



# 中华人民共和国国家标准

GB 44721—XXXX  
代替 GB/T 44721—2024

## 智能网联汽车 自动驾驶系统安全要求

Intelligent and connected vehicle — Safety requirements for  
automated driving system

（报批稿）

（本草案完成时间：2026 年 6 月 3 日）

XXXX – XX – XX 发布

XXXX – XX – XX 实施

国家市场监督管理总局  
国家标准化管理委员会 发布



# 目 次

前 言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	5
5 ADS 技术要求.....	5
6 保障要求 .....	12
7 保障要求检验 .....	18
8 安全档案检验 .....	19
9 确认性试验 .....	21
10 同一型式判定 .....	21
11 标准的实施 .....	22
附 录 A （规范性） 接管能力监测技术要求.....	23
附 录 B （规范性） 应用于高速公路和/或城市快速路的 3 级自动驾驶功能具体技术要求....	24
附 录 C （规范性） 4 级自动驾驶功能具体技术要求.....	35
附 录 D （规范性） 安全档案.....	39
参 考 文 献 .....	57

## 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。

本文件代替GB/T 44721—2024《智能网联汽车 自动驾驶系统通用技术要求》，与GB/T 44721—2024相比，除结构调整及编辑性改动外，主要技术变化如下：

- 更改了标准名称，明确安全要求；
- 更改了标准范围（见第1章，2024年版的第1章）；
- 更改了规范性引用文件（见第2章，2024年版的第2章）；
- 更改了术语和定义（见第3章，2024年版的第3章）；
- 增加了缩略语（见第4章）；
- 更改了动态驾驶任务要求（见5.1，2024年版的第4、5章和6.3）；
- 更改了人机交互要求（见5.2，2024年版的6.2和第7章）；
- 更改了用户告知要求（见5.3，2024年版的第8章）；
- 更改了保障要求（见第6章，2024年版的附录A.2）；
- 增加了保障要求检验（见第7章）；
- 增加了安全档案检验（见第8章）；
- 更改了确认性试验（见第9章，2024年版的附录B）；
- 增加了同一型式判定（见第10章）；
- 增加了标准的实施（见第11章）；
- 更改了接管能力监测技术要求（见附录A，2024年版的6.1）；
- 增加了应用于高速公路和/或城市快速路的3级自动驾驶功能具体技术要求（见附录B）；
- 增加了4级自动驾驶功能具体技术要求（见附录C）；
- 更改了安全档案（见附录D，2024年版的附录A.1、A.3~A.6）。

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并归口。

本文件及其所代替文件的历次版本发布情况为：

- 2024年首次发布为GB/T 44721—2024；
- 本次为第一次修订。

# 智能网联汽车 自动驾驶系统安全要求

## 1 范围

本文件规定了智能网联汽车自动驾驶系统的技术要求、保障要求、同一型式判定，描述了相应的保障要求检验、安全档案检验和确认性试验等方法。

本文件适用于装备3级和/或4级驾驶自动化系统的M类和N类车辆，不适用于自动泊车系统。

## 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 41798 智能网联汽车 自动驾驶功能场地试验方法及要求

GB 44497 智能网联汽车 自动驾驶数据记录系统

GB/T 44719 智能网联汽车 自动驾驶功能道路试验方法及要求

GB/T 45312 智能网联汽车 自动驾驶系统设计运行条件

GB/T 47025 智能网联汽车 自动驾驶功能仿真试验方法及要求

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**自动驾驶系统** automated driving system

具备持续执行全部动态驾驶任务能力的车辆硬件和软件共同组成的系统。

### 3.2

**动态驾驶任务** dynamic driving task

车辆驾驶所需的感知、决策及执行控制等行为，包括对车辆运动、照明及信号装置等的控制。

### 3.3

**自动驾驶功能** ADS feature

ADS在特定的设计运行条件下执行全部DDT的功能。

### 3.4

**3级自动驾驶功能** level 3 ADS feature

**L3自动驾驶功能** level 3 ADS feature

有ODD限制且需要后援用户的自动驾驶功能。

注：指GB/T 40429—2021定义的3级驾驶自动化功能。

### 3.5

**4级自动驾驶功能** level 4 ADS feature

**L4自动驾驶功能** level 4 ADS feature

有 ODD 限制且不需要后援用户的自动驾驶功能。

注：指GB/T 40429—2021定义的4级驾驶自动化功能。

3.6

**激活状态** active state

ADS 执行 DDT 以控制车辆的运行状态。

3.7

**就绪状态** available state

自动驾驶功能的设计运行条件已符合但 ADS 尚未执行控制的状态。

3.8

**激活** activation

将自动驾驶功能由就绪状态转换为激活状态的行为。

3.9

**退出** deactivation

将自动驾驶功能由激活状态转换为不执行控制的行为。

3.10

**设计运行范围** operational design domain

驾驶自动化系统设计时确定的适用于其功能运行的外部环境条件。

注：典型的外部环境条件有道路、交通、天气、光照等。

3.11

**设计运行条件** operational design condition

驾驶自动化系统设计时确定的适用于其功能运行的各类条件的总称，包括设计运行范围、车辆状态、驾乘人员状态及其他必要条件。

3.12

**计划接管事件** planned takeover event

ADS预先已知并需要发出介入请求的事件。

3.13

**用户** user

使用装备 ADS 的车辆的人员。

3.14

**车内用户** occupant

位于装备 ADS 的车辆内的用户。

3.15

**后援用户** fallback user

在自动驾驶功能激活状态下，被指定执行接管的车内用户。

3.16

**乘客** passenger

非驾驶人或后援用户的车内用户。

3.17

**干预** intervention

用户主动通过已明确的有效方式影响 ADS 执行 DDT 的行为。

3.18

**ADS 后援响应** ADS fallback response

ADS 发出介入请求和/或执行最小风险策略。

## 3.19

**介入请求** request to intervene

ADS 请求后援用户执行接管的提示。

## 3.20

**接管** take over

后援用户响应介入请求，从 ADS 获得车辆驾驶权的行为。

## 3.21

**最小风险状态** minimal risk condition

一种尽可能降低碰撞风险的稳定且静止的车辆状态。

## 3.22

**最小风险策略** minimal risk maneuver

ADS 无法继续安全执行 DDT 时，所采取的使车辆达到最小风险状态的控制策略。

## 3.23

**其他道路使用者** other road user

任何其他使用道路基础设施的实体。

## 3.24

**行为能力** behavioral competency

ADS 在其 ODC 内操控车辆时，表现出符合预期且可验证的能力。

## 3.25

**失效** failure

由于故障出现导致系统或组件预期行为的终止。

## 3.26

**故障** fault

能够引起系统或组件失效的异常情况。

## 3.27

**安全保障要求** safety maintenance specification

一种系统性的安全管理方法，包括并整合了组织、人员和技术要素：

- a) 通过规范的程序和方法来管理已识别的风险，理解风险之间及其与缓解措施的关联性和相互作用，并确保无不可预期的结果；
- b) 确保由具备相应技能、培训和认知能力的人员对 ADS 全生命周期进行监测，识别风险并制定适当的缓解措施，并充分考虑人为失误的可能性；
- c) 运用适当的工具和设备支持安全管理。

## 3.28

**仿真试验** simulation test

在仿真场景中使用仿真工具链对 ADS 或装备 ADS 的车辆开展试验的方式。

## 3.29

**仿真工具链** simulation toolchain

为进行仿真试验，由一组或多组仿真试验工具和模型组合的总称。

注：仿真工具指用于 ADS 仿真试验的硬件和/或软件设备。

## 3.30

**安全档案** safety case

通过充分、有说服力且容易理解的方式证明 ADS 符合本文件中相关的 ADS 技术要求且不会对用户及 ORU 构成不合理风险的结构化文档。

3.31

**声明 claim**

安全档案中可验证的陈述。

3.32

**论据 argument**

在安全档案中存在的书面解释，旨在阐明某项声明与其实现的证据之间的逻辑关联。

3.33

**证据 evidence**

为证明某项声明的有效性而提供的相关材料。

示例：实车试验结果、仿真试验结果、带有支持数据的分析等。

3.34

**安全概念 safety concept**

在 ADS 设计时，为保障 ADS 在其 ODC 相关的各种运行条件下，使其不会对用户和 ORU 造成不合理风险所采取的安全措施的描述。

3.35

**场景 scenario**

对在特定行程中可能出现的一系列行驶情况的描述。

3.36

**标称场景 nominal scenario**

任何不属于风险场景或失效场景的场景。

3.37

**风险场景 critical scenario**

所涉及的其他道路使用者及其行为、道路设施、障碍物等对合格且专注驾驶人执行 DDT 的风险较高，可能导致合格且专注驾驶人通过执行紧急的运动控制以避免碰撞或缓解碰撞后果的场景。

注：对于紧急的运动控制，假设仅采用制动措施，则车辆减速度大于一定的数值（例如， $3\text{ m/s}^2$ ）才能避免碰撞。

3.38

**失效场景 failure scenario**

失效会影响 ADS 执行 DDT 能力的场景。

3.39

**接管能力监测 takeover capability monitoring**

对后援用户是否具备响应介入请求并从 ADS 获得车辆驾驶权的能力进行监测。

3.40

**换道控制 lane change**

从转向信号灯首次开启，到车辆从本车道完全行驶至目标车道且转向信号灯关闭的过程。

3.41

**换道执行阶段 lane change manoeuvre phase**

从车辆外廓开始跨越目标车道边线外侧至车辆完全行驶至目标车道的阶段。

注：换道执行阶段是变更车道的一部分。

3.42

**MRM 换道控制 MRM lane change**

在执行 MRM 期间，ADS 执行的换道控制。



## 3.43

常规换道控制 regular lane change

在未执行MRM期间，ADS执行的换道控制。

## 3.44

远程协助 remote assistance

对于4级自动驾驶功能，当ADS处于激活状态且遇到难以处置的情况时，ADS接收由远程方式发送的协助信息，以继续完成行程。

注1：远程协助信息如行驶轨迹引导、停车等。

注2：策略性功能（例如，目的地选择）不属于远程协助。

## 3.45

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。

## 3.46

车辆严重失效 severe vehicle failure

任何影响 ADS 执行 DDT 能力且影响人工驾驶的失效。

## 4 缩略语

下列缩略语适用于本文件。

ADS	自动驾驶系统	Automated Driving System
APS	自动泊车系统	Automated Parking System
ASIL	汽车安全完整性等级	Automotive Safety Integrity Level
DDT	动态驾驶任务	Dynamic Driving Task
DSSAD	自动驾驶数据记录系统	Data Storage System for Automated Driving
ECU	电子控制器	Electronic Control Unit
FIT	失效率	Failures in Time
FMEA	失效模式与影响分析	Failure Mode and Effects Analysis
FTA	故障树分析	Fault Tree Analysis
HAZOP	危害和可操作性分析	HAZard and OPerability analysis
KPI	关键性能指标	Key Performance Indicators
MRC	最小风险状态	Minimal Risk Condition
MRM	最小风险策略	Minimal Risk Maneuver
ODD	设计运行范围	Operational Design Domain
ODC	设计运行条件	Operational Design Condition
ORU	其他道路使用者	Other Road User
PMHF	随机硬件失效概率度量	Probabilistic Metric for random Hardware Failures
PVPA	潜在车辆存在区域	Potential Vehicle Presence Area
SMS	安全保障要求	Safety Maintenance Specification
SOTIF	预期功能安全	Safety Of The Intended Functionality
STPA	系统理论过程分析	System Theoretic Process Analysis

## 5 ADS 技术要求

## 5.1 DDT 执行

### 5.1.1 一般要求

5.1.1.1 ADS 的安全水平应至少达到正在承担驾驶任务的合格且专注驾驶人的水平。

注：合格且专注指符合相关法律法规规定的驾驶水平。

5.1.1.2 ADS 不应对用户和 ORU 造成不合理的安全风险。

5.1.1.3 ADS 应识别当前情况是否符合自动驾驶功能的 ODC。

5.1.1.4 在激活状态下，ADS 应执行全部 DDT。

注：当坐在驾驶位的车内用户进行干预时，车内用户对车辆横向运动和/或纵向运动的控制可能优先于 ADS。

5.1.1.5 ADS 应执行合理的控制策略应对感知系统的性能衰退。

5.1.1.6 对于 3 级自动驾驶功能，若其 ODD 包括高速公路和/或城市快速路以外的道路，ADS 应至少具备车道巡航、换道控制和交叉路口（除环形路口外）通行的能力。

注：仅在专用车道内运行的快速公共汽车交通可能不具备换道控制的能力。

5.1.1.7 对于 4 级自动驾驶功能，若其 ODD 仅包括高速公路和/或城市快速路，ADS 应至少具备车道巡航、换道控制和为绕行前方障碍物而部分或全部驶入相邻车道的能力；若其 ODD 还包括高速公路和/或城市快速路以外的道路，ADS 应至少具备车道巡航、换道控制、交叉路口（除环形路口外）通行、为绕行前方障碍物而部分或全部驶入相邻车道、倒车和掉头的能力。

### 5.1.2 标称场景下的 DDT 执行

5.1.2.1 ADS 的驾驶行为不应导致碰撞。

5.1.2.2 ADS 应避免与安全相关目标发生碰撞。

注：安全相关目标指若发生碰撞可能会对车辆造成非轻微损坏，或可能对 ORU、用户或基础设施构成安全风险的目标。

5.1.2.3 根据安全风险，ADS 应调整其驾驶行为，应至少包括：

- a) 预判驾驶环境中的风险，以降低遇到风险场景的可能性；
- b) 根据安全风险调整行驶速度；
- c) 控制车辆的纵向和横向运动以与 ORU 保持适当的距离。

5.1.2.4 ADS 应以合理的控制策略应对无法充分探测区域内存在的安全风险。

注：无法充分探测区域如由 ORU 或障碍物遮挡造成的盲区、道路拓扑或形状造成的盲区等。

5.1.2.5 ADS 应探测与响应和其执行 DDT 相关的目标和事件。

5.1.2.6 ADS 应与 ORU 安全交互，应至少包括：

- a) 展现预期行为，保持稳定的驾驶行为；
- b) 进行有效的信息交互（例如，转向信号灯、制动灯等）。

5.1.2.7 对于 4 级自动驾驶功能，若乘客按照 C.3.1.2 的方法请求停车，则 ADS 应使车辆安全静止。

5.1.2.8 根据安全风险，ADS 应避免不合理地扰乱交通流而导致通行效率下降。

5.1.2.9 ADS 执行 DDT 应符合道路通行规定。

5.1.2.10 ADS 应探测与响应享有优先通行权的车辆（例如，执行紧急任务的警车、消防车、救护车、工程救险车），当妨碍享有优先通行权的车辆通行时，应至少符合以下要求：

- a) 对于 3 级自动驾驶功能，执行让行控制或执行 ADS 后援响应；
- b) 对于 4 级自动驾驶功能，执行让行控制。

5.1.2.11 ADS 应探测与响应交通警察现场指挥，应至少符合以下要求：

- a) 对于 3 级自动驾驶功能，按照交通警察现场指挥通行或执行 ADS 后援响应；
- b) 对于 4 级自动驾驶功能，按照交通警察现场指挥通行。

### 5.1.3 风险场景下的 DDT 执行

5.1.3.1 只要合理可行，ADS 在风险场景下执行 DDT 应符合 5.1.2 的要求，最小化整体安全风险。

5.1.3.2 当自动驾驶功能处于激活状态时，当碰撞不可避免时，除碰撞导致 ADS 失去对车辆的运动控制外，ADS 应降低事故伤害或损失。

注：碰撞是否可避免以合格且专注正在承担驾驶任务的驾驶人的水平为基线。

5.1.3.3 当自动驾驶功能处于激活状态时，当检测到发生碰撞后，除碰撞导致 ADS 失去对车辆的制动控制外，ADS 应使车辆静止。

### 5.1.4 失效场景下的 DDT 执行

5.1.4.1 只要合理可行，ADS 在失效场景下执行 DDT 应符合 5.1.2 的要求，最小化整体安全风险。

5.1.4.2 ADS 应探测影响其在 ODD 内执行 DDT 能力的故障和功能异常。

5.1.4.3 当发生故障时，ADS 应符合以下任一要求。

- a) 若故障使 ADS 不能安全地执行 DDT，执行 ADS 后援响应且禁止激活受影响的其他自动驾驶功能；若执行 MRM，符合 5.1.6 的要求。
- b) 若 ADS 仍能安全地执行 DDT，根据故障的严重程度调整执行 DDT 的能力。

### 5.1.5 不符合 ODC 场景下的 DDT 执行

5.1.5.1 ADS 应能安全响应不符合 ODC 的情况。对于可预见的不符合 ODC 的情况，ADS 还应能预判。

5.1.5.2 当自动驾驶功能未处于激活状态时，若存在不符合 ODC 的情况，则相应自动驾驶功能不应被激活。

5.1.5.3 当自动驾驶功能处于激活状态时，若存在不符合 ODC 的情况，ADS 应执行 ADS 后援响应。若执行 MRM，应符合 5.1.6 的要求。

5.1.5.4 ADS 在执行 ADS 后援响应过程中，只要合理可行，应符合以下要求：

- a) 在标称场景下，5.1.2 的要求继续适用；
- b) 在风险场景下，5.1.3 的要求继续适用；
- c) 在失效场景下，5.1.4 的要求继续适用。

### 5.1.6 最小风险策略

5.1.6.1 对于 3 级自动驾驶功能，若后援用户未完成接管或发生安全档案中描述的直接执行 MRM 的情况，ADS 应执行 MRM 使车辆达到 MRC，且应符合以下要求：

- a) 具备执行换道控制的能力；
- b) 最小化对用户和 ORU 的安全风险；
- c) 目标将车辆移至不妨碍交通的道路边侧安全静止，当车辆严重失效或 ADS 严重失效导致无法安全移至道路边侧，至少使车辆在本车道安全静止，在执行 MRM 过程中和使车辆达到 MRC 后，ADS 不禁止后援用户干预和退出；
- d) 在 ADS 执行 MRM 过程中和使车辆达到 MRC 后合理使用危险警告信号；
- e) 当 ADS 使车辆达到 MRC 后，仅在车辆重新启动动力系统（发动机自动启停除外）后，ADS 才能被激活。

5.1.6.2 对于 4 级自动驾驶功能，若发生安全档案中描述的执行 MRM 的情况，ADS 应执行 MRM 使车辆达到 MRC，且应符合以下要求：

- a) 具备执行换道控制的能力；

- b) 最小化对用户和 ORU 的安全风险；
- c) 目标将车辆移至不妨碍交通的安全区域静止，至少将车辆移至不妨碍交通的道路边侧安全静止；
- d) 当车辆严重失效导致无法安全移至道路边侧，至少使车辆在本车道安全静止；
- e) 在 ADS 执行 MRM 过程中和使车辆达到 MRC 后合理使用危险警告信号。

