自动驾驶汽车车辆性能指南

A. 指南

根据现行法律，制造商要自证其生产的公共道路车辆符合适用的联邦机动车辆安全标准（FMVSS）。因此，如果汽车没有越过现行的 FMVSS 监管框架并保持传统的汽车设计，对于正在出售的高度自动驾驶汽车目前还没有具体的联邦法律屏障。

然而，制造商和设计新自动驾驶汽车系统的其他实体接受 NHTSA 缺陷、召回和执法部门的管制。交通部预计制造商和计划测试和部署高度自动驾驶汽车的其他实体将使用本指南、行业标准和最佳实践，以确保系统在实际道路条件下高度可靠。

NHTSA 预计将在本指南发布后采取后续行动，如在效益评估、人员因素、网络安全、性能指标、客观测试和其他将在未来鉴定的领域进行更多的研究。如前所述，交通部计划召开公众研讨会，就本指南和本政策的其他内容征求意见。本指南突出了制造商和设计高度自动驾驶汽车系统的其他实体在设计、测试和部署高度自动驾驶汽车时应考虑和解决的重要领域。本指南为非强制性文件。NHTSA 可能会考虑在未来通过监管行动将本指南中的某些内容升级为具有约束力的硬性规定。本指南无意让各州将其作为自动驾驶汽车开发、设计、生产和测试的法律要求。本指南结尾部分列出了未来要采取的一些措施。

B. 范围

本指南应引起所有在美国制造、设计、测试和/或计划销售自动驾驶汽车系统的个体和公司的重视。这些个体和公司包括传统汽车制造商和涉及制造、设计、供应、测试、销售、运营或部署高度自动驾驶汽车的其他实体。这些实体包括但不限于设备设计商和供应商、提供用于测试、商业销售和/或公共道路使用的具有自动化能力或高度自动化汽车设备的车辆的实体、运输公司、自动化车队运营商、“无人驾驶“出租车公司，以及通过利用高度自动驾驶汽车提供服务的其他个体或实体。

本指南适用于那些接受测试和在公共道路上使用的车辆，包括轻型、中型和重型车辆。本指南针对融入了高度自动驾驶汽车系统的车辆，如用于没有人类驾驶员的车辆的系统，或有人类驾驶员但其将车辆控制权交给高度自动驾驶汽车系统并在一段时间内不执行任何驾驶相关任务的车辆的系统。

本指南应适用于测试和生产级汽车。如果一辆汽车由公众而非制造商或其他测试/生产实体的员工或代理操作，本指南视该操作为部署（而非测试）。

为了在公共道路上行驶，自动驾驶汽车必须满足所有适用的 FMVSS。如果制造商或其他实体希望测试或操纵无法满足适用安全标准的汽车，“NHTSA 鼓励制造商在适当的时候寻求使用 NHTSA 的豁免权以实地测试能够展示完全自动驾驶汽车安全益处的车队。”该声明同样适用于按照 NHTSA 规定传统上可能不被视为“制

造商”的实体（如：汽车改装商)。

除了安全性，自动驾驶汽车可以满足残疾人、老年人和传统设计方案可能不考虑的其他人的出行需求，改变他们的生活，具有重大的意义。交通部鼓励制造商和其他实体在开发过程中照顾到各类用户并考虑他们的具体需求。

C. 概述：交通部车辆性能指南

图 I 为交通部车辆性能指南整体框架。制造商或其他实体根据国际自动机工程师学会(SAE International)公布的定义自行确定系统的自动驾驶汽车层级。（NHTSA 将审查制造商的自动化层级分配，如果其不同意制造商分配的层级将向后者提出建议。）该图表确定了制造商和其他实体在公共道路测试或部署汽车时要解决的关键领域。

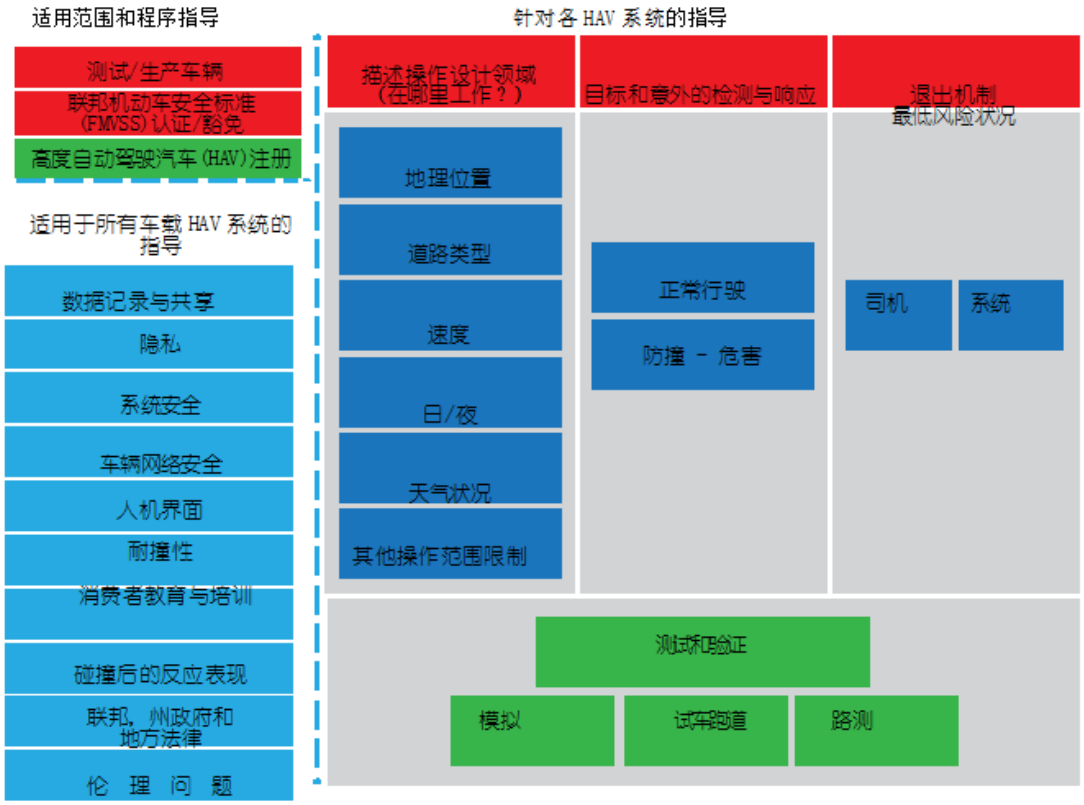
该框架适用于试验和生产车辆，也适用于自动驾驶系统的原装设备以及替换设备和更新（包括系统更新/升级)。该框架包括交叉领域（如适用于所有车载自动化功能的领域）以及适用于各个具体车载自动化功能的领域。交叉领域包括：数据记录和分享、隐私、系统安全、网络安全、人机交互界面（HMI)、耐撞性能和用户教育与培训。针对每个自动化功能的领域包括：操作设计领域（ODD）描述、目标和意外的检测与响应（OEDR）和退出机制（最低风险条件)。

