NVIDIA 自动驾驶
安全报告

我们的使命

下一代交通工具是自动化的从共享出行和个人驾驶，到长途和短途旅行，再到货物配送和物流，自动驾驶将从根本上改善世界的移动方式。在 NVIDIA，我们汽车团队的使命是开发自动驾驶技术，以改善道路安全、减少交通拥堵，让每个人自由出行。

> “安全性是自动驾驶汽车的首要考量。NVIDIA 致力于构建安全的自动驾驶平台，这是我们最引以为傲的事业之一，并为汽车制造商将自动驾驶汽车推向市场提供至关重要的支持。”
>
> **黄仁勋**，NVIDIA 创始人兼首席执行官

目录

简介

NVIDIA 率先采用加速计算解决其他企业无法攻克的难题。我们在 AI 和工业数字化领域的工作对社会产生了深远的影响，同时还改变了全球规模最大的一些行业——从游戏到机器人开发，从挽救生命的医疗行业、应对气候变化到我们共同连接和创造的虚拟世界。

NVIDIA 还将我们技术驱动的愿景、计算性能和能源效率应用于交通运输行业，帮助全球各地的汽车制造商实现安全可靠的自动驾驶汽车梦想。从概念设计到工程制造、销售服务，NVIDIA 的技术正在简化整个汽车行业的工作流程。

尤其是自动驾驶汽车将改变运输业。它们可能会大幅减少交通事故造成的伤亡、缓解交通拥堵、提高生产力，并为不方便开车的人群提供出行便利。

AI 与加速计算领域的突破正在为未来的车队带来引人注目的新功能，几十年来首次将车辆架构彻底转变为真正由 AI 定义的架构。与所有现代计算设备一样，这些智能车辆背后都会有一个庞大的 AI 专家和软件工程师团队提供支持，他们致力于随着技术的进步不断提升汽车的性能与功能。在汽车的整个生命周期内，功能和服务可通过无线更新添加。

NVIDIA 与全球汽车制造商、供应商、传感器制造商和初创公司携手合作。从 AI 辅助汽车、卡车到全自主通勤车和无人驾驶出租车，我们提供构建所有类型车辆所需的系统架构、AI 超级计算硬件和完整的软件堆栈。借助从云端到汽车的开放式模块化架构，制造商可以使用精选解决方案或完整开发工作流。

借助 NVIDIA DRIVE® 一切都可以实现，这是我们的高度可扩展平台，可实现美国汽车工程师学会（SAE）定义的所有级别的自动驾驶。这些级别包括高级驾驶辅助系统（SAE L2 级：驾驶辅助）和无人驾驶出租车（SAE L5 级：完全自动驾驶）。

完全自动驾驶对计算能力的要求极高，比目前生产的先进汽车动辄超出 100 倍。借助 NVIDIA DRIVE，我们的合作伙伴可以通过计算硬件、传感器套件和软件堆栈的多样性和冗余架构来实现最高级别的安全性。

为简化开发，我们创建了单一的软件定义可扩展架构，在保留核心架构的同时，利用额外的硬件和软件来提升每个级别的自主性。同样的策略亦可适用于安全。通过额外的模块化硬件和软件，所达到的安全级别可扩展，以满足高级别自动驾驶更为严格的要求。

NVIDIA 已为构建自动驾驶汽车的研究、开发和部署的强大系统打造了关键技术，涵盖从数据中心到汽车等领域。我们提供一系列硬件和软件解决方案，从高性能的 GPU 和服务器到完整的 AI 训练基础设施和车载自动驾驶超级计算机。我们还为学术研究和早期开发者提供支持，与全球数十所大学合作，并在 NVIDIA 深度学习培训中心开设 AI 开发课程。当我们发现挑战时，我们会将其转化为机遇并找到解决方案。

本报告概述了 NVIDIA 的自动驾驶汽车技术，我们在安全架构、协同设计软硬件、设计工具和方法论tocs的独特贡献，以及实现最高级别可靠性和安全性的最佳实践。

AV 2.0：AI 为车辆安全保驾护航

在复杂的物理世界中构建安全导航的自动驾驶系统是一项艰巨的挑战。系统需要全面感知并了解周围环境，然后在毫秒级别的时间内做出正确、安全的决策。这需要类似于人的态势感知能力，以应对潜在危险或罕见情况。

AV 2.0 与端到端驾驶

自动驾驶汽车软件开发传统上基于模块化方法，具有用于物体检测与跟踪、轨迹预测以及路线规划和控制的独立组件。

如今，自动驾驶汽车技术已迈入新时代——AV 2.0。AV 2.0 以大型、统一的 AI 模型为特色，可控制车辆堆栈从感知、规划到控制的多个环节。

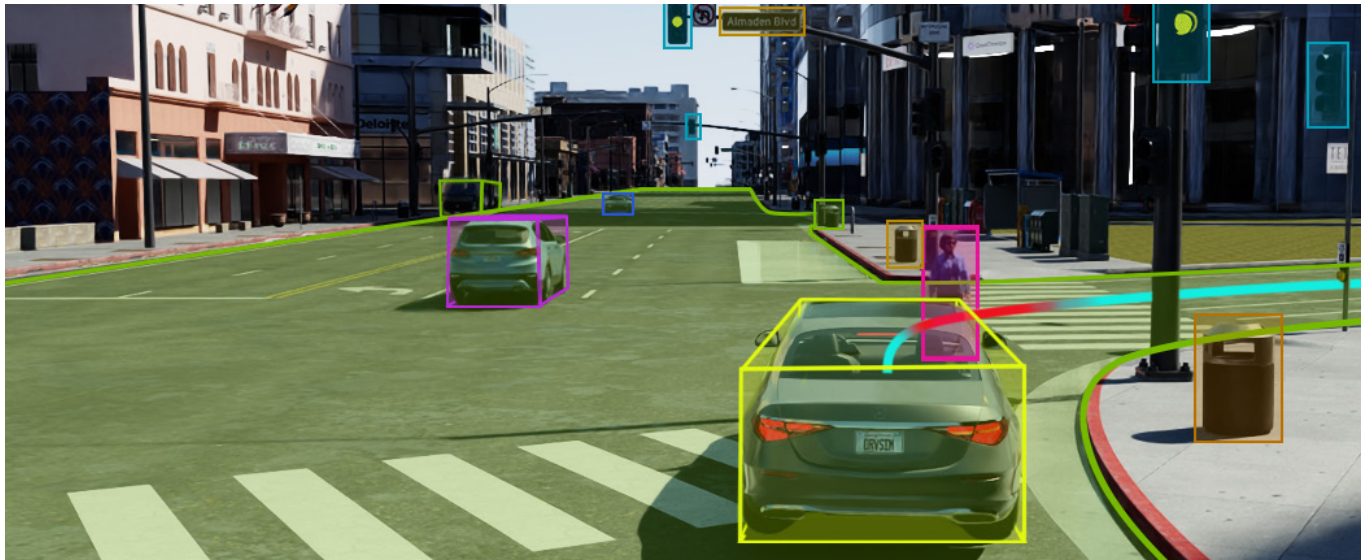
与专注于使用多个深度神经网络改进车辆感知能力的 AV 1.0 相比，AV 2.0 则需要全面的车载智能，借助一种称为“端到端驾驶”的方法来推动在动态、真实环境中的决策。

端到端自动驾驶系统采用统一的模型接收传感器输入并生成车辆轨迹。这有助于避免过度复杂的流水线，并提供一种更全面的数据驱动方法以应对真实世界的场景。

注重安全性

AV 2.0 将在构建与验证安全的自动驾驶系统方面发挥重要作用。NVIDIA 技术在该领域的应用示例包括：

1. **仿真：**安全的自动驾驶汽车系统必须做好准备，能够安全应对罕见及异常情况。NVIDIA 正在开发高质量、逼真的交通和传感器仿真功能，并根据安全关键场景的自然语言描述构建反事实情境。在开发过程中，这些功能可增强真实世界的训练数据，以提高自动驾驶汽车模块的稳定性。在评估时，还可为大规模验证自动驾驶汽车系统提供额外的机制，作为现实世界测试和验证的补充。
2. **安全交互：**当自动驾驶汽车系统部署上路时，它们必须与人类道路使用者进行交互。NVIDIA 在利用 AI 学习驾驶行为预测模型，并借助这些预测了解自动驾驶汽车行为对其他道路使用者的影响。通过使用这些功能，开发者可设计出能够可靠地与其他驾驶员和行人交互的自动驾驶汽车系统，最大限度地降低事故风险。



