ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 44721—2024

智能网联汽车
自动驾驶系统通用技术要求

Intelligent and connected vehicle—
General technical requirements for automated driving system

2024-09-29 发布　　2024-09-29 实施

国家市场监督管理总局
国家标准化管理委员会　发布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：中国汽车技术研究中心有限公司、华为技术有限公司、上海汽车集团股份有限公司、工业和信息化部装备工业发展中心、东风汽车集团有限公司、重庆长安汽车股份有限公司、上汽大众汽车有限公司、广州汽车集团股份有限公司、宇通客车股份有限公司、公安部道路交通安全研究中心、一汽解放汽车有限公司、梅赛德斯一奔驰(中国)投资有限公司、上海机动车检测认证技术研究中心有限公司、中国第一汽车集团有限公司、广州小鹏汽车科技有限公司、宝马(中国)服务有限公司、北京百度智行科技有限公司、博世汽车部件(苏州)有限公司、宁波吉利汽车研究开发有限公司、华人运通(山东)科技有限公司、长城汽车股份有限公司、东风商用车有限公司、厦门金龙旅行车有限公司、浙江万安科技股份有限公司。

本文件主要起草人：吴志新、张行、刘楠、陆军琰、孙航、刘法旺、刘光、徐优志、张华桑、陈达兴、张嘉芮、刘燕、王祥、刘振楠、赵光明、李艳文、郝值、吕明、费音、崔茂源、陈金凤、张存玺、彭伟、李迎宾、金晨、何彦、李建冰、李阳、尤双和、傅直全。

引　言

现阶段智能网联汽车自动驾驶技术处于快速发展时期，产品形态、落地场景和测评方法都处于探索阶段，呈现产品形态迭代快、落地场景多样化、测评方法基础弱的特点。为适应智能网联汽车自动驾驶功能技术特点，国际范围内已初步形成采用“多支柱”方法（包含审核评估、仿真试验、场地试验、道路试验等）综合验证自动驾驶功能安全性的共识。

根据当前产业发展特点和国际共识，我国在智能网联汽车自动驾驶领域已启动制定多项标准。其中，本文件针对自动驾驶系统提出通用性技术要求，并通过附录加强本文件与自动驾驶功能场地试验、道路试验和仿真试验等标准相互配合，共同支撑设计运行范围包含公路和城市道路的自动驾驶系统的验证工作；同时，本文件为自动泊车、港口自动驾驶、末端配送自动驾驶等标准提供基础通用要求，支撑相关标准的验证工作。

智能网联汽车
自动驾驶系统通用技术要求

1 范围

本文件规定了自动驾驶系统的总体要求、动态驾驶任务执行要求、动态驾驶任务后援要求、人机交互要求等。

本文件适用于装备自动驾驶系统的M类、N类汽车。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 34590.1 道路车辆 功能安全 第1部分:术语

GB/T 34590.3—2022 道路车辆 功能安全 第3部分:概念阶段

GB/T 40429—2021 汽车驾驶自动化分级

GB/T 41798 智能网联汽车 自动驾驶功能场地试验方法及要求

GB/T 43267—2023 道路车辆 预期功能安全

GB/T 44298—2024 智能网联汽车 操纵件、指示器及信号装置的标志

GB/T 44373—2024 智能网联汽车 术语和定义

GB/T 44719 智能网联汽车 自动驾驶功能道路试验方法及要求

3 术语和定义

GB/T 34590.1、GB/T 40429—2021、GB/T 43267—2023、GB/T 44373—2024界定的以及下列术语和定义适用于本文件。

3.1

自动驾驶功能 automated driving function

驾驶自动化系统在特定的设计运行条件下代替驾驶员持续自动地执行全部动态驾驶任务的功能。

注:GB/T 40429—2021中规定的3级及以上驾驶自动化功能的总称,包括有条件自动驾驶、高度自动驾驶和完全自动驾驶功能。

[来源:GB/T 44373—2024,6.4]

3.2

自动驾驶系统 automated driving system;ADS

由实现自动驾驶功能的硬件和软件所共同组成的系统。

注:“自动驾驶系统”为GB/T 40429—2021规定的3级及以上驾驶自动化系统。

[来源:GB/T 44373—2024,5.3]