应用该指导框架，制造商或其他实体需要首先确保满足所有适用的 FMVSS 标准或向 NHTSA 申请解释或豁免（如需要)。本政策第三部分“NHTSA 现行监管方式”提供了更多关于解释和豁免的信息。其次，制造商或其他实体应遵守现行的交通部识别/注册要求（见美国联邦法规 49 号 566 和 567 部分)。

对于所有的高度自动驾驶汽车系统，制造商或其他实体应该解决交叉项目，因为设计和开发汽车或设备是为了确保这辆车具有数据记录和分享功能，应用了适当的功能安全和网络安全最佳实践，遵循了人机界面(HMI)设计最佳实践，设计了适当的车辆耐撞性能/乘员保护，以及解决了用户教育和培训问题。

除了交叉项目，对于每个具体的高度自动驾驶汽车系统，制造商或其他实体应明确界定操作设计范围和该系统对应的 SAE 层级。操作设计范围针对每个高度自动驾驶汽车系统可能有所不同。它将限定此功能在以下场景启动的条件，包括道路类型、地理位置、速度范围、运行光照条件（白天和/或晚上)、天气条件和其他操作范围限制。要确定高度自动驾驶汽车在预期范围内安全运行需要哪些目标和意外的检测与响应能力，一个定义明确的操作设计范围是必不可少的。目标和意外的检测与响应要求是通过评估在操作范围内可能出现的正常驾驶场景、预期风险（如：其它车辆、行人）和未指明意外（如：紧急救援车辆、临时施工区域）而得出的。

图 1：车辆性能指导框架



该框架中的回退最低风险状况涵盖每个高度自动驾驶汽车(HAV)系统。从自动控制过渡到手动控制时，如果 HAV 系统发生故障或人类驾驶者响应失败，那么回退最低风险状况的限定、测试和验证能够确保车辆处于最小的危险状况之中。

最后，如图 1 所示，通过测试的开发和进行，可以评估（借助模拟、试车跑道或公路的组合测试）并验证高度自动驾驶汽车(HAV)系统是否能够在指定的操作设计领域（ODD）内安全运行，且能在需要时回退到最低风险状况。

D. 致 NHTSA 的安全评估信

为了监督高度自动驾驶汽车，NHTSA 将要求制造商和其他实体自愿报告他们是如何遵守“指导意见”的。

该报告程序在未来可能会通过规章制度被强制执行。预计这要求各实体向 NHTSA 的首席律师办公室提交每个高度自动驾驶汽车(HAV)系统的《安全评估》报告，简述他们如何在将其产品付诸公共道路使用（测试或部署）前达到“指导意见”的要求。该《安全评估》将有助于 NHTSA 和公众评价从事于开发和测试高度自动驾驶汽车(HAV)系统的制造商和其他实体在安全方面的表现。

《安全评估》将包括以下几个方面:

- 数据记录和共享
- 隐私
- 系统安全
- 整车网络安全
- 人机界面
- 耐撞性
- 消费者教育和培训
- 注册和认证
- 碰撞后的反应
- 联邦，州政府和地方法律
- 伦理问题
- 操作设计领域
- 目标和意外的检测与响应
- 退出机制（最低风险状况）
- 验证方法

提交的《安全评估》应当简洁并且完整。如果制造商和其他实体认为有必要更充分地表达其工艺、计划、办法或其他方面，则他们可以提交更多信息。NHTSA 可能会要求提供更多关于“指导意见”方方面面的详尽信息，以便更好地评估高度自动驾驶汽车(HAV)系统的安全问题。对于每一个方面，《安全评估》应报告以下三项内容的任一项:

- 符合“指导意见”的方面_____
- 不符合“指导意见”的方面_____
- 不适用“指导意见”的方面_____

除了以上列出的核对项目，提交的报告还应包括公司授权负责人的姓名、职务和签名及日期。《安全评估》中的每个方面都应涵盖这些内容。此举旨在确保汇报组织内的适当透明度、认知和监督。

直到 NHTSA 完成《文书削减法案》(PRA）要求的程序之后，“指导意见”的这一规定方才生效。一旦该程序结束、最终调整完毕、NHTSA 在“联邦公报”上发布过通知，那么“指导意见”的报告规定就是有效的。对于已经被测试并部署的高度自动驾驶汽车(HAV)系统，考虑到制造商和其他实体可能想对报告进行后续补充，NHTSA 希望他们在《文书削减法案》(PRA）程序完成后的四个月内提交《安全评估》。同样，对于在《文书削减法案》(PRA）程序进行时或完成后被推出、测试或部署的车辆，NHTSA 期望制造商和其他实体至少在启动新自动化功能[11]公共道路测试前的四个月提交《安全评估》。

当制造商或其他实体对车辆或 HAV 系统作出任何显著的更新后，他们需向 NHTSA 提交新的《安全评估》。若更新会引起 15 个安全评估方面的任何一个指标发生变动，则称之为显著的更新。更新报告的目的是向 NHTSA 描述更新的性质，对性能的预期影响以及提供与安全评估报告意图相一致的其它相关信息。

软件和硬件更新

对于以测试或生产为目的部署在公共道路上的 HAV 系统，NHTSA 设想制造商和其他实体可能会通过空间下载技术或其他方式更新车辆软件。至于车型更新、新汽车平台或其他技术改进等，硬件可以有所改变和/或更新。