3. **异常检测：**自动驾驶汽车需要能够可靠地处理异常情况的系统来保障安全。预测场景演变的 AI 模型可使系统评估哪些异常情况可能对安全产生关键影响，需要执行故障安全行为，而哪些异常情况可以安全地忽略不计。NVIDIA 正在探索如何将学习到的未来预测模型用于评估感知失败风险。

终级铁人三项比赛

开发安全自动驾驶汽车的竞赛并非短跑冲刺，而是永无止境的铁人三项比赛，有三个截然不同但至关重要的部分同时运行：AI 训练、仿真和自动驾驶。各部分都需要有自己的加速计算平台。这些专门构建的全栈系统共同构成了强大的三合一体系，可实现持续的开发周期，不断提升性能和安全性。

模型首先在 NVIDIA DGX™ 等 AI 超级计算机上进行训练。然后，使用 NVIDIA Omniverse™ 平台并在 NVIDIA OVX™ 系统上运行，在进入车辆之前进行仿真测试和验证。最后，NVIDIA DRIVE AGX™ 平台使用安全 AI 定义自动驾驶车辆的操作系统 **NVIDIA DriveOS™**，通过模型实时处理传感器数据。

AV 2.0 在构建和验证更安全自动驾驶汽车系统方面表现出广阔的前景。对任何 AI 系统来说，重要的是能够可靠地使用。我们主张以高质量不确定性量化和防护措施增强生成式 AI 系统。借助这些功能，自动驾驶汽车能更安全、更可靠地驾驭复杂和不可预测的世界。

观看 CVPR 2024 大会端到端自动驾驶大挑战赛冠军得主 NVIDIA Research 的关于 **Hydra-MDP 模型**的视频。

安全自动驾驶的四大支柱

NVIDIA 提供统一的硬件与软件架构，贯穿自动驾驶汽车研究、设计和部署基础设施的整个过程。我们提供的技术旨在解决实现安全自动驾驶汽车所必需的四大支柱。

- 支柱 1：AI 设计与实施平台
- 支柱 2：面向深度学习的开发基础设施
- 支柱 3：用于自动驾驶汽车开发的物理精准传感器仿真
- 支柱 4：卓越的全方位安全和网络安全计划

支柱 1：AI 设计与实施平台

NVIDIA DRIVE 是全球首个可扩展 AI 平台，实现从 AI 辅助驾驶到自动驾驶出租车的自动驾驶领域全覆盖。该平台由硬件、软件和固件组成，它们协同工作，实现自动驾驶系统和自动驾驶汽车的批量生产。

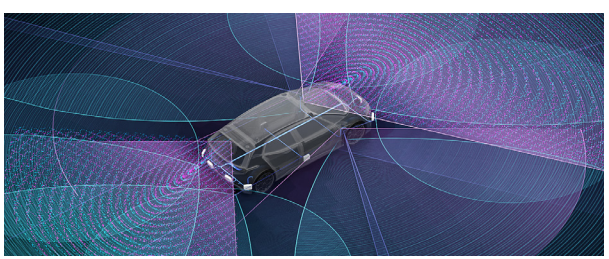
我们的平台融合深度学习与传统软件，以提供安全的驾驶体验。借助高性能计算，车辆能实时感知周围发生的情况，精准自我定位并规划安全的行驶路线。

我们的统一架构从数据中心延伸到车辆，提供了满足国内和国际安全标准要求的全面解决方案。

深度神经网络 (DNN) 在 NVIDIA DGX™ 平台上进行训练，该平台将出色的 NVIDIA 软件、基础设施和专业知识融入现代化统一的 AI 开发解决方案。接下来，在 NVIDIA OVX 上进行仿真测试和验证，然后无缝部署至车载 AI 计算机上运行。NVIDIA OVX 是一款专为支持大规模 Omniverse 数字孪生而设计的计算系统。为确保安全运行，自动驾驶车辆需要能够实时处理所有传感器数据的车载超级计算机。

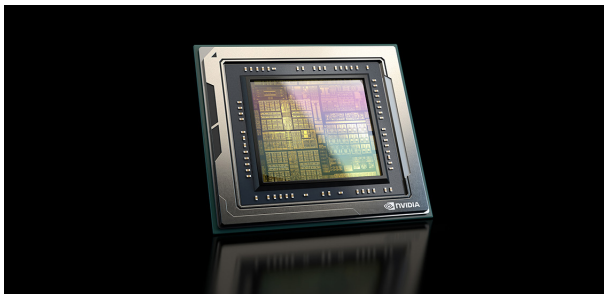
NVIDIA DRIVE 硬件

我们的底层硬件解决方案包括：



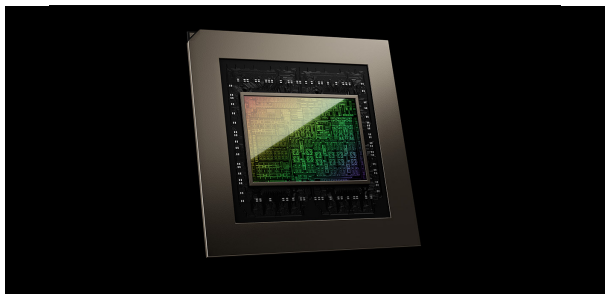
NVIDIA DRIVE AGX Hyperion

NVIDIA DRIVE AGX Hyperion™ 是用于设计自动驾驶汽车的端到端模块化参考架构。它将基于 DRIVE AI 的计算和完整的传感器套件（包括外部和内部摄像头、超声波传感器、雷达和激光雷达）相结合，加速开发、测试和验证。



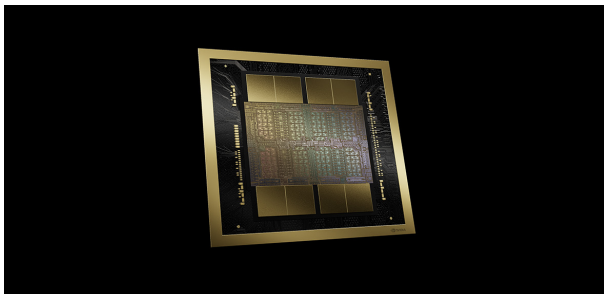
NVIDIA DRIVE AGX Orin

NVIDIA DRIVE AGX Orin™ SoC（片上系统）可提供高达 254 TOPS（每秒万亿次运算）的性能，是智能车辆的中央计算机。它是理想的解决方案，为自动驾驶功能、置信视图、数字集群以及 AI 驾驶舱提供动力支持。借助可扩展的 DRIVE AGX Orin 产品系列，开发者只需在整个车队中构建、扩展和利用一次开发投资，便可从 L2+ 级系统一路升级至 L5 级全自动驾驶汽车系统。



NVIDIA DRIVE AGX Thor

DRIVE AGX Thor™ SoC 是我们的下一代集中式车载计算机，将功能丰富的驾驶舱功能与高度自动化及自动驾驶功能整合在一个安全可靠的系统上。这款自动驾驶处理器采用了我们最新的 CPU 和 GPU 技术，包括 NVIDIA Blackwell GPU 架构，用于转换器和生成式 AI 功能。DRIVE AGX Thor 支持 8 位浮点数 (FP8)，可提供前所未有的 1,000 INT8 TOPS/1,000 FP8 TFLOPS/500 FP16 TFLOPS 性能，同时降低整体系统成本。



NVIDIA Blackwell 架构

NVIDIA Blackwell 平台开启计算新时代，将使各地的组织能够在万亿参数的大语言模型上构建并运行实时生成式 AI，且成本和能耗降低至上一代产品的二十五分之一。Blackwell GPU 架构拥有加速计算的变革性技术，包括全球最强大的芯片。