3.3

未激活状态 inactive state

ADS未执行车辆运动控制的状态。

3.4

就绪状态　ready state

ADS 能被激活的未激活状态。

3.5

激活状态　active state

ADS 执行车辆运动控制的状态。

3.6

ADS严重失效　severe ADS failure

ADS 关键部件失效导致严重影响 ADS 安全运行的失效。

示例:核心计算单元失效。

3.7

车辆严重失效　severe vehicle failure

任何同时影响 ADS 执行动态驾驶任务(DDT)能力且影响人工驾驶的失效。

示例:电源掉电、制动系统失效、胎压突然下降。

3.8

计划接管事件　planned takeover event

ADS 预先知晓并需要发出介入请求的事件。

示例:达到设计运行范围(ODD)边缘。

4　总体要求

4.1　ADS 应具备明确的设计运行条件(ODC)。

4.2　ADS 应只能在其设计运行条件(ODC)下被激活。

4.3　ADS 应具备足够的目标和事件探测与响应(OEDR)能力,支持其安全地执行全部动态驾驶任务(DDT)。

4.4　ADS 应及时响应用户的有效操作。若用户的操作将导致危急的碰撞风险,ADS 可根据车辆制造商声明的方式暂缓或抑制响应。若 ADS 具备暂缓或抑制响应用户操作的功能,应明确暂缓或抑制条件。

4.5　ADS 应执行合理的控制策略应对可合理预见的用户误用。

4.6　ADS 应持续对自身状态进行监测,以确认 ADS 是否存在失效以及 ADS 能否执行全部动态驾驶任务(DDT)。

4.7　ADS 在激活状态下应执行全部动态驾驶任务(DDT)且不应造成不合理的安全风险。

4.8　ADS 在激活状态下执行动态驾驶任务(DDT)时,应符合道路交通规定。

4.9　ADS 在激活状态下执行动态驾驶任务(DDT)时,应符合其他道路使用者的合理预期。

4.10　ADS 在激活状态下,对于支持驾驶员恢复人工驾驶所需的装置或系统,应确认该装置或系统是否处于适合人工驾驶的运行状态。若相关装置或系统处于不适当的运行状态,ADS 应执行合理的控制策略。

注:所需的装置或系统如除雾装置、前风窗玻璃刮水器、照明装置等。

4.11　ADS 在激活状态下,不应导致任何可合理预见且可预防的碰撞事故。

4.12　ADS 在激活状态下,当碰撞不可避免时,应执行合理控制策略以降低事故伤害或损失。

4.13　ADS 在激活状态下,当检测到车辆发生碰撞后,除车辆制造商声明的情况,应使车辆静止。

4.14　ADS 在激活状态下,当设计运行条件(ODC)即将不满足或已经不满足时,应执行合理的控制策略。

4.15 ADS 在激活状态下，应与其他道路使用者进行有效的信息交互。

注：信息交互方式如转向信号灯、制动灯等。

4.16 ADS 在激活状态下，不应扰乱正常的交通流而导致整体通行效率下降。

4.17 ADS 不应存在由于功能异常表现引起的危害而导致的不合理风险，应符合附录 A。

4.18 ADS 不应存在因预期功能或其实现的功能不足引起的危害而导致的不合理风险，应符合附录 A。

4.19 装备 ADS 的车辆应装备自动驾驶数据记录系统(DSSAD)。

4.20 应在审核 ADS 开发设计过程和材料的基础上，合理选择仿真试验、场地试验、道路试验等试验方法验证 ADS 符合本文件的要求，试验类型可参考附录 B 进行选择。

4.21 对于设计运行范围(ODD)包含公路或城市道路的 ADS，若进行场地试验，应至少按照 GB/T 41798 进行试验；若进行道路试验，应至少按照 GB/T 44719 进行试验；若进行仿真试验，应至少按照自动驾驶功能仿真试验方法相关国家标准进行试验。

5 动态驾驶任务执行

5.1 ADS 应能持续识别是否满足其设计运行条件(ODC)。

5.2 ADS 的感知系统应具备与 ADS 的 ODC 相适配的探测范围。

5.3 ADS 应能确定自车位置、探测周围环境中的目标和事件。

注：常见目标如道路(含道路类型、道路表面条件、道路几何、车道特征、道路边缘等)、道路设施(含交通标志、交通信号灯等)、目标物(含机动车、非机动车、行人、障碍物等)、天气环境(含天气、光照条件等)、数字信息环境(含无线通信、位置信号等)。