## 5.2 人机交互

### 5.2.1 一般要求

- 5.2.1.1 ADS 应确保自动驾驶功能被安全激活和退出。
- 5.2.1.2 车辆每次动力系统启动后（发动机自动启停除外），ADS 不应自动激活。
- 5.2.1.3 ADS 的安全相关提示应符合以下要求：
  - a) 在所有 ADS 运行状态下都能被目标的车内用户注意到；
  - b) 易于理解且无歧义；
  - c) 在必要时采用多种提示模式（例如，光学、声学 and 触觉）。
- 5.2.1.4 当执行 ADS 后援响应时，ADS 应向车内用户持续发出执行 ADS 后援响应的提示信号。
- 5.2.1.5 若 ADS 影响车门控制，ADS 应确保车内用户对车门的操作优先于 ADS。
- 5.2.1.6 当自动驾驶功能处于激活状态时，当检测到发生碰撞时，ADS 应向车内用户发出提示；该提示应至少持续至 ADS 退出完成或经用户确认。
- 5.2.1.7 若自动泊车功能与自动驾驶功能（非自动泊车功能）共用人机交互方式，相关人机交互方式及其合理性应在安全档案中予以说明。

注：共用人机交互方式可能包括专用的操纵方式、系统状态提示等。

### 5.2.2 允许行驶中退出至人工驾驶的自动驾驶功能

#### 5.2.2.1 一般要求

- 5.2.2.1.1 ADS 的设计应能防止可合理预见的车内用户误用。
- 5.2.2.1.2 ADS 应配备供车内用户激活和退出的专用操纵方式。
  - 注1：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。
  - 注2：APS可能共用相同的激活和退出专用操纵方式。
- 5.2.2.1.3 专用于 ADS 的车辆操纵件应清晰标识、易于区分且仅响应与之适配的操作。
- 5.2.2.1.4 ADS 应指示自动驾驶功能是否可被激活。
  - 注：当APS处于激活状态下，同驾驶自动化级别的其他自动驾驶功能可能无需指示是否可被激活。
- 5.2.2.1.5 当自动驾驶功能处于激活状态时，符合以下要求。
  - a) 与人工执行 DDT 相关的操纵件应被合理控制以防止对 ADS 执行 DDT 造成不安全的干扰，若采用抑制方式，符合以下要求：
    - 1) ADS 应具备相应控制策略，以避免出现控制权模糊或对 DDT 产生非预期影响；
    - 2) 当坐在驾驶位的车内用户对转向控制和/或制动控制的干预超过防止误用而设计的合理阈值时，ADS 应发出干预提示并按照 5.2.2.3 执行退出策略；
    - 3) 对操纵件超过抑制阈值的干预不应是触发 ADS 执行退出策略的主要方式，且该阈值应在安全档案中予以说明。
  - b) 对于 3 级自动驾驶功能，ADS 不应导致前方视野受限；对于 4 级自动驾驶功能，若 ADS 导致前方视野受限，当车内用户执行 DDT 时，ADS 应将前方视野立即恢复至适合人工驾驶的状态；

- c) 若非 ADS 导致前方视野受限，当车内用户执行 DDT 时，ADS 目标应执行合理控制策略恢复前方视野至适合人工驾驶的状态。
- 5.2.2.1.6 对于坐在驾驶位的车内用户干预转向控制和/或制动控制的情况，若提供干预后不执行退出策略的设置且车内用户选择该设置，ADS 应提示相关安全风险，并在干预期间发出干预提示。
- 5.2.2.1.7 当自动驾驶功能处于激活状态时，应至少有一种退出的操纵方式对坐在驾驶位的车内用户保持可见。
- 5.2.2.1.8 当自动驾驶功能处于激活状态时，ADS 应持续向车内用户提示以下信息：
  - a) ADS 状态信息；
  - b) 因 ADS 失效而导致的 DDT 执行调整情况。
- 5.2.2.1.9 当 3 级自动驾驶功能处于激活状态时，ADS 应符合以下要求：
  - a) 持续评估后援用户是否具备接管能力并符合附录 A；
  - b) 当检测到后援用户不具备接管能力时，执行有效控制策略以使其恢复接管能力；
  - c) 当不能使后援用户安全地恢复接管能力时，执行 ADS 后援响应并使车辆达到 MRC；
  - d) 若发出介入请求，确保预留充分时间，以便后援用户感知到介入请求并安全接管 DDT。

#### 5.2.2.2 自动驾驶功能激活

- 5.2.2.2.1 当 ADS 处于就绪状态时，应持续向车内用户直观地提示。
- 5.2.2.2.2 当车内用户尝试激活自动驾驶功能时，应向车内用户及时提示是否成功激活的信息。
- 5.2.2.2.3 ADS 应按照 5.3.3 的要求确认坐在驾驶位的车内用户完成 ADS 的使用培训，并按照 5.3.5 的要求确认坐在驾驶位的车内用户已阅读并理解使用说明后才允许进入激活状态。
- 5.2.2.2.4 当 3 级自动驾驶功能激活时，ADS 应立即且明确提示后援用户仍需准备响应介入请求。
- 5.2.2.2.5 ADS 在从 4 级自动驾驶功能向 3 级自动驾驶功能切换前，ADS 应获得坐在驾驶位的车内用户同意其担任后援用户的确认。
- 5.2.2.2.6 若允许自动泊车功能向自动驾驶功能（非自动泊车功能）切换，安全切换策略应在安全档案中予以说明，并符合以下要求：
  - a) 若允许自动泊车功能向同级别的自动驾驶功能（非自动泊车功能）切换且无需车内用户确认，切换时 ADS 应提示相关信息；
  - b) 若允许 3 级自动泊车功能向 4 级自动驾驶功能（非自动泊车功能）切换且无需车内用户确认，切换时 ADS 应提示相关信息；
  - c) 若允许 4 级自动泊车功能向 3 级自动驾驶功能（非自动泊车功能）切换，每次切换前 ADS 应符合以下要求：
    - 1) 符合 3 级自动驾驶功能（非自动泊车功能）的激活条件；
    - 2) 获得坐在驾驶位的车内用户同意其担任后援用户的确认；
    - 3) 向车内用户提示切换相关信息。

#### 5.2.2.3 退出至人工驾驶

- 5.2.2.3.1 车内用户发起 ADS 退出请求后，ADS 应执行退出策略，将 DDT 控制权安全地移交给坐在驾驶位的车内用户。
- 5.2.2.3.2 ADS 应响应车内用户发起的 ADS 退出请求。若 ADS 未判定车内用户坐在驾驶位，ADS 不应启动退出策略。若 ADS 暂缓退出，则应向车内用户提示该情况。

注：当因 ADS 退出可能造成不安全时，ADS 可能暂缓退出。

- 5.2.2.3.3 ADS 应在退出完成前评估坐在驾驶位的车内用户是否做好充分准备以恢复执行 DDT。除

坐在驾驶位的车内用户对转向控制和/或制动控制的干预超过防止误用而设计的合理阈值外，至少应符合以下全部条件，才视为车内用户做好充分准备以恢复执行 DDT：

- a) 手握转向盘；
- b) 视线注视驾驶任务相关区域，且持续时长足以支持安全恢复执行 DDT。

5.2.2.3.4 针对 5.2.2.3.3 b) 的要求，当视线监测结果暂不可用时，若采用其他措施替代视线监测，这些措施应在安全档案中予以说明。

5.2.2.3.5 自动驾驶功能应保持激活状态直至退出完成或使车辆达到 MRC。

5.2.2.3.6 当自动驾驶功能退出完成时，ADS 应向车内用户明确提示自动驾驶功能已退出。

5.2.2.3.7 当自动驾驶功能退出完成时，车辆控制权应移交给驾驶人且不应导致：

- a) 应急辅助系统自动关闭；
- b) 部分驾驶辅助系统或组合驾驶辅助系统自动激活。

注：应急辅助系统指GB/T 40429—2021定义的0级驾驶自动化系统；部分驾驶辅助系统指GB/T 40429—2021定义的1级驾驶自动化系统；组合驾驶辅助系统指GB/T 40429—2021定义的2级驾驶自动化系统。

5.2.2.3.8 在 ADS 退出期间，除实体操纵件被车内用户手动调整外，与人工执行 DDT 相关的操纵件、外部环境的前方视野装置、间接视野装置、指示器、警报信号和信号装置应设置为适合人工驾驶的状态。

5.2.2.3.9 若 ADS 控制锁止装置（例如，车门锁止装置），在 ADS 退出完成后不应再影响锁止装置或与其相关的控制装置。

### 5.2.3 不允许行驶中退出至人工驾驶的自动驾驶功能

5.2.3.1 ADS 应向乘客提供与安全相关的信息。

5.2.3.2 当自动驾驶功能处于激活状态时，若出现对乘客有安全风险的情况（例如，安全带未系好、乘客未就座），ADS 应按照安全档案中描述的控制策略作出响应。

5.2.3.3 若装备 ADS 的车辆配备有为人工驾驶提供的操纵件（例如，转向、行车制动、驻车制动、加速和照明等操纵件），其操纵件相关设计应能防止在 ADS 执行 DDT 时对 DDT 产生任何影响，或应采取合理的防护措施防止为人工驾驶提供的操纵件被接触。

## 5.3 用户告知

5.3.1 对于装备 ADS 的车辆，除机动车产品使用说明书外，车辆制造商还应通过公开可获取的方式向用户提供关于 ADS 的使用说明。

注：公开可获取的方式如通过车辆制造商官方网站、车载显示终端、移动智能终端等获取ADS的使用说明。

5.3.2 使用说明书的表述应易于用户阅读、理解和操作，且应至少包括以下内容：

- a) 自动驾驶功能及其能力、驾驶自动化等级和局限性的说明；
- b) 当 ADS 遇到不可避免碰撞的风险场景时，其控制策略的说明；
- c) 自动驾驶功能的激活、退出、接管（适用于 3 级自动驾驶功能）、干预、最小风险策略的说明，包括接管和干预的区别（适用于 3 级自动驾驶功能）、退出方式的推荐使用顺序等；
- d) 用户角色转换机制和过程的说明；

注：用户角色转换如用户激活ADS、用户发起的ADS退出、用户响应介入请求、ADS在从4级自动驾驶功能向3级自动驾驶功能切换时用户角色转变等。

- e) 针对 3 级自动驾驶功能，介入请求发出后，预留给后援用户接管的时间及需要后援用户执行操作的说明；
- f) 自动驾驶功能激活状态下，允许用户开展的非驾驶相关活动及相关风险的说明；
- g) 自动驾驶功能的相关状态及状态转换的说明，以及相关状态提示信号的说明，包括光学、声学 and 触觉等；

注：常见状态如就绪状态、激活状态、执行MRM状态等。

- h) ADS发生故障后，其执行DDT能力变化的说明；
  - i) 若配备人工驾驶的操纵件（例如，转向、行车制动、驻车制动、加速和照明等操纵件），提供关于自动驾驶功能如何响应用户对操纵件输入的说明；
  - j) 若存在可能减弱或抑制用户干预的情况，相关情况及对ADS执行DDT影响的说明；
  - k) 针对4级自动驾驶功能，提供乘客请求停车方法的说明；
  - l) 用户在使用ADS前，需采取的任何额外安全预防措施（例如，查验ADS传感器是否被遮挡）的说明；
  - m) 当使用ADS发生交通事故时，用户应急处置建议的说明；
  - n) 为保障ADS安全运行所需的维护操作的相关说明（例如，定期检修等）；
  - o) 对于支持多用户管理的车辆，相关风险和和建议的说明（例如，车辆移交前提示登出当前账号）；
  - p) 对于可在挂接挂车的情况下激活ADS的车辆，对ADS所适配的挂车要求的说明（例如，外廓尺寸、最大允许总质量和制动性能等）以及使用ADS的相关风险说明（例如，需要用户确保挂车符合车辆制造商说明的要求）。
- 5.3.3 除不允许行驶中退出至人工驾驶的自动驾驶功能外，车辆每次重新启动动力系统（发动机自动启停除外），应至少通过以下一种方式确认坐在驾驶位的车内用户是否完成ADS使用培训：
- a) 对坐在驾驶位的车内用户进行ADS的使用培训并确认完成；
  - b) 生物识别；
  - c) 在车辆处于静止状态下账号登录。

5.3.4 当采用5.3.3 c)的方式时，ADS应通过驾驶人输入数字或其他形式密码的方式确认其是否完成ADS的使用培训。

注：其他形式密码如输入字母、手势密码等。

- 5.3.5 除不允许行驶中退出至人工驾驶的自动驾驶功能外，车辆应向坐在驾驶位的车内用户提供已阅读并理解使用说明的确认方式，且应符合以下要求：
- a) 仅在车辆处于静止状态时允许进行确认；
  - b) 所提供的确认方式包括长按保持或至少两个有目的操作（例如，双击等）；
  - c) 若因软件升级导致使用说明发生变化，则在下一次激活前向坐在驾驶位的车内用户提供确认方式；
  - d) 当检测到最迟30天坐在驾驶位的车内用户未进行确认，则在下一次激活前向坐在驾驶位的车内用户提供确认方式。

## 5.4 其他要求

5.4.1 装备ADS的车辆应装备符合GB 44497要求的DSSAD。

5.4.2 ADS应接收和管理来自其他的车辆系统的信号。上述信号的清单及其管理方式，应在安全档案中描述。

5.4.3 当4级自动驾驶功能处于激活状态时，ADS应按照安全档案中描述的方式执行原本应由驾驶人完成的非DDT相关操作。若ADS不执行此类必要操作，安全档案中应说明这些操作是如何执行的。

5.4.4 对于可在挂接挂车的情况下激活ADS的车辆，车辆制造商应证明与挂车相关的实施策略符合本文件的安全要求。

5.4.5 对于3级自动驾驶功能，若其ODC包括高速公路和/或城市快速路，除符合本章要求，还应符合附录B的要求。

5.4.6 对于4级自动驾驶功能，除符合本章要求，还应符合附录C的要求。

## 6 保障要求

### 6.1 安全保障要求

#### 6.1.1 一般要求

车辆制造商应建立、实施SMS，并记录SMS相关的过程和活动。

#### 6.1.2 安全方针

6.1.2.1 安全方针应概述车辆制造商为实现预期的安全成果所设立的目标。

6.1.2.2 车辆制造商应提供证据，证明其安全方针落实了以下方面：

- a) 安全方针与原则；
- b) 组织的安全目标，以及制定安全档案中所用安全性能指标的过程；
- c) 考虑法律法规（例如，道路通行规定）、标准、最佳实践指南以及 ADS 应用场景，建立适用于 SMS 的架构，并将其组织架构、过程及工作成果对应到 SMS 中；
- d) 安全文化；
- e) 安全管理，包括管理承诺、清晰的责任划分及岗位职责；
- f) 质量管理体系。

#### 6.1.3 风险管理

6.1.3.1 SMS 应包括一套整体风险管理过程，用于识别、评估并缓解组织、人员和技术层面的风险，并体现风险缓解措施、相关风险之间的关联。

6.1.3.2 车辆制造商应记录其风险管理过程和活动，包括以下内容：

- a) 风险识别；
- b) 风险分析；
- c) 风险评估；
- d) 风险处置；
- e) 确保持续更新风险评估的过程；
- f) 对组织的安全绩效及风险控制有效性的评审过程。

#### 6.1.4 安全保证

6.1.4.1 车辆制造商应证明定期进行独立的内审和外部检验，以确保 SMS 的过程持续执行。

6.1.4.2 车辆制造商应与参与 ADS 开发、制造或部署后阶段的任何组织（例如，签约供应商、服务提供商或车辆制造商子组织）建立适当的工作机制（例如，合同管理、质量管理体系和开发接口协议）。车辆制造商应记录其过程和活动，包括以下方面：

- a) 供应链管理方针；
- b) 供应链风险的管控机制；
- c) 对供应商 SMS 的评估及相应审核过程；
- d) 建立协议（例如，合同）的过程，以确保开发、生产和部署后阶段的安全；
- e) 分布式安全活动的过程；
- f) 具备向相关方提供安全相关信息的过程，以证明履行其法律义务。

6.1.4.3 SMS 文档应根据 SMS 的任何相关变更定期更新。在审核和变更 SMS 时，应使用差距分析；在制定更合适的新 SMS 之前，应查验当前的安全文化，以确保问题得到充分解决。

6.1.4.4 车辆制造商应建立过程，以实现以下目标：



- a) 确保 SMS 记录的所有实践和活动得以执行；
- b) 确保对相关要求的符合性进行独立查验，至少查验方不是待查数据提供方；
- c) 确保对 SMS 进行持续评估，使其保持有效。

#### 6.1.4.5 车辆制造商应定义适当的 KPI，以衡量 SMS 在 ADS 全生命周期中的有效性。

注：全生命周期一般包括开发、生产和部署后阶段。

### 6.1.5 安全提升

#### 6.1.5.1 SMS 应包括持续改进的过程。SMS 文档的更改应按要求上报。

#### 6.1.5.2 车辆制造商应建立并维护以下机制：

- a) 内部关于安全事项的有效沟通机制；
- b) 与外部的信息共享机制；
- c) 关于 SMS 的培训计划。

### 6.1.6 设计与开发管理

#### 6.1.6.1 SMS 应包括在设计阶段落实安全方针的证明，包括以下方面：

- a) 设计与开发阶段相关人员的角色和职责；
- b) 负责做出影响安全决策人员的资质和经验；
- c) 在设计和生产活动之间的角色、责任和信息传递的协调。

#### 6.1.6.2 车辆制造商应执行相应过程和活动，以确保设计与开发阶段的鲁棒性，包括以下方面：

- a) 组织如何开展所有设计与开发活动的总体描述；
- b) 装备 ADS 的车辆中与 ADS 相关的设计、开发、集成和实现，以及安全档案相关过程和活动，包括但不限于以下内容：
  - 1) 需求管理（例如，需求获取与确认）；
  - 2) 实车试验条件；
  - 3) 仿真试验条件；
  - 4) 工具管理；
  - 5) 系统集成；
  - 6) 软件开发保障；
  - 7) 硬件开发保障；
  - 8) 功能安全与 SOTIF 管理，包括对风险评估及风险间交互的持续评估与更新，包括相关分析方法（例如，FMEA、FTA、STPA 或任何适用于功能安全和 SOTIF 的其他方法）；
  - 9) 人为因素管理，包括以人为本的设计安全相关交互设计过程。
- c) 变更管理过程，包括但不限于以下内容：
  - 1) 主要设计决策；
  - 2) ADS 设计修改；
  - 3) 负责做出影响安全决策的关键人员变动；
  - 4) 用于 ADS 安全验证所采用的工具和关键参数。