如果这些软件或硬件更新在实质上改变了车辆遵从（或违背）“指导意见”中 15 个安全评估方面的任何一个指标（例如车辆 ODD、OEDR 性能、或回退方式）的方式，那么 NHTSA 将认为制造商和其他实体应提交概述此种具体变化的《安全评估》。

例如，对于 ODD，如果软件或硬件更新改变了 HAV 系统在速度范围、行驶道路类型、地理区域、环境条件（天气，白天/夜间）内的性能，那么这些都将使 HAV 系统的操作领域发生显著变化并存在 NHTSA 需要监控的安全问题。因此，制造商应针对这些功能提交新的《安全评估》。

对于 HAV 的 OEDR 性能，如果软件或硬件更新改变了正常行驶场景（行为能力）的设定或 HAV 系统的预碰撞场景性能，那么这变化也应在修订后的《安全评估》中有所概述。

同样，如 F 节所述，当 HAV 系统出现问题时，制造商应该设有过渡到车辆最低风险状况的回退方式。如果软件或硬件更新改变了回退策略和最低风险状况的实际执行，那么这种变化应在新撰写的或修改的《安全评估》中有所描述。

E. “指导意见”的交叉领域

1.数据记录和共享

制造商和其他实体应备案测试、验证和收集事件、事故和碰撞数据的过程，以达到记录故障、退化或失灵的目的，从而找到出现任何此类问题的原因。收集到的数据应当用于测试和运营（包括事件重建）。如以下隐私部分所说，制造商所录数据的收集、记录、共享、存储、审计和解构，包括但不限于碰撞事件发生的时间，一定要严格遵守厂家的消费者隐私和安全协议以及声明。

为了达到碰撞重建的目的（包括在测试期间），数据应能被实体本身和美国国家公路交通安全管理局(NHTSA)存储、维护和随时获取。美国交通部(DOT)建议制造商和其他实体收集与以下事件相关的数据：（1）死亡和人身伤害，或（2）使任何机动车辆一定程度上不能以常规方式通过自身动力驱动而需要牵引的损坏，但不存在对车辆、交通元素、道路造成的其他更大的损失或危害。在最低限度内，车辆应记录与事件和系统性能相关的所有信息，以便该事件的情境可以被重建。数据也应该包含与高度自动驾驶汽车(HAV)系统状态有关的信息，是否 HAV 系统或驾驶人员在当时控制了车辆。制造商或其他实体应具有分享相关所录信息的技术和法律能力。

为了制定新的安全衡量标准，除了汇报上面列出的状况(事件、事故和碰撞数据)以外，制造商和其他实体还应当收集、存储和分析相关的积极成果数据。积极成果是指 HAV 系统正确地检测到与安全相关的情况，并成功地避免了事件（例如，“有惊无险”和边缘情况）的发生。该数据包括与安全相关的事件，如高度自动驾驶汽车和其他车辆或道路使用者（例如，行人和骑自行车的人）之间的近乎碰撞。收集数据（并使其适用于整个操作过程）的价值在于捕捉到此类事件：自动化功能正确检测并识别由其他道路使用者（例如，其他机动车或行人）引发的危险机率，并采取适当的应对措施成功避免事件、事故或碰撞的发生。

高度自动驾驶汽车具有利用数据共享加强和扩大安全效益的巨大潜力。因此，每个实体应制定与其他实体分享事件重建和其他相关数据的计划。这种共享数据有助于促进对高度自动驾驶汽车性能的认识和了解，并可以用来增强高度自动驾驶汽车系统的安全性、建立消费者对高度自动驾驶汽车技术的信心。一般情况下，与第三方共享的数据应该去除身份(即删除使人能把数据直接地或合理地联想到特定 HAV 所有者或用户的元素)。制造商和其他实体应采取措施确保共享数据符合适用于汽车的隐私和安全协议及声明（通常允许去身份数据的共享），或遵照车主/用户的同意。

数据共享是一个迅速发展的领域，需要利益相关者通过更多研究和讨论制定出共同认可的数据标准。例如，许多制造商和其他实体可能想要从它们制造或销售的车辆上获取数据，并将该数据存储一段时间。整个行业应当与相关标准机构（电气和电子工程师协会，国际自动机工程师学会等）共同合作制定统一的方法来解决数据记录和共享问题。无论总产量多少，所有制造商和其他实体也应参与*预警汇报计划（EWR）*并按季度提交预警汇报计划信息。此外，有意通过第三方共享的数据不应包含任何个人身份信息。

直到 NHTSA 完成《文书削减法案》(PRA）要求的数据收集和汇报程序之后，“指导意见”的这一规定方才生效。一旦该程序结束、最终调整完毕、NHTSA 在“联邦公报”上发布过通知，那么“指导意见”的这项规定就是有效的。

2. 隐私

根据《白宫消费者隐私权法案》和联邦贸易委员会的隐私指引，美国运输部和美国国家公路交通安全管理局坚决信奉个人隐私权保护。2014 年 11 月，汽车制造商联盟和全球汽车制造商协会发布《车辆技术和服务的隐私原则》。鉴于这些可用资源，高度自动驾驶汽车制造商和其他实体应该单独或联合采取措施保护消费者的隐私。制造商的隐私政策和实际操作应确保：

a. 透明度：为消费者提供易懂、清晰和有意义的数据隐私和安全声明/协议，其中应包括《白宫消费者隐私权法案》列出的基本保护措施，并解释实体如何收集、使用、共享、保护、审计和销毁从其车辆中产生或获取的数据；

b. 选择：让车主在有关数据的收集、使用、共享、保存和解构方面有所选择，

包括可能合理联想到他们本人的地理定位、生物特征识别和驾驶行为数据(即个人数据);

c. 背景尊从:使用从高度自动驾驶汽车生产中收集到的数据的方式仅与收集该数据的初始目的相一致(在适用数据隐私声明/协议中有所解释);

d. 最小化、去身份和保留:按照适用数据隐私声明/协议和原则,仅收集和保留用于合法商业目的的最少必要个人数据,并采取措施去除实用的身份敏感数据;

e. 数据安全:采取措施保护数据,这与数据丢失或未经授权泄露导致的危害同样重要;

f. 完整性和存取:采取措施保护个人数据的准确性,当数据被直接或合理地联想到特定的车辆或人时,允许车辆运营商和车主审查和纠正这些信息;

g. 问责:采取合理措施,诸如评估和审计隐私和数据保护的方法和做法,从而确保收集或获得消费者数据的实体遵守适用数据隐私和安全协议/声明。

3.系统安全

制造商和其他实体应遵循基于系统工程方法的强大设计和验证程序,且将避免不合理的安全风险视作 HAV 系统的设计目标。该程序应包括预期功能设计,使得车辆即使在电气、电子或机械发生故障或软件出现错误时能处于安全状态。