5.4 ADS 应能探测目标的位置以及动态目标的移动速度。

5.5 ADS 应执行合理的控制策略应对感知系统的性能衰退。

注：性能衰退一般指由于传感器自身的老化而造成的性能下降。

5.6 ADS 应执行合理的控制策略应对探测到但无法识别类型的目标物。

5.7 ADS 应执行合理的控制策略应对无法探测区域内存在的安全风险。

注：无法探测区域如传感器布置及感知范围造成的盲区、由其他道路使用者或障碍物遮挡造成的盲区、道路拓扑或形状造成的盲区等。

5.8 ADS 在激活状态下，应合理规划和控制车辆行驶路径与行驶速度，以适应道路、道路设施、目标物、天气环境、数字信息环境等。

5.9 ADS 在激活状态下，应控制车辆与其他道路使用者保持安全距离；若因其他道路使用者的行为导致当前距离无法满足安全距离要求，则应执行合理的控制策略以降低安全风险并在后续合适时机调整保持安全距离。

5.10 ADS 在激活状态下，应执行合理控制策略应对静止的其他道路使用者。

5.11 ADS 在激活状态下，应至少探测由于前方车辆减速、车辆切入或突然出现的障碍物而导致碰撞的风险，并应自动执行合理的控制策略以最大限度地减少对用户和其他道路使用者的安全风险。

5.12 ADS 在激活状态下，不应与车辆前方无遮挡的行人发生碰撞；若因行人导致无法避免碰撞，则应减缓碰撞。

5.13 ADS 在激活状态下，不应导致车辆失去控制和单车事故。

5.14 ADS 在激活状态下，应合理控制车辆的照明和光信号装置，包括但不限于转向信号灯、危险警告信号、制动灯。

6 动态驾驶任务后援

6.1 驾驶员接管能力监测

6.1.1 一般要求

6.1.1.1 对于需要传统驾驶员执行接管的ADS,应具备驾驶员接管能力监测功能。

6.1.1.2 驾驶员接管能力监测功能至少应具备在位监测和执行动态驾驶任务(DDT)能力监测。

6.1.2 驾驶员在位监测

对于需要传统驾驶员执行接管的ADS,在激活状态下,当发生以下任一情况时,ADS应按照6.2发出介入请求:

a) 驾驶员不在驾驶位超过1 s;

b) 驾驶员未系安全带。

6.1.3 驾驶员执行动态驾驶任务(DDT)能力监测

6.1.3.1 对于需要传统驾驶员执行接管的ADS,应至少通过2种有效的指标对驾驶员是否具备执行动态驾驶任务(DDT)的能力进行判定,且应确保判定周期是合理的。

注:指标如特定的人机交互动作、眼部状态、头部运动或身体运动等。

6.1.3.2 对于需要传统驾驶员执行接管的ADS,当ADS处于激活状态且驾驶员被判定为不具备执行动态驾驶任务(DDT)的能力时,ADS应立即发出明确的接管能力不足提示信号,每次发出的接管能力不足提示信号应在满足以下任一条件时关闭:

a) 监测到驾驶员恢复执行动态驾驶任务(DDT)能力;

b) ADS发出介入请求;

c) ADS执行最小风险策略(MRM);

d) ADS退出。

6.2 接管

6.2.1 一般要求

对于需要传统驾驶员执行接管的ADS,发出介入请求和响应驾驶员接管的控制策略应安全、可靠和有效,并应能及时检测驾驶员是否执行接管操作。

6.2.2 发出介入请求

6.2.2.1 对于需要传统驾驶员执行接管的ADS,应具备明确的介入请求触发条件,且ADS应能识别需要发出介入请求的所有情况。除6.2.2.2 c)和6.2.2.3的特殊情况外,当不满足7.1.2.1中任一条件或接管能力不足提示信号达到设定时长时,ADS应发出介入请求。

6.2.2.2 介入请求的发出时机应确保驾驶员有足够的时间安全接管车辆,至少满足以下要求。

a) 对于计划接管事件,ADS应在适当的时刻发出介入请求,以确保即使驾驶员未接管,最小风险策略(MRM)仍能使车辆在计划接管事件发生前静止。

b) 对于非计划接管事件,ADS应在检测到该事件时及时发出介入请求。

注:非计划接管事件是指ADS预先未知晓但需要发出介入请求的事件,如道路临时施工、车道标线消失等。

c) 对于影响ADS运行的失效,ADS应在检测到该失效时立即发出介入请求。若该失效为

ADS 严重失效或车辆严重失效，则 ADS 可不发出介入请求直接执行最小风险策略（MRM）。

6.2.2.3 若发生车辆制造商所声明的无法保障驾驶员有充足的时间接管车辆的事件，ADS 不应发出介入请求，可立即执行最小风险策略（MRM）。

示例：企业声明在“事件 X”下无法保障驾驶员有充足的时间接管车辆并证明该声明的合理性，则 ADS 在“事件 X”下就不必也不能发出介入请求。

6.2.3 介入请求阶段

6.2.3.1 在介入请求发出过程中，ADS 应保持激活状态并执行全部动态驾驶任务（DDT）。

6.2.3.2 除车辆制造商声明的特殊情况，在介入请求发出过程中，ADS 不应使车辆静止。

6.2.3.3 在介入请求发出过程中，介入请求应在发出后合理时长内升级并保持升级状态至介入请求终止。

6.2.3.4 介入请求从发出到因执行最小风险策略（MRM）而终止的时长应不小于 10 s，使驾驶员有充足的时间接管车辆。

注：在驾驶员持续未接管的情况下，介入请求发出、升级以及开始执行 MRM 的时序关系示意图如图 1。

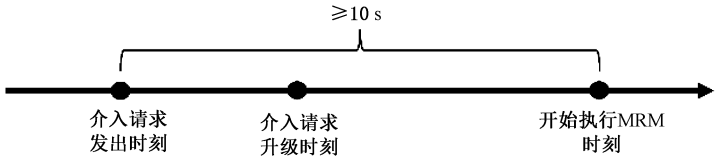

图 1 介入请求发出、升级以及开始执行 MRM 的时序关系示意图

6.2.4 终止介入请求

仅当 ADS 退出或执行最小风险策略（MRM）时，才应终止介入请求。

6.3 最小风险策略（MRM）

6.3.1 执行最小风险策略（MRM）

6.3.1.1 ADS 应有明确的执行最小风险策略（MRM）的条件，且应能识别需要执行最小风险策略（MRM）的所有情况，至少应包括：

a) 对于需要传统驾驶员执行接管的 ADS，驾驶员未在规定的时间（不小于 10 s）内响应介入请求；

b) 对于不需要传统驾驶员执行接管的 ADS，当设计运行条件（ODC）即将不满足，ADS 及时执行最小风险策略（MRM）并能使车辆在不满足设计运行条件（ODC）之前达到静止；若因特殊情况使设计运行条件（ODC）突然不满足，ADS 立即执行最小风险策略（MRM）并能使车辆达到静止。

