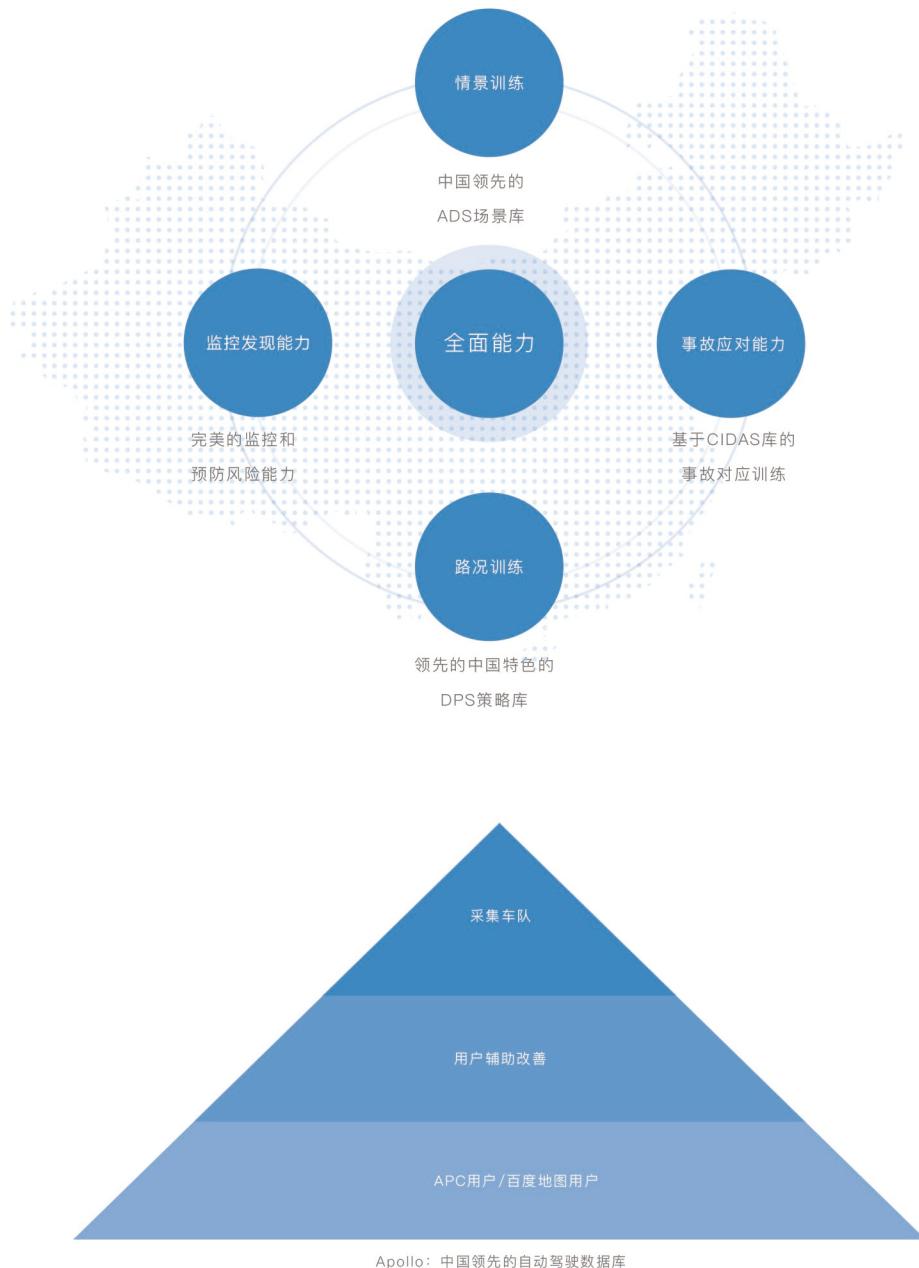
### 熟练

驾驶员需要不断地总结自己的驾驶经验，形成一定的驾驶策略，才能逐步达到一个合格的国宾司机标准。

我们先来看一个人类成熟的国宾级老司机典型成长历程，大致会有三个阶段：驾考、实习、熟练。

从驾驶学员成长为经验老到的国宾司机，人类驾驶员一般需要经历5–6年的时间，进行数万公里的驾驶经验积累。

APC系统也是按照类似的过程，通过对四个方面的海量数据收集和训练，来培养出一个合格的具有全面能力的自动驾驶国宾级老司机的。



## Section 3.1

# 安全驾驶的基石-中国领先的ADS场景库

数据是人工智能时代的基石，自动驾驶数据规模和采集能力决定了自动驾驶能力的发展速度。为了具备安全的自动驾驶能力，百度构建了一个完备的数据采集体系：



专业采集车队

百度筹建的数千辆自动驾驶采集车队安装了高清摄像头、激光雷达等多种传感器，该车队由具备测绘作业资质的专业团队支持，可以为百度Apollo提供精确及详细的多种自动驾驶学习信息。



用户辅助改善

搭载了图像以及传感器设备的数百万辆车，参与“驾驶安全改善计划”，可以为百度Apollo提供大量真实场景道路的数据及司机驾驶行为信息。



数据生态

百度Apollo和百度地图数亿的日活用户的实时数据，经过依法脱敏后，为百度Apollo提供了一个实时生态感知体系。通过这些方式采集，我们构建了中国领先的ADS场景库。

百度Apollo打造的ADS库，完整覆盖APC设计的三大场景，并且包含光照、季节、时间段、天气、全国各种区域和地形、障碍物类型、路面状况、隧道匝道、分流合流等各种常见和极限驾驶状况的数据。



#### 高速/城市快速路

Apollo已采集覆盖了上百种环境状态下的全国每一公里的高速公路和环路场景。



#### 停车场泊车

Apollo已采集室内外数万个停车场的环境、车位等各类信息。



#### 城市拥堵跟车

Apollo城市道路的拥堵跟车采集里程已达到上亿公里。



为此我们收集数亿公里的真实道路场景数据用于百度Apollo的训练学习。