#### 6.1.6.3 车辆制造商应在实现功能安全、SOTIF、网络安全以及车辆其他安全的相关方（例如，外部供应商、车辆制造商内部专业部门）之间建立有效的沟通机制。

#### 6.1.6.4 SMS 应包括用于制定安全档案中安全性能指标（例如，SOTIF 中的接受准则和功能安全中的 FIT 值、PMHF 值）的过程。

### 6.1.7 生产管理

6.1.7.1 车辆制造商应在 SMS 中建立并记录生产过程和活动。该记录至少应涵盖以下方面：

- a) 质量管理体系；
- b) 对车辆制造商执行所有生产职能的描述，包括工作条件、过程运行环境、设备和管理。

6.1.7.2 车辆制造商应在 SMS 中建立并记录其分布式生产过程及活动。这些过程和活动应包括：

- a) 车辆制造商与供应链中涉及的所有其他组织（例如，供应商、合作伙伴或分包商）之间的合作机制；
- b) 供应链涉及的其他组织所生产子系统或组件的验收准则，或将生产保障要求部署到供应链中。

#### 6.1.8 部署后安全管理

车辆制造商应具备安全监测与管理的能力。

### 6.2 试验条件

#### 6.2.1 仿真试验

##### 6.2.1.1 一般要求

车辆制造商应证明各仿真工具链符合6.2.1.2~6.2.1.9的要求，以证实适用于仿真试验。

##### 6.2.1.2 数据管理

###### 6.2.1.2.1 一般要求

6.2.1.2.1.1 在 ADS 的全生命周期内，车辆制造商应管理用于验证、确认和更新仿真工具链的相关数据。车辆制造商应考虑该数据的完整性、准确性和一致性。

6.2.1.2.1.2 车辆制造商应记录用于确认仿真工具链的数据。

6.2.1.2.1.3 当不受车辆制造商控制的其他组织的数据或工具集成至仿真工具链时，车辆制造商应说明为确保相应数据或工具的质量和完整性所采取的措施。

6.2.1.2.1.4 车辆制造商应量化仿真工具链及其输出中因数据质量（例如，数据覆盖率、信噪比和传感器的不确定性/偏差/采样率）而产生的不确定性。

###### 6.2.1.2.2 输入数据及仿真工具链参数的管理

车辆制造商应记录用于验证和确认仿真工具链的输入数据，记录文档至少应说明：

- a) 输入数据的重要质量特性；
- b) 输入数据覆盖了仿真试验拟评估的自动驾驶功能；
- c) 用于拟合仿真工具链相关参数的校准程序；
- d) 仿真工具链新版本发布时，数据或参数变化的原因。

###### 6.2.1.2.3 输出数据的管理

6.2.1.2.3.1 车辆制造商应记录用于确认仿真工具链的输出数据。每条输出记录应能追溯到生成该输出的输入数据。

6.2.1.2.3.2 车辆制造商应对输出数据进行统计分析，并记录通过该分析得出的所有重要质量特性。

6.2.1.2.3.3 车辆制造商应证明输出数据的质量足以支持以下工作：

- a) 确认仿真工具链及其组件；
- b) 支持对仿真工具链及其组件进行一致性或合理性查验；
- c) 生成支撑安全档案的证据。

6.2.1.2.3.4 若仿真工具链中存在随机模型，关于随机模型的管理，车辆制造商应符合以下要求：

- a) 描述仿真工具链输出的方差；
- b) 确保仿真工具链能够进行确定性地重复执行。当确定性不能被保证时，车辆制造商提供证据证明其对于可信度的影响是可以被接受的。

注1：随机模型是指涉及或包括与偶然性或概率相关的一个或多个随机变量的模型。

注2：确定性地重复执行是指在相同输入、相同配置、相同版本的条件下，多次运行仿真，最终输出结果能够稳定落在预先定义的要求或指标范围内。

### 6.2.1.3 人员能力

6.2.1.3.1 车辆制造商应记录并提供以下人员能力胜任的理由：

- a) 开发仿真工具链及其组件的人员；
- b) 评估仿真工具链及其组件的人员；

注：评估包括管理、分析、验证、确认。

- c) 使用仿真工具链对 ADS 进行确认试验的人员。

6.2.1.3.2 车辆制造商应建立并实施相关过程和程序，以识别并保持开发、评估和使用仿真工具链所需的技能、知识和经验，至少应建立、维护并记录以下过程：

- a) 识别和评估建模与仿真活动所需的必要人员能力；
- b) 培训人员以使其有能力执行建模与仿真活动。

6.2.1.3.3 车辆制造商应存储参与仿真工具链开发、评估和使用的人员记录，证明他们已接受必要的培训，且被认为具备完成需要的建模与仿真活动的的能力。

6.2.1.3.4 车辆制造商应与仿真工具链相关的支持方建立适当工作机制，以确保这些支持方人员具备完成所分配任务的相应能力。

6.2.1.3.5 车辆制造商与支持方建立的工作机制应符合 6.1.4.2 和 6.1.6.3 的要求。

### 6.2.1.4 发布管理

6.2.1.4.1 在仿真工具链的整个生命周期内，车辆制造商应管理和维护用于仿真试验的仿真工具链。对于仿真工具链的管理和维护应直至 ADS 部署后阶段结束。

6.2.1.4.2 车辆制造商应管理和记录仿真工具链的发布管理过程，至少应记录以下内容：

- a) 每次仿真工具链发布相关修改的描述；
- b) 所有相关软件（例如，特定软件产品、名称和版本）和硬件配置的信息；
- c) 仿真工具链验收和发布的内部评审活动。

### 6.2.1.5 仿真工具链假设、已知限制和不确定性量化

6.2.1.5.1 车辆制造商应描述指导仿真工具链设计的建模假设和考虑因素。

6.2.1.5.2 车辆制造商应提供以下信息：

- a) 开发每个仿真工具链及其组件期间所做的假设，以及这些假设对其范围和适用性的限制；
- b) 每个仿真工具链及其组件保真度水平的选择依据。

注：保真度是指模型与建模对象的相似程度。

6.2.1.5.3 车辆制造商应证明与仿真工具链相关的公差是适当的，并符合验收试验和验收准则。

6.2.1.5.4 车辆制造商应详细说明每个仿真工具链及其组件中的不确定性来源，并评估其对试验结果的影响。

### 6.2.1.6 仿真工具链适用范围

- 6.2.1.6.1 车辆制造商应记录每个仿真工具链的适用范围，并确定其局限性。
- 6.2.1.6.2 车辆制造商应证明仿真工具链能在其定义的适用范围内使用。
- 6.2.1.6.3 仿真工具链适用范围应参考 ODC，并确定其适用于 ODC 的任何限制条件。
- 6.2.1.6.4 车辆制造商应证明每个仿真工具链如何仿真相关的物理现象，并符合必要的准确度水平。
- 6.2.1.6.5 车辆制造商应提供用于确认仿真工具链的试验项目清单、相应参数和已知限制。

#### 6.2.1.7 仿真工具链关键性分析

车辆制造商应评估仿真工具链的关键性以及其对安全档案中声明的影响。

#### 6.2.1.8 仿真工具链验证

##### 6.2.1.8.1 一般要求

车辆制造商应证明仿真工具链不会对未经明确试验的有效输入表现出不现实的行为。

注：有效输入指符合仿真工具链预设的规则和范围，以触发其正常响应的输入数据。

##### 6.2.1.8.2 仿真工具链代码验证

- 6.2.1.8.2.1 车辆制造商应记录评估每个仿真工具链及其组件时所用代码验证技术（例如，静态/动态代码验证、收敛性分析）的执行情况。
- 6.2.1.8.2.2 车辆制造商应证明已充分探索输入参数空间，以确定是否存在会导致仿真工具链表现出不稳定或不现实行为的参数组合。
- 6.2.1.8.2.3 车辆制造商应执行仿真工具链代码的合理性和一致性查验程序，并提交相关结果信息，以证明仿真工具链的鲁棒性。

##### 6.2.1.8.3 仿真工具链计算验证

- 6.2.1.8.3.1 车辆制造商应记录数值误差（例如，离散误差、舍入误差、迭代程序收敛误差）的估计。
- 6.2.1.8.3.2 车辆制造商应审查分析结果，并证明对数值误差已进行充分理解和限制，以确保仿真工具链能用于仿真试验。

##### 6.2.1.8.4 仿真工具链敏感性分析

- 6.2.1.8.4.1 车辆制造商应证明已通过适当的敏感性分析技术确定对仿真工具链输出影响最关键的输入数据和参数，以表征整个仿真工具链输出的不确定性。
- 6.2.1.8.4.2 车辆制造商应证明已采用鲁棒校准程序为所有仿真参数（特别是最关键参数）分配适当的数值。

#### 6.2.1.9 仿真工具链确认

- 6.2.1.9.1 车辆制造商应根据定量指标进行确认分析，以确定每个仿真工具链与其所表征的真实系统的准确程度。
- 6.2.1.9.2 车辆制造商应提供仿真工具链输出结果与实车试验结果具有一致性和相关性的证据。
- 6.2.1.9.3 车辆制造商应基于一组具备充分代表性的试验进行仿真工具链确认，以证实仿真工具链能在其适用范围内使用。
- 6.2.1.9.4 车辆制造商应定义用于比较实车试验结果和仿真工具链输出结果的性能观测量。
- 6.2.1.9.5 车辆制造商应使用适当的统计方法比较实车试验结果和仿真工具链的相应输出。
- 6.2.1.9.6 车辆制造商应在每个仿真工具链及其组件的开发过程中规定验收试验和验收准则，并证明

已符合相应验收准则。

6.2.1.9.7 车辆制造商应根据仿真试验用途定义用于每个仿真工具链确认的方法和试验，至少包括以下一个或多个：

- a) 子系统确认（例如，环境模型、传感器模型或车辆动力学模型）；
- b) 车辆系统确认（车辆系统指车辆动力学模型与环境模型的结合）；
- c) 传感器系统确认（传感器系统指传感器模型与环境模型的结合）；
- d) 集成系统确认（集成系统指传感器模型与受车辆动力学模型影响的环境模型的结合，或传感器模型、车辆动力学模型与环境模型的结合）。

6.2.1.9.8 车辆制造商应明确仿真工具链的适用范围与 ODC 的匹配程度。

6.2.1.9.9 车辆制造商应证明已符合仿真工具链开发过程中定义的准确度准则。

6.2.1.9.10 车辆制造商应证明已落实与确认活动相关的过程。

6.2.1.9.11 车辆制造商应记录不确定性特征分析结果和仿真工具链使用方法，以及在用于仿真试验时采用的安全裕度。

注：安全裕度指利用仿真工具链进行仿真试验时，为了补偿其不确定性等误差而有意施加的额外余量。

6.2.1.9.12 车辆制造商应证明：

- a) 具备估计各仿真工具链关键输入的方法；
- b) 估计方法已应用；
- c) 估计结果已记录。

6.2.1.9.13 车辆制造商应识别每个仿真工具链及其组件中的关键参数。在适当情况下，关键参数应给出限定范围或给出参数分布的相关特征量或者统计量。

6.2.1.9.14 车辆制造商应证明基于仿真工具链的假设已对每个仿真工具链及其组件的不确定性完成了适当的表征。

6.2.1.9.15 车辆制造商应证明已区分仿真工具链相关的偶然不确定性和认知不确定性。

注1：偶然不确定性指数据信息中的固有噪声。

注2：认知不确定性指由于对建模过程的知识缺乏所导致的不确定性。

## 6.2.2 场地试验

车辆制造商应证明场地试验的设施、环境和能力与场地试验的预期用途及其在整体试验方案中的作用相匹配，并能收集支撑安全档案的证据。此外，车辆制造商还应证明：

- a) 所开展的场地试验包括可体现ODC和预期运行工况的静态和动态元素；
- b) 场地试验期间使用的设备已定期进行查验、维护和校准，以确保测量结果具备足够的准确度和精度。

## 6.2.3 道路试验

车辆制造商应证明道路试验的道路、设施、环境和能力与道路试验的预期用途及其在整体试验方案中的作用相匹配，并能收集支撑安全档案的证据。此外，车辆制造商还应证明：

- a) 所选试验路线能使 ADS 有足够概率遇到以下场景：
  - 1) 大量 ORU；
  - 2) 少见的道路基础设施、非典型道路条件、非典型环境条件。
- b) 道路试验期间使用的设备已定期进行查验、维护和校准，以确保测量结果具备足够的准确度和精度。

## 7 保障要求检验

### 7.1 安全保障要求检验

#### 7.1.1 一般要求

7.1.1.1 检验人员应检验车辆制造商的 SMS 符合 6.1 的要求。

7.1.1.2 检验人员应对车辆制造商的 SMS 进行检验，检验车辆制造商在管理安全风险及确保 ADS 全生命周期（开发、生产、部署后阶段）安全相关的过程具备鲁棒性。

7.1.1.3 检验人员应评估车辆制造商监测 SMS 活动过程的鲁棒性，并应评估车辆制造商采取适当的纠正或预防措施解决所有安全问题的能力。

#### 7.1.2 安全方针检验

检验人员应检验车辆制造商的安全方针符合6.1.2的要求，并涵盖以下方面：

- a) SMS 建立、运行和维护所依据的原则和目标；
- b) 适合组织需求的组织架构、安全管理要素；
- c) 安全承诺的声明；
- d) 引导组织内相关人员融入安全文化的措施和方法。

#### 7.1.3 风险管理检验

检验人员应检验车辆制造商的风险管理过程符合6.1.3的要求，并涵盖以下方面：

- a) 已具备应对和预防风险的措施；
- b) 风险包括但不限于：
  - 1) ADS 本身的风险；
  - 2) 在 ADS 全生命周期中所识别的风险，包括参与方的风险；
  - 3) 影响 SMS 有效性的组织或人员产生的风险；
  - 4) 影响 ADS 安全性的组织或人员产生的风险。
- c) 风险管理过程和活动覆盖 ADS 整个生命周期并被实施。

#### 7.1.4 安全保证检验

检验人员应检验车辆制造商的安全保证过程符合6.1.4的要求，并涵盖以下方面：

- a) 定期进行独立的内审和外部检验；
- b) 供应链以及可能影响 ADS 安全的相关组织的管理过程；
- c) 已具备的变更管理过程；
- d) 已具备纠正措施过程，以维持可接受的安全水平；
- e) 适用于 ADS 和 SMS 的纠正措施；
- f) 已具备衡量 KPI 的监测实践；
- g) 适用于 ADS 和 SMS 的监测实践；
- h) 已设立履行合规评估和审核工作的独立职能。

#### 7.1.5 安全提升检验

检验人员应检验车辆制造商的安全提升过程符合6.1.5的要求，并涵盖以下方面：

- a) 能履行职责人员的能力水平；
- b) 提高人员能力的培训过程；

- c) 内外部的安全沟通途径;
- d) 持续改进的过程。

#### 7.1.6 设计与开发管理检验

检验人员应检验车辆制造商的设计与开发过程符合6.1.6的要求，并涵盖以下方面：

- a) 设计与开发阶段的管理过程；
- b) 安全方针、风险管理、安全保证和安全提升在设计与开发过程中应用的证明文档。

#### 7.1.7 生产管理检验

检验人员应检验车辆制造商的生产管理过程符合6.1.7的要求，并涵盖以下方面：

- a) 生产阶段的管理过程；
- b) 安全方针、风险管理、安全保证和安全提升在生产管理过程中应用的证明文档。

#### 7.1.8 部署后安全管理检验

检验人员应检验车辆制造商安全监测与管理的能力符合6.1.8的要求。

### 7.2 试验条件检验

#### 7.2.1 仿真试验条件检验

7.2.1.1 检验人员应检验车辆制造商的仿真试验条件符合 6.2.1 的要求并适合开展仿真试验。

注：检验人员可能要求车辆制造商展示仿真工具链的执行及结果的生成。

7.2.1.2 检验人员应确认检验的结果及额外试验（如有）的结果与车辆制造商提供的信息的一致性。

注：检验人员可能要求开展额外的试验。

#### 7.2.2 场地试验条件检验

检验人员应检验车辆制造商的场地试验条件符合6.2.2的要求并适合开展场地试验。

注：检验人员可能要求车辆制造商开展部分场地试验。

#### 7.2.3 道路试验条件检验

检验人员应检验车辆制造商的道路试验条件符合6.2.3的要求并适合开展道路试验。

注：检验人员可能要求车辆制造商开展部分道路试验。

## 8 安全档案检验

### 8.1 一般要求

检验人员应检验由车辆制造商根据附录D提供的安全档案。

### 8.2 内容检验

8.2.1 检验人员应检验车辆制造商的安全档案的完整性，安全档案的完整性应至少符合以下要求：

- a) 系统描述符合 D.1 的要求；
- b) 安全概念一致且完整符合 D.2 的要求；
- c) 声明、论据和证据至少符合以下要求：

- 1) 依据 D.3.1.2, 所涉及的每项要求均通过一个或多个声明得到阐释;
- 2) 依据 D.2.1.1、D.2.6.1.1、D.3.1.3, 声明的集合能够证明 ADS 不存在不合理风险;
- 3) 依据 D.3.1.1 a), 每个声明均有一个或多个论据支持;
- 4) 依据 D.3.1.1 b), 每个论据均有一个或多个证据支持;
- 5) 依据 D.2.6.1.1, 车辆制造商已记录与声明相关的指标及验收准则;
- 6) 依据 D.3.1.1 c), 对声明、论据和证据进行唯一地标识;
- 7) 依据 D.3.1.6, 从要求到证据的前后追溯性;
- 8) D.3.1.4 和 D.3.1.7~D.3.1.9。