6.3.1.2 当 ADS 执行最小风险策略（MRM）时，应将用户和其他道路使用者的安全风险降至可接受水平。

注：在执行最小风险策略（MRM）期间，ADS 可能不再有能力满足本文件的要求，但其目标是使安全风险降至可接受水平。

6.3.1.3 当 ADS 执行最小风险策略（MRM）时，应开启并保持危险警告信号，在换道过程中应根据道路交通规定合理使用危险警告信号。

6.3.2 终止最小风险策略（MRM）

6.3.2.1 仅当 ADS 退出或 ADS 使车辆静止时，才应终止最小风险策略（MRM）。

6.3.2.2 当因车辆静止而终止最小风险策略(MRM)后,不应因 ADS 退出导致危险警告信号关闭。

7 人机交互

7.1 激活和退出

7.1.1 一般要求

7.1.1.1 ADS 应配备供用户激活和退出 ADS 的专用操纵方式,该方式应防止可合理预见的用户误用。

注:专用操纵方式如专用的操纵件或对操纵件的专用操纵方法等。

7.1.1.2 当 ADS 处于激活状态时,应至少有一种退出 ADS 的操纵方式对用户保持可见。

7.1.1.3 车辆每次点火(上电)后(发动机自动启停除外),ADS 应处于未激活状态。

7.1.2 激活

7.1.2.1 对于需要传统驾驶员执行接管的 ADS,仅当驾驶员执行激活操作且满足以下所有条件时,ADS 才应被激活:

a) 驾驶员坐在驾驶位置上,且系好安全带;
b) 驾驶员具备执行动态驾驶任务(DDT)能力;
c) 不存在影响 ADS 运行的失效;
d) 自动驾驶数据记录系统(DSSAD)处于可记录状态;
e) 车辆未在执行影响 ADS 运行的软件升级;
f) 除 a)~e)外,车辆制造商声明的其他设计运行条件(ODC)。

7.1.2.2 对于不需要传统驾驶员执行接管的 ADS,仅当用户执行激活操作且满足以下所有条件时,ADS 才应被激活:

a) 不存在影响 ADS 运行的失效;
b) 自动驾驶数据记录系统(DSSAD)处于可记录状态;
c) 车辆未在执行影响 ADS 运行的软件升级;
d) 除 a)~c)外,车辆制造商声明的其他设计运行条件(ODC)。

7.1.3 退出

7.1.3.1 满足以下任一条件时,ADS 应退出:

a) 用户通过专用操纵方式退出 ADS;
b) 驾驶员按照 7.2.2.1 干预横向运动控制;
c) 驾驶员按照 7.2.3.1、7.2.3.2 干预纵向运动控制,且驾驶员手握方向盘;
d) 在介入请求发出或执行最小风险策略(MRM)过程中,除 a)~c)外,ADS 确认驾驶员手握方向盘且专注于动态驾驶任务(DDT);
e) 因车辆静止而终止最小风险策略(MRM)。