1位具备1年驾驶经验的司机平均拥有5000公里道路的行驶经验，而每一辆百度自动驾驶车辆自诞生之初就掌握了数亿公里的驾驶经验。通过海量数据的不断训练进化百度Apollo不仅能够第一时间认识当前的路面环境，而且会将判识结果与驾驶的法律法规相结合，明确当前情况下驾驶行为是否合法，比如路面上有白色实线时法律规定不允许变道，路旁的限速标牌指示着当前的最高速度限制。

同时，经过数亿中国真实道路数据的学习，百度Apollo可以清晰的区分环境中不同的属性及特征，当三轮车和摩托车同时出现时，百度Apollo不仅能够知道他们都是人类驾驶的车辆，而且能够了解他们速度和行为的差异，为后续的应对策略提供准确信息。

## Section 3.2

# 安全可靠的教师 – 领先的中国特色DPS策略库

前面章节介绍过，百度构建了一个适合当前社会环境的全面的可解释的DPS库，来保证驾驶行为的安全。这个DPS库也是通过大数据训练的方法，辅助以人工审核的模式，在不断的演进和优化。

### 收集国宾司机的丰富经验

众所周知，经验丰富的国宾司机与初学者在驾驶行为上差异很大，经验丰富的司机不但能够提前预估风险并采取措施合理规避，而且行驶同样的里程，有经验的国宾司机会比初学者的油耗更低。为此百度APOLLO和众多出行公司合作，对驾龄超过10年且无事故记录的国宾司机的驾驶行为数据进行了收集分析，来提升整个驾驶过程的安全性。

例如我们发现国宾司机会做预判，在高速上巡航遇到路过进出匝道口时，他们会认为驾驶风险提升，通常就会适当拉大与前车的安全距离；因此APC在高速上自动驾驶时，也学会通过高精地图确认即将通过的道路信息，当遇到匝道时会和国宾司机一样进行预判和适当调整来提升安全性。



### 收集中国特色的驾驶策略DPS

中国道路情况复杂，人口总数近14亿，汽车保有量超3亿，几乎各大城市都存在着严重程度不一的交通拥堵，密集的车辆，熙攘的行人、以及独特的文化铸就了中国特有的驾驶习俗。

因此，在某些情形下，更符合法规要求的驾驶行为并不一定更安全。例如，当发生交通拥挤时，为了避免前车碰撞，法规要求我们保持足够大的安全车距，但是在中国的驾驶环境下，过长的安全距离更容易引发其他车辆的近距离切入，反而为我们带来更高的安全隐患和事故几率。