NVIDIA DRIVE 软件开发套件

软件是将车辆变成智能机器的关键。开放的 NVIDIA DRIVE SDK 为开发者提供了自动驾驶所需的所有基础模组和算法堆栈。该软件帮助开发者更高效地构建和部署各种先进的自动驾驶应用，包括感知、定位和建图、规划和控制、驾驶员监控以及自然语言处理。

- DRIVE 软件堆栈的基础是 DriveOS，这是首个用于车载加速计算的安全操作系统。它包括用于实现高效并行计算的 NVIDIA® CUDA® 库、用于实时 AI 推理的 NVIDIA TensorRT™，以及用于传感器输入处理的 NvMedia。
- NVIDIA DriveWorks 在 DriveOS 的基础上提供对自动驾驶汽车开发至关重要的中间件功能。这些功能包括传感器抽象层 (SAL) 和传感器插件、数据记录器、车辆 I/O 支持和 DNN 框架。该工具拥有模块化和开放的特点，符合汽车行业软件的设计标准。
- NVIDIA 提供了一个 AI 辅助驾驶平台，能够安全地在高速公路和城市交通之间自由穿梭。该平台使用 NVIDIA DRIVE AGX Hyperion 的高性能计算和传感器组合，实现从一地前往另一地的驾驶。如果您想要自己驾驶，系统也会提供主动安全功能，并且能够在危险情况下进行干预。
- NVIDIA 还可为车辆驾乘人员提供了全新的、始终开启的智能服务。NVIDIA Avatar Cloud Engine (ACE) 作为数字助手，提供建议、帮助预订、拨打电话、调控车辆设置并使用自然语言发出提醒。

支柱 2：面向深度学习的开发基础设施

除了车载超级计算硬件，NVIDIA 还设计和开发超级计算机，用于解决安全自动驾驶汽车开发和部署过程中面临的关键挑战。一辆测试车每年可产生数百万亿字节（PB）级别的数据。捕捉、管理和处理整个车队的海量数据需要全新的计算架构和基础设施。

NVIDIA AI 训练和仿真

NVIDIA 提供开发自动驾驶技术所需的完整数据中心硬件、软件和工作流程，涵盖从原始数据采集到验证全过程。它提供了神经网络开发、训练、验证以及仿真测试所需的端到端基础模组。

- **NVIDIA DGX 系统：**这些是专为训练深度神经网络而构建的专用 AI 超级计算机，可以在大型数据集上训练自动驾驶所需的高度复杂的模型。DGX 系统能够训练出足以应对复杂驾驶场景的强大 AI 模型。通过对在多样化和广泛的数据集上进行训练，模型可以更好地适应各种真实世界的条件，从而提高安全性。
- **NVIDIA Omniverse Cloud Sensor RTX™：这套用于开发自动驾驶技术的云端工具提供了高保真的仿真环境，具有逼真的物理和传感器模型，极大地提高了测试的准确性。**Omniverse 允许真实世界部署之前在虚拟环境中进行广泛的测试。这有助于在受控环境中识别和缓解潜在的安全问题，降低实际操作中的风险。

数据管理和云服务

高效的数据管理和基于云的服务对于自动驾驶汽车的开发至关重要：

- **NVIDIA AI 基础设施：**利用 NVIDIA 在高性能计算和 AI 领域的专业知识，该基础设施可满足自动驾驶汽车开发的大规模数据处理和存储需求。NVIDIA AI 基础设施是面向整个行业的解决方案。目前，一家领先的汽车制造商正在使用超过 35,000 个 GPU 来推进其自动驾驶汽车的开发和测试。

支柱 3：用于自动驾驶汽车开发的物理精准传感器仿真

在任何自动驾驶汽车能够安全上路行驶之前，工程师必须首先训练、验证和测试 AI 算法和其他软件，使车辆能够自主行驶。AI 赋能的自动驾驶汽车必须能够对其可能遇到的各种紧急情况做出适当的响应，例如紧急避让车辆、行人、动物和几乎无穷无尽的其他障碍物，包括在现实世界中太危险而难以测试的情况。

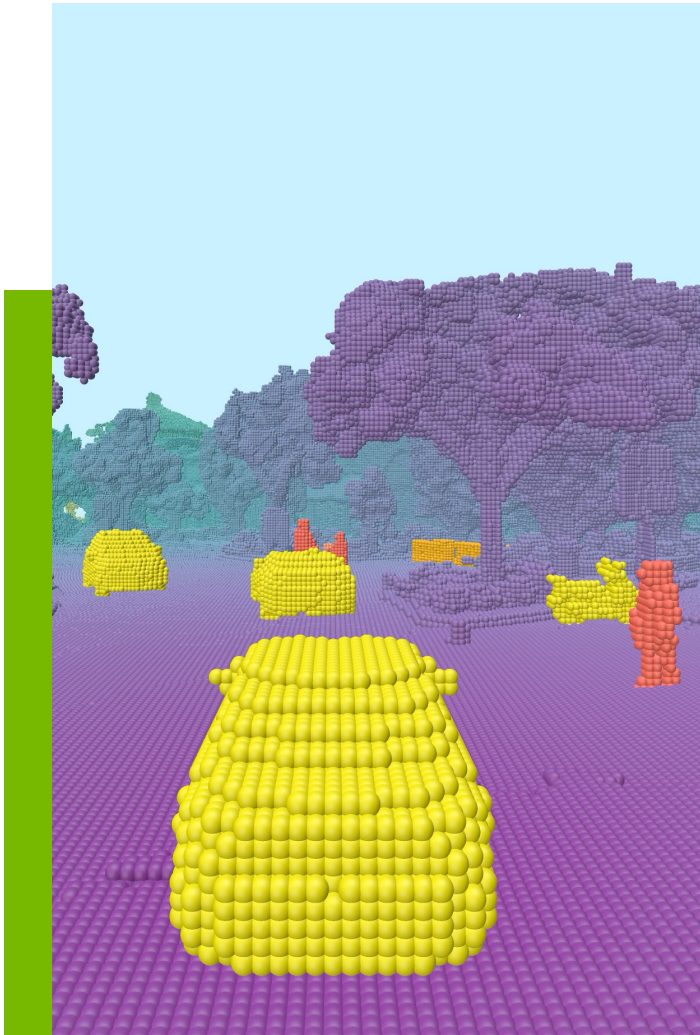
此外，自动驾驶汽车还必须在不同天气、道路或照明条件下行驶。但车辆的实际道路测试难以覆盖所有情况，且道路测试也缺乏足够的可控性、可重复性、详尽性和高效性。在真实仿真环境中进行测试的能力对于提供安全的自动驾驶汽车至关重要。将实际道路行驶里程与数据中心的仿真里程结合，这是开发和验证自动驾驶汽车的关键所在。

自动驾驶汽车仿真对时间、可重复性和实时性能具有超高的要求，并且必须能够大规模运行。此外，在基于物理效果的虚拟世界中，从自动驾驶汽车多传感器生成数据需要巨大的计算负载。

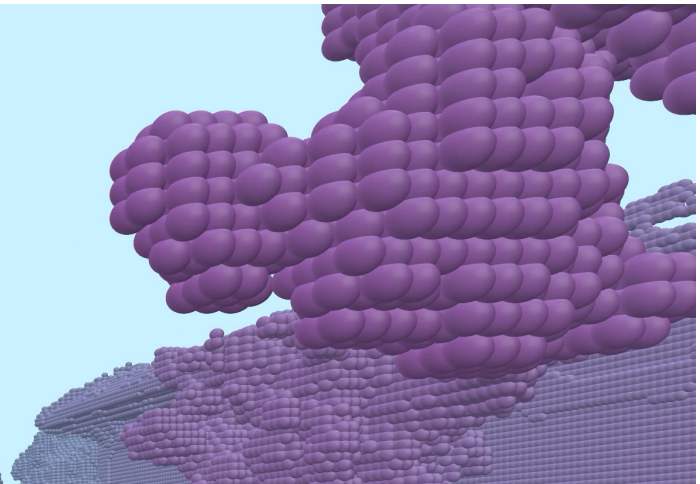
基于 OpenUSD 构建的 NVIDIA Omniverse Cloud Sensor RTX 旨在让开发者通过高保真传感器仿真、物理特性和逼真的行为来增强自动驾驶汽车仿真工作流。借助这些 API，您可以与构建车辆动力学和交通仿真工具的庞大合作伙伴生态系统建立连接。您还可以引入通用场景描述 (USD) 内容，以扩展至新地区，应对新的运行设计域（ODD）。