7.1.3.2 在发生车辆严重失效或 ADS 严重失效的情况下,ADS 可执行车辆制造商声明的其他安全退出的控制策略。

7.1.3.3 除 7.1.3.1、7.1.3.2 以及 ADS 到达预设目的地外,ADS 不应退出。

7.1.3.4 仅当用户执行的退出操作将导致危急的碰撞风险时,ADS 可暂缓退出。

7.1.3.5 ADS 的退出不应导致:

a) 任何应急辅助功能自动关闭;
b) 任何部分驾驶辅助功能或组合驾驶辅助功能自动激活。

7.2 干预

7.2.1 一般要求

ADS 响应驾驶员干预的控制策略应安全、可靠和有效，并应能检测驾驶员是否执行干预操作。

7.2.2 横向运行控制干预

7.2.2.1 当驾驶员对转向控制的干预超过车辆制造商声明的为防止误用而设计的合理阈值时，驾驶员输入的转向控制应被执行。

7.2.2.2 ADS 应检测驾驶员是否专注于动态驾驶任务(DDT)，7.2.2.1 中的阈值应与驾驶员专注于动态驾驶任务(DDT)的情况相关。

7.2.3 纵向运动控制干预

7.2.3.1 当驾驶员对制动控制的干预产生比 ADS 引起的减速度更大或通过任何制动系统使车辆保持静止时，驾驶员输入的制动控制应被执行。

7.2.3.2 当驾驶员对加速控制进行干预时，驾驶员的输入可被执行，但不应导致 ADS 不符合本文件的要求。

7.2.3.3 对于需要传统驾驶员执行接管的 ADS，当驾驶员仅干预制动或加速控制且超过为防止误用而设计的合理阈值时，ADS 应发出介入请求。

7.2.3.4 对于不需要传统驾驶员执行接管的 ADS，当驾驶员仅干预制动或加速控制且超过为防止误用而设计的合理阈值时，ADS 应执行合理的控制策略。

7.2.4 干预抑制

若驾驶员的干预将导致危急的碰撞风险，ADS 可根据车辆制造商声明的方式减弱或抑制驾驶员的干预对任何控制的影响。

7.2.5 其他干预策略

7.2.5.1 在发生车辆严重失效或 ADS 严重失效的情况下，ADS 可执行车辆制造商声明的其他安全响应干预的控制策略。

7.2.5.2 若用户操纵车辆其他干预装置(如有)，ADS 应对用户进行提示，并执行车辆制造商声明的控制策略。

注：其他干预装置如转向信号灯操纵件。

7.3 系统状态提示

7.3.1 一般要求

7.3.1.1 ADS 应持续向用户提示明确、充分的 ADS 状态信息，各状态信息应易于区分，且不应对用户造成干扰。

7.3.1.2 当 ADS 状态发生变化时，ADS 应及时向用户提供必要的提示信息。

7.3.2 未就绪状态提示

若由于 ADS 处于未就绪状态而导致用户激活系统失败，则应向用户直观地提示。

注：未就绪状态是指ADS不能被激活的未激活状态。

7.3.3 就绪状态提示

当 ADS 处于就绪状态时，宜至少通过光学信号向用户提示系统可被激活。

示例：文字信息、图形标志等。

7.3.4 激活状态提示

7.3.4.1 ADS 由未激活状态进入激活状态时，应至少通过专用的光学信号向用户提示 ADS 已激活。

7.3.4.2 ADS 处于激活状态时，应至少通过光学信号持续向用户提示 ADS 处于激活状态。

7.3.5 退出提示

ADS 由激活状态退出至未激活状态时，应通过至少两种方式向用户提示 ADS 已退出，至少包括光学信号。由于驾驶员接管导致 ADS 退出，可仅用光学信号提示。

7.3.6 介入请求

7.3.6.1 未升级的介入请求的提示方式应在光学信号的基础上附加声学和/或触觉信号。其中光学信号应直观且明确地提示驾驶员介入请求的响应方式，标志应符合 GB/T 44298—2024 表 1 中序号 5 的要求。

7.3.6.2 按照 6.2.3.3 进行介入请求升级后，升级的介入请求至少应增加持续或间歇性的触觉提示。

7.3.7 最小风险策略（MRM）提示

7.3.7.1 在 ADS 执行最小风险策略（MRM）过程中，应对用户给出明显提示，提示方式应在光学信号的基础上附加声学和/或触觉信号。

7.3.7.2 ADS 处于最小风险状态（MRC）时，应至少以光学、声学或触觉中的两种信号提示用户直至 ADS 退出。

7.3.7.3 对于需要传统驾驶员接管的 ADS，最小风险策略（MRM）的提示信号应与介入请求不同。

7.3.8 失效提示

在 ADS 激活状态下，若检测到 ADS 失效，ADS 应向用户发出明显提示，至少包括光学提示信号。

7.3.9 接管能力不足提示

接管能力不足提示信号应明显区别于 ADS 激活状态下车辆其他提示信号。

7.3.10 暂缓或抑制响应用户操作提示

若 ADS 暂缓或抑制响应用户的操作，应明确提示且区别于 ADS 激活状态下车辆其他提示信号。

8 说明书

对于装备 ADS 的车辆，其产品说明书至少应包含：

a） “本车具备 ADS”等内容的说明；

b） ADS 的设计运行条件（ODC）的说明；

c） 激活 ADS 的方法及条件的说明；

d） 退出 ADS 的方法及条件的说明；

e） 干预 ADS 的方法及结果的说明；

f) ADS 各状态提示信号的说明；
g) 若 ADS 不需要接管，“本车 ADS 无需被驾驶员接管”等内容的说明；
h) 若 ADS 需要接管，“本车 ADS 在特定条件下需要被驾驶员接管”等内容的说明；
i) 若 ADS 需要接管，介入请求的说明；
j) 若 ADS 需要接管，接管 ADS 的方法及结果的说明；
k) 若 ADS 需要接管，接管能力不足提示信号的说明；
l) ADS 执行最小风险策略（MRM）的条件的说明；
m) ADS 执行最小风险策略（MRM）的车辆行为及结果的说明；
n) 若 ADS 激活状态下发生碰撞事故，对用户的建议。