基于对国宾司机的驾驶行为分析，在符合中国法律法规的前提下，我们提炼了一个确保安全的更完善的拥堵跟车车距保持的策略模型，从而真正提升这个场景下的驾驶安全。

## Section 3.3 防患于未然 — 危险发现和监控

好的老司机能够做到防患于未然，靠的就是日积月累对安全隐患的排查和危机意识。相应的APC也有一套完整的监控诊断机制。

### 实时监控



为了保障自动驾驶车辆在驾驶途中的安全运转，我们设计了自动驾驶车辆状态的实时监控系统，用于监控环境状态、车辆自身状态、自动驾驶硬件和软件状态、驾驶员状态。

通过对各种状态变化的判断，我们会进行相应的提示、警示和接管策略触发，从而保证自动驾驶的过程始终是可控的、安全可靠的。例如，一旦自动驾驶过程中驾驶员解开了安全带，系统就会监控到这个信号并作出安全要求提示，如果驾驶员不做响应，出于碰撞安全考虑，自动驾驶系统就会要求驾驶员接管以把风险控制在安全范围内，如果驾驶员仍不作出响应，系统会自动寻找安全区域进行刹停并开始进行报警。

### 在线诊断

在发现问题之后，我们也提供一套在线诊断系统，帮助用户迅速判断自动驾驶系统的问题所在，并提供可行的处理办法，帮助用户尽快把系统恢复到可用的安全状态。

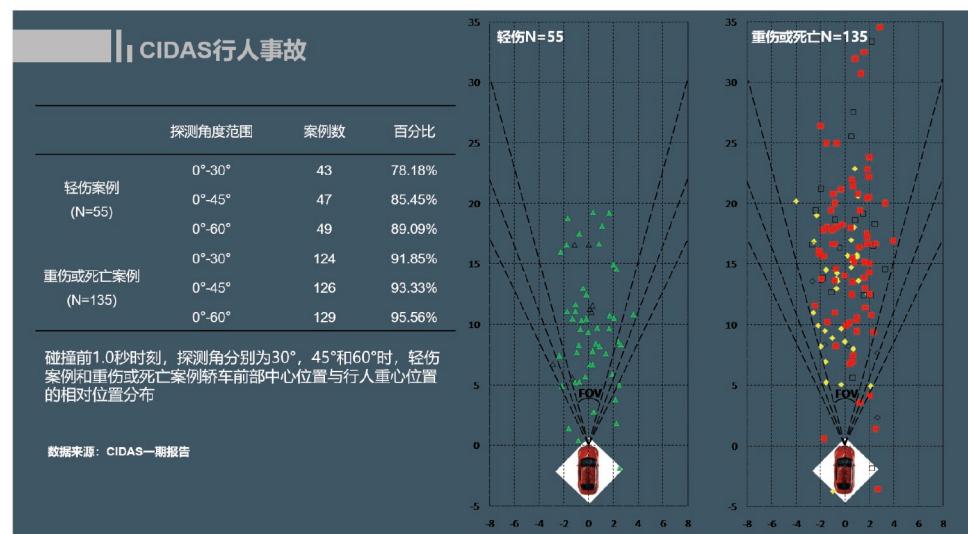
## Section 3.4 临危不乱 – 危险应对能力

当发生碰撞风险时，除了车辆本身提供标准的安全防护措施如安全气囊等，APC自动驾驶系统也会提供额外的应对能力。



在无法避免的碰撞（比如很近距离切入、后车追尾等）发生前，APC会通过前向、侧向、后向的感知系统，预判碰撞风险，在碰撞即将到来时进行紧急制动、侧向安全区域躲避、安全带预张紧等必要操作，来最大程度降低碰撞可能造成的伤害。

同时，APC和中国最权威的CIDAS中国事故安全研究中心合作，通过对几千例中国交通事故的深入分析，在大量真实交通事故和危险场景数据的基础上，通过深度学习、仿真等多种技术方法，进行反复的训练和测试，确保可以在现实场景发生变化时第一时间感知危险并及时做出合适的应对措施，降低危险发生的概率。