注: 检验人员可能要求提供支持性文件或协助复现证据。

#### 8.2.2 检验人员应检验车辆制造商的安全档案的鲁棒性, 安全档案的鲁棒性应至少符合以下要求:

- a) 安全概念中所有已识别的风险全部被降低、缓解或接受, 并且总体残余风险(定性或定量)低于不合理风险阈值;
- b) ADS 及其功能开发、验证和确认的完整性等级足以将风险降至不合理风险阈值以下;
- c) 车辆制造商已采取措施限制由 ADS 或与其交互的其他的车辆系统导致的潜在非预期功能;
- d) 依据 D.3.2.1, 获取证据的试验条件均达到可接受的可信度水平, 且在参数变化时表现稳定;
- e) 依据 D.3.2.5.1, 试验证据来源于经过充分描述的仿真试验、场地试验和道路试验的组合, 并表明试验方法间结果的一致性;
- f) 依据 8.3, 提供的证据可复现, 且安全目标保持一致;
- g) 证据合理覆盖预期运行区域内可预见的运行条件和事件, 符合 D.2.5.2.7 和 D.2.5.2.8 的要求, 包括在 ODD 内及可能超出 ODD 的情况;
- h) 依据 D.4, 车辆制造商已开展一项或多项内审, 并针对发现的问题采取整改措施。

注: 检验人员可能要求提供支持性文件或协助复现证据。

### 8.3 试验活动检验

#### 8.3.1 一般要求

8.3.1.1 检验人员应检验车辆制造商采用的试验方法适用于证明安全档案以及性能或功能要求符合性。

8.3.1.2 检验人员应检验试验(仿真试验、场地试验、道路试验等)结果的综合覆盖范围足以支撑安全档案的声明。

#### 8.3.2 场景及其管理检验

8.3.2.1 检验人员应检验车辆制造商采用并记录适当的过程, 以得出与 ADS 的 ODC 及安全档案相关的 ADS 行为能力。

8.3.2.2 检验人员应检验车辆制造商识别和生成场景的方法及过程适当并符合 D.3.2.2.2 的要求。

8.3.2.3 检验人员应检验车辆制造商识别和生成的场景符合 D.3.2.2.3 的要求。

8.3.2.4 检验人员应检验车辆制造商在选择具体场景时符合 D.3.2.2.4 的要求。

#### 8.3.3 试验过程检验

检验人员应检验车辆制造商的试验过程符合 D.3.2.3.1 和 D.3.2.3.2 的要求。

#### 8.3.4 试验证据检验

##### 8.3.4.1 一般要求

8.3.4.1.1 检验人员应检验车辆制造商在证明安全档案时使用不同试验方法提供的证据, 试验方法包括:

- a) 仿真试验;



b) 场地试验;

c) 道路试验。

8.3.4.1.2 检验人员应检验车辆制造商提供的用于证明 ADS 执行 DDT 能力的证据。

8.3.4.1.3 检验人员应检验车辆制造商提供的用于证明 ADS 与用户安全交互能力的证据。

8.3.4.1.4 检验人员应检验与 ADS 交互相关的特定试验用例符合 D.3.2.5.5 的要求。

8.3.4.1.5 检验人员应检验所开展的试验项目适用于作为支持安全档案的证据,包括覆盖范围、一致性和相关性等方面。

8.3.4.1.6 检验人员应检验试验结果能证明 ADS 在执行 DDT 时的行为能力符合 D.3.2.4.2 的要求。

#### 8.3.4.2 仿真试验证据的检验

8.3.4.2.1 检验人员应检验车辆制造商开展的仿真试验,仿真试验应依据 6.2.1 的要求在仿真工具链中充分考虑了假设、准确性和不确定性等因素。检验人员应检验仿真试验结果体现上述考量因素。

8.3.4.2.2 检验人员应检验任何使用包括随机元素的仿真工具链开展的仿真试验均已考虑试验结果中可能存在的不确定性。

8.3.4.2.3 检验人员应检验仿真试验已包括风险场景及低概率事件,符合 D.3.2.5.2 的要求。

#### 8.3.4.3 场地试验证据的检验

8.3.4.3.1 检验人员应检验车辆制造商为支持安全档案所提供的场地试验证据。

8.3.4.3.2 检验人员应检验场地试验的场景符合 D.3.2.5.3 的要求。

#### 8.3.4.4 道路试验证据的检验

检验人员应检验车辆制造商为支持安全档案所提供的道路试验证据符合 D.3.2.5.4 的要求。

### 9 确认性试验

检验人员应根据安全档案使用多种试验方法确认自动驾驶功能的表现,场地试验应按照 GB/T 41798 开展,道路试验应按照 GB/T 44719 开展。若采用仿真试验,检验人员应按照 GB/T 47025 开展仿真试验。

### 10 同一型式判定

#### 10.1 直接视同条件

如符合以下全部规定,则视为同一型式:

- a) 整车生产企业相同;
- b) 自动驾驶系统安全要求检验检测报告中保障要求相关内容有效且其签发日期未超过三年;
- c) 除车辆型号信息外,安全档案中声明相同;
- d) ADS 相关的感知系统及相关部件的类型、生产企业、名称、型号、数量以及安装位置相同;
- e) ADS 相关的定位系统及相关部件的类型、生产企业、名称、型号、数量相同;
- f) 构成 ADS 的 ECU 硬件的生产企业、名称、型号、数量相同;
- g) ADS 的软件(感知、规划和决策等)生产企业、软件型号、软件版本相同,但在不影响 ADS 表现的前提下允许软件版本不同;
- h) ADS 软件架构特征(包括感知、规划、决策、地图等模型框架或端到端模型框架,并提供图示及说明)相同;

- i) ADS 感知定位系统及相关部件、ECU 之间的逻辑连接关系相同；
- j) 自动驾驶功能的人机交互方式（激活、干预、退出）相同；
- k) 自动驾驶功能的不同状态（例如，就绪状态、激活状态等）及状态转换（例如，激活、退出等）的用户提示信息及策略相同；
- l) ADS 或自动驾驶功能的 ODC 相同；
- m) 自动驾驶功能相同；
- n) 对于 3 级自动驾驶功能，接管事件与介入请求控制策略相同；  
注：接管事件包含计划接管事件和非计划接管事件。
- o) MRM 的策略和 MRC 相同；
- p) 对于 3 级自动驾驶功能，后援用户接管能力监测组件的类型、生产企业、名称、型号、数量相同；
- q) 对于 3 级自动驾驶功能，后援用户接管能力监测的指标及阈值设置相同；
- r) 对于 3 级自动驾驶功能，后援用户接管能力不足提示信息方式（光学、声学、触觉等）及策略相同。

## 10.2 检验检测验证后视同条件

若 ADS 涉及 10.1 条件变更，若符合以下全部规定，仅需对变更参数相关的技术要求进行补充检验检测，经审批许可后获得扩展：

- a) 整车生产企业相同；
- b) 自动驾驶系统安全要求检验检测报告中保障要求相关内容有效且其签发日期未超过三年；
- c) 除车辆型号信息外，安全档案中声明相同；
- d) ADS 相关的感知系统及相关部件的类型、数量以及安装位置相同；
- e) ADS 相关的定位系统及相关部件的类型、数量相同；
- f) 构成 ADS 的 ECU 硬件生产企业、名称、型号、数量相同；
- g) ADS 的软件（感知、规划和决策等）生产企业、软件型号、软件版本相同，但在不影响 ADS 表现的前提下允许软件版本不同；
- h) ADS 软件架构特征（包括感知、规划、决策、地图等模型框架或端到端模型框架，并提供图示及说明）相同；
- i) ADS 感知定位系统及相关部件、ECU 之间的逻辑连接关系相同；
- j) 自动驾驶功能相同；
- k) 对于 3 级自动驾驶功能，介入请求控制策略相同；
- l) 除以下条件外，ADS 或自动驾驶功能的 ODC 其他要素相同：
  - 1) ADS 或自动驾驶功能的 ODC 中的道路类型相同或减少；
  - 2) ADS 或自动驾驶功能的 ODC 中时间相同或减少；
  - 3) ADS 或自动驾驶功能的 ODC 中的最高车速相同或降低；
  - 4) ADS 或自动驾驶功能的 ODC 中的天气条件相同或程度降低；
  - 5) ADS 或自动驾驶功能的 ODC 中的车道类型相同或减少。

## 11 标准的实施

对于新申请型式批准的车型，自本文件实施之日起开始执行。

对于已获得型式批准的车型，自本文件实施之日起第 13 个月开始执行。

附 录 A  
(规范性)  
接管能力监测技术要求

A.1 安全带监测要求

A.1.1 ADS应持续监测后援用户是否系好安全带。

A.1.2 当自动驾驶功能处于激活状态时，若后援用户未系安全带，ADS应发出介入请求。

A.2 在位监测要求

A.2.1 ADS应持续监测后援用户是否坐在驾驶位。

A.2.2 当自动驾驶功能处于激活状态时，若后援用户未坐在驾驶位超过1 s时，ADS应发出介入请求。

注：后援用户未坐在驾驶位，指后援用户所处位置无法支持后援用户执行DDT。

A.3 执行 DDT 能力监测要求

A.3.1 ADS应至少通过2种有效的指标独立确认后援用户在上一个时间周期（不大于30 s）内具备执行DDT的能力，否则视为不具备执行DDT能力。

注1：指标如特定的人机交互动作、眼部运动、头部运动、身体运动、语音输出和生理特征等。

注2：在任何时候都可能认为后援用户不具备执行DDT能力。

A.3.2 当自动驾驶功能处于激活状态时，若可监测的指标不足2种或后援用户被判定为不具备执行DDT的能力，ADS应符合以下要求：

- a) 立即发出明确的执行 DDT 能力不足提示信号；
- b) 执行 DDT 能力不足提示信号明显区别于 ADS 激活状态下车辆其他提示信号；
- c) 在 ADS 发出执行 DDT 能力不足提示信号期间，若监测到后援用户恢复执行 DDT 能力，关闭执行 DDT 能力不足提示信号；
- d) 在 ADS 发出执行 DDT 能力不足提示信号期间，若未监测到后援用户恢复执行 DDT 能力，发出介入请求，且发出介入请求不晚于执行 DDT 能力不足提示信号发出 15 s。

## 附录 B

### (规范性)

#### 应用于高速公路和/或城市快速路的 3 级自动驾驶功能具体技术要求

##### B.1 DDT 执行

###### B.1.1 一般要求

B.1.1.1 ADS 在激活状态下应使车辆保持在车道内行驶并确保不会无目的跨越任何车道边线（前轮外边缘越过车道边线外边缘）。ADS 目标应使车辆在车道内保持稳定的横向和纵向运动以避免对 ORU 造成干扰。

B.1.1.2 ADS 在无需采取紧急避撞控制来响应交通扰动的前提下，当交通扰动解除后，ADS 应恢复初始的安全行车状态。

注：交通扰动指由 ORU 的行为所引起的、对 ADS 的正常行驶状态造成干扰，并可能迫使 ADS 采取规避动作的交通情况。

B.1.1.3 若 ADS 除车道巡航外，还具有跨越车道线的能力，则 ADS 应具备足够的前向、侧向和后向探测能力以评估跨越到其他车道内的风险性。

B.1.1.4 若 ADS 具备为绕行前方障碍物而部分驶入相邻车道的能力，应符合以下要求：

- a) ADS 仅在无法触发常规换道控制（例如，受当前交通流情况限制、相邻车道不可用）且不会对车内用户和 ORU 造成不合理的安全风险的情况下，才允许通过部分驶入相邻车道的方式来应对前方障碍物；
- b) 该应对方式不危及车内用户和 ORU，并符合以下要求：
  - 1) 确保与道路边界、ORU 有足够的横向和纵向距离；
  - 2) 除由于弯道曲率产生的横向加速度外，由该应对方式所产生的额外横向加速度目标不大于  $1 \text{ m/s}^2$ ；
  - 3) 若 ADS 控制车辆跨越车道边线（前轮外边缘越过车道边线外边缘）大于  $1 \text{ m}$ ，则符合 B.1.2.3 对后向安全距离评估的要求。

B.1.1.5 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、道路设施和天气环境。

B.1.1.6 ADS 在激活状态下，应具备控制车辆在前方静止的 ORU 或阻碍通行的车道前完全静止以避免碰撞的能力。

B.1.1.7 ADS 在激活状态下应探测碰撞风险，包括但不限于前方车辆减速、车辆切入和突然出现的障碍物，并应执行合理的控制策略以降低对车内用户和 ORU 的安全风险。

B.1.1.8 对于前方车辆切入、无遮挡的行人横穿等情况，ADS 的 DDT 执行能力应至少达到正在承担驾驶任务的合格且专注驾驶人将风险最小化的水平。

B.1.1.9 当车辆所在车道内存在前方逆向行驶的其他车辆时，ADS 应以减轻潜在碰撞后果为目的采取合理的控制策略进行响应。

###### B.1.2 换道控制要求

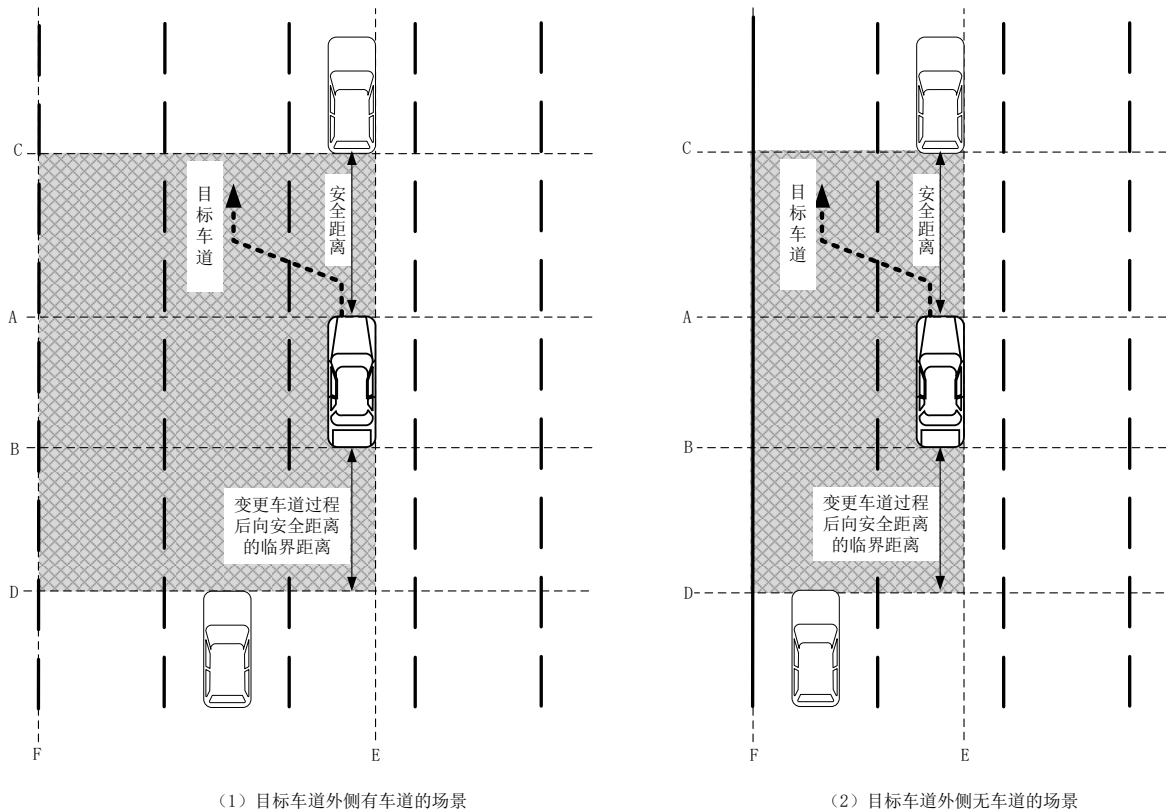
###### B.1.2.1 一般要求

- B.1.2.1.1 ADS执行的换道控制不应给车内用户和ORU造成不合理的安全风险,且应符合以下要求:
- 在ADS规划的换道控制路径上,ADS执行换道控制不与ORU发生碰撞;
  - ADS执行的换道控制对ORU是能被预期和安全响应的。
- B.1.2.1.2 ADS执行的换道控制不应无故延迟完成。
- B.1.2.1.3 ADS应能合理控制相应转向信号灯的开启和关闭。
- B.1.2.1.4 ADS应按照B.1.2.3对后向安全距离进行评估,且在评估中应考虑本车辆的任何减速或加速行为。
- B.1.2.1.5 若在完成换道控制时与后方车辆没有足够的安全距离,ADS在完成换道控制后至少2 s内不应增加减速度,除以下任一情况外:
- 为避免或减缓急迫的碰撞风险且同时为符合本文件其他相关要求(例如,为符合新的道路限速值,保持与前车有足够的安全距离);
- 注:急迫的碰撞风险指ADS无法以低于 $5\text{ m/s}^2$ 的减速度指令避免车辆与ORU、道路设施或障碍物发生碰撞的情况。
- 在执行MRM过程中为确保抵达目标停车区域需要增加减速度。
- B.1.2.1.6 ADS在激活状态下,当以下任一条件不符合时,不应触发常规换道控制:
- ADS具备符合B.3.1要求的感知能力;
  - 不存在影响ADS安全执行换道控制的失效;
  - 目标车道内具备或即将具备足够可用空间。
- B.1.2.1.7 ADS执行常规换道控制目标应避免车辆在两个车道之间处于静止状态。若无法避免(例如,由于周围交通流造成的),则应适时继续完成本次换道控制或返回至原车道。
- B.1.2.1.8 对于常规换道控制,ADS在激活状态下,在符合B.1.2.1.1~B.1.2.1.7的基础上,当以下任一条件不符合时,不应触发常规换道控制:
- 存在明确的换道控制原因(例如,沿导航路线行驶、提升通行效率、避免碰撞风险);
  - 目标车道可通行。
- B.1.2.1.9 对于MRM换道控制,在符合B.1.2.1.1~B.1.2.1.5的基础上,应符合以下要求:
- 在触发换道控制前,在适当的情况下,通过控制车辆的速度以适应目标车道中的其他车辆;
  - 除以下任一情况外,换道控制不在开始执行MRM 3 s内触发:
    - 为尽快抵达最小风险化的目标停车区域(例如,应急车道即将在前方终止或由于ADS、车辆发生失效);
    - 该换道控制的风险性与执行常规换道控制相同。

## B.1.2.2 换道执行阶段

- B.1.2.2.1 触发换道控制后,ADS目标应使车辆在换道执行阶段内的横向运动保持连续。
- B.1.2.2.2 在换道执行阶段,除由于弯道曲率产生的横向加速度外,ADS目标应避免由于执行换道控制所额外产生大于 $1\text{ m/s}^2$ 的横向加速度。
- B.1.2.2.3 当目标车道相关区域(至少包括PVPA)预计在换道执行阶段中不会被其他车辆占用时(例如,在本车辆邻车道内没有其他车辆意图执行与本车辆轨迹冲突的换道控制),ADS才应使车辆进入换道执行阶段。