附 录 A
（规范性）
适用于ADS的安全性的特殊要求

A.1 总则

本附录旨在确保车辆制造商在ADS设计和开发过程中对功能安全和预期功能安全等进行了充分的考虑，并贯穿整个车辆的生命周期过程（开发、生产、运行、服务、报废），以避免因ADS故障、预期功能不足导致的对用户和其他道路使用者造成不合理的风险，确保ADS的运行安全。

本附录规定了ADS在功能安全和预期功能安全等方面的特殊要求。

本附录不针对ADS的标称性能，也不作为ADS功能安全和预期功能安全开发的具体指导，而是规定ADS设计、验证和确认过程中应遵循的方法和应具备的信息，作为满足功能安全和预期功能安全等的依据。

A.2 总体要求

A.2.1 车辆制造商应建立安全管理体系，采用有效的过程、方法和工具管理ADS在车辆全生命周期（包含开发、生产、运行、服务、报废）中的安全性，并证明ADS在声明的设计运行条件（ODC）内（包括边界）不会对用户和其他道路使用者造成不合理的风险。

A.2.2 车辆制造商应建立设计开发过程，包括安全管理体系、需求管理、需求实施、测试、失效跟踪、维护和发布。

A.2.3 车辆制造商应在负责ADS的功能安全、预期功能安全、信息安全和其他安全的部门间建立并保持有效的沟通渠道。

A.2.4 车辆制造商应具有一个或多个过程，用于监控由ADS引发的安全相关事件，以及管理ADS潜在风险并能升级ADS。

A.2.5 车辆制造商应定期进行独立的内部过程审核，以确保根据A.2.1～A.2.4建立的过程得到一致的实施。

A.2.6 车辆制造商应管理供应商（例如，合同管理、质量管理体系等），以确保供应商的安全管理体系符合A.2.1～A.2.3和A.2.5中相关的要求。

A.3 系统描述

A.3.1 ADS功能描述

A.3.1.1 车辆制造商应具有相应的文档，用于说明ADS的功能（包括其对应的驾驶控制策略）。

A.3.1.2 车辆制造商应具有相应的文档，用于说明ADS的设计运行条件（ODC）以及在设计运行条件（ODC）内执行动态驾驶任务（DDT）所采取的方法。

A.3.1.3 车辆制造商应具有相应的文档，用于说明ADS与用户和其他道路使用者预期的交互，包括当达到ADS的设计运行条件（ODC）时的人机交互（HMI）策略。

A.3.1.4 车辆制造商应具有相应的文档，用于说明ADS激活、干预（包括干预的阈值，例如力矩、角度、持续时间）、最小风险策略（MRM）和退出等，包括ADS如何防止用户合理可预见的误用，以及如何通过最小风险策略（MRM）使安全风险降至可接受水平。

A.3.1.5 对于需要传统驾驶员接管的ADS，车辆制造商还应具有相应的文档，用于说明ADS向驾驶员发出介入请求的各种情况和ADS如何确认驾驶员状态[例如，是否具备动态驾驶任务（DDT）执行

能力]、接管能力不足提示信号以及驾驶员执行动态驾驶任务(DDT)能力的判定周期等。

A.3.1.6 车辆制造商应具有相应的文档,用于说明感知系统的输入、输出,感知系统正常工作范围(包括应对传感器的衰退)以及感知系统对 ADS 行为的影响。

A.3.1.7 车辆制造商应具有相应的文档,用于说明决策系统的输出,以及对车辆运动控制的影响等。

A.3.1.8 如果在 ADS 运行阶段使用连续的学习算法,车辆制造商应具有相应的文档,用来对数据处理过程进行描述。

A.3.2 系统布局和原理图

A.3.2.1 系统组件清单

A.3.2.1.1 车辆制造商应具有组件清单,该清单应包含 ADS 的所有单元,同时也应列出为实现自动驾驶功能所需的车辆其他系统。

注:车辆其他系统如自动驾驶数据记录系统(DSSAD)。

A.3.2.1.2 车辆制造商应具有 ADS 布局及原理图,且能够清晰地展示组件分布和相互连接,原理图应包括以下内容:

a) 感知系统(包含地图和定位系统,如适用);
b) 决策系统;
c) 执行系统;

注:执行系统自身的功能安全要求在GB 17675、GB 12676和GB 21670中已有具体要求。

d) 由远程后台提供的远程监控(如适用)。

A.3.2.2 单元功能

车辆制造商应具有相应的文档,用来概述以下内容:

a) ADS 各单元的功能,并展示该单元与其他单元或车辆其他系统间的连接,可使用带标记的框图或其他示意图说明;
b) 信号传输与各单元的对应关系,以及信号的优先级(如适用)。