整个程序应采用并遵循行业标准,如用于道路车辆的功能安全程序标准,同时涵盖车辆的整个设计领域。制造商和其他实体应遵照“指导意见”、最佳实践、设计原则和现有标准组织(如国际标准化组织(ISO)和国际自动机工程师学会)制定的标准,以及航空、航天和军事(例如,美国国防部发布的系统安全标准做法)等其他行业制定的标准和程序,因为它们具有相关性和适用性。NHTSA 于 2016 年 6 月发布报告“汽车电子控制系统的安全标准评估”评价此类标准的优势和局限,NHTSA 认为此举可以有助于强大的汽车电子控制系统功能安全办法在未来的发展.

这一程序应包括高度自动驾驶汽车系统的危害分析和安全风险评估步骤,HAV 系统如何融入整车设计,何时适用,更广泛的交通系统。

针对高度自动驾驶汽车系统故障的处理,该程序应规定设计冗余和安全策略。

该程序应着重强调软件开发、验证和确认。软件开发过程应精心规划、有序控制、记录明确,以便检测和矫正软件开发和更改中出现的意外结果。全面而大量的软件测试应补充说明结构化的和被记录在案的软件开发过程。汽车工业应监测人工智能(AI)的演化、实施和安全评估,机器学习能力,以及其他相关的软件技术和算法,从而提高高度自动驾驶汽车的有效性和安全性。

设计决策应与可能影响关键系统功能安全的风险评估挂钩。设计的安全性应注意以下方面（包括但不限于）：设计结构、传感器、执行器、通信故障；潜在的软件错误；可靠性；潜在的控制不足和不良的控制动作；与周围物体和其他道路使用者的潜在碰撞、由 HAV 系统的行为引起的的潜在碰撞；车道偏离、牵引力或稳定性损失、交通法规的违反、正常（预期）驾驶行为的偏离。

所有设计决策应作为子系统和整车架构的一部分进行测试、验证和核实。

整个程序应被完全备案，所有变更、设计选择、分析、相关的测试和数据应充分地有迹可寻.

4.整车网络安全

制造商和其他实体应遵循健全的、基于系统工程学方法的产品开发流程，将安全风险降至最低，包括由网络安全威胁和漏洞造成的风险。这一过程应包括系统的、持续的高度自动驾驶汽车系统、集成时整车设计和更广泛的交通生态系统（适用时）安全风险评估。使用识别、保护、检测、响应和恢复功能作出风险管理决策，消除风险和威胁，快速应对网络安全事件并从中吸取经验教训。

虽然这是一个不断发展的领域，并且在提出监管标准之前有必要进行更多的研究，我们鼓励各实体按照公认的信息物理汽车系统的最佳实践设计自己的高度自动驾驶汽车系统。特别是，各实体应考虑并采纳本指南、最佳实践以及国家标准技术研究所（NIST）、美国国家公路交通安全管理局（NHTSA）、国际自动机工程师学会（SAE International）、汽车制造商联盟（Alliance of Automobile Manufacturers）、全球汽车制造商协会（Association of Global Automakers）、汽车信息共享分析中心（Information Sharing and Analysis Center）和其他有关组织发布的设计原则。

完整记录结合诸多网络安全考虑因素的整个过程，可以在一个强大的文档版本控制环境内追溯所有的行为、改动、设计选择、分析、关联测试和数据。

至于安全数据，网络安全行业共享非常重要。行业成员的经验教训不应来自相同的网络漏洞。这正是成立 Auto-ISAC 的目的所在：促进小组学习。为此，不管是不是会员，各实体都应尽快向 Auto-ISAC 报告在事故现场、内部测试或外部安全研究发现的所有漏洞。涉及高度自动驾驶汽车的实体应考虑采取漏洞披露政策。

5.人机交互界面

理解车辆和驾驶员之间的交互（通常称为“人机交互界面”）在汽车设计过程中一直扮演了重要的角色。高度自动驾驶汽车承担驾驶任务让问题变得更加复杂，部分原因是该汽车必须能够将意图和车辆性能信息准确地传达给驾驶员。这在 SAE 3 级系统中尤为如此，驾驶员将重新承担监控任务，并接管车辆；但是，按照人类保持警觉的能力，让驾驶员随时从车辆驾驶解除状态重新回到全面接管汽车，实现这点有一定难度。制造商和其他实体应考虑将驾驶员参与监控融入 3 级

高度自动驾驶汽车系统是否合理和适当。此外，制造商和其他实体还应考虑高度自动驾驶汽车针对周围环境（如：行人、骑车人、其他车辆）是如何发出信号表达意图的。

制造商和其他实体应记录评估、测试以及车辆人机交互界面验证过程。考虑要素应包括驾驶员、操作员、乘员和与高度自动驾驶汽车进行交互的外部参与者（其他车辆、行人等）。人机交互界面设计也应考虑是否有必要将关于高度自动驾驶汽车相对于周边环境的运行状态信息传达给行人、普通汽车以及自动驾驶汽车（例如：高度自动驾驶汽车系统是否识别了处于十字路口并正往后退的行人）。

考虑到该领域突飞猛进的发展和正在进行的研究，制造商和其他实体应考虑并应用本指南、最佳实践以及国际自动机工程师学会、国际标准化组织（ISO）、美国国家公路交通安全管理局、美国国家标准学会（American National Standards Institute，ANSI）、国际照明委员会（CIT）和其他有关组织发布的设计原则。