NVIDIA Omniverse Cloud Sensor RTX 微服务为广泛部署在自动驾驶车辆上基于物理效果的传感器（如摄像头、激光雷达、雷达和超声波传感器）及其神经网络渲染提供支持。渲染出的合成数据和真值标签可用于训练感知模型，以及在闭环测试中验证自动驾驶软件堆栈。

神经重建引擎是用于自动驾驶汽车仿真平台的全新 AI 工具集，其利用多个 AI 网络将记录的传感器数据转化为面向仿真的可用世界模型。新的工作流利用 AI 自动提取仿真所需的关键组件，包括环境、3D 素材和场景。然后将这些片段重构为既拥有数据记录的真实感，又具有完全的主动性、可根据需要进行操纵的仿真场景。手动实现这种细节丰富和多样性的场景，不仅成本高、耗时长，而且也不具备扩展性。



此外，**fVDB**还有一个全新的开源深度学习框架，可用于生成大规模场景，利用现实世界的 3D 数据训练自动驾驶汽车。它基于 OpenVDB 构建 AI 操作工具，以创建现实世界环境的高保真虚拟表征。这些丰富的 3D 数据集已为 AI 做好准备，可用于高效的模型训练和推理。很快，fVDB 功能将作为 NVIDIA NIM 微服务提供，使开发者能够将 fVDB 核心框架整合到通用场景描述 (OpenUSD) 工作流中。fVDB NIM 微服务在 NVIDIA Omniverse 中生成基于 OpenUSD 的几何图形。



支柱 4：卓越的全方位安全和网络安全计划

安全性

在自动驾驶汽车研究、开发和部署过程的每一步，保障安全性始终是我们的首要任务。我们采用安全为先的方法，注重整个自主系统在设计、验证、确认和生命周期支持中的多样性和冗余性。我们在流程、产品和安全架构中遵循并开发一流的解决方案。NVIDIA 安全性专为软件定义的自动驾驶而设计，因为它可接受、应对并利用自动驾驶汽车的复杂性。

为了制定自动驾驶汽车安全计划，我们遵循美国交通部国家公路交通安全管理局在 2017 、2018 和2020 年出版物中的建议。[1]

在整个计划中，我们遵循国际标准化组织制定的汽车行业安全标准，包括：

功能安全 (ISO 26262)

自动驾驶汽车必须能够在系统发生故障时安全运行。对于 L2/L2+ 级别，我们必须检测并缓解故障（将控制权交还给驾驶员），而对于 L3/L4 级别，我们必须确保系统继续安全运行并达到最小风险状态。我们将功能安全性应用于硬件、软件和系统所有层面，从应用程序到中间件和操作系统、电路板和电路板上的芯片，直至提供自动驾驶功能的系统。

预期功能安全 - SOTIF (ISO 21448)

专为功能安全性设计的系统 (ISO 26262)[2] 还必须进行设计和测试，以在与预期功能相关的所有安全关键指标上表现良好 (ISO 21448)[3]。

即使系统按设计正常运行，未发生故障，也可能存在安全隐患。SOTIF 的重点在于确保不存在因预期功能缺陷或可合理预见的误用而造成危害的不合理风险。例如，感知失败的发生率必须足够低，以便自动驾驶汽车很少无法检测到行驶道路上的行人。

安全与 AI

我们积极参与 AI 安全相关的持续标准化倡议，如 ISO PAS 8800[4]（制定中）、ISO/IEC TR 5469[5]及其后续的 ISO/IEC TS 22440 标准[6]（制定中）。

法规及标准

我们遵守国际和美国法规，包括全球 NCAP（新车评鉴规程）、欧洲 Euro NCAP 和联合国欧洲经济委员会的规定。我们还影响、共同制定并遵守国际标准组织、新车评价规程、SAE 以及其他行业标准。

我们为电气电子工程师学会 (IEEE) 的标准化倡议做出贡献，例如 IEEE 2846-2022（安全相关自动车辆行为模型假设）[7]和 IEEE P2851（关于 IP、SoC 和混合信号 IC 安全分析和安全验证的交换/互操作性格式[8]）。

除了遵守政府和行业指南外，我们还实行公开披露并与行业专家合作，以确保掌握所有当前和未来安全问题的最新动态。我们还在多个安全工作组中担任领导职务，以推动尖端技术和探索新的研究领域，如 AI 系统的安全性和可解释 AI。

符合最高标准

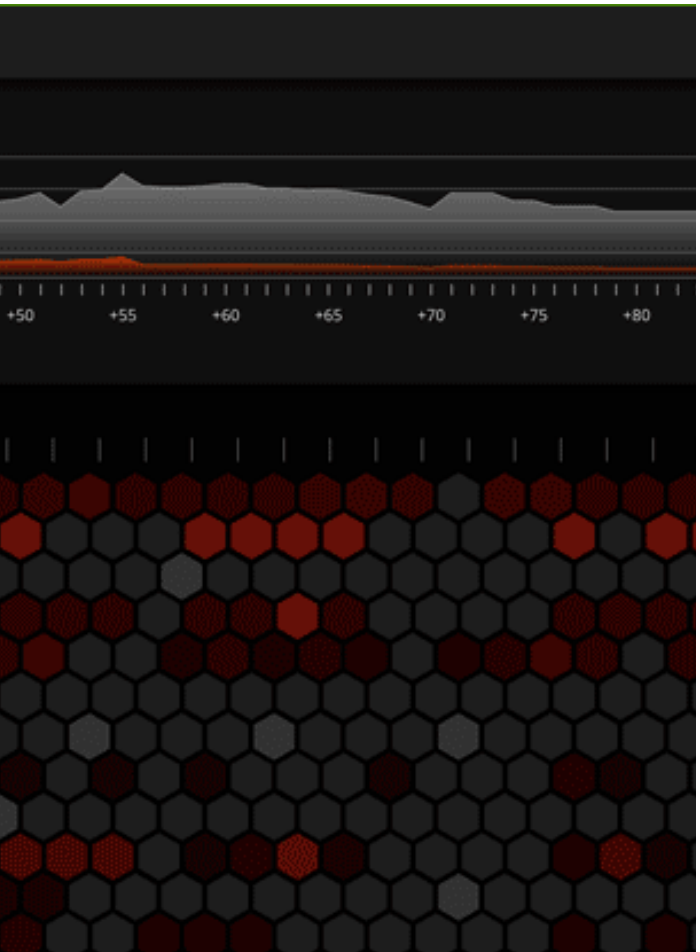
为提升交通安全性，自动驾驶汽车必须拥有符合最高标准的流程和底层系统。

NVIDIA 通过独立且经认可的评估机构 TÜV SÜD 确保符合国际标准化组织 (ISO) 26262:2018 “道路车辆功能安全”标准。

NVIDIA DRIVE AGX 平台和流程最近通过了 TÜV SÜD 认证和评估：

- NVIDIA DRIVE 核心开发流程已通过 ISO 26262 汽车安全完整性等级 (ASIL) D 级认证。
- NVIDIA DRIVE AGX Orin SoC 完成了概念和产品评估，并被认为符合 ISO 26262 ASIL D 级系统要求以及 ASIL B 级随机故障管理要求。
- NVIDIA DRIVE AGX Orin 主板完成了概念评估，并被认为符合 ISO 26262 ASIL D 级要求。
- 基于 NVIDIA DRIVE AGX Orin 的系统整合 DRIVE AGX Orin SoC 和 DRIVE AGX Orin 主板，完成了概念评估，并被认为符合 ISO 26262 ASIL D 级要求。
- NVIDIA DriveOS 6.x 的开发工作正在进行中，TÜV SÜD 将评估其 ASIL D 级合规性。这是继 DriveOS 5.2 ASIL B 级认证变更后的又一次认证，包括用于实时 AI 推理的 NVIDIA CUDA 库和 NVIDIA TensorRT 软件开发套件。