A.3.2.3 单元的识别

A.3.2.3.1 车辆制造商应具有相应的文档,文档中应能清晰明确地识别每个单元(例如,硬件单元、软件单元)并提供相应的说明。

A.3.2.3.2 车辆制造商应明确标识硬件和软件的版本。

A.3.2.4 感知系统部件的安装说明

车辆制造商应具有相应的文档,用来说明感知系统中单个部件的安装信息。这些信息应包括但不限于:

a) 部件在车辆上的位置;
b) 部件外表面的材料;
c) 部件外表面的尺寸和形状;
d) 部件外表面的光洁度;
e) 对 ADS 性能影响大的安装规范。

A.4 功能安全要求

A.4.1 危害分析和风险评估

车辆制造商应根据装备 ADS 的车辆的目标使用场景及目标用户,在整车层面开展面向功能安全

的危害分析和风险评估，并定义相应的汽车安全完整性等级（ASIL）和安全目标，符合 GB/T 34590.3—2022 第 6 章的要求。

A.4.2 功能安全概念

A.4.2.1 车辆制造商应进行系统层面的面向功能安全的安全概念活动，以保障系统在故障条件下，对用户和其他道路使用者不存在不合理的风险。

注：安全概念包括功能安全概念和技术安全概念。

A.4.2.2 车辆制造商应进行安全分析活动，并制定对应的安全措施，以说明系统一旦发生失效，该系统如何避免或减轻可能对用户和其他道路使用者的安全产生影响的危害。安全分析至少包括以下内容。

a） 系统层面的安全分析，可采用潜在失效模式与影响分析（FMEA）、故障树分析（FTA）、系统理论过程分析（STPA）或适合系统安全分析的其他类似过程。

b） 考虑如下因素可能导致的危害以开展安全分析：

1） 感知系统故障；

2） 决策系统故障；

3） 执行系统故障。

注：执行系统相关安全分析活动参考相关国家标准。

A.4.2.3 车辆制造商应具备文档，用于描述 ADS 提示信号优先级以及 ADS 在典型故障情况下向用户提供的提示信号。

A.4.2.4 车辆制造商应进行安全措施制定，以确保安全概念实现。ADS 可采取如下安全措施。

a） 使用部分系统维持运行。若选择在某些故障条件下（如探测相邻车道的传感器故障）维持部分性能（例如，维持在本车道，不支持变道）的运行模式，应说明这些故障条件并确定部分系统维持运行的效果。

b） 切换到备用系统。若选择备用系统实现动态驾驶任务（DDT），应说明切换机制的原理、冗余的逻辑和层级、备用系统的状态检查机制并界定备用系统的效果。

c） 退出自动驾驶功能。若选择退出，过程应符合本文件要求。

A.4.3 验证和确认

A.4.3.1 车辆制造商应执行验证和确认活动，并对验证和确认计划及结果进行检查，以证明满足面向功能安全的安全概念。验证和确认应基于仿真试验、场地试验、道路试验或其他适当的方法。

A.4.3.2 车辆制造商应通过模拟 ADS 组件的典型故障，以检查系统组件发生失效情况下的安全表现。

A.5 预期功能安全要求

A.5.1 危害识别和风险评估

车辆制造商应根据装备 ADS 的车辆的目标使用场景及目标用户，在整车层面开展面向预期功能安全的危害识别和风险评估，并确定风险接受准则，符合 GB/T 43267—2023 第 6 章的要求。

A.5.2 预期功能安全措施的制定

A.5.2.1 车辆制造商应制定面向预期功能安全的安全措施，以保障对于功能不足，ADS 不会对用户和其他道路使用者造成不合理的风险。ADS 可采取如下安全措施：

a） 改善系统性能；

b） 限制系统激活；

c） 向用户发出警告；

d） 请求驾驶员接管；

e） 降速运行；

f） 最小风险策略（MRM）。

A.5.2.2 车辆制造商应进行安全分析活动，以识别和评估系统潜在功能不足和潜在触发条件，并制定对应的安全措施，以说明在对应的场景下，该 ADS 如何避免或减轻可能对用户和其他道路使用者的安全产生影响的危害。安全分析至少包括以下内容。

a） 系统层面的安全分析，见 GB/T 43267—2023 中的表 4 和 B.3，或任何适合系统安全分析的其他类似过程。

b） 考虑如下因素可能导致的危害以开展安全分析：

1） 感知系统、决策系统和执行系统的常见功能不足；

2） 未能充分考虑或未遵守道路交通规定；

3） 可合理预见的误用；

4） 设计运行条件（ODC）边界场景识别不足。

A.5.3 验证和确认策略制定

车辆制造商应针对 ADS 制定验证和确认策略，包括验证和确认方法及合理性证明，符合 GB/T 43267—2023 第 9 章的要求。

A.5.4 验证和确认

A.5.4.1 车辆制造商应执行验证和确认活动，并对验证和确认计划及结果进行检查，以证明满足面向预期功能安全的接受准则。验证和确认应基于仿真试验、场地试验、道路试验或其他适当的方法。