指示器至少应该能够告知操作员或乘员高度自动驾驶汽车系统目前：

1. 运行正常；
2. 处于自动驾驶模式；
3. 自动驾驶不可用；
4. 高度自动驾驶汽车系统出现故障；和
5. 请求由高度自动驾驶汽车系统控制转为操作员控制。

制造商和其他实体应为完全自动驾驶汽车设计满足残疾人需要的人机交互界面（例如：视觉、听觉、触摸显示屏）。

设计没有驾驶员和乘员的高度自动驾驶汽车时，远程调度员或中控机构应该能够始终了解高度自动驾驶汽车的状态。这些车辆可能包括自动运输车辆、最后一公里专用地面无人驾驶车辆和自动驾驶维修车。

6. 耐撞性能

a. 乘客保护

高度自动化汽车有望满足美国国家公路交通安全管理局制定的耐撞标准，原因是不管高度自动化汽车的防撞能力如何，车辆厂商和其他实体仍需要考虑到其他车辆与之相撞的可能性。此外，各实体应开发和增加新的乘客保护系统，这种系统利用高度自动化汽车运行所需的高级传感技术信息，向不同年龄和不同体型的乘客提供增强保护。不管高度自动化汽车是处于全自动模式，还是由真人驾驶，一旦传感器失灵，乘客保护系统都应保持其预期性能水平。

除了按目前标准评估的座位配置外，高度自动化汽车厂商等实体还应实施并论证耐撞标准，根据车辆座位和内部配置向所有乘客提供相应保护措施。论证手段不应局限于物理测试，还应包括车辆和人体模型的虚拟测试。

b. 兼容性

预期的耐撞标准还应考虑到无人驾驶车辆的碰撞安全性能上，这些车辆应在外形和能量吸收方面与目前马路上行驶的车辆相兼容。原本用于提供产品、服务或应用于其他无人驾驶场景的高度自动化汽车应符合该款车型车辆碰撞兼容性。

7. 消费者的教育培训

要确保自动化车辆的安全部署，进行适当的教育培训很有必要。因此，车辆厂商等实体应对员工、经销商、分销商和消费者的教育培训计划进行开发、记录和维护，让公众了解高度自动化汽车与目前的传统车辆在使用和操作上有何不同。此类计划的目的是让目标用户理解如何正确、高效和安全地使用这些技术。

各实体应该确保其员工（包括但不限于其营销和销售团队）理解该技术，同时也能对其经销商、分销商和终端消费者进行教育培训。

消费者教育培训的内容包括高度自动化汽车的开发意图、操作参数、功能和局限、签约与解约方法、人机接口、紧急退出机制场景、操作边界责任以及改变服务功能行为的潜在机制。

作为教育培训计划的一部分，高度自动化汽车厂商、经销商、分销商应在发给客户之前考虑到行车切身体验。这种体验体现了高度自动化汽车操作方法和人机接口功能。此外，也应考虑其他创新方法（如：虚拟现实），并对其进行测试和使用。要对这些计划的有效性进行评估，并做例行更新，这包括经销商、客户和和其他数据源的反馈。

8. 注册与认证

美国国家公路交通安全管理局清楚由于软件更新，车辆可能在车辆使用寿命期内改变自动化水平。随着高度自动化汽车完成测试、实现商业化销售，再到上路行驶，老款汽车可以进行升级，使之具有与新车类似的功能。随着新功能和技术引入市场，即使硬件几年前就已问世，厂商也可以选择将车辆当前的自动化水平升级到更高水平。

美国国家公路交通安全管理局要求生产联邦机动车安全标准（FMVSS）相关产品的机动车和机动车设备厂商提交生产产品的确认信息和产品描述（参见美国联邦法规 49 号，566 部分 厂商资料）。车辆厂商和其他实体还应向美国国家公路交通安全管理局提交其产品的确认信息和产品描述。他们生产的产品是由/和高度自动化汽车系统和特点配合使用的。

此外，车辆厂商还应提供车载手段，以便将高度自动化汽车的主要功能信息传输给车主或司机。例如，整车厂商或其他实体可以向车辆提供半永久性的标签，将其贴在司机座位能看得见的地方，或如果不切合实际的话，贴在左前方座位旁的

门锁柱上。车内所贴信息包括此项功能的权限，操作设计领域，以及车主可以获得更多信息的来源（人员或地方）。另外，由于软件和/或硬件可以在车辆服务期限内进行更新，从而获得更多更新的功能和车载信息，因此，车辆也应更新以体现这些变化。

车辆厂商和其他实体应在车主和/或操作人员手册中，或通过车载人机接口详细描述高度自动化汽车每个操作设计领域的功能和局限，包括运行速度、地理区域、天气和其他相关信息。

9. 碰撞发生后的行为

车辆厂商和其他实体应该进行存档，以备碰撞发生后高度自动化汽车恢复功能的过程进行评估、测试和验证。如果传感器或关键安全控制系统出现损坏，车辆不应在高度自动化汽车模式下运行。在对车辆进行诊断的过程中，高度自动化汽车应在最低的风险状况运行，直至功能恢复正常。

10. 联邦、州及地方法规

车辆厂商和其他实体应该制定计划，记录他们欲遵守联邦、州和地方法律的详细过程。根据操作设计领域，高度自动化汽车应遵守交通法规和道路交通规则。

在某些关键性安全场景下（如，必须穿过行车道上的双黄线，或从路上抛锚的车辆以及出现的危险障碍物旁边安全通过等），司机可以临时违反某些州的机动车驾驶法规。而我们可以预期，高度自动化汽车可以安全地处理此类问题。此外，车辆厂商和其他实体应该进行记录存档，以备对这些看似合理的案例进行独立的评估、测试和验证。车辆厂商和其他实体会对记录的数据进行分析，这些数据可能会证明高度自动化汽车执行的动作可以提高安全性。

州与州，甚至城市与城市间的交通法规都不相同。高度自动化汽车应遵守适用操作设计领域的所有法律。这包括限速、交通控制设备、单行道、行车限制（如，人行横道、自行车道）、U 形弯道、红灯亮时可以右转场景、匝道控制和其他交通环境和场景。由于法规一定会随时间的推移而发生变化，所以车辆厂商和其他实体应更新高度自动化汽车系统，使之适应新的法律要求。