网络安全



网络安全未得到保障，自动驾驶汽车平台则不可能被认为是安全的。全面的安全工程实践和开发对提供汽车行业所需的功能和整体安全性至关重要。

安全漏洞可能会削弱系统实现基本安全目标的能力。为了提供消费者可高度信任的一流汽车安全平台，我们组建了一支世界级的安全团队，并遵守政府和国际标准及法规。我们还建立了强大的合作伙伴关系，以应对安全事件，并作为保护客户数据隐私的良好管理者。

NVIDIA 遵循适用于硬件和软件安全功能实施的国际和国内标准（包括加密原则）。我们遵守美国国家标准与技术研究院（NIST）[9]和《通用数据保护条例》（GDPR）[10]制定的标准，以保护所有个人的数据和隐私。

我们的网络安全团队与汽车信息共享和分析中心 (Auto-ISAC)、NHTSA、SAE 和美国商务部工业与安全局合作。我们还为自动识别系统（美国国土安全部）、联邦信息处理标准（《美国联邦信息安全管理法案》）和通用标准标准或规范的制定做出了贡献。

我们遵循并维护联合国欧洲经济委员会第 155 号法规[11]中规定的网络安全管理系统。此外，我们采用 ISO/SAE 21434 网络安全流程并相应地调整汽车开发实践，以便更轻松地发布合规声明，同时根据 ISA/IEC 62443 标准利用其他网络安全敏感行业的流程和实践。

我们参与了 SAE J3101 标准的制定，确保在硬件和系统软件层面实现必要的网络安全基础模组。我们审查平台代码的安全一致性，使用静态和动态代码分析技术进行早期检测，并执行渗透测试和其他攻击性安全技术进行验证。此外，我们还参与了 SAE 8477，以确保我们的安全测试方法能够与时俱进。

NVIDIA 在系统设计和危害分析流程中采用了严格的安全开发生命周期，包括安全要求的端到端可追溯性、覆盖整个自动驾驶系统的威胁模型。这包括硬件、软件、制造和 IT 基础设施，确保安全设计和编码指南到位。DRIVE AGX 平台还具备多层防御能力，可提供应对持续攻击的弹性。

NVIDIA 网络安全团队通过与包括汽车在内的 NVIDIA 各业务部门沟通需求，为其提供可参考的信息。包括提供安全威胁传播、扩散深入研究计划

NVIDIA 还维持有专门的产品安全事件响应团队，在内部以及与合作伙伴一同管理、调查和协调安全漏洞信息。这使我们能够控制和修复任何直接威胁，同时与合作伙伴开放合作，从安全事件中恢复。

此外，我们与供应商密切合作，确保构成整个自动驾驶平台的组件提供必要的安全功能。当从原始数据到处理输入和控制操作的所有环节都符合安全要求时，复杂平台的网络安全就得到了保障。NVIDIA 还与供应商合作，确保他们具备应对新威胁或未发现威胁的网络安全响应能力。

最后，由于车辆系统的使用寿命比许多其他类型的计算系统更长，我们利用先进的机器学习技术来检测车辆通信和行为中的异常情况，并提供额外的零日攻击监控能力。

安全架构

概述

NVIDIA 设计了 DRIVE AGX 平台，以确保自动驾驶汽车在预期的运行设计域（ODD）内安全行驶。当车辆处于其定义的 ODD 以外或因条件动态变化而不在其 ODD 内时，我们的产品可使车辆恢复到最小风险状态（也称为“安全回退状态”）。例如，如果自动驾驶系统检测到突发变化，如暴雨影响传感器，从而影响其在运行设计域内的驾驶能力，该系统会将控制权移交给驾驶员。若检测到重大危险，系统将会立即安全停车。

NVIDIA 在 DRIVE 平台开发的每个阶段都遵循 V 模型（包括验证和确认）。我们还对产品的功能和相关危害进行详细分析，以制定产品安全目标。对于每个已识别的危险，我们都会制定安全目标来降低风险，对每个目标评估 ASIL 等级。ASIL 等级 A、B、C 或 D 表示所需的风险缓解水平，其中 ASIL D 级代表最高等级。满足这些安全目标是我们进行设计的最高级别要求。通过将安全目标融入功能设计说明，我们可以制定更详细的功能安全要求。

在系统开发层面，我们通过将功能安全要求应用于特定系统架构来优化安全设计。故障模式及影响分析 (FMEA)、故障树分析 (FTA) 和相关失效分析 (DFA) 等技术分析方法可通过迭代的方式用于识别薄弱点并改进设计。相关的技术安全要求将提交给硬件和软件团队，以指导下一级别的开发。我们还为自动驾驶汽车系统设计了冗余和多样化功能，以使其尽可能具有弹性。这确保了在检测到故障或进行故障补偿重新配置时，车辆仍可继续安全运行。

在硬件开发层面，我们通过将技术安全要求融入电路板和 SoC 硬件设计，以完善整体设计。技术分析则用于识别薄弱点并改进硬件设计。对最终的硬件设计进行分析，可用于验证硬件故障相关的风险是否得到充分缓解。

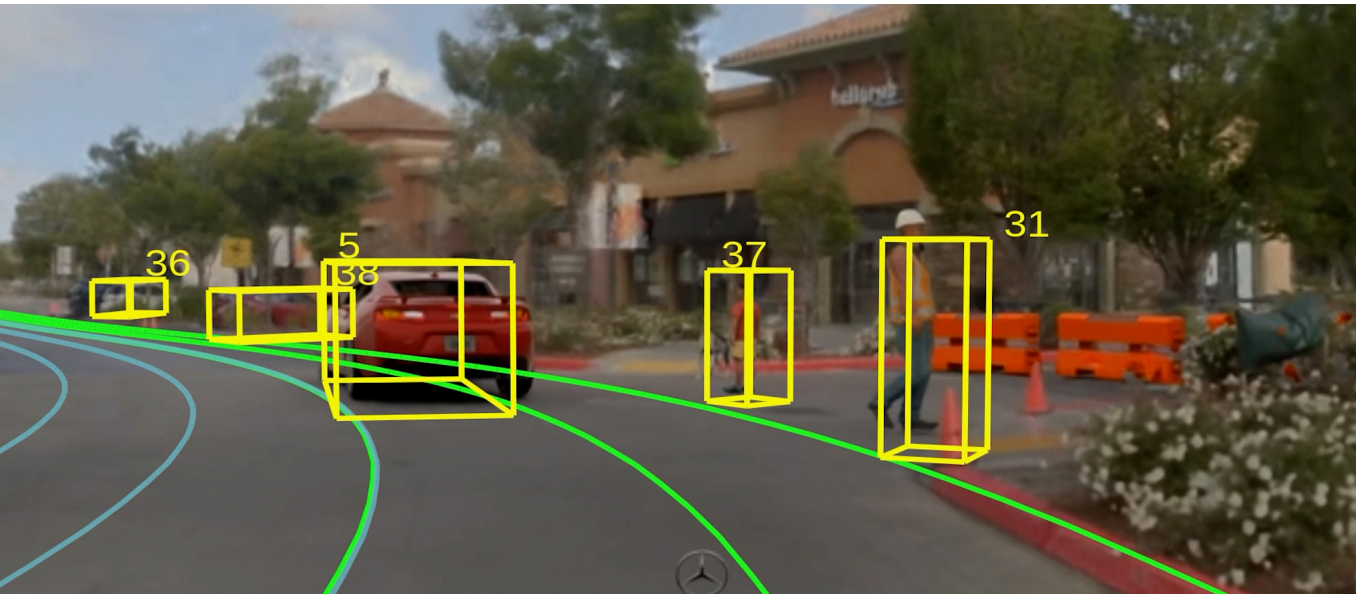
在软件开发层面，我们考虑包括固件在内的所有软件。我们通过将技术安全要求融入软件架构来完善整体设计。我们还在单元和集成级别执行代码检查、审查、自动化代码结构测试和代码功能测试。专用于软件的故障模式及影响分析也被用于设计更好的软件。此外，我们还设计了接口、基于需求、故障注入和资源使用验证方法的测试用例。