A.5.4.2 车辆制造商应对 ADS 的设计运行条件（ODC）下典型的可合理预见的场景进行充分确认。

A.5.4.3 车辆制造商应检查在关键典型场景下 ADS 的目标和事件探测与响应（OEDR）、系统决策和人机交互（HMI）等是否符合本文件的要求。

A.5.5 运行阶段预期功能安全监控

车辆制造商应建立并落实现场监控流程，以确保 ADS 运行阶段的预期功能安全，符合 GB/T 43267—2023 第 13 章的要求。

示例：面向 ADS 的现场监控流程可包括但不限于自动驾驶数据记录系统（DSSAD）、汽车事件数据记录系统（EDR）、车载安全监控系统或远程安全监控系统。

A.6 系统评估报告

车辆制造商应基于本附录的要求进行系统评估并输出评估报告。评估报告应具有可追溯性。

附 录 B
（资料性）
技术要求与试验类型对应表

为了对本文件相关技术要求的验证提供指导，制定了技术要求与试验类型对应表。试验类型的选择宜参考表 B.1。

表 B.1 技术要求与试验类型对应表

序号	技术要求条款	仿真试验	场地试验	道路试验
1	4.1	可选	可选	可选
2	4.2	可选	必选	必选
3	4.3	可选	必选	必选
4	4.4	可选	必选	可选
5	4.5	可选	必选	可选
6	4.6	必选	可选	可选
7	4.7	可选	必选	必选
8	4.8	必选	必选	必选
9	4.9	可选	可选	可选
10	4.10	可选	必选	可选
11	4.11	必选	必选	可选
12	4.12	必选	可选	可选
13	4.13	可选	必选	可选
14	4.14	可选	必选	必选
15	4.15	可选	必选	可选
16	4.16	可选	可选	必选
17	5.1	可选	必选	必选
18	5.2	可选	必选	可选
19	5.3	可选	必选	可选
20	5.4	可选	可选	可选
21	5.5	必选	可选	可选
22	5.6	可选	可选	可选
23	5.7	可选	必选	可选
24	5.8	可选	必选	必选
25	5.9	可选	必选	可选
26	5.10	可选	必选	可选
27	5.11	可选	必选	可选
28	5.12	可选	必选	可选

表 B.1　技术要求与试验类型对应表(续)

序号	技术要求条款	仿真试验	场地试验	道路试验
29	5.13	可选	可选	可选
30	5.14	可选	必选	可选
31	6.1.1.1	可选	可选	可选
32	6.1.1.2	可选	可选	可选
33	6.1.2	可选	必选	可选
34	6.1.3.1	可选	必选	可选
35	6.1.3.2	可选	必选	可选
36	6.2.1	可选	可选	可选
37	6.2.2.1	可选	必选	可选
38	6.2.2.2	必选	必选	可选
39	6.2.2.3	可选	必选	可选
40	6.2.3.1	可选	必选	可选
41	6.2.3.2	可选	必选	可选
42	6.2.3.3	可选	必选	可选
43	6.2.3.4	可选	必选	可选
44	6.2.4	可选	必选	可选
45	6.3.1.1	必选	必选	可选
46	6.3.1.2	可选	必选	可选
47	6.3.1.3	可选	必选	可选
48	6.3.2.1	可选	必选	可选
49	6.3.2.2	可选	必选	可选
50	7.1.1.1	可选	必选	可选
51	7.1.1.2	可选	必选	可选
52	7.1.1.3	可选	必选	可选
53	7.1.2.1	必选	必选	可选
54	7.1.2.2	必选	必选	可选
55	7.1.3.1	可选	必选	可选
56	7.1.3.2	可选	可选	可选
57	7.1.3.3	必选	必选	可选
58	7.1.3.4	可选	必选	可选
59	7.1.3.5	可选	必选	可选
60	7.2.1	可选	可选	可选
61	7.2.2.1	可选	必选	可选
62	7.2.2.2	可选	必选	可选

表 B.1　技术要求与试验类型对应表(续)

序号	技术要求条款	仿真试验	场地试验	道路试验
63	7.2.3.1	可选	必选	可选
64	7.2.3.2	可选	必选	可选
65	7.2.3.3	可选	必选	可选
66	7.2.3.4	可选	必选	可选
67	7.2.4	可选	可选	可选
68	7.2.5.1	可选	可选	可选
69	7.2.5.2	可选	必选	可选
70	7.3.1.1	可选	必选	可选
71	7.3.1.2	可选	必选	可选
72	7.3.2	可选	必选	可选
73	7.3.3	可选	必选	可选
74	7.3.4.1	可选	必选	可选
75	7.3.4.2	可选	必选	可选
76	7.3.5	可选	必选	可选
77	7.3.6.1	可选	必选	可选
78	7.3.6.2	可选	必选	可选
79	7.3.7.1	可选	必选	可选
80	7.3.7.2	可选	必选	可选
81	7.3.7.3	可选	必选	可选
82	7.3.8	可选	必选	可选
83	7.3.9	可选	必选	可选
84	7.3.10	可选	必选	可选

注：“必选”是指对条款要求进行试验时，至少采用该试验类型；“可选”是指对条款要求进行试验时，根据产品功能、试验能力等实际情况，合理选择该试验类型共同支持条款验证工作。

参 考 文 献

[1] GB 12676 商用车辆和挂车制动系统技术要求及试验方法
[2] GB 17675 汽车转向系 基本要求
[3] GB 21670 乘用车制动系统技术要求及试验方法