11. 伦理考量

高度自动化汽车的计算机“驾驶员”做出的各种决定将会带来伦理方面的影响。对不同道路使用者产生的不同结果可能由现实同一种情况导致的，这种情况是基于高度自动驾驶汽车电脑做出的决策，而电脑决策是由程序化的决策规则和机器学习程序决定的。即使在没有明确的伦理规则的情况下，高度自动驾驶汽车的程序也会确立一个暗含的或固有的能产生重大伦理后果的决策规则。汽车厂商和其他实体应与监管机构和其他利益相关者（如司机、乘客和处于弱势地位的道路使用者）开展密切合作，解决这些情况，确保此种道德判断和决策是在有意识的情况下做出的。

大多数车辆操作人员有三个合理的目标：安全性、移动性和合法性。大多数情况下，这三种目标可以同时实现，而且不会发生冲突。而在某些情况下，这几种目标会发生冲突。例如，多数州的法律都禁止机动车横穿行车道的中间双黄线。如果双车道公路上还有一辆车并排停放或阻挡了行车道，(向目的地行驶）的移动性的目标可能与安全性和合法性目标发生了冲突。这种冲突可以通过不同的方式解决，可以通过高度自动驾驶汽车编程的决策规则进行解决。甚至可以通过驾驶员或乘坐人员进行设置予以解决。

同样,要解决一辆车与另一辆车上的乘坐人员安全问题，就会在安全目标内产生冲突。在这种情况下,一个人的安全得到保护是以牺牲另一个人安全为代价的。在这种两难的情况,高度自动化汽车的编程就会对每一个当事人的结果产生重大影响。

由于这些决定可能不仅对自动化车辆和乘客造成影响,还会对周围的道路使用者造成影响，所以应该集思广益来解决这些冲突。因此，要考虑是否需要高度自动驾驶汽车将某些特定决策规则应用到安全性、移动性和合法性目标的冲突上。要利用联邦和各州的监管机构、司机、乘客和处于弱势地位的道路使用者提出的意见，并考虑到高度自动驾驶汽车的行为对他人产生的结果，以透明公开的方式开发解决这些冲突的算法。

F. 自动化功能

1. 操作设计范围

制造商或其他实体应明确和记录测试/公共道路车辆上每个 HAV 系统的操作设计范围 (ODD)。ODD 应说明 HAV 系统具体的正常运行设计操作范围。一个清晰的 ODD 应包括以下信息以明确 HAV 系统性能：

- HAV 系统安全运行的道路类型；
- 地理区域；
- 速度范围；
- HAV 运行环境条件（天气、白天/夜间等），以及
- 其他范围限制条件。

针对每个 HAV 系统，制造商或其他实体应记录评估、测试和验证该系统性能的过程和程序。

制造商和其他实体应开发测试和验证方法来评估 HAV 系统性能以确保较高的安全水平。随着交通部在 HAV 系统领域积累越来越多的经验和专门知识，NHTSA 未来可能会出台具体的性能测试和标准。目前，制造商和其他实体应开发和应用测试与标准，为每个 HAV 系统确立可靠的 ODD。

HAV 应能够在设计好的 ODD 内安全运行。如果 HAV 超出规定的 ODD 或条件变化超出 HAV 的 ODD，车辆应转换到最低风险条件。车辆应向乘员明示人机交互界面章

节列出的类型，告知正转换至最低风险条件，HAV 系统当前不可用。

为了让驾驶员和车辆操作员对 ODD 有更好的了解，车辆使用手册应以简洁明了的语言对 ODD 进行概括性描述，包括对车辆 HAV 系统运行和闲置状况的清晰描述。这些用法指南应帮助车辆驾驶员或操作员更好地理解各 HAV 系统的性能和局限。

2. 目标和意外检测与响应

目标和意外检测与响应（OEDR）指驾驶员或 HAV 系统检测到任何与驾驶任务直接相关的事件并针对该事件作出适当的响应。根据本指南，当 ODD 和自动化功能运行时，HAV 系统负责执行 OEDR。

实体应记录评估、测试和验证 OEDR 性能的过程。在 ODD 范围内，HAV 的 OEDR 功能将检测并对其他车辆（同一/不同行车路线）、行人、骑车人、动物以及可能影响 HAV 安全运行的物体作出响应。

在 ODD 范围内，HAV 的 OEDR 应能够处理多种状况，包括应急车辆、临时工作区和可能影响 HAV 安全运行的其他异常情况（如手动指挥交通的警察、管制交通的建筑工人、应急响应人员）。

a. 正常行车

制造商和其他实体应记录评估、测试和验证适用于 HAV 的行为能力的过程。行为能力指自动驾驶车辆在经常遇到的各种交通状况下依然能够运行的能力，包括保持车辆在车道内行驶、遵守交通法规、遵循合理的规矩和对其他车辆、道路使用者或常见危险作出响应。

下列行为能力实例集改编自加州大学伯克利分校研究团体“先进交通技术合作伙伴”进行的研究：

- 检测并响应速度限制变化和建议速度
- 高速并道（例如：高速公路）
- 低速并道
- 驶离行车道并停车（例如：停到路肩实现最低风险）
- 检测并响应驶近的对面来车
- 检测超车区和禁止超车区，进行超车
- 跟车行驶（包括停车和起步）
- 检测并响应停止的车辆
- 检测并响应车道变换
- 检测并响应车辆行车道静态障碍
- 检测交通信号和停车/让行标志
- 响应交通信号和停车/让行标志
- 通过十字路口并转弯
- 通过环形交叉路口

- 通过停车场，找到停车位
- 检测并响应通行限制（单行道、禁止转弯、斜坡道等）
- 检测并响应工作区和意外/计划事件中指挥交通的人
- 作出恰当的先行权决策
- 遵守当地和州汽车驾驶方面的法律
- 跟随管制交通的警方/第一响应者（作为交通管制设备）
- 跟随控制交通模式的建筑区工人（缓行/停车标志支架）
- 响应碰撞事故后指挥交通的公民
- 检测并响应临时交通管制设备
- 检测并响应应急车辆
- 在十字路口、三岔路口和其他交通管制状况下为执法车、紧急医疗救援车、消防车和其他应急车辆让行
- 在十字路口和人行横道为行人和骑行人让行
- 与路边的车辆、行人和骑行人保持安全距离
- 检测/响应交通模式中的绕行和/或其他临时变动