# Chapter 4

## Functional Safety

站在巨人的肩膀上  
—功能安全

严谨的流程是保证自动驾驶的基础，百度拥有软件行业领先的软件工程流程。与此同时，在研发自动驾驶技术的过程中，百度团队认识到汽车行业百年发展的工程实践才是能保证自动驾驶系统安全，稳定的运行在道路上的基础，因此我们会确保自己所做的事情都是完全符合汽车业界已有的安全规范的。



百度于2018年4月获得中国首个互联网公司ISO26262认证

百度投入了巨大的精力通过了汽车业界的功能安全流程认证，这是由国际标准化组织（ISO）制定的 ISO26262（Functional Safety, 功能安全），并且借鉴了MIL-STD-882E标准，形成了百度最为严谨的安全研发流程。

## Section 4.1 安全流程

我们在设计之初，就和整车厂的工程师严密合作，充分考虑匹配自动驾驶系统的整车各种可能出现的失效，以及由失效带来的风险，并且提出前面规避 / 降低这些风险的措施。工程师从各个层面去实践这些分析，从整车，到自动驾驶系统，再分解到系统的硬件和软件。我们使用HARA, FMEA, FTA, FMEDA, SFMEA等全面的业界标准安全分析方法，对自动驾驶系统的设计提出从上而下，一整套全面的安全需求。

这些需求进一步的被从软件，硬件，系统集成以及整车层面，在各种场景下进行测试，以此验证自动驾驶系统真正的满足了这些需求，并且能够保证自动驾驶系统的安全运行。每一个与安全相关的设计与需求就这样被严谨而全面的分析，设计，实现以及验证。这是百度安全流程的关键部分。

在百度建立自动驾驶团队之初，我们就组建了车辆测试团队，测试数据被实时的收集分析。潜在的危险场景数据会实时提交到安全分析团队以及仿真数据库，形成一个高效的设计－验证－反馈迭代提升闭环。根据和相关政府部门的合作，以及百度测试车队的数据，百度建立了完善的失效场景仿真数据库，这被认为是自动驾驶安全设计的前提和基础。

我们相信，真正的安全并不是通过某一个或者几个技术措施来实现的。而是我们从系统开发的第一步开始，每一个工程师都贯彻“安全为最高优先级”的理念，以消除 / 降低系统不可接受的风险为目的，综合考虑所有的安全措施，并最终通过全面的测试和验证，来确保系统的安全性。

## Section 4.2

# 安全功能设计

在必要的时候，我们的自动驾驶系统可以保证系统进入并维持在安全状态。这是通过全面的诊断功能来检测系统的状态，足够的系统冗余来保证Fail – Operational。

异常类别	状态空间合集
传感器异常	摄像头、雷达等实时的通信以及数据状态
高精地图异常	高精地图数据的有效性及实时性
软件运行异常	系统软件稳定可靠的运行实现预期功能
计算平台异常	主/备系统的硬件安全诊断机制
执行器响应异常	车辆执行器是否按照预期执行自动驾驶的命令
车辆状态异常	车辆供电，散热，等导致出现异常
司机行为异常	司机行为监控确保没有对自动驾驶系统的错误使用

我们的诊断系统设计实时的监控系统的软件，硬件运行状态，以及和自动驾驶系统相关的整车状态。

传感器在自动驾驶中扮演着举足轻重的作用，因此我们的自动驾驶系统车身周围各个区域都布置了冗余探测范围的传感器，传感器同时又使用不同的探测技术。系统监控模块会实时的监控摄像头，雷达等传感器的硬件回路以及传输数据的有效性。当有相应的失效发生时，安全管理系統根据定义的安全策略进入相应安全状态。

我们有冗余的自动驾驶控制器（Apollo Computing Unit），每一套控制器都有独立的输入和算法来进行决策。硬件系统全部实施了相应的安全机制保证满足最终的失效率目标。与此同时每一套系统都实现了对自身的全面诊断功能，包括全面的硬件以及软件运行状态监控，确保软件系统是按照我们设计的方式安全、稳定的运行在安全可靠的硬件上。

与此同时，我们系统要求整车关键的执行系统是独立且冗余的，比如转向和刹车系统。只有冗余的系统才能保证自动驾驶系统的Fail – Operational，也就是说当一套系统发生关键失效时，我们的系统仍然有能力持续地安全运行一段时间，满足司机对“自动驾驶”系统的需求。