当完成所有必要的硬件和软件组件开发后，我们会集成并启动系统级的校验证和确认过程。除了自动驾驶汽车仿真外，我们还进行系统测试和验证。

软件定义的自动驾驶安全性

我们的安全方案专为软件定义的自动驾驶而打造。与传统系统的安全方案相比，NVIDIA 的安全策略：

- 专为动态系统配置打造
- 是内含丰富软硬件的灵活平台
- 针对越来越多的功能进行优化
- 生态系统友好，系统边界开放
- 专为 AI 硬件、软件和工具设计
- 可扩展以适应新算法
- 支持可分解式安全概念
- 设计用于执行百万级代码
- 可轻松无线更新
- 功能感知、数据导向且经过验证
- 硬件-固件-软件协调



一体化：AI 训练、仿真和测试

NVIDIA 的基础设施平台包含一个用于标注数百万图像的数据工厂。其使用来自 NVIDIA 内部集群的 NVIDIA DGX 系统进行 DNN 训练，借助 DRIVE Constellation 进行硬件在环仿真，并整合其他工具。

自动驾驶汽车软件开发首先要从全球不同的环境和场景下的车辆中收集海量数据。跨越多个地区的众多团队访问这些数据，进行标注、索引、归档和管理，然后才能将这些数据用于 AI 模型训练和验证。此外，对于罕见或难以标注的场景，可以使用仿真的合成数据增强真实数据。我们将自动驾驶汽车工作流程的第一步称为“数据工厂”。

当标注的数据被用于训练感知和其他自动驾驶功能的模型时，AI 模型的训练就开始了。这是一个迭代的过程。数据工厂利用初始模型挑选下一个待标注的数据集。深度学习工程师根据需要调整模型参数，然后重新训练 DNN，此时下一个标注数据集被添加到训练集中。这个过程持续进行，直至达成所需的模型性能和准确性。

在开发过程中，自动驾驶技术必须在各种驾驶条件下进行一次又一次的评估，以确保自动驾驶的安全性远超人类驾驶的车辆。仿真在虚拟世界中运行试驾场景，向驾驶堆栈提供渲染的传感器数据并执行驾驶堆栈发出的驾驶命令。重新仿真将先前记录的现实世界传感器数据回放至驾驶堆栈。然后根据大量且不断增长的测试数据来验证 AI 模型。

硬件

NVIDIA DRIVE AGX 硬件架构具有可扩展性，涵盖从入门的高级驾驶辅助系统到完全自动驾驶出租车等各个领域。当前这一代 DRIVE AGX Orin SoC 安全架构由数百名架构师、设计师和安全专家基于对数百个安全相关模块的分析开发。

NVIDIA DRIVE AGX Orin 是一款软件定义平台，旨在实现从 L2 级到 L5 级完全自动驾驶汽车的架构兼容平台，使 OEM 能够开发大规模、复杂的软件产品系列。NVIDIA 所有的 DRIVE AGX SoC 产品系列（DRIVE AGX Thor、Orin 和 Xavier™）均可通过开放的 CUDA 以及 TensorRT API 和库进行开发，因此开发者可在多代产品中充分利用他们的投资。

2022 年，NVIDIA 推出了为安全自动驾驶汽车设计的新一代集中式计算机 DRIVE AGX Thor。它支持 8 位浮点 (FP8) 技术，提供前所未有的 1,000 INT8 TOPS/1,000 FP8 TFLOPS/500 FP16 TFLOPS 性能。

这款新一代自动驾驶汽车处理器将智能功能（包括高级驾驶辅助和车载信息娱乐）统一到单一架构中，以提高效率、安全性和保障性。

它还具备先进的 AI 功能并将集成全新的 NVIDIA Blackwell GPU 架构，专为Transformer、LLM 和生成式 AI 工作负载而设计。

DRIVE AGX Thor 将用于汽车制造商的 2025 车型，与此同时通过将更高的性能和先进的功能推向市场加速推动生产路线图。

软件

DRIVE SDK 中的感知模组获取传感器数据，并结合深度学习和传统信号处理来确定对车辆环境的理解，即“世界模型”。一旦了解环境，规划模组就会利用这些信息查找和评估一组轨迹并确定最佳路线。车辆动态控制模组可将选择的路线转换为车辆动作执行。

DRIVE SDK 目前使用 20 多个 DNN 模型同时运行，此外还具有大量的计算机视觉和机器人开发算法。并且，DNN 的数量及其覆盖的功能仍在持续增长中。

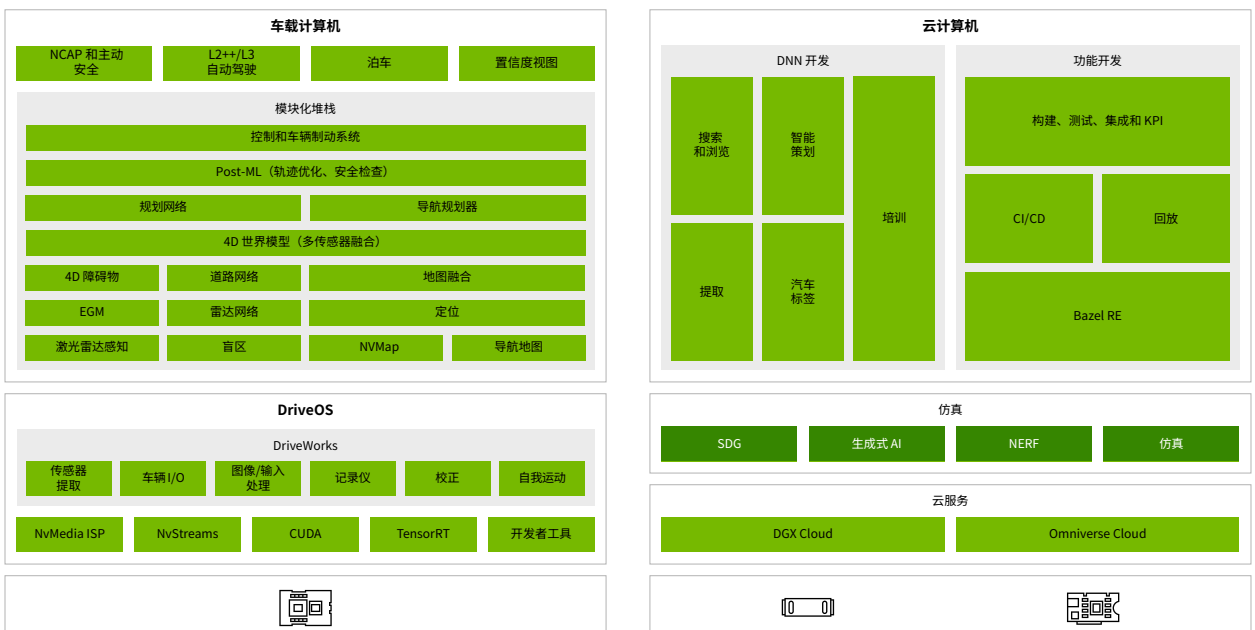
每个主要功能（如传感器处理、基于 AI 的感知、定位、轨迹规划和地图）都采用了多种冗余和多样化的方法来实现最高级别的安全性。例如，DRIVE SDK 使用嵌入式模块检测并处理障碍物和可行驶空间。对于等待条件，我们检测交通灯、停车标志、十字路口和停车线。DRIVE SDK 目前使用 20 多个同时运行的深度神经网络（DNN）模型，此外还具有大量的计算机视觉和机器人算法。这种检测是在多个帧上进行的，并能随着时间的推移跟踪对象。

我们还使用多种类型传感器（雷达、摄像头、激光雷达和超声波传感器）实现分层多样性。各种 DNN 的组合、多帧的对象跟踪，以及不同类型传感器的存在，确保了在运行设计域内的安全运行。此外，集成的功能安全机制在系统发生故障时可确保安全运行。