HAV 系统将展示和例行执行的所有行为能力依赖于 HAV 系统、ODD 和退出办法。制造商和其他实体应考虑所有已知的行为能力并记录那些他们认为不适用的详细理由。此外，应全面记录实施、验证、测试和展示适用行为能力的方法。

b. 防撞能力- 危险

基于 ODD，HAV 应能够处理与失控、越道碰撞、变道/并道、正面和反向、追尾、车道偏离和低速情形（如倒车和停车）有关的预碰撞情景。根据 ODD，HAV 将能处理许多交通部在报告《自动驾驶车辆操作的益处评估框架》中定义的预碰撞场景。

如果诸如道路维修和交通模式中的工程变更、警察指挥交通、行车道故障车辆和其他意外在特定 ODD 内能够合理地预料到，这些意外应该得到解决。如果 HAV 无法安全运行，其应退出自动驾驶机制，由驾驶员接管车辆，将风险降至最低。

制造商和其他实体应记录评估、测试和验证防碰撞能力和设计选择的过程。

3. 退出机制（最低风险条件）

制造商和其他实体应记录遇到问题时转换到最低风险条件的过程。正在路上运行的 HAV 应能检测到 HAV 系统已经失灵、在降级状态下运行、在 ODD 范围以外运行，并告知驾驶员，让后者重新确定车辆控制权，或允许 HAV 系统自主的退回到最低风险条件。

退出策略应考虑到驾驶员可能因为酒精或其他物质、困倦或身体损害而注意力不集中，尽管这些都是法律法规所禁止的。

实施退出步骤应有助于车辆安全运行，尽量减少反常的驾驶行为。这些退出步骤

还应最大限度的减少在转换到手动控制过程中和之后驾驶员识别错误和决策失误所造成的不利影响。

在可能没有驾驶员的更高自动化情况下，HAV 必须能够退回到车上可能没有驾驶员的最低风险条件。

最小风险条件将根据给定故障的类型和程度有所不同，包括让车辆自动安全地停下来，最好是在繁忙交通车道以外的车道（假设有这样的车道）。制造商和其他实体应记录评估、测试和验证退出方法的过程。

4. 验证方法

鉴于不同的自动化功能在范围、技术和能力上差异很大，制造商和其他实体应制定测试和验证方法，以确保 HAV 运行时达到很高的安全水平。

测试应证明 HAV 系统正常运行时应表现出的行为能力、防碰撞情况下 HAV 系统的性能以及与 HAV 的 ODD 有关的退出策略性能。

为了证明 HAV 系统的预期性能，测试方法应包括模拟、测试赛道和上路测试。制造商和其他实体应确定并记录适合 HAV 系统的方法组合。测试可以由制造商和供货商进行，也可以由独立的第三方机构来执行。

我们鼓励制造商和其他实体与 NHTSA 和其他标准组织（SAE 和 NIST 等）合作开发和更新适用创新性方法和必要测试设备功能标准的测试。

G. 低层级自动驾驶汽车系统指南

根据 NHTSA 提交给国会的报告《乘用车电子系统性能》，电子器件和软件的广泛应用促进了很多已被证实的安全技术的发展和应用，例如：电子稳定系统。软件和电子器件继续为汽车行业开发和部署更先进的 HAV 技术提供动力。

电子器件和软件是所有自动驾驶汽车系统的核心。基于自动系统使用和运行时是否依赖驾驶员，HAV 系统（SAE 3 级、4 级和 5 级）和低层级自动化（SAE 2 级及以下）之间存在明显的技术区别。然而，这种区别并没有对制造商和其他实体在产品开发、测试和部署时利用本指南内容的领域造成多大改变。

本指南大部分内容和高度自动驾驶汽车车辆性能指南交叉领域列举的考虑因素（例如：数据采集和分享、隐私、系统安全、整车网络安全、人机交互界面、耐撞性能、和用户教育与培训）通常适用于所有的自动驾驶汽车系统。

此外，“注册和认证”、“碰撞后行为”和“伦理考量”章节规定的指南也适用于那些能够同时提供持续横向和纵向控制的自动驾驶车辆系统（归类为 SAE 2 级的系统）。低层级自动驾驶车辆系统制造商还应考虑“联邦、州和地方法律”章节下的指南，开发和部署让驾驶员清楚地了解系统如何操控功能和对待驾驶员角色

的系统。

再者，制造商和其他实体应着重评估驾驶员自满和滥用 2 级系统的风险，制定有效的对策帮助驾驶员像制造商希望的那样正确使用系统。自满是指“.....【操作员】过度依赖或过分相信自动化，未能保持警惕和/或履行监督职责。”(巴拉苏罗，1997)。SAE 2 级系统不同于 HAV 系统，驾驶员要始终参与驾驶任务，主要是监视系统是否操作适当并在必要时立刻接管车辆，不论系统是否发出警告。然而，与 HAV 系统一样，SAE 2 级系统在既定的设计范围内同时执行持续的纵向和横向控制。制造商和其他实体应假设自动化水平（例如 2 级和 3 级之间）之间的技术差别对用户或一般公众来说可能不是很清楚。而且，驾驶员对系统的期望和他们对自身“监管”角色重要性的理解可能存在重大差异。

制造商和其他实体应开发试验、验证和核查方法来评估系统有效的防自满和滥用对策。例如，2 级车辆可能有一个系统来监控驾驶员的参与程度，如果判定驾驶员没有充分参与，将会让车回到安全的退出条件。认识到围绕 SAE 2 级系统复杂的人为因素，交通部鼓励汽车行业与 NHTSA 合作制定合适的方法和指标来理解和量化有效的人为因素办法，以解决自满和可预见系统滥用导致的潜在风险。

本指南讨论的 ODD 概念、OEDR、相关试验和验证方法主要集中于 HAV 系统（归类为 SAE 3 级、4 级和 5 级的系统）。因为 HAV 系统应设计为在没有驾驶员参与的情况下在 ODD 范围内承担全部驾驶任务并监控环境。本指南着重于设计和验证可以在 ODD 内有效地实现该目标的 HAV 系统。