注:PVPA指在该区域内存在与ADS执行换道控制相关的其他车辆,如图B.1中CDFE围成的区域所示。图B.1中C线和D线的位置将会根据装备ADS的车辆的行驶速度而变化。



标引序号说明:

A——装备ADS的车辆最前端位置的平行线;

B——装备ADS的车辆最后端位置的平行线;

C——一条与装备ADS的车辆行驶方向垂直, 从装备ADS的车辆最前端点开始测量、位于安全档案中描述的安全距离的前向车辆车尾所处的位置线;

D——一条与装备ADS的车辆行驶方向垂直, 从装备ADS的车辆最后端点开始测量、位于B.1.2.3评估的换道控制后向安全距离的临界距离的后向车辆车头所处的位置线;

E——一条与装备ADS的车辆行驶方向平行, 位于非目标车道侧的装备ADS的车辆侧轮廓所处的位置线;

F——一条与装备ADS的车辆行驶方向平行, 目标车道外侧车道的远端车道标线所处的位置线, 若目标车道外侧无其他车道, 则是指目标车道自身的远端车道标线所处的位置线。

图B.1 PVPA 示意图

B.1.2.2.4 若无法完成换道执行阶段且交通条件允许, ADS 应使车辆驶回原车道。

B.1.2.2.5 对于常规换道执行阶段, 在符合 B.1.2.2.1~B.1.2.2.4 的要求的基础上, ADS 不应导致与在冲突轨迹上的其他车辆发生碰撞。

B.1.2.2.6 对于 MRM 过程中的换道执行阶段, 在符合 B.1.2.2.1~B.1.2.2.4 的要求的基础上, 还应符合以下要求:

- a) 提前通过开启相应的转向信号灯来代替危险警告信号以对 ORU 进行提示;
- b) 一旦完成换道执行阶段, 及时关闭转向信号灯并重新开启危险警告信号。

B.1.2.3 后向安全距离评估要求

B.1.2.3.1 一般要求

**B.1.2.3.1.1** ADS 应仅在换道控制不会导致目标车道上的后向接近车辆被迫采取不合理地减速时才准许触发换道控制，且符合以下要求：

- a) 对于常规换道控制，ADS 目标应使换道控制不导致目标车道上的后向接近车辆减速，尤其是对于没有紧急的换道控制需求的情况（例如，换道控制的目的是超越前方慢行车辆）；但因 B.1.2.1.6 a) 而需要执行换道控制的，在进入换道执行阶段时，不导致目标车道的后向接近车辆以大于  $3 \text{ m/s}^2$  的减速度制动，并符合以下要求之一：
  - 1) ADS 对后向安全距离的评估符合 B.1.2.3.2 的要求；
  - 2) 车辆制造商提供 ADS 对后向安全距离的评估策略说明，包括合理性和安全性的验证。
- b) 对于 MRM 换道控制，ADS 目标应进入换道执行阶段时，不导致目标车道的后向接近车辆以大于  $3.7 \text{ m/s}^2$  的减速度制动，并符合以下要求之一：
  - 1) ADS 对后向安全距离的评估符合 B.1.2.3.3 的要求；
  - 2) 车辆制造商提供 ADS 对后向安全距离的评估策略说明，包括合理性和安全性的验证。

**B.1.2.3.1.2** 在向常规车道执行换道控制中，若 ADS 控制车辆发生减速，则该减速行为应被纳入与后向接近车辆的安全距离评估中；除为避免或减缓急迫的碰撞风险或在执行 MRM 过程中为确保抵达目标停车区域所需外，ADS 发出的减速度指令不应大于  $2 \text{ m/s}^2$ 。

### **B.1.2.3.2 常规换道控制的后向安全距离评估**

**B.1.2.3.2.1** 当 ADS 探测到目标车道存在后向接近车辆时，在车辆距目标车道最近的前轮外侧接触到目标车道边线外侧  $A \text{ s}$  后，不应导致后向接近车辆以大于  $3 \text{ m/s}^2$  的减速度制动，且确保与后向接近车辆之间的纵向时距始终不小于  $1 \text{ s}$ 。其中  $A$  等于以下任一值：

- a) 若本车辆已经在距目标车道最近的前轮外侧接触到目标车道边线外侧开始前，在其横向移动过程中，ADS 已持续探测出后向接近车辆全宽至少  $1 \text{ s}$ ，则取值为  $0.4$ ；
- b) 若不符合 a) 的条件，则取值为  $1.4$ 。

**B.1.2.3.2.2** 当 ADS 未探测到目标车道上存在后向接近车辆时，仍应基于 B.1.2.3.2.1 对后向安全距离的评估，并应采用如下假设：

- a) 后向接近车辆与本车辆的距离等于 ADS 当前实际的后向探测范围能力边界；
- b) 后向接近车辆的车速比道路最高限速值高  $30 \text{ km/h}$ ；
- c) 在本车辆横向移动过程中，ADS 已持续探测出后向接近车辆全宽至少  $1 \text{ s}$ 。

**B.1.2.3.2.3** 当 ADS 探测到目标车道存在与本车辆等速或慢于本车辆的后向车辆时，在换道执行阶段，ADS 应确保本车辆车身后端与后向车辆车身前端的纵向距离不小于后向车辆行驶  $1 \text{ s}$  的距离。

### **B.1.2.3.3 MRM 换道控制的后向安全距离评估**

**B.1.2.3.3.1** 当 ADS 探测到目标车道存在后向接近车辆时，ADS 目标应使车辆距目标车道最近的前轮外侧接触到目标车道边线外侧  $A \text{ s}$  后不导致后向接近车辆以大于  $3.7 \text{ m/s}^2$  的减速度制动，且确保本车辆与后向接近车辆之间的纵向时间距离始终不小于  $B \text{ s}$ 。其中  $A$  和  $B$  应符合以下取值：

- a)  $A$  等于以下任一值：
  - 1) 若本车辆在跨越车道边线前已持续开启相应的转向信号灯至少  $3 \text{ s}$  且本车辆横向移动已至少持续  $1 \text{ s}$ ，同时后向接近车辆全宽已被 ADS 探测，则取值为  $0$ ；

- 2) 若本车辆已经在距目标车道最近的前轮外侧接触到目标车道边线外侧开始前,在其横向移动过程中,ADS已持续探测到后向接近车辆全宽至少1s,则取值为0.4;
- 3) 未满足1)或2),则取值为1.4。

b) B等于以下任一值:

- 1) 若目标车道为限制速度更低的车道或硬路肩,则取值为0.5;
- 2) 对于其他条件,则取值为1。

**B.1.2.3.3.2** 当ADS未探测到目标车道上存在后向接近车辆时,仍应按照B.1.2.3.3.1对后向安全距离的评估,并应采用如下假设:

- a) 后向接近车辆与本车辆的距离等于ADS当前实际的后向探测范围能力边界;
- b) 后向接近车辆的车速比道路最高限速值高30 km/h;
- c) 若目标车道为应急车道或硬路肩,本车辆在开始换道执行阶段时,后向接近车辆的速度为80 km/h或比本车辆高40 km/h,两者取较低值;
- d) 在本车辆横向移动过程中,ADS已持续探测出后向接近车辆全宽至少1s。

**B.1.2.3.3.3** 当ADS探测到目标车道存在与本车辆等速或慢于本车辆的后向车辆时,在换道执行阶段,ADS应确保本车辆车身后端与后向车辆车身前端的纵向距离不小于后向车辆行驶0.7s的距离。

### **B.1.3 紧急避撞控制要求**

#### **B.1.3.1 一般要求**

**B.1.3.1.1** 当存在急迫的碰撞风险时,ADS应执行紧急避撞控制。

注1:紧急避撞控制一般包括紧急制动或紧急转向等。

注2:ADS发出高于 $5\text{ m/s}^2$ 制动减速度指令视为紧急避撞控制。

**B.1.3.1.2** 若发生影响车辆制动或转向性能的失效,紧急避撞控制的执行应考虑车辆制动或转向的剩余能力。

**B.1.3.1.3** 除ADS按照B.1.3.2执行跨车道线避撞控制外,在横向避撞控制过程中车辆不应跨越车道边线(前轮外边缘到车道边线外边缘)。在横向避撞控制执行完成后,ADS目标应使车辆恢复至稳定的运动状态。

**B.1.3.1.4** 除急迫的碰撞风险已消失或ADS被后援用户退出外,ADS执行的紧急避撞控制不应被终止,且应符合以下要求:

- a) 由于急迫的碰撞风险消失导致紧急避撞控制终止后,ADS仍保持激活状态;
- b) 若由于执行紧急避撞控制造成车辆处于静止状态,ADS开启危险警告信号。若车辆又重新起步,ADS关闭危险警告信号。

#### **B.1.3.2 跨车道线避撞控制要求**

**B.1.3.2.1** 当符合B.3.1的感知探测范围内已存在或即将出现碰撞风险,但该风险尚未达到急迫的碰撞风险程度,ADS目标应避免执行跨车道线避撞控制。

**B.1.3.2.2** 若执行跨车道线避撞控制是ADS执行紧急避撞控制的一部分,ADS应确保其对车内用户和ORU的安全性不低于通过制动来避免急迫的碰撞风险的安全性。

**B.1.3.2.3** 仅当符合以下条件时,ADS才应执行跨车道线避撞控制来应对急迫的碰撞风险:

- a) ADS充分探测到前向、侧向和后向的交通情况;
- b) ADS能评估跨越车道线的安全风险;



c) ADS 确保不会导致跨线方向相邻车道内的其他车辆被迫不合理地减速。

B.1.3.2.4 ADS 在执行跨车道线避撞控制过程中不应导致在其轨迹上与 ORU 发生碰撞。

B.1.3.2.5 若 ADS 的运动规划意图是跨越车道线，则 ADS 应开启相应转向信号灯以对 ORU 进行提示。

#### B.1.4 介入请求过程要求

B.1.4.1 ADS 应具备明确的介入请求触发条件，且 ADS 在激活状态下，应能识别需要发出介入请求的所有情况。

B.1.4.2 介入请求的发出时机应确保后援用户有足够的时间安全接管车辆，至少应符合以下要求：

a) 对于计划接管事件，ADS 适时发出介入请求，以确保即使后援用户未接管，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 在识别到该事件时及时发出介入请求；

注：非计划接管事件指ADS预先未知晓但需要发出介入请求的事件，例如，遇恶劣天气等。

c) 对于影响 ADS 安全执行 DDT 的失效，ADS 在检测到该失效时及时发出介入请求；

d) 当不符合 B.2.1.1 a) ~h) 中任一条件时，除在本文件中有其他不同的规定，ADS 适时发出介入请求。

B.1.4.3 若 ADS 具备常规换道控制能力，若 ADS 已知在换道控制中会发出介入请求，则 ADS 不应触发该换道控制；除为安全响应道路设施、道路交通标志或标线（例如，施工改道、前方车道数变少等）外，其目标应是常规换道控制不属于介入请求阶段的一部分。

B.1.4.4 除安全档案中描述的特殊情况外，在介入请求发出过程中，ADS 不应使车辆静止，且应符合以下要求：

a) 若按照安全档案中描述的特殊情况，ADS 使车辆维持静止状态，则及时开启危险警告信号；

b) 在介入请求发出过程中，最迟在发出介入请求 4 s 后按照 B.2.3.1 c) 的要求升级介入请求并保持升级状态直至介入请求终止。

注1：安全档案中描述的特殊情况如前方出现阻碍车辆继续行驶的其他车辆或障碍物。

注2：在介入请求发出过程中，ADS可能降低车速以确保其安全行驶。

B.1.4.5 仅当 ADS 退出或执行 MRM 时，才应终止介入请求，且应符合以下要求：

a) 介入请求从发出到因执行 MRM 而终止的时长不少于 10 s，使后援用户有充足的时间接管车辆；

b) 若发生 ADS 严重失效或车辆严重失效，允许 ADS 可不发出介入请求直接执行 MRM。

#### B.1.5 MRM要求

B.1.5.1 除 ADS 在执行 MRM 过程中被人工退出外，MRM 应使车辆达到 MRC。

B.1.5.2 在执行 MRM 过程中，除安全档案中描述的特殊情况外，ADS 应以不大于  $4.0 \text{ m/s}^2$  的减速度指令进行减速。

注：安全档案中描述的特殊情况如发生ADS严重失效、发生车辆严重失效、应对急迫的碰撞风险等。

B.1.5.3 当执行 MRM 时，应开启并保持危险警告信号，在换道控制中应按照 B.1.2.2.6 的要求合理使用危险警告信号。

B.1.5.4 除 ADS 退出或 ADS 使车辆达到 MRC 后，ADS 不应终止 MRM。

B.1.5.5 当因车辆达到 MRC 而终止 MRM 后，不应因 ADS 退出导致危险警告信号关闭。

## B.2 人机交互

### B.2.1 激活和退出

B.2.1.1 除驾驶人执行激活操作且符合以下所有条件外，ADS 不应被激活：

- a) 驾驶人坐在驾驶位，且系好安全带；
- b) 驾驶人具备执行 DDT 能力；
- c) 不存在影响 ADS 运行的失效；
- d) 车辆配备的 DSSAD 处于可用状态，且存储区域未被锁定事件占满；
- e) 天气环境和道路设施允许 ADS 运行；
- f) ADS 自检确认；
- g) 车辆未在影响 ADS 运行的软件升级；
- h) 除上述 a) ~g) 外，安全档案中描述的其他 ODC。

注：若允许3级自动泊车功能向应用于高速公路和/或城市快速路的3级自动驾驶功能切换，ADS可能在满足a)~h)条件下无需通过驾驶人执行激活操作。

B.2.1.2 符合以下任一条件时，ADS 应执行退出策略：

- a) 后援用户通过专用操纵方式退出 ADS；
- b) 后援用户按照 B.2.2.1 的方式干预横向运动控制；
- c) 后援用户按照 B.2.2.3 或 B.2.2.4 的方式干预纵向运动控制，且手握转向盘；
- d) 除 a) ~c) 外，安全档案中描述的其他后援用户操作导致 ADS 退出的操作。

注1：当紧急避撞控制正在执行时，ADS的退出可能暂缓至急迫的碰撞风险消失。

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行安全档案中描述的其他安全退出控制策略。

注3：ADS退出策略可能与B.2.2.2确认的后援用户注意力相关，当后援用户注意力不集中时，ADS的退出可能暂缓至后援用户注意力集中。

B.2.1.3 对于 B.2.1.2 c) 中后援用户手握转向盘的条件，若车辆制造商有其他的确认后援用户控制横向运动的方式，应在安全档案中予以说明。

B.2.1.4 ADS 不应因后援用户执行除 B.2.1.2 以外的操作而退出。

B.2.1.5 任何退出应按照 B.2.3.2.2 提示后援用户。

### B.2.2 干预

B.2.2.1 当后援用户对转向控制的干预超过安全档案中描述的为防止误用而设计的合理阈值时，后援用户输入的转向控制应被执行。该阈值应包括特定的力或力矩，以及相应的持续时间，且应与 B.2.2.2 确认的后援用户注意力情况相关，并在安全档案中予以说明。

注1：若后援用户对转向控制的干预将导致急迫的碰撞风险，ADS可能根据安全档案中描述的方式减弱或抑制后援用户的干预对任何控制的影响。

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行安全档案中描述的其他安全响应转向控制的干预策略。

B.2.2.2 ADS 应检测后援用户是否注意力集中。当以下情况均不符合时，不应视为注意力集中：

- a) 确认后援用户注视前方道路；
- b) 确认后援用户注视后视镜；
- c) 确认后援用户头部运动主要朝向驾驶任务相关区域；
- d) 安全档案中与 a) ~c) 同等安全的其他情况。

注：ADS检测后援用户是否注意力集中，可能包括a)~d)的行为和持续时间。

**B.2.2.3** 当后援用户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使车辆保持静止时，后援用户输入的制动控制应被执行。

注1：若后援用户对制动控制的干预将导致急迫的碰撞风险，ADS可能根据安全档案中描述的方式减弱或抑制后援用户的干预对任何控制的影响。

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行安全档案中描述的其他安全响应制动控制的干预策略。

**B.2.2.4** 若后援用户对加速控制的干预被执行，不应导致 ADS 不符合本文件的要求。

## **B.2.3 系统状态提示**

### **B.2.3.1 一般要求**

ADS应向后援用户提示以下信息，其中光学信号应具有适当尺寸和对比度，声学信号应响亮、清晰：

- a) B.2.3.2 所定义的 ADS 状态；
- b) ADS 激活状态下，任何影响 ADS 执行 DDT 的故障，至少通过光学信号提示；
- c) 未升级的介入请求应在光学信号的基础上附加声学 and/或触觉信号进行提示，最迟在发出介入请求 4s 后，介入请求应符合以下要求：
  - 1) 升级介入请求并保持升级状态直至介入请求终止；
  - 2) 在车辆非静止状态下，升级的介入请求增加持续或间歇的触觉提示。
- d) 在 MRM 执行过程中，在光学信号的基础上附加声学 and/或触觉信号进行提示；
- e) 在紧急避撞控制执行过程中，通过光学信号提示；
- f) 在执行换道控制中，至少通过光学信号提示。