## Section 4.3 预期功能安全

自动驾驶的技术高速发展，硬件和软件的复杂性，驾驶场景的复杂性，给传统的ISO26262方法论带来了挑战——如何确认自动驾驶的安全。

因此，我们在应用ISO26262的方法论时，不仅仅是从上而下的，自设计之初就将“安全 / 防止失效”做为一个目标，从系统设计，软硬件设计，开发，验证等等都以满足这个目标为最高优先级。与此同时，我们会充分的评估所有的自动驾驶关键的功能。通常业内称这种方法叫做预期功能安全（Safety of the Intended Function）。

对预期功能的充分评估其中最重要的一个因素，就是将自动驾驶功能置于可能失效的各关键失效场景，全方位的测试 / 验证系统，以此找到自动驾驶系统能力不足的地方并进行改进。并且最终，通过对该功能的大量的里程累积以获得统计性的数据证明最终系统的安全性。

比如说，为了验证我们的系统具有在高速公路上自动驾驶的能力，我们的系统必须在中国高速道路的各种交通情况，天气，路面，照明等场景下都充分验证，以此验证自动驾驶系统有能力处理所有非预期的情况。

为了达到这个目的，一个完善，充分，并且专门针对中国地区的特别的训练 / 测试数据库是关键。百度在启动自动驾驶项目之初就认识到数据对自动驾驶安全的重要性，投入巨大的精力和资源打造了中国最全面，最精确的场景库。

百度通过各种层面的测试对自动驾驶的关键功能进行测试，我们确保自动驾驶系统能够安全的处理在实际驾驶行为中一些不可预期的因素。

# Chapter 5

## Quality Safety

完整严格的质量保证  
--质量安全

质量是安全很重要的组成部分，APC有完备的质量测试体系和充分的整车里程测试来保证产品质量，并有业界领先的信息安全机制来作为自己的坚实护盾。

## Section 5.1 充分测试 – 安全上路的前提

APC自动驾驶系统从研发到用户手中，将会经历非常充分的大量级测试，以保证交付产品的质量。我们从模块开始，对不同场景不同功能以及整车运行分别进行单元、仿真、台架、在环、整车等测试，不仅在仿真系统中进行数百亿公里的魔鬼验证测试，也会针对APC所设计的自动驾驶场景进行百万公里以上的实际道路整车测试。

整车		半开放/开放道路测试 平均覆盖全国每1公里高速/环路道路4次			
功能		高速/环路 台架、封闭 场地测试	自主泊车 台架、封闭 场地测试	城市拥堵 台架、封闭 场地测试	
模块		感知 数据包测试、 仿真测试	DPS 仿真测试	XMI 台架测试	硬件 台架测试

以高速/环路自动驾驶功能的整车测试阶段举例，在交付前，将会确保进行120万公里以上的整车测试，相当于对全国30万公里的高速和环路的每一公里都进行4次全量覆盖，在测试过程中还会通过调度系统进行各种环境条件如光照、时段、季节、天气等的覆盖，确保验证的充分。