车辆和传感器

DRIVE AGX Hyperion 是 DRIVE AGX 平台的参考车辆实施方案，可实现自动驾驶跨级别的开发、数据采集和提取、校验和验证。该平台利用多种传感器模式（包括摄像头、雷达、激光雷达、IMU 和超声波传感器），并可部署于各种类型的车辆上。

DRIVE 软件架构



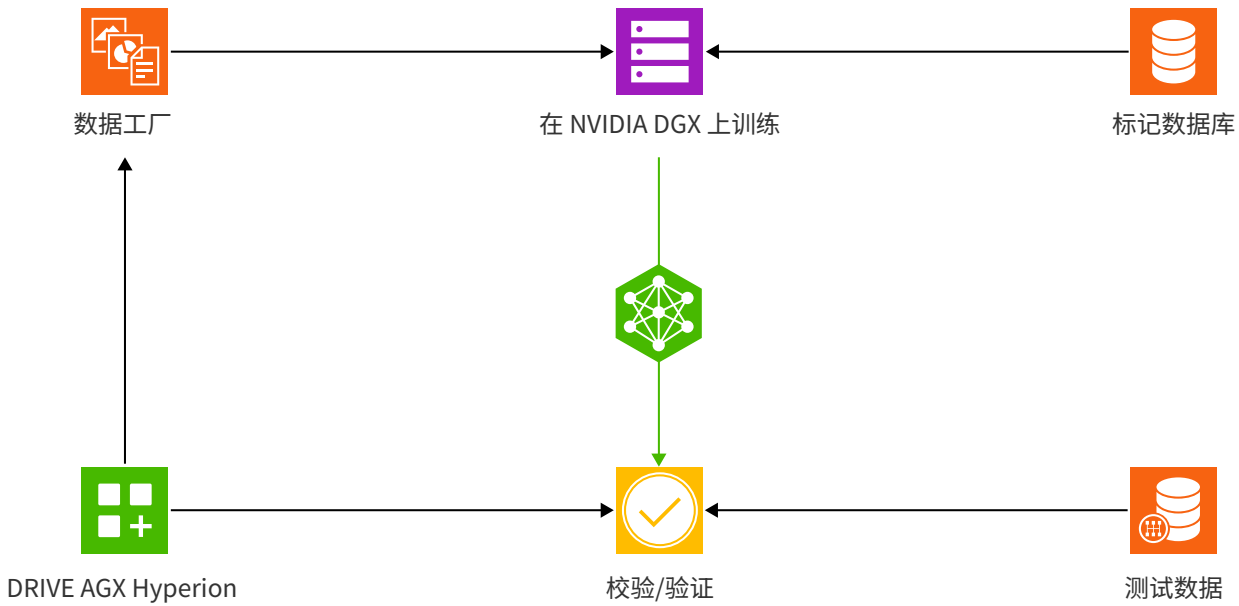
计算机 1 - 汽车平台　　计算机 2 — 数据中心平台

数据中心

在采集传感器数据后，我们会对其进行处理，若为摄像头数据，则挑选要标注的图像用于训练 AI。整个过程会持续验证。我们不仅标注捕获帧中的物体和图像，还会标注视频序列中的场景和条件。我们拥有的多样化和无偏差数据越多，DNN 安全性就越高。我们还定义了衡量采集数据质量的关键性能指标，并利用 NVIDIA Omniverse Replicator 将合成数据添加到我们的训练数据集中。这让开发者可以生成预先标记的真实数据来引导算法开发。最终目标是不断添加训练数据，以构建全面的位置、条件和场景矩阵。神经网络模型性能使用独立测试数据进行验证，并在新数据上训练模型时重新测试。

除了标注图像中的物体外，我们还标注了采集数据的条件。这样可提供我们用作测试数据集的条件矩阵，以测试我们的 DNN 模型在各种场景、天气条件和一天中各个时间段的性能。

数据中心的 GPU 广泛用于研究具有多样化数据集的新 DNN、持续训练神经网络模型、分析工作流结果、以及使用大规模系统测试和验证结果，以在虚拟世界中仿真和重放采集的数据。



道路测试

NVIDIA 制定了《DRIVE 道路测试操作手册》，以确保安全、标准化的道路测试流程。该文件规定每次道路测试之前、期间和完成后必须采取哪些措施。如美国交通部报告*《准备迎接未来交通：自动驾驶汽车 4.0》*[2] 中的建议，NVIDIA 的流程依据美国联邦航空局认证*《飞行员操作手册》*，美国每一架通用航空飞机在飞行时必须携带该手册。

道路测试始终由训练有素的安全驾驶员执行，他们持续监控车辆行为，并在必要时随时进行干预。测试操作员也在车中监控自动驾驶软件，例如检查汽车检测到的物体是否与实时观察到的物体对应，以及车辆路线是否适合当前道路状况。

在无法派人测试时，我们也可以修改流程。NVIDIA 远程操控系统允许人类副驾驶能够远程监控车辆，而虚拟测试平台使得安全、可靠地虚拟测试车辆成为可能。

在允许软件上路测试之前，需要通过单元测试、集成测试和系统仿真进行广泛测试。

开发者培训和教育

NVIDIA 致力于让开发者教育变得更容易获取，帮助专家和学员了解这些突破性技术的详情。NVIDIA 深度学习培训中心（DLI）提供关于如何为自动驾驶车辆设计、训练和部署 DNN 的多门课程。我们还制作了广泛的内容来回答常见问题，目前已拥有 200 多万注册开发者，涵盖深度学习、加速计算、自主机器和自动驾驶汽车等八个不同的领域。

此外，NVIDIA 还举行 GTC 大会，帮助学生、开发者和高管了解加速计算、AI 和自动驾驶汽车。每次大会都包含数百场分会议、小组讨论和实践课程，以及突破性的技术演示和合作伙伴展览。每次大会都以首席执行官黄仁勋发表主题演讲拉开序幕，并举办数百场分会议、小组讨论和实践课程，以及突破性的技术演示和合作伙伴展览。

总结

NVIDIA 为安全可靠的软件定义自动驾驶汽车的设计、开发和制造提供基础技术。我们将视觉和高性能计算的力量与人工智能和成熟的软件开发相结合，使我们成为全球汽车制造商及运输公司的宝贵合作伙伴。

我们在设计和实施强大的 NVIDIA DRIVE AGX 平台时遵循业界最严格的安全标准，并与行业专家携手合作解决当前和未来的安全问题。我们的平台完全符合并支持自动驾驶汽车制造商和自动驾驶出租车公司的安全目标。

打造安全的自动驾驶汽车技术是我们公司有史以来最大、最复杂的项目之一。我们投入数十亿美元用于研发，公司内有数千名工程师致力于这一目标。迄今为止，我们已在汽车安全流程上每年有超过 1500 名工程师投入其中。

目前，已有超过 80 家自动驾驶汽车公司上路测试采用 NVIDIA 技术的车辆。他们深知，强大的车载计算能力可实现冗余和多样化的软件算法，为每位驾驶员提供更高的安全保障。

我们坚信，自动驾驶汽车将为社会带来变革性的好处。通过最终抵消驾驶过程中的人为错误，我们可以杜绝绝大多数事故并将发生事故的影响降到最低。我们还可以提升道路效率和减少车辆尾气排放。最后，无法驾驶汽车的人也能够轻松召唤自动驾驶汽车，享受出行的自由。

NVIDIA 在自动驾驶汽车开发中发挥着关键作用，将在未来几十年彻底改变交通运输行业。对于我们而言，没有什么比攻克技术难题、改善人们的生活、提升道路安全更令人兴奋的事情了。