注：若允许3级自动泊车功能与应用于高速公路和/或城市快速路的3级自动驾驶功能之间切换，切换时状态提示可能相同。

### **B.2.3.2 系统状态**

#### **B.2.3.2.1 激活状态提示**

**B.2.3.2.1.1** 当自动驾驶功能处于激活状态时，应至少通过专用光学信号持续向后援用户提示自动驾驶功能处于激活状态。光学信号提示应位于后援用户与车辆前方的直接视线附近且易于察觉（例如，仪表盘或转向盘）。

注1：光学信号提示可能包括带有“A”或“AUTO”的转向盘或车辆标志。

注2：在介入请求和执行MRM过程中，可能根据注1中的提示替换为介入请求的提示。

**B.2.3.2.1.2** 激活状态的光学信号应持续到自动驾驶功能退出。

#### **B.2.3.2.2 退出时状态提示**

自动驾驶功能由激活状态退出至未激活状态时，应至少通过光学信号和声学信号向后援用户提示自动驾驶功能已退出。

注1：由于后援用户接管导致自动驾驶功能退出，可能仅用光学信号提示。

注2：若允许3级自动泊车功能与应用于高速公路和/或城市快速路的3级自动驾驶功能之间切换，切换时可能不发出退出提示。

#### **B.2.3.2.3 介入请求和 MRM 的状态提示**

**B.2.3.2.3.1** 在介入请求和执行 MRM 过程中，ADS 应以直观和明确的方式提示后援用户接管车辆，指示标志应包括显示双手和转向盘的图形信息（例如，图 B.2），并附带额外的说明和警告信息。



图B.2 介入请求指示标志示意图

**B.2.3.2.3.2 MRM 开始执行时，提示信号应改变特性，以强调后援用户执行接管的紧迫性。**

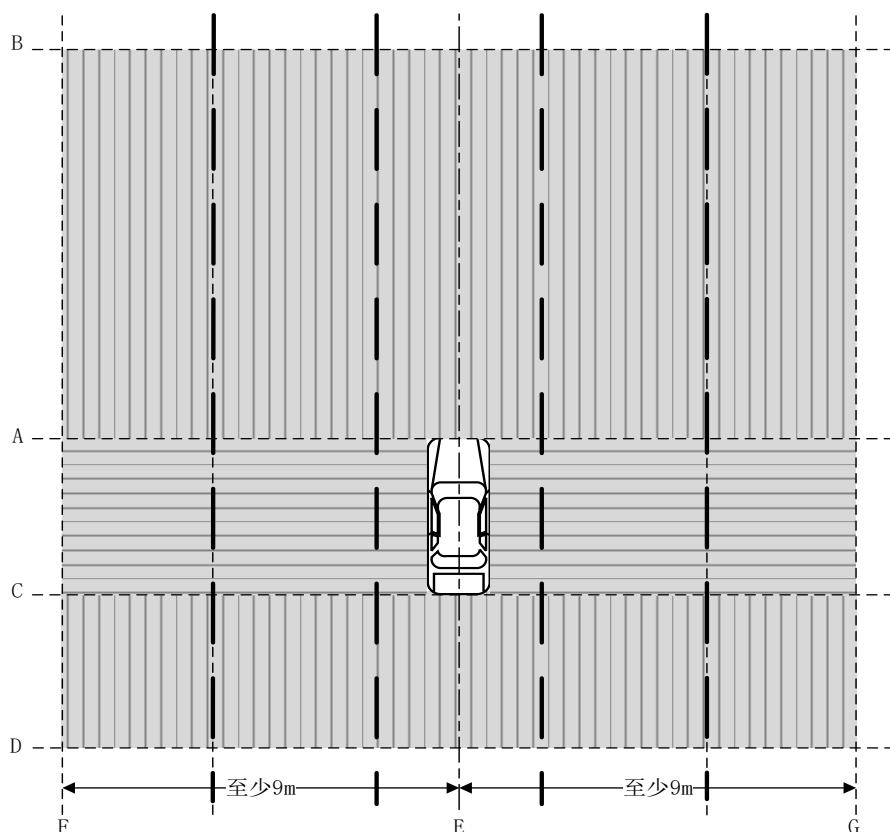
### B.3 感知系统

### B.3.1 一般要求

**B.3.1.1** ADS 的感知系统应至少能探测以下区域（见图 B.3 中 BDFG 围成的区域）的驾驶环境（例如，前方道路几何形状、车道线）和交通动态（例如，车辆、行人等的动态）：

- a) 覆盖前向探测范围（B.3.2）到后向探测范围（B.3.4）；
- b) 沿车辆全长，从装备 ADS 的车辆中心线向左右两侧均分别延伸至少 9 m 宽（B.3.3）所围成区域。

注：探测范围是指考虑到车辆使用寿命期间由于时间和使用导致的感知系统组件的性能衰退，ADS能够可靠地探测目标（例如，车辆、行人等）并能据此生成控制信号的距离。



标引序号说明:

A——装备ADS的车辆最前端位置的平行线;

B——装备ADS的车辆感知系统的前向探测范围的平行线;

C——装备ADS的车辆最后端位置的平行线;

D——装备ADS的车辆感知系统的后向探测范围的平行线；

E——装备ADS的车辆中心线；

F——装备ADS的车辆感知系统从前向到后向的左侧侧向探测范围的平行线，与E相距至少9 m；

G——装备ADS的车辆感知系统从前向到后向的右侧侧向探测范围的平行线，与E相距至少9 m。

图B.3 具备换道控制能力的自动驾驶功能的感知探测范围示意图

B.3.1.2 ADS 应执行控制策略来探测和补偿因环境条件造成的感知系统探测范围的降低（例如，不激活 ADS、发出介入请求和在能见度过低时降低车速）。

B.3.1.3 对于可在挂接挂车的情况下激活 ADS 的车辆，ADS 的感知能力应覆盖所连接挂车长度的感知需求。

### B.3.2 前向探测范围要求

B.3.2.1 对于最高设计运行速度不大于 60 km/h 的 ADS，前向探测范围应至少为 50 m。

注：前向探测范围从装备ADS的车辆最前端开始测量。

B.3.2.2 应在同时符合以下要求时，ADS 最高设计运行速度才能大于 60 km/h：

- a) 车辆具备减速度值不小于  $5 \text{ m/s}^2$  的减速度能力；
- b) 前向探测范围达到表 B.1 中所对应的最小前向探测范围。

表B.1 ADS 最高设计运行速度与最小前向探测范围的对应表

最高设计运行车速 km/h	最小前向探测范围 <sup>a</sup> m
0~60	50
70	50
80	60
90	75
100	100
110	110
120	130
<sup>a</sup> 对于表中未提到的值，应采用线性插值。	

B.3.2.3 若特定情况下（例如，在湿滑的道路上），当车辆无法达到  $5 \text{ m/s}^2$  的减速度或 ADS 无法达到最小前向探测范围时，ADS 应根据实际探测范围和实际减速能力调整其最高运行速度，以保证 ADS 在最高运行速度下具备控制车辆在前方静止的 ORU 或阻碍通行的车道前完全静止以避免碰撞的能力。

B.3.2.4 ADS 的前向探测范围应能够覆盖从装备 ADS 的车辆中心线向左右两侧各至少 9 m 宽的区域，见图 B.3 中 ABFG 围成的区域。

### B.3.3 侧向探测范围要求

B.3.3.1 ADS 的侧向探测范围应覆盖从装备 ADS 的车辆中心线向左右两侧各至少 9 m 宽的区域，见图 B.3 中 ACFG 围成的区域。

### B.3.4 后向探测范围要求

B.3.4.1 ADS 的后向探测范围应符合 B.1.2.3 要求。

注：后向探测范围以装备ADS的车辆最后端为起点。

B.3.4.2 ADS 的后向探测范围应覆盖从装备 ADS 的车辆中心线向左右两侧各至少 9 m 宽的区域，见图 B.3 中 CDFG 围成的区域。

## 附录 C

## (规范性)

## 4 级自动驾驶功能具体技术要求

## C.1 DDT 执行

## C.1.1 一般要求

C.1.1.1 ADS 在激活状态下应使车辆保持在车道内行驶并确保不会无目的跨越任何车道边线（前轮外边缘到车道边线外边缘）。ADS 目标应使车辆在车道内保持稳定的横向和纵向运动以避免对 ORU 造成干扰。

C.1.1.2 ADS 应具备采取合理控制策略应对道路因施工、交通管制等情况发生临时变更的能力。

C.1.1.3 ADS 在激活状态下，应识别以下碰撞风险，并执行合理的控制策略，最小化对车内用户和 ORU 的安全风险：

- a) 前车减速、邻车切入、逆向行驶车辆以及突然出现的障碍物；
- b) 行人、自行车骑行者等弱势道路使用者；
- c) 无法识别类型的目标。

C.1.1.4 若车辆允许乘客站立或不佩戴乘客约束系统，除安全档案中描述的特殊情况外，ADS 发出的水平方向加速度和减速度指令均不应大于  $2.4 \text{ m/s}^2$ ，水平方向加速度和减速度变化率均不应大于  $5.0 \text{ m/s}^3$ 。

注：水平方向加速度和减速度指横向和纵向的综合计算值。

C.1.1.5 若 ADS 支持远程协助，ADS 应符合 C.2 的要求。

## C.1.2 换道控制要求

ADS 执行换道控制应符合 B.1.2.1、B.1.2.2.1、B.1.2.2.3 和 B.1.2.2.4 的要求。

## C.1.3 紧急避撞控制要求

C.1.3.1 ADS 执行的紧急避撞控制应符合 B.1.3.1.1~B.1.3.1.3 和 B.1.3.2 的要求。

C.1.3.2 除急迫的碰撞风险已消失外，ADS 执行的紧急避撞控制不应被终止且应符合以下要求：

- a) 由于急迫的碰撞风险消失导致紧急避撞控制终止后，ADS 仍保持激活状态；
- b) 若由于执行紧急避撞控制造成车辆处于静止状态，ADS 开启危险警告信号。若车辆又重新起步，ADS 关闭危险警告信号。

## C.1.4 MRM 要求

C.1.4.1 在 ADS 执行 MRM 过程中，除安全档案中描述的特殊情况外，ADS 应以不大于  $4.0 \text{ m/s}^2$  的减速度指令进行减速。

注：安全档案中描述的特殊情况如发生 ADS 严重失效、发生车辆严重失效、应对急迫的碰撞风险等。

C.1.4.2 在 ADS 执行 MRM 过程中，应开启并保持危险警告信号，对于执行 MRM 过程中的换道执行阶段，应符合以下要求：

- a) 提前通过开启相应的转向信号灯来代替危险警告信号以对 ORU 进行提示；
- b) 一旦完成换道执行阶段，及时关闭转向信号灯并重新开启危险警告信号。

C.1.4.3 在未确认导致 ADS 执行 MRM 的原因消除前，ADS 不应使车辆脱离 MRC。

注：确认方式可能包括 ADS 自检、车内用户查验（如适用）或远程查验（如适用）等。

## C.2 远程协助

### C.2.1 一般要求

#### C.2.1.1 ADS 不应依赖远程协助执行 DDT。

#### C.2.1.2 远程协助过程中，ADS 应独立执行全部 DDT，且不对车内用户和 ORU 造成不合理的安全风险。

注：对于允许坐在驾驶位的车内用户干预的4级自动驾驶功能，车内用户对车辆横和/或纵向运动的控制可能优先于 ADS。

#### C.2.1.3 ADS 应基于行驶环境安全响应远程协助信息。

#### C.2.1.4 除在安全档案中描述的情况外，ADS 不应触发远程协助。

注：触发远程协助的情况如车辆发生碰撞、车辆需要脱困、车辆和/或ADS失效等。

### C.2.2 通信要求

#### C.2.2.1 ADS 应具备符合远程协助技术特性的车端安全策略。

示例：当远程平台服务器故障时，ADS 有安全策略保障车辆安全运行。

#### C.2.2.2 ADS 应能检测远程协助所需的通信状态（例如，信号强度、网络时延或网络时延抖动等）。当通信状态不符合需求导致 ADS 触发远程协助失败时，ADS 应执行合理的控制策略（例如，执行 MRM 等），最小化对车内用户和 ORU 的安全风险。

### C.2.3 信息交互要求

#### C.2.3.1 ADS 应能够及时发送和接收远程协助信息。

#### C.2.3.2 ADS 应至少具备上传以下信息的能力：

- a) 车辆状态信息（例如，速度、车辆失效、碰撞等）；
- b) ADS 状态信息（例如，ADS 运行状态、ADS 失效等）；
- c) 车辆周围环境信息（例如，感知目标、道路情况等）；
- d) 远程协助信息接收结果。

## C.3 人机交互

### C.3.1 一般要求

#### C.3.1.1 除用户执行激活操作且符合以下所有条件外，ADS 不应被激活：

- a) 不存在影响 ADS 运行的失效；
- b) 车辆配备的 DSSAD 处于可用状态，且存储区域未被锁定事件占满；
- c) 天气环境和道路设施允许 ADS 运行；
- d) ADS 自检确认；
- e) 车辆未在执行影响 ADS 运行的软件升级；
- f) 规划的路径不超出 ODD 的道路类型范围；
- g) 除上述 a) ~f) 外，安全档案中描述的其他 ODC。

注1：路径为4级自动驾驶功能的出发地到目的地的路径。

注2：若允许自动泊车功能向4级自动驾驶功能（非自动泊车功能）切换，ADS可能在满足a)~g)条件下无需通过用户执行激活操作。

#### C.3.1.2 ADS 应向乘客提供请求停车的方法。



C.3.1.3 ADS 应向车内用户提供行程相关的信息。

### C.3.2 允许行驶中退出至人工驾驶的自动驾驶功能

#### C.3.2.1 激活和退出

C.3.2.1.1 若在车辆驾驶区域外设置了自动驾驶功能激活操纵方式，在人工驾驶过程中，位于非驾驶位的用户操作该激活操纵方式，自动驾驶功能在激活前应获得驾驶人确认。

C.3.2.1.2 除以下情形外，若车辆未处于静止状态，4 级自动驾驶功能不应退出：

- a) 将车辆控制权安全地移交给车内用户；
- b) 安全切换至 3 级自动驾驶功能；
- c) 安全切换至自动泊车功能。

注1：当紧急避撞控制正在执行时，ADS 的退出可能暂缓至急迫的碰撞风险消失；

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行车辆制造商声明的其他安全退出控制策略。

C.3.2.1.3 若在车辆驾驶区域外设置了自动驾驶功能退出操纵方式，对于非驾驶位的用户操作该退出操纵方式退出自动驾驶功能至人工驾驶，ADS 应获得坐在驾驶位的车内用户同意其担任驾驶人的确认。

C.3.2.1.4 任何退出应按照 C.3.2.3.2.4 提示用户。

#### C.3.2.2 干预

C.3.2.2.1 若 ADS 允许坐在驾驶位的车内用户干预转向控制，当该车内用户对转向控制的干预超过安全档案中描述的为防止误用而设计的合理阈值时，该车内用户输入的转向控制应被执行。该阈值应包括特定的力或力矩，以及相应的持续时间，且应与 C.3.2.2.2 确认的该车内用户注意力情况相关，并在安全档案中予以说明。

注1：若车内用户对转向控制的干预将导致急迫的碰撞风险，ADS可能根据安全档案中描述的方式减弱或抑制车内用户的干预对任何控制的影响。

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行安全档案中描述的其他安全响应转向控制的干预策略。

C.3.2.2.2 若 ADS 允许被坐在驾驶位的车内用户干预转向控制，ADS 应检测该车内用户是否注意力集中。当以下情况均不符合时，不应视为注意力集中：

- a) 确认该车内用户注视前方道路；
- b) 确认该车内用户注视后视镜；
- c) 确认该车内用户头部运动主要朝向驾驶任务相关区域；
- d) 安全档案中与 a) ~c) 同等安全的其他情况。

注：ADS检测车内用户是否注意力集中可能包括a)~d)的行为和持续时间。

C.3.2.2.3 若 ADS 允许被坐在驾驶位的车内用户干预制动控制，且当车内用户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使车辆保持静止时，车内用户输入的制动控制应被执行。

注1：若坐在驾驶位的车内用户对制动控制的干预将导致急迫的碰撞风险，ADS可能根据安全档案中描述的方式减弱或抑制车内用户的干预对任何控制的影响。

注2：在发生车辆严重失效或ADS严重失效的情况下，ADS可能执行安全档案中描述的其他安全响应制动控制的干预策略。

C.3.2.2.4 若坐在驾驶位的车内用户对加速控制的干预被执行，不应导致 ADS 不符合本文件的要求。

### C.3.2.3 系统状态提示

#### C.3.2.3.1 一般要求

ADS应向车内用户提示以下信息,其中光学信号应具备适当尺寸和对比度,声学信号应响亮、清晰:

- a) C.3.2.3.2 要求的 ADS 状态;
- b) ADS 激活状态下,任何影响 ADS 执行 DDT 的故障,至少通过光学信号提示。

注:若允许4级自动泊车功能与4级自动驾驶功能(非自动泊车功能)之间切换,切换时状态提示可能相同。

#### C.3.2.3.2 系统状态

C.3.2.3.2.1 当自动驾驶功能处于激活状态时,应至少通过专用光学信号持续向车内用户提示自动驾驶功能处于激活状态。

注1:光学信号提示可能包括带有“A”或“AUTO”的转向盘或车辆标志。

注2:在执行MRM过程中,可能根据注1中的提示替换为MRM的提示。

C.3.2.3.2.2 自动驾驶功能激活状态的光学信号应持续到自动驾驶功能退出。

C.3.2.3.2.3 自动驾驶功能由激活状态退出至未激活状态时,应至少通过光学信号和声学信号向车内用户提示自动驾驶功能已退出。

注:若允许4级自动泊车功能与4级自动驾驶功能(非自动泊车功能)之间切换,切换时可能不发出退出提示。

C.3.2.3.2.4 在执行MRM和处于MRC时,ADS应至少发出明确的光学提示信息。

### C.3.3 不允许行驶中退出至人工驾驶的自动驾驶功能

#### C.3.3.1 激活和退出

C.3.3.1.1 对于支持行驶过程中激活的自动驾驶功能,若在车辆驾驶区域外设置了自动驾驶功能激活操纵方式,在人工驾驶过程中,位于非驾驶位的用户操作该激活操纵方式,ADS在激活前应获得驾驶人确认。

C.3.3.1.2 除安全切换至4级自动泊车功能外,若车辆未处于静止状态,4级自动驾驶功能(非自动泊车功能)不应退出。

C.3.3.1.3 ADS如具备为人工驾驶或维修等模式提供的退出操作装置,该装置应仅在车辆静止状态下被响应。

#### C.3.3.2 系统状态提示

ADS应向车内用户提示以下信息,其中光学信号应具备适当尺寸和对比度,声学信号应响亮、清晰:

- a) 提示 C.3.2.3.2 要求的 ADS 状态;
- b) 允许车内用户激活的自动驾驶功能,若 ADS 因不可用而不能响应车内用户的激活操作,则应及时直观的向车内用户发出提示。

注:若允许4级自动泊车功能与4级自动驾驶功能(非自动泊车功能)之间切换,切换时状态提示可能相同。

附 录 D  
(规范性)  
安全档案

## D.1 系统描述

### D.1.1 一般要求

车辆制造商应提供系统描述，至少包括D.1.2和D.1.3的内容。

### D.1.2 功能描述

#### D.1.2.1 系统描述应包括以下内容：

- a) ADS的预期用途；

示例：个人车辆使用、城市出租车车队运营、货运运输服务等。

- b) ADS的配置和运行特性，包括每项自动驾驶功能、预期用途和使用该功能的限制；
- c) 每项自动驾驶功能的ODC如何被定义，并按照GB/T 45312说明其ODC；
- d) 自动驾驶功能的激活条件；
- e) 执行MRM的条件；
- f) 自动驾驶功能的退出条件；
- g) 发出介入请求的条件（如适用）；
- h) 本附录外其他需要在安全档案中描述的相关内容。