在较低的自动化层级(SAE0 级、1 级和 2 级)中，驾驶员继续全面参与驾驶任务。驾驶员在感知和决策方面是这些系统的组成部分。尽管可能无法一再将本指南概括的 HAV ODD 概念延伸到 2 级系统，但是低层级自动驾驶车辆系统常常有一个预定 ODD (IODD)。虽然这类系统由于驾驶员作为系统预期的一部分可能无法完全限制系统在 IODD 的使用，当有合理的预期（或风险）发现系统在 IODD 之外被使用或驾驶员没有发挥他们应起的安全保障作用，制造商和其他实体应当通过可用的手段进行通知、监控和限制自动驾驶车辆系统的使用。

与 HAV 不同，制造商必须确保系统自身在 ODD 范围内的稳健性，如果没有警醒的驾驶员参与到决策中，L1-L2 自动驾驶车辆系统的稳健性在 IODD 范围内得不到保证。然而，将自动化功能在 L2 车辆的适用限定在 IODD 范围内实际上应减少这些系统遇到它们可能无法处理的情况的可能性。此外，在驾驶员没有执行其应采取的措施时，限制系统使用应降低驾驶员注意力不够集中时自动化系统失灵的可能性。

表 1：指导领域对应 SAE 等级 2-5 自动驾驶汽车系统的适用范围

自动化水平	SAE 等级 3，4，5（高度自动驾驶汽车）	SAE 等级 2
发至 NHTSA 的安全评估书	是	是
C. 交叉领域	完全	部分
C.1 数据记录和共享	是	是
C.2 隐私	是	是
C.3 系统安全	是	是
C.4 整车网络安全	是	是
C.5 人机界面	是	是
C.6 耐撞性	是	是
C.7 消费者教育和培训	是	是
C.8 注册和认证	是	是
C.9 碰撞后的反应	是	是
C.10 联邦、州政府和地方法律	是	对司机说明
C.11 伦理考量	是	是
F. 自动功能 [47]	完全	部分
F.1 操作设计领域	是	否
F.2 目标和意外的检测与响应	是	否
F.3 退出机制(最低风险状况)	是	否
F.4 验证方法	是	是
G. 低等级自动驾驶汽车系统的指导	否	是

H. 下步：完善，丰富及监管该政策指导的行动

接下来数月，美国国家公路交通安全管理局(NHTSA)会随着技术进步，经验和知识的累积，采取步骤不断改进和完善该指导意见。

1.获取公众意见和建议：美国国家公路交通安全管理局(NHTSA)通过《意见征求书》对此部分及该指导其他部分寻求公众的意见和建议。

2.公开研讨会：美国国家公路交通安全管理局(NHTSA)计划举办公开研讨会，互动讨论该政策，并收集补充今后思考的意见和建议。

3. 专家评论：在举办公众研讨会的同时，美国国家公路交通安全管理局(NHTSA)将邀请外聘专家同行对此指导意见给出他们的审查意见。

4.完成用于安全评估书备案的《文书削减法》制定过程：美国国家公路交通安全管理局(NHTSA)将推进车辆性能指导中标识的安全评估书进行备案的《文书削减法》制定过程。

5.公共安全评估模板：美国国家公路交通安全管理局(NHTSA)将发布一项范本，

用于生产商和其他实体递交安全评估书。

6.进行匿名数据共享：美国国家公路交通安全管理局(NHTSA)将探索新机制促进测试和部署高度自动驾驶汽车的当事方之间的匿名数据共享。该机制将促进符合反垄断和竞争法要求的内容分享，可能安排第三方进行整合。待共享具体数据元素需进一步细化过程中，共享机制就会建立起来。

7.优先安全领域工作计划：为进一步完善此指导意见，产业界的具体行动能推动改善因素的出现。NHTSA 将正式要求具体的行业组织和集团(如 SAE)采取行动，解决优先安全领域的问题。这些努力预计会带来更为详细的发现，以及各方基于该指导意见所进行的数据收集和测试程序方面的方向指引。

8.持续协作：NHTSA 将和各州伙伴合作，确保指导意见和州政策模式部分相互补充。

9. 自动驾驶汽车分类：NHTSA 将公布一项目标方法，各生产商和其他实体可以用来分类他们的自动驾驶汽车系统。

10. 收集数据：当必要且适宜收集数据时，运用特别及普通命令权力 48。

11. 强制执行安全评估：执行指导意见中标识的强制递交安全评估书的规定。

12. 高度自动驾驶汽车注册:规则的制定考虑是要求计划在公共道路测试和运营高度自动驾驶汽车（也就是带有对应 SAE 等级 3-5 系统的车辆）的每个实体到美国国家公路交通安全管理局(NHTSA)进行注册并向该机构文件备份和报告与指导意见相关的项目如数据记录，网络安全，以及用于确保道路运营安全的测试与评估程序和方法。NHTSA 将会复制这一模式到其他需报告制度的规定如预警汇报（EWR)。

13. 美国联邦机动车安全标准（FMVSS）的更新考虑：众多可能性中，可以提供附加标准来完善美国联邦机动车安全标准，生产商将为没有控制选项允许人类司机进行操作的高度自动驾驶汽车(也就是，没有转向轮，刹车踏板，转向信号等)进行验证。这样的标准不适用于更低自动化等级的车辆。新标准对多种类型设备的性能要求作出规定，确保这些车辆在美国公路上的安全。

描述了这些下步动作，该指导意见只是走出了第一步，该机构和产业界会进一步共同努力，快速推进。这些包括在探究监管高度驾驶汽车的初步测试和部署的过程中，DOT/NHTSA 可能采取的设计和执行新标准的监管行为。随着 NHTSA 研究的继续，科技的发展和成熟，以及统一标准得到更广范围的认同，NHTSA 旨在颁布新的美国联邦机动车安全标准，并运用其他监管方式和权力来促进安全不断进步的高度自动驾驶汽车发展，并促进这些车辆的安全运行。依据进展情况，在一年内或更早，美国交通部(DOT)打算发布此项政策的更新版本包括新数据，NHTSA 开展调查和活动中所累积的经验，以及持续的意见征询。