#### 全球道路覆盖次数+自动驾驶累计里程

交付前：120万公里

【每公里覆盖4次】



中国高速网统计:全国高速+城市环路长度约33-34万公里

## Section 5.2

# 信息安全 – 安全运行的护盾

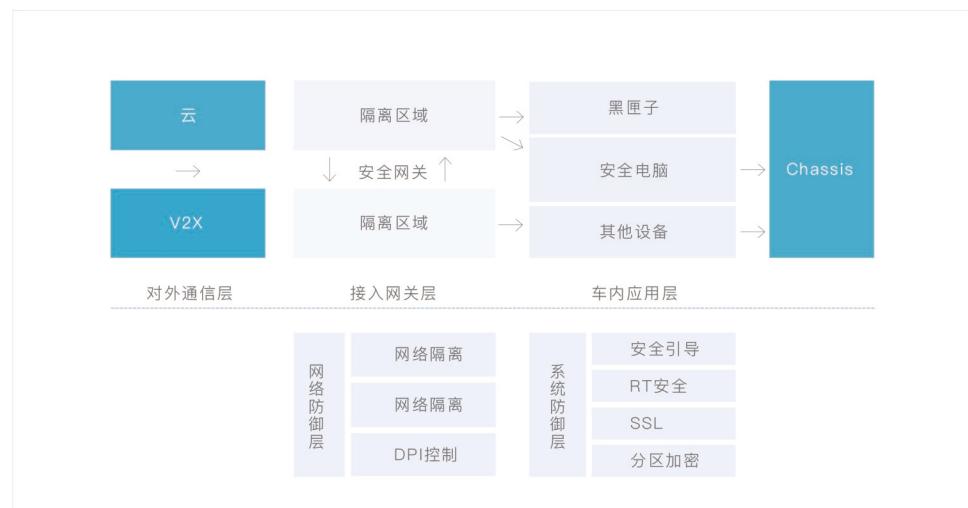
百度Apollo对于信息安全非常重视，在自动驾驶业务启动之初就成立了信息安全团队，将相关领域的信息安全标准与指南、方法与实践贯穿于研发Apollo的整个过程。基于实践积累，2018年4月19日，Apollo汽车信息安全实验室正式宣布成立。实验室的战略合作单位包括中国汽车技术研究中心有限公司、中国信息通信研究院，首批重点合作单位包括中国第一汽车集团有限公司、奇瑞汽车股份有限公司、北京新能源汽车股份有限公司、清华大学、北京航空航天大学、北京理工大学。

在自动驾驶的信息安全领域要实现核心目标是“防御外部入侵，防范核心应用和隐私数据泄露，防范控车威胁”。





我们构建了基于多层次纵深防御体系的汽车信息安全解决方案，并将在三个重点层面实现车规级的信息安全。



## 对外通信层

完整的PKI体系为参与自动驾驶系统的设备签发证书，提供必须的密钥和证书管理服务。自动驾驶系统的设备之间、车端跟云端之间进行安全通信，确保通信数据的保密性、完整性、身份真实性和防篡改。安全升级套件保证OTA的安全可靠。

## 接入网关层

专用的车载安全网关对车载网络和Internet、车载子网络之间进行隔离、访问控制，并鉴别指令、发现并且阻止异常的网络行为及非可信车辆的操作指令，保证车载网络安全。

## 车内应用层

基于芯片硬件安全，从操作系统引导到应用程序运行，全程进行可信度量，防止操作系统、核心应用、数据等被篡改；隐私系统为核心知识产权IP和重要商业价值数据提供保护。

## 云端信息安全

通过对云端平台进行安全评估、渗透测试、部署抗DDOS、WEB应用防火墙及安全日志分析工具等，保障云端平台的安全运行。针对移动应用，利用内存混淆技术、专利性的虚拟机加密技术、高强度保护壳技术等，来确保应用不会被黑客利用进行车辆攻击。

# Chapter 6

## OTA System 越开越安全--安全进化

世界上没有100%安全的系统。

安全是相对的，世界上并不存在绝对的安全。纵使我们有完善的安全设计，使用了海量的数据用于训练学习，多种策略规避危险，也无法保障绝对的安全。我们认为，一个安全的系统，是更多依赖安全的生态和机制，只有构造一个能不断获得学习、不断自动进化的自动驾驶系统，才是可以安全行驶的关键。

## Section 6.1

# 快速发现安全问题

通过对大量APOLLO用户、地图生态用户等回传的实时数据进行依法脱敏后的深度挖掘，我们搭建了一套快速问题发现系统。

例如，针对某条道路的大量轨迹分析，我们可以获知该地点较大概率存在环境不安全因素；通过整体的用户特定场景下的驾驶行为分析，我们可以发现DPS策略的优化空间；通过对监控诊断数据的分析，我们可以发现影响自动驾驶安全的新的不安全因子。

每一辆车的数据汇集起来，就会变成一个能力特别强大的智囊团，比传统分散在每个人手中的汽车更加快速更加精准的发现问题所在，作为快速解决问题的基础。



## Section 6.2

# OTA – 快速解决问题的关键

OTA是Over the Air的缩写，即通过空中的方式升级，OTA可以理解为一种远程无线升级技术。

OTA主要包含了以下双层含义：

FOTA(Firmware Over the Air),即固件远程升级；

DOTA(Data Over the Air),即数据远程升级。



百度APOLLO的OTA系统包括两部分的升级：软件系统和数据。

当软件和数据发生了变更时，我们会在最快的时间为您自动更新。这意味着，也许三个月前还没有高精地图无法自动驾驶的区域，三个月后已经解锁了自动驾驶能力，也许一个月前百度APOLLO还不能很好处理的场景，现在已经可以表现的更好。百度APOLLO，通过不断的自我学习，随时可能为您带来全新的体验。