D.1.2.2 系统描述应明确ADS设计用于与之交互的ORU类别（例如，行人、骑自行车的人等），并说明这些ORU类别与ADS之间的交互策略。

D.1.2.3 系统描述应明确ADS设计所针对的用户，并说明这些用户与ADS之间的交互策略。

D.1.2.4 针对允许行驶中退出至人工驾驶的自动驾驶功能，系统描述应说明：

- a) ADS如何对用户视线进行监测以及如何判定用户视线朝向驾驶任务相关区域；
- b) ADS在此类区域内为符合5.2.2.3.3 b)所使用的用于判定视线持续时间的各项参数。

D.1.2.5 针对接管能力监测，系统描述应包括以下内容：

- a) 后援用户安全带监测方式及判定方法，说明每种监测方式的评估周期和评估指标；
- b) 后援用户是否坐在驾驶位的监测方式及判定方法，说明每种监测方式的评估周期、评估指标及阈值；
- c) 后援用户执行DDT能力的监测方式及判定方法，说明每种监测方式的评估周期、评估指标及阈值。

D.1.2.6 若ADS可请求远程协助，系统描述应说明此类交互的策略及流程。

D.1.2.7 系统描述应说明激活、干预、接管或退出自动驾驶功能的方法。

D.1.2.8 系统描述应说明自动驾驶功能可实现的MRC，包括：

- a) MRM的过程；
- b) MRC的风险评估。

D.1.2.9 系统描述应包括以下信息：

- a) 可识别的ADS故障清单；
- b) 除ADS自身外，其失效会直接导致ADS无法执行DDT的其他的车辆系统或部件清单。

D.1.2.10 系统描述应说明自动驾驶功能对失效情况的响应方式。

### D.1.3 系统布局 and 原理

D.1.3.1 系统描述应包括 ADS 硬件组件及其功能的概要、软件组件及其功能的概要及 ADS 与其他的车辆系统的关系，概要应包括。

- a) 框图和/或示意图，至少包括：
  - 1) 在硬件组件概要中说明 ADS 硬件组件分布；
  - 2) 在框图和/或示意图中整合 ADS 各组件的硬件标识，并提供列表，将硬件标识与软件标识相关联；
  - 3) 对于集成在单一组件（例如，控制单元）中，但在图中以多个模块呈现的功能，采用单一硬件标识。
- b) ADS 的组件或功能，以及与符合本文件要求相关的其他的车辆系统的组件或功能，至少包括：
  - 1) 展示 ADS 组件或功能与其他的车辆系统组件或功能之间的互连，通过电路图展示电子传输链路、通过管道图展示气动或液压传输设备、通过布置简图展示机械连接；
  - 2) 硬件和软件组件概要、示意图和/或框图中的传输链路，与对应功能的概要、示意图和/或框图中组件及系统之间传输的信号，有明确的对应关系；
  - 3) 当信号优先级影响性能或安全时，确定多路复用数据传输链路上信号的优先级。
- c) 实现以下功能和内容的方式：
  - 1) 对目标和事件的感知；
  - 2) 决策与规划；
  - 3) 由远程方式提供的相关功能和内容（如适用）；
  - 4) 信息显示或用户交互界面；
  - 5) 数据记录系统（例如，DSSAD）；
  - 6) 组件和/或连接的冗余（如适用）。
- d) 硬件组件概要应提供用于组成感知系统的各个组件的安装选项信息，至少包括：
  - 1) 当感知系统安装在车上，包括但不限于部件在车辆内或车辆上的位置、部件周边的材料、部件周边材料的尺寸和几何形状、部件周边材料的表面光洁度；
  - 2) 包括对 ADS 表现至关重要的安装规范（例如，安装角度公差）；
  - 3) 感知系统的各个组件或安装选项的任何更改都在文档中更新。

D.1.3.2 系统描述应提供所有 ADS 的 ECU 输入的清单（包括来自传感器的输入），并定义这些输入的工作范围，同时说明感知输入与 ADS 控制功能的关系，以及对 ADS 行为的潜在影响。还应包括每个传感器的标称范围和覆盖区域。

D.1.3.3 系统描述应提供所有 ADS 的 ECU 输出的清单，并在每种场景下解释输出是直接控制车辆还是通过其他的车辆系统控制。还应定义对每个变量的控制范围以及控制执行器的标称能力。

D.1.3.4 系统描述应说明 ADS 如何探测 ODC 的符合情况，并说明其响应方式。

## D.2 安全概念

### D.2.1 一般要求

D.2.1.1 车辆制造商应将其安全概念形成文档，文档应包含根据 6.1.3 活动所识别出的与 ADS 相关的风险，并应说明这些风险是如何被降低、缓解或接受的。

D.2.1.2 车辆制造商应证明 ADS 在非故障和故障状态下实现了功能概念和安全概念。

D.2.1.3 车辆制造商安全概念文档应说明 ADS 的功能概念、为实现安全目标而制定的安全策略、安全措施、开发过程和方法，以证明 ADS：

- a) 通过设计保证系统在非故障和故障状态下实现了功能概念和安全概念；

- b) 符合本文件规定的非故障和故障状态下的性能要求；
- c) 开发过程和方法是适用的。

D.2.1.4 文档应包括 D.2.1.5 规定的提交的文档和 D.2.1.6 规定的备查的文档。

D.2.1.5 车辆制造商应提交以下文档，并对所提交的文档与产品实际开发的一致性、可追溯性做出自我声明，具体包括：

- a) 危害分析和风险评估总结（见 D.2.2.1）；
- b) 接受准则和确认目标总结（见 D.2.3）；
- c) 安全措施说明（见 D.2.4）；
- d) 整车层面的安全分析总结（见 D.2.5.2）；
- e) 系统层面的安全分析总结（见 D.2.5.4）；
- f) 功能安全验证确认计划和结果总结（见 D.2.6.2）；
- g) 预期功能安全验证确认计划和结果总结（见 D.2.6.4）；
- h) 安全评估发布报告总结（见 D.2.7）。

D.2.1.6 车辆制造商应具有下列相关文档，并对所保管的文档一致性、可追溯性及所采取的安全策略不会对车辆安全运行产生影响做出自我声明，具体包括：

- a) 详细危害分析和风险评估（见 D.2.2.2）；
- b) 详细整车层面的安全分析（见 D.2.5.3）；
- c) 详细系统层面的安全分析（见 D.2.5.5）；
- d) 详细功能安全验证确认计划和结果（见 D.2.6.3）；
- e) 详细预期功能安全验证确认计划和结果（见 D.2.6.5）；
- f) 其他支撑性材料或数据（若有）。

## D.2.2 危害分析和风险评估

### D.2.2.1 危害分析和风险评估总结

D.2.2.1.1 车辆制造商应提交危害分析和风险评估总结。其中，功能安全危害分析和风险评估总结应符合 D.2.2.1.2，预期功能安全危害分析和风险评估总结应符合 D.2.2.1.3。

D.2.2.1.2 车辆制造商应提交功能安全危害分析和风险评估总结，描述 ADS 系统的功能异常表现、整车层面危害、汽车安全完整性等级（ASIL）和安全目标。危害分析和风险评估总结的结果应至少涵盖表 D.1 中的整车危害及对应的安全目标。

表D.1 ADS 相关危害的功能安全要求

序号	整车危害 <sup>a</sup>	安全目标	ASIL <sup>b</sup>	安全度量 <sup>c</sup>
1	非预期的侧向运动	避免自动驾驶功能运行过程中，车辆非预期的转向或过大转向或横向失稳，导致与 ORU、道路基础设施、障碍物等发生碰撞	D	——非预期的侧向运动导致的侧向加速度变化不超过安全阈值； ——非预期的侧向运动导致的侧向位移不超过安全阈值； ——非预期的侧向运动导致的横摆角速度变化不超过安全阈值； ——非预期的侧向运动导致的转向盘转角变化不超过安全阈值；

序号	整车危害 <sup>a</sup>	安全目标	ASIL <sup>b</sup>	安全度量 <sup>c</sup>
				——非预期侧向运动导致的转向车轮转角变化不超过安全阈值。
2	非预期的失去侧向运动控制	避免自动驾驶功能运行过程中，非预期失去车辆侧向运动控制，导致与 ORU、道路基础设施、障碍物等发生碰撞	D	——非预期失去侧向运动控制导致的侧向加速度变化不超过安全阈值； ——非预期失去侧向运动控制导致的侧向位移变化不超过安全阈值； ——非预期失去侧向运动控制导致的横摆角速度变化不超过安全阈值； ——非预期失去侧向运动控制导致的转向盘转角变化不超过安全阈值； ——非预期失去侧向运动控制导致的转向车轮转角变化不超过失去侧向运动控制的安全阈值； ——失去侧向运动控制的时间不超过安全阈值。
3	非预期的减速	避免自动驾驶功能运行过程中，非预期或过大的减速，导致被后方 ORU 追尾	B 或 C <sup>d</sup>	——非预期减速导致的纵向减速度或纵向速度变化不超过安全阈值； ——非预期减速导致的纵向位移变化不超过安全阈值。
4	非预期的主动减速能力丢失或降低	避免自动驾驶功能运行过程中，非预期丢失车辆减速或减速不足，导致与 ORU、道路基础设施、障碍物等发生碰撞	D	——非预期丢失减速或减速不足导致的纵向减速度或纵向速度变化不超过安全阈值； ——非预期丢失减速或减速不足导致的纵向位移变化不超过安全阈值； ——非预期丢失减速或减速不足导致的自车与 ORU、道路基础设施、障碍物的距离变化不超过安全阈值。
5	非预期的加速	避免自动驾驶功能运行过程中，非预期或过大的加速，导致与 ORU、道路基础设施、障碍物等发生碰撞	D	——非预期加速导致的纵向加速度或纵向速度变化不超过安全阈值； ——非预期加速导致的纵向位移变化不超过安全阈值。
6	非预期的纵向移动（从静止位置）	避免自动驾驶功能运行过程中，非预期发生纵向移动，导致与 ORU 如弱势道路使用者、车辆等发生碰撞	B 或 D <sup>e</sup>	——非预期纵向移动导致的纵向位移变化不超过安全阈值。
7	非预期的自动驾驶功能激活	避免自动驾驶功能在不符合 ODC 条件时被激活，或无法正确识别非 ODC 条件导致功能不退出，产生与 ORU、道路基础设施、障碍物等发生碰撞的风险。	B	——非预期的自动驾驶功能激活及运行不超过 ODC 范围条件的安全阈值。
8	非预期丢失或错误的 MRM	避免自动驾驶功能运行过程中，非预期丢失或错误的 MRM	B 或 D <sup>f</sup>	——非预期丢失或错误的 MRM 导致偏离目标停车位置不超过安全阈值。
9	不响应车内用户的干预	避免自动驾驶功能的异常导致车辆不响应车内用户的干预	D 或不分配 ASIL <sup>g</sup>	——响应人员干预的转向操纵力不超过安全阈值；

序号	整车危害 <sup>a</sup>	安全目标	ASIL <sup>b</sup>	安全度量 <sup>c</sup>
				——响应人员干预的制动踏板力或行程不超过安全阈值； ——响应人员干预的加速踏板力或行程不超过安全阈值（如适用）。
10	人机提醒丢失、不足或错误 <sup>h</sup>	避免自动驾驶功能的异常导致人机提醒丢失、不足或错误	B	——人机提醒丢失、不足或错误导致声音提醒的响度、振动力度、光学提醒亮度、提醒发起及持续时间的偏差不得超过安全阈值。
11	非预期车辆可见性丢失、降低或错误	避免自动驾驶功能运行过程中，非预期车辆外部照明、指示灯、雨刮、除雾等功能的丢失、降低或错误，导致可见性丢失	A 或不分配 ASIL <sup>i</sup>	——非预期车辆照明及灯光丢失、降低或错误导致照明亮度、指示灯亮度及点亮时间的偏差不得超过安全阈值； ——非预期车辆人员视野丢失、降低或错误导致车窗视野可见区域面积偏差不得超过安全阈值。
<p><sup>a</sup> 本表规定的整车危害及与其相关安全目标、ASIL 等级和安全度量，可能因系统功能及 ODC 的差异而发生变化，车辆制造商可根据实际情况进行合理定义。</p> <p><sup>b</sup> 若车辆制造商定义更高的 ASIL 等级，视为符合要求；如有外部措施，可对表格中规定的 ASIL 等级进行合理地降低，并在危害分析和风险评估中进行说明，但需要在安全确认活动中检验外部措施的独立性和有效性。</p> <p><sup>c</sup> 车辆制造商应针对相关整车危害定义安全度量，例如：加速度、速度、位移变化（包括变化值或最大值或变化率）等在某个安全范围内。车辆制造商可基于产品特性采用表格中的部分或全部度量，也可采用其他合适的度量指标。</p> <p><sup>d</sup> 本条安全目标的 ASIL 等级与车辆的减速能力相关，对于 M<sub>1</sub>、N<sub>1</sub> 类车辆 ASIL 等级应满足 C；对于 M<sub>2</sub>、M<sub>3</sub>、N<sub>2</sub>、N<sub>3</sub> 类车辆 ASIL 等级应满足 B 或 C。</p> <p><sup>e</sup> 对于仅用于高速公路和/或城市快速路场景的自动驾驶功能 ASIL 等级应满足 B，对于其他道路场景的自动驾驶功能 ASIL 等级应满足 D。</p> <p><sup>f</sup> 对于 3 级自动驾驶功能 ASIL 等级应满足 B，对于 4 级自动驾驶功能 ASIL 等级应满足 D。</p> <p><sup>g</sup> 对于允许车内用户干预车辆控制行为的 ADS，ASIL 等级应满足 D；对于不允许车内用户干预的 ADS，可不分配 ASIL 等级。</p> <p><sup>h</sup> 提醒包含对系统及车辆安全相关的工作状态、人员接管请求（仅适用于 3 级自动驾驶功能）、人员误操作等的提醒。</p> <p><sup>i</sup> 对于避免车内人员视野丢失，3 级自动驾驶功能 ASIL 等级应满足 A，4 级自动驾驶功能可不分配 ASIL 等级；对于非预期车辆外部照明丢失或降低、指示灯丢失或错误，3 级自动驾驶功能和 4 级自动驾驶功能 ASIL 等级应满足 A。</p>				

D.2.2.1.3 车辆制造商应提交预期功能安全危害识别和评估总结。危害识别和评估总结的结果应至少涵盖表 D.1 中适用的整车危害。

#### D.2.2.2 详细危害分析和风险评估

车辆制造商应具有详细危害分析和风险评估以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

#### D.2.3 接受准则和确认目标总结

##### D.2.3.1 接受准则

D.2.3.1.1 车辆制造商应提交 ADS 安全接受准则总结，包括：危害行为接受准则和残余风险接受准

则。

注：接受准则考虑因系统功能不足、故障等原因可能导致的风险。

#### D.2.3.1.2 ADS 危害行为接受准则应至少涵盖表 D.1 中的整车危害。

注：危害行为接受准则指判断车辆行为是否属于危害行为而可能导致危害事件的准则，例如当某特定行为被认为是危害行为时系统所对应的安全度量物理参数。

#### D.2.3.1.3 车辆制造商应定义 ADS 残余风险接受准则，考虑现有的事故数据（例如，人驾事故数据、驾驶辅助事故数据、自动驾驶事故数据等）以及行业内先进的技术。

注1：残余风险接受准则指判断车辆运行过程中残余风险是否处于合理水平的准则，例如，考虑目标市场交通事故统计的单位时间或单位里程的最大事件数、正向风险平衡原则等。

注2：考虑将ADS引入市场，与原有风险情况相比，不会导致风险恶化。根据中国国家统计局、道路交通事故统计年报等数据集，设定残余风险接受准则，即：碰撞等事故率低于 $10^{-4}/h$ 。考虑不同伤害程度的风险，设定残余风险接受准则，即：轻伤事故率低于 $10^{-5}/h$ 、重伤事故率低于 $10^{-6}/h$ 、致命事故率低于 $10^{-7}/h$ 。车辆制造商可以使用其他指标。

#### D.2.3.1.4 对于因系统功能不足、故障可能导致的碰撞风险，总体应符合残余风险接受准则的要求。

### D.2.3.2 验证的准则和确认目标

#### D.2.3.2.1 车辆制造商应提交 ADS 安全验证准则和确认目标总结。

#### D.2.3.2.2 针对危害行为验证的接受准则应至少符合表 D.1 中的安全目标和安全度量要求；

注1：危害行为的验证接受准则基于对ODC范围内的人类驾驶场景和行为数据的研究得出。

注2：危害行为的验证接受准则用于判断在验证和确认过程中，对应于危害场景的危害行为可接受准则，一般是反映客观物理世界关系的量，例如，时间型、距离型、综合型指标等。

#### D.2.3.2.3 车辆制造商应设计量化的残余风险确认目标，以论证是否符合残余风险接受准则。

注1：参考GB/T 43267—2023中C.3的方法，针对残余风险接受准则 $10^{-4}/h$ 定义确认目标为16000小时，以论证验证和确认阶段若该累积运行时间内没有发生功能不足、故障导致的安全相关事件，则有80%的置信度认为该系统符合定义的残余风险接受准则。车辆制造商可以使用其他方法定义确认目标。

注2：确认目标的实际达成效果，依赖于试验场景对ADS ODD的代表性。

### D.2.4 安全措施说明

#### D.2.4.1 一般要求

车辆制造商应提交安全措施的说明。其中，功能安全措施应符合D.2.4.2，预期功能安全措施应符合D.2.4.3。

#### D.2.4.2 功能安全措施

D.2.4.2.1 车辆制造商应提交功能安全措施说明，描述 ADS 如何识别和应对危害、对应采取的功能安全措施，涵盖 D.2.4.2.2~D.2.4.2.16 的要求，并确保为实现安全目标而选择的安全措施不会在故障及非故障条件下影响车辆的安全运行。

D.2.4.2.2 安全概念应描述相应策略以避免 ADS 在系统无法执行 DDT 时操控车辆。这些策略可能包括技术解决方案或其他相关措施。

D.2.4.2.3 自动驾驶功能运行过程中，应对可能影响安全运行进而引发危害的车辆故障进行探测，若存在影响安全运行的情况，应通过警告信号或提示信息等方式告知用户，并执行后援响应。