附录

附录A：NVIDIA 的专家组活动

NVIDIA 作为相关领域的专家组织备受推崇，我们的专家在国际标准化工作小组中发挥着积极的领导作用即为明证。受益于我们专业知识的工作组包括：

- ISO TC 22/SC 32/WG 8，ISO 26262 “功能安全”和 ISO 21448 “预期功能的安全”
- ISO TC 22/SC 32/WG 13，ISO TS 5083 “自动驾驶系统的功能安全和网络安全—设计、验证和确认方法”
- ISO TC 22/SC 32/WG 14, ISO PAS 8800 “安全和人工智能”
- ISO TC 22/SC 32 和 SAE TEVEES 18A，ISO/SAE 21434 “网络安全工程”
- ISO/TR 9839 “根据 ISO 26262-5 应用预测性维护”
- IEC 61508 “电气/电子/可编程电子安全系统的功能安全”
- IEEE 2846-2022 “自动驾驶汽车决策安全考虑因素的形式模型”
- IEEE P2851 “可靠性生命周期内互操作性功能安全数据格式标准”
- IEEE 计算机学会功能安全标准委员会 (FSSC)
- ISO/IEC JTC1 SC42 JWG4, ISO/IEC TR 5469 和 ISO/IEC TS 22440 “人工智能——功能安全性和 AI 系统”
- 欧洲汽车供应商协会，欧洲新车安全评鉴协会（Euro NCAP）
- 汽车装备及零部件建设联络委员会
- 联合国欧洲经济委员会自动驾驶车辆功能要求 (FRAV) 和自动驾驶验证方法 (VMAD) 工作组
- 联合国欧洲经济委员会动态控制辅助系统工作组 (DCAS)
- SAE 汽车功能安全和自动地面车辆 AI 委员会
- 多个全球研发联盟、技术审查委员会和研发主席角色

附录B：国家和国际安全法规和建议

NVIDIA 遵守的国家和国际安全建议包括：

国际标准化组织 (ISO)

我们遵守 ISO 26262 和 ISO 21448 (SOTIF) 标准。ISO 2626210 针对道路车辆的功能安全。我们将 ISO 26262 应用于应用程序、中间件、操作系统、电路板和芯片层级。ISO 2144811 则面向道路车辆预期功能的安全性。它沿用并拓展了 ISO 26262 开发流程，以解决 SOTIF 问题。我们还密切关注 ISO PAS 8800、ISO/IEC TR 5469 和 ISO/IEC TS 22440 正在推进的 AI 安全标准化工作。

全球新车安全评鉴协会（NCAP）

区域 NCAP 会根据其特定市场调整安全实践，并且 NVIDIA 将与所有本地 NCAP 一起评估性能。欧洲新车安全评鉴协会（Euro NCAP）为消费者提供在欧洲销售车辆的独立安全评估。Euro NCAP 发布了 2025 年路线图[12]，提出重视一级、二级和三级车辆安全的愿景和战略。目前，我们正在积极落实以下 Euro NCAP 建议：

- 自动紧急转向
- 行人和骑车人安全
- 辅助驾驶测试
- 仿真和评估测验
- 儿童存在检测
- 自动紧急制动
- 网络安全
- V2X
- 驾驶员监控
- 人机界面 (HMI)
- 行人和骑车人安全
- 仿真和评估测验
- 儿童存在检测
- 网络安全

附录

附录 C：
NHTSA 安全要素

美国国家公路交通安全管理局（NHTSA）在报告中概述了自动驾驶安全的关键话题。**自动驾驶系统 2.0：安全愿景**在代表行业达成的公共道路上使用自动驾驶系统安全共识的 12 个安全要素中，有 10 个与 NVIDIA 有关。

系统安全NVIDIA 已制定一个系统安全计划，该计划基于系统工程方法集成强大的设计和验证流程，其目标是设计最高安全级别的自动驾驶系统，并且不存在不合理的安全风险。

物体与事件检测和响应物体与事件检测和响应是指检测与当前驾驶任务相关的任何情况，并对这种情况作出适当的驾驶员或系统响应。NVIDIA DRIVE 自动驾驶汽车模组负责检测和响应道路内外的环境刺激。NVIDIA DRIVE IX 模组可帮助监控驾驶员状态，并在需要时采取缓解措施。

设计适用范围根据 NHTSA 的建议，NVIDIA 已为单个驾驶自动化系统或功能开发了一组广泛的运行设计域。每个运行设计域至少包括以下信息，以确定产品的能力边界：道路类型、地理区域及地域条件、速度范围、环境条件（天气、时间等）和其他限制。

后备计划（最小风险状态）我们的产品使车辆能够检测到系统故障或违反运行设计域的情况，然后根据警告和降级策略将系统过渡到安全或降级运行模式。每个 NVIDIA 自动驾驶系统都包含一种后备策略，使驾驶员能够重新获得对车辆的适当控制，或者允许自动驾驶车辆独立恢复到最小风险状态。我们的 HMI 产品可用于通知驾驶员潜在危险事件，并独立地将车辆恢复到最小风险状态，或提醒驾驶员重新取得适当控制。最小风险状态根据给定故障的类型和程度而有所不同。

验证方法验证方法建立了自主系统能够实现其预期功能的信心。我们的开发流程包含严格的方法来验证和确认我们产品的行为功能和部署。为了证明自动驾驶汽车在公共道路上部署的预期性能，我们的测试方法包括仿真、测试轨道和道路测试的结合。这些方法在广泛变动的状态下也能展现性能，例如部署后备策略时。

人机界面DRIVE IX 为驾驶舱解决方案提供商提供开放式软件堆栈，构建和部署将个人车辆转换为交互环境的功能，以实现智能助手、图形用户界面以及沉浸式媒体和娱乐。

车辆网络安全NVIDIA 在系统设计和危害分析流程中采用严格的安全开发生命周期，包括涵盖整个自动驾驶系统的威胁模型，如硬件、软件、制造和 IT 基础设施。NVIDIA DRIVE AGX 平台还具备多层防御能力，可抵御持续攻击。

NVIDIA 还设有专门的产品安全事件响应团队，在内部以及与合作伙伴一同管理、调查和协调安全漏洞信息。这使我们能够控制和修复任何直接威胁，同时与合作伙伴开放合作，以从安全事件中恢复。

数据记录NVIDIA 回放功能可以将行驶在公共道路上的测试车辆上传感器的真实数据输入到模拟中。为更大限度地提升自动驾驶汽车的安全性，NVIDIA 提供了仿真数据来测试危险道路场景，并结合了回放的真实世界数据。

消费者教育和培训我们不断开发、记录和维护资料，以教育我们的员工、供应商、客户和最终消费者。我们通过 **NVIDIA 深度学习培训中心**NVIDIA 深度学习培训中心提供多种 AI 课程，并在**NVIDIA**全球 GTC 大会上报道新知识和发展动态。我们还与研究机构合作开发更好的自动驾驶方法，保持最高的职业操守以在自动驾驶汽车领域共同打造世界级的思想领导力。

联邦、州和地方法律我们的运营原则是将安全放在首位，并遵守国际、联邦、州和地方法规以及安全和功能安全标准。我们还经常与监管机构沟通，以确保我们的技术超越所有安全标准和期望。我们积极参与标准化组织，推动自动驾驶的未来发展。

附录 D：
参考资料

1. NHTSA 自动驾驶系统：**https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems**
2. ISO 26262：道路车辆功能安全国际标准化组织 (ISO)，2018 年。第一部分：词汇：术语和定义：**https://www.iso.org/standard/68383.html**
3. ISO 21448 “道路车辆—预期功能安全”，2022**https://www.iso.org/standard/77490.html**
4. ISO/CD PAS 8800:**ISO/CD PAS 8800—2000 道路车辆；安全和人工智能**
5. ISO/IEC TR 5469:2024: **ISO/IEC TR 5469:2024—人工智能；功能安全和 AI 系统**
6. ISO/IEC AWI TS 22440-1/-2/-3: **ISO/IEC AWI TS 22440-1—人工智能；功能安全和 AI 系统，第 1 部分：要求**
7. IEEE 2846-2022 网页：**IEEE SA - IEEE 2846-2022**
8. IEEE P2851 网页：**https://sagroups.ieee.org/2851/**
9. NIST 网络安全：**https://www.nist.gov/topics/cybersecurity**
10. GDPR: **https://gdpr.eu/**
11. 联合国欧洲经济委员会第 155 号法规：**https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security**
12. 准备迎接未来交通：自动驾驶汽车 4.0 (AV 4.0)，2020：**https://www.transportation.gov/av/4**