# OTA 做到天级别安全更新

驾驶安全、BUG、地图类更新



功能升级更新



新增功能更新



# Chapter 7

# Social Security

## 承担社会责任--机制安全

在安全的设计框架保证下，在安全的质量控制下，自动驾驶汽车可以比人工驾驶汽车的安全等级进行大幅提升，事故率可以降低至少一个量级。

但是事故的发生是多种因素综合构成的，还是存在一定发生几率，因此APC系统在量产上市前，我们也在积极推动事故处理机制、相关法律法规、保险和援助机制等和自动驾驶相关的机制在中国逐步走向成熟，积极主动承担Apollo这个中国自动驾驶领导者所应承担的社会责任。

# 规范

- 自动驾驶路测法规（已实现）
- 自动驾驶上路运行法规（推动中）
- 自动驾驶国家安全标准（推动中）

2017年12月19日，在Apollo和众多伙伴推动下，北京市颁发《北京市自动驾驶车辆道路测试管理实施细则（试行）》，并于2018年3月22日向百度Apollo颁发第一张自动驾驶测试牌照在规范指导下更安全的进行测试。

2018年4月11日，工信部、公安部、交通部三部委联合印发《智能网联汽车道路测试管理规范（试行）》的国家测试规范，对于自动驾驶的安全测试更具指导意义。



后续百度还将和Apollo众多合作伙伴一起努力，继续推动自动驾驶在中国的安全合法的进步和发展。

# 保障

- 自动驾驶保险产品（已达成意向）
- 自动驾驶事故援助基金（建设中）
- 自动驾驶事故处理专项机构（建设中）

Apollo目前已和多家保险公司达成合作意向，在自动驾驶量产前，将会推出针对APC的保险产品，全面保障用户的自动驾驶使用风险和使用安全。

Apollo也在筹备专业的自动驾驶事故援助（事故医疗费用优先垫付、法律援助、专家医疗援助等）机构和专业的事故处理机构，保障用户的使用权益。



## EDR — 自动驾驶系统黑匣子

根据国家《智能网联汽车道路测试管理规范》，百度Apollo研发了汽车黑匣子软硬件产品。黑匣子提供了系统安全、数据加密及数据安全存储等完整的解决方案，并通过与国家相关机构合作来保证数据的权威可信。考虑到事故责任判定的需要，还开发了配套的数据读取及展示软件，授权后可对数据进行解密读取，并以视频形式将事故现场进行还原，提供可靠证据，同时也为事后故障分析、产品以及算法等的改进提供支持。



## RVC — 远程客服控制系统

根据国家《智能网联汽车道路测试管理规范》对智能网联汽车的安全要求，APC也具备符合国家安全规范的远程客服控制系统，在紧急情况下可以由汽车厂商的客服系统对车辆进行远程援助，帮助用户脱离危险。



## Apollo Pilot 更安全.更经济.更舒适

百度Apollo已经在践行自动驾驶量产安全的路上前行了2年时间，在2020年量产之前，我们的安全工作还将不断改善继续进化，将本报告所提到的各项安全工作做到符合量产要求。我们很高兴能和Apollo众多合作伙伴一起，能为改善中国驾驶安全贡献自己的一份真实贡献。

更多关于百度Apollo自动驾驶信息和意见建议，请百度一下“Apollo”。

## 合作伙伴

- Apollo汽车信息安全实验室
- Mobileye, An Intel Company

## 鸣谢指导单位

- 公安部道路安全研究中心
- 中国汽车技术研究中心
- 国家智能交通中心
- 中国信息通信研究院
- 北京警察学院
- 美国土木工程协会智能网联车委员会

## 引用

- CIDAS 中国交通事故深入研究 中文数据库 (<http://114.255.167.200:8092/cidas/>)
- 特斯拉AutoPilot HW2硬件和功能介绍 (<https://www.tesla.cn/autopilot>)
- Mobileye RSS (<https://www.mobileye.com/responsibility-sensitive-safety/>)

Baidu 百度 | apollo