D.2.4.2.4 在 ADS 运行过程中发生安全相关故障时，安全概念应描述为符合安全目标至少采用以下一种或多种安全措施（含外部措施）：

a) 使用 ADS 的部分系统实现 ADS 后援响应；

注：描述的内容包括激活该模式的条件（例如，失效类型）、在此模式下自动驾驶功能行为和能力（例如，到达MRC）、向后援用户发出预警的策略（如适用）。

b) 使用独立系统实现冗余设计；

注：描述的内容包括独立系统实现的冗余、切换机制的原则、用于确定切换的逻辑架构、该措施的局限性。

c) 执行相同功能的多样性系统设计；

注：描述的内容包括多样性系统实现的冗余、切换机制的原则、用于确定切换的逻辑架构、该措施的局限性。

d) 限制部分或全部自动驾驶功能。

注：描述的内容包括按照本文件的相关规定来执行此操作的方法、与自动驾驶功能相关的所有输出控制信号的抑制策略。

D.2.4.2.5 在 ADS 运行过程中，避免因电气/电子系统的单点故障导致完全失去主动转向、主动制动和主动驻车能力。

注1：根据ADS是否需要后援用户接管、故障发生的潜在可能性等，合理定义故障诊断覆盖率的要求。

注2：采用容错架构方案，适度提高MRM能力的冗余度，如采用冗余组件或通过其他系统实现替代功能，以降低因故障导致丢失MRM能力的风险到合理可接受的水平。

D.2.4.2.6 ADS 的故障不应直接导致车辆应急辅助功能的关闭，但对于 ADS 与应急辅助系统的共用组件发生严重故障的情况除外。

D.2.4.2.7 对于 3 级自动驾驶功能，避免因电气/电子系统的单点故障导致完全失去提醒能力。

注：用户提醒能力包含声学提醒（例如，车内语音等）、触觉提醒（例如，安全带震动、座椅震动、点刹等）和光学提醒（例如，仪表、中控屏幕、氛围灯、转向灯带等）等可被用户感知的方式。

D.2.4.2.8 对于可能导致丢失 MRM 的严重故障或极端情况，其残余风险应控制在合理的水平。

注1：对于合理水平的评估，在考虑累加其他潜在风险的同时，不违背残余风险接受准则的要求。

注2：对于非电气/电子系统故障导致的丢失MRM的评估，参考适用的相关技术领域标准及行业实践。

D.2.4.2.9 若存在导致系统无法执行 MRM 的严重故障或极端情况，车辆制造商应予以声明。

注：对于其他技术领域可能导致丢失MRM能力的严重故障，例如，爆胎、底盘物理损坏等，在总体残余风险评估中作为外部交互予以考虑，所分解出来的要求传递给对应技术领域。

D.2.4.2.10 对于支持远程协助的 ADS，应对远程通信链路的故障进行探测，若存在安全相关故障，不应使能远程协助功能。

注：若远程协助作为ADS系统安全运行时的必须项，则及时进入MRM。

D.2.4.2.11 车辆制造商应提交 ADS 运行阶段安全保障措施的说明，针对 ADS 运行阶段可能出现的故障，具备安全监测、风险探测和缓解措施，确保系统运行阶段符合残余风险接受准则。

注：监测、探测和缓解措施可能包括车载措施和/或非车载措施（如云端措施）。

D.2.4.2.12 安全监测和风险探测应涵盖以下异常事件的判定，以发现 ADS 潜在的安全相关故障：

a) 系统输入异常，例如，系统无输入信号、不正确的输入（含故障）；

b) 系统输出异常：

1) 未输出；

2) 不正确的输出。

c) 安全事件/事故：

- 1) 故障导致 MRM 激活的事件；
- 2) ADS 直接或间接涉及的碰撞事故。

D.2.4.2.13 针对监测到的因故障导致的安全相关事件，应具备风险评估机制，以支持判断可继续运行或需要采取应对措施。

注：风险评估考虑安全相关事件的发生率、严重度和措施的有效性。

D.2.4.2.14 应具备现场运行中因故障导致风险问题的管理流程，包括事件或事故上报、问题调查、风险评估、对策管理、应对措施的实施和效果反馈等。

D.2.4.2.15 针对因故障导致的不可接受的运行风险事件，应具备如下风险应对措施：

- a) 开展调查行动以确定风险原因（例如，基于现场采集的数据重构场景）；
- b) 如适用，针对系统性故障进行系统设计更新（例如，OTA 升级）。

D.2.4.2.16 功能安全措施实施后，应针对其有效性进行监测和评估，若风险仍然不合理，应进行调整。

### D.2.4.3 预期功能安全措施

D.2.4.3.1 车辆制造商应提交预期功能安全措施说明，涵盖 D.2.4.3.2~D.2.4.3.22 的要求，描述 ADS 存在的功能不足及对应的触发条件、导致的整车危害、对应采取的安全措施。

D.2.4.3.2 自动驾驶功能运行过程中，应对可能影响安全运行进而引发危害的预期功能安全问题进行探测，若存在影响安全运行的情况，应通过警告信号或提示信息等方式告知用户，并及时执行后援响应。

注：相关预期功能安全问题的安全分析参考D.2.5和表D.2。

D.2.4.3.3 与 ODC 相关的安全概念应包括以下内容：

- a) ADS 如何判定 D.1.2.1 c) 所述条件的存在与否，以及任何相关联或依赖条件（例如冰雪天气下的减速）；
- b) ADS 在其运行中可合理预见的触发条件，包括但不限于环境和地理条件，和/或某些存在或缺失的交通/道路特征，并说明预期条件与 D.1.2.1 c) 所述的 ADS 的 ODD 如何匹配；
- c) 可合理预见的触发条件清单应至少涵盖表 D.2 中的条件；
- d) 确保功能在不符合 ODC 的情况下无法开启的方法；
- e) 对即将或突然不符合 ODC 的情况，发起后援用户响应；
- f) 应对突然不符合 ODC 的情况以及限制 ADS 频繁激活或退出情况的策略。

D.2.4.3.4 终止自动驾驶功能的预期功能安全策略应包括：

- a) 针对运行中预期功能安全风险问题的判断；
- b) 针对不符合安全相关 ODC 条件进行判断；
- c) 针对用户关闭功能或接管合理性的判断，含用户状态的判定。

D.2.4.3.5 ADS 系统与其他驾驶自动化系统之间的转换策略应包括：控制优先级、导致其他驾驶自动化系统的抑制或中断等。

D.2.4.3.6 可控性策略应包括：

- a) 对于终止自动驾驶过程中确保可控性的策略；
- b) 对允许用户干预/接管的 ADS 确保用户可控性的策略；
- c) ODC 边界条件下合理的系统可控性保障策略（如通过识别天气情况主动降速）。

注：对于3级自动驾驶功能主动发起介入请求的情况，从首次报警信息发出后，后援用户未接管合理的介入请求持续时间一般不少于10s，若计时结束后后援用户未接管或在此过程中风险升级，系统立即执行MRM，以最小化车辆运行风险。对于潜在的介入请求持续时间不足10s的情况，提供风险合理性的说明。

D.2.4.3.7 针对不允许行驶中退出至人工驾驶的自动驾驶功能，应描述对于乘客的安全风险清单（例

如未系安全带、乘客未就座等可合理预见的误用），并描述在自动驾驶功能处于激活状态时，如何管理这些安全风险。管理安全风险的措施应包括：

- a) 自动驾驶功能处于激活状态时，通过警告信号或提示信息告知乘客不安全的行为；
- b) 对于发出警告提示后一定时间内乘客不纠正误用行为或期间发生风险升级时，发起 MRM 并视情况进入 MRC；
- c) 对因误用引发碰撞不可避免时，执行紧急减速、紧急转向等策略以降低事故伤害或损失。

**D. 2. 4. 3. 8** 如适用，针对不允许行驶中退出至人工驾驶的自动驾驶功能，应描述实施的措施或策略，防止或减轻车内用户可能影响 DDT 安全执行的滥用、误用及操作失误（例如，车内用户试图接触驾驶操纵件）。

注1：通过隐藏、隔离（如机械或电子方式）等，阻断用户对驾驶控制装置的错误操作。

注2：通过提升作用力、施加反向力等方式，抵抗用户未按照接管/干预程序对驾驶控制装置的不安全操作。

**D. 2. 4. 3. 9** 如适用，车辆制造商应提交防止、减轻或阻止外部来源对车内用户造成伤害（例如，未授权人员试图进入载有车内用户的车辆）的措施说明。

注：避免未经授权的车外人员打开车门及前后盖，但特殊情况除外（例如，车辆发生碰撞、热失控等）。

**D. 2. 4. 3. 10** 如适用，车辆制造商应提交防止、减轻或阻止外部来源对车辆或其 ADS 的滥用、误用（例如，车辆运行期间被放置异物、试图损坏车辆的行为）的措施说明。

**D. 2. 4. 3. 11** 应描述相应的策略以避免 ADS 在车辆工作条件不佳（例如，轮胎、外部负载等的异常状态）时操控车辆。这些策略可能包括技术解决方案、物理查验或其他相关措施。

注：针对无法通过系统自身查验的问题，如不可探测的车身改装、轮胎磨损、外部拖挂负载等，通过产品使用说明告知用户。

**D. 2. 4. 3. 12** 针对用户误用的策略应包括：

- a) 探测用户状态的策略，例如对 3 级自动驾驶功能后援用户接管准备能力的判断及响应；
- b) 判断用户操作合理性的策略，例如对用户误干预的判断及响应；
- c) 对可合理预见的用户误用的风险减轻策略。

**D. 2. 4. 3. 13** 应描述 ADS 为避免碰撞而应采取的安全措施，包括：

- a) 对道路和路面情况（例如，施工、障碍物、低附着系数路面等）进行监测；
- b) 对 ORU 进行监测和行为预判；
- c) 合理应对未知目标物；
- d) 合理应对 ORU 的非预期行为；
- e) 合理应对不可见区域；
- f) 保持安全速度和距离；
- g) 必要时通过应急响应避免碰撞。

**D. 2. 4. 3. 14** 应描述 ADS 用于判定车辆是否与安全相关目标发生碰撞的策略。

示例：通过传感器等方式识别车辆与安全相关目标发生的碰撞。

**D. 2. 4. 3. 15** 应描述 ADS 用于判定与安全相关目标发生碰撞是否会造成重大损害的策略。

注1：基于碰撞目标对象、碰撞位置、碰撞相对速度、自车车速等，判定与目标发生碰撞的损害严重程度。

注2：基于历史事故或风险事件数据集，得到 ADS 与目标发生碰撞造成损害严重程度的规律。

**D. 2. 4. 3. 16** 若碰撞无法避免，ADS 应对碰撞进行检测，并尽可能减轻风险，包括：

- a) 通过调整自车速度以降低相对碰撞速度从而减轻碰撞严重度；
- b) 使车辆达到静止状态。

D.2.4.3.17 车辆制造商应提交 ADS 运行阶段安全保障措施的说明,针对 ADS 运行阶段可能出现的功能不足,具备安全监测、风险探测和缓解措施,确保系统运行阶段符合残余风险接受准则。

D.2.4.3.18 安全监测和风险探测应涵盖以下异常事件的判定,以发现 ADS 潜在的安全相关功能不足:

- a) 系统输入异常:
  - 1) 系统无输入信号、不正确的输入(含感知系统磨损和老化);
  - 2) 突然离开 ODD 范围;
  - 3) 人员不合理操作或未正确接管。
- b) 系统输出异常:
  - 1) 未输出;
  - 2) 不正确的输出。
- c) 安全事件/事故:
  - 1) 功能不足导致 MRM 激活的事件;
  - 2) ADS 涉及的潜在风险事件(例如,应急辅助功能激活事件);
  - 3) ADS 直接或间接涉及的碰撞事故。

D.2.4.3.19 针对监测到的因功能不足导致的安全相关事件,应具备风险评估机制以支持判断可继续运行或需要采取应对措施。

D.2.4.3.20 应具备现场运行中因功能不足导致风险问题的管理流程,包括事件或事故上报、问题调查、风险评估、对策管理、应对措施的实施和效果反馈等。

D.2.4.3.21 针对不可接受的因功能不足导致的运行风险事件,应具备如下风险应对措施:

- a) 开展调查行动以确定风险原因(例如,基于现场采集的数据重构场景);
- b) 如适用,限制功能使用范围、功能降级、功能停用;
- c) 如适用,针对系统功能不足进行系统设计更新(例如,ODD 更新、OTA 升级);
- d) 如适用,告知用户使用风险、更新操作限制、更新操作指导等。

注:根据现场风险紧迫性的评估,采取立即行动或长期演进。

D.2.4.3.22 安全措施实施后,应针对其有效性进行监测和评估,若风险仍然不合理,应进行调整。

## D.2.5 安全分析

### D.2.5.1 一般要求

D.2.5.1.1 车辆制造商应提交整车层面和系统层面的安全分析,说明对导致表 D.1 中整车危害的故障、功能不足进行了有效识别和处理。

D.2.5.1.2 安全概念应证明车辆制造商在危害识别过程中采用了自上而下(从潜在危害到设计)和自下而上(从设计到潜在危害)的方法。

示例: FMEA、FTA、HAZOP、STPA 等。

D.2.5.1.3 系统层面的安全分析应采用适合系统安全分析的方法(例如, FMEA、FTA、STPA 或其他类似方法)。

D.2.5.1.4 针对 D.2.5.2、D.2.5.4 规定的整车及系统层面的安全分析总结,应列出系统所监测的参数,针对安全分析中的每一种故障情况,列出给予用户、维修人员、检验人员的警告信号。

D.2.5.1.5 针对 D.2.5.2、D.2.5.4 规定的整车及系统层面的安全分析总结,应描述对应的措施,确保系统在性能受环境条件(例如,气候、温度、灰尘进入、进水、冰封等)影响时,不会妨碍车辆的安全运行。

### D.2.5.2 整车层面的安全分析总结

D.2.5.2.1 车辆制造商应提交整车层面的安全分析总结，且符合 D.2.5.2.2～D.2.5.2.9 的要求。

D.2.5.2.2 应描述自动驾驶功能如何识别和应对危害，包括以下内容：

- a) ADS 如何表现（例如，控制策略）以减轻或避免可能影响用户和 ORU 安全的危害；
- b) ADS 如何应对未知危害场景。

D.2.5.2.3 应描述 ADS 与车辆其他系统的交互（含故障条件下）可能导致的潜在安全风险及对应的安全措施。

D.2.5.2.4 应描述 ADS 系统故障可能引起的整车安全风险及对应的安全措施。

D.2.5.2.5 应描述自动驾驶功能不足可能引起的整车安全风险（如由于对车辆环境感知不足导致的风险、可合理预见的误用）及对应的安全措施。

D.2.5.2.6 应描述车辆制造商推导行为能力和 ODD 相关场景的方法。

示例：基于功能不足和触发条件分析的方法。

D.2.5.2.7 应描述场景识别与生成的方法，并说明该方法如何符合以下要求：

- a) 涵盖适当的标称、风险及失效等场景；
- b) 采用数据驱动、知识驱动、随机方法等方式系统性地识别危害事件及其他安全相关事件；

示例：数据驱动方法如已有场景或事件数据集等，知识驱动方法如行业标准、最佳实践、专家经验、推演等，随机方法如随机场景抽样等。

- c) 涵盖 ODD 内体现实际交通状况的要素（尤其是动态要素）；

- d) 涵盖所有相关场景要素的已识别特征和行为。

D.2.5.2.8 应描述车辆制造商的场景选择方法，该方法应覆盖 ADS 会遇到的以下可合理预见的场景及条件：

- a) 充分选取了需要触发 ADS 后援响应的场景（例如，接近 ODD 边界）；
- b) ADS 不可预防的场景（例如，与 ORU 的不安全行为或基础设施故障相关的）；

示例：如 ORU 切入、横穿等不安全行为；道路施工、红绿灯故障等基础设施故障。

- c) 在选择具体场景时，使用适当的技术来探索参数空间。

示例：通过数据统计、随机生成方法。

D.2.5.2.9 应说明所定义的 ODC 场景条件的代表性。

### D.2.5.3 详细整车层面的安全分析

车辆制造商应具有详细整车层面的安全分析以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

### D.2.5.4 系统层面的安全分析总结

D.2.5.4.1 车辆制造商应提交系统层面的安全分析总结，且符合 D.2.5.4.2 至 D.2.5.4.5 的要求。

D.2.5.4.2 应描述 ADS 系统架构层级要素、要素的功能、要素的潜在安全相关失效模式及失效影响（含系统层面和整车层面）。

D.2.5.4.3 应描述针对系统要素失效建立的安全机制，并说明其有效性。

D.2.5.4.4 应描述系统架构要素的功能不足、触发条件及系统/整车层面安全影响。

D.2.5.4.5 应描述针对功能不足及触发条件建立的安全措施，并说明其有效性。

#### D.2.5.5 详细系统层面的安全分析

车辆制造商应具有详细系统层面的安全分析以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

#### D.2.6 验证确认计划和结果

##### D.2.6.1 一般要求

D.2.6.1.1 车辆制造商应提交验证确认计划和结果。其中，功能安全验证确认计划和结果应符合 D.2.6.2，预期功能安全验证确认计划和结果应符合 D.2.6.4。

D.2.6.1.2 应描述车辆制造商如何确定适合的过程、资源和专业人员，以实现以下内容：

- a) 设计和执行试验，用于提供支撑 ADS 安全档案的证据；
- b) 选择用于场地试验的场景，由静态和动态元素组成，用于正确复现真实交通场景；
- c) 识别道路试验的试验路线，包含 ODD 可预见的相关元素（例如，道路类型和拓扑结构）、标称场景中的相关元素（例如，ORU、交通标识、交通信号）及典型的动态条件（例如，拥挤/稀疏的交通流）。

注：道路试验的试验路线也能用于标称场景中对人机交互的试验验证，包括从ODD外到在ODD内以及从ODD内到超出ODD的情况。

- d) 评估 ADS 在每个场景下的 DDT 执行是否符合行为能力要求；
- e) 评估 ADS 能力以保障用户安全及 ADS 的使用安全。

##### D.2.6.2 功能安全验证确认计划和结果总结

D.2.6.2.1 车辆制造商应提交整车层面和系统层面的验证确认计划和结果，说明对影响表 D.1 中安全目标的所有危害和故障，进行了验证和确认。验证确认应基于硬件在环测试、实车测试或其他适当的方法。

注：系统层面的范围，包括实现系统功能的传感器、控制器、执行器相关接口及处理部分。

D.2.6.2.2 功能安全验证和确认计划总结应包含以下信息：

- a) 准则和目标，并解释如何选择验证及确认的场景；
- b) 验证准则的评估方法；
- c) 为选择的验证准则提供合理说明；
- d) 包含证明目标被达成的证据的验证及确认结果（例如，验证准则符合接受准则）。

D.2.6.2.3 车辆制造商应提交系统层面的验证计划和结果总结，说明对所有影响系统功能安全概念的系统内部故障、外部接口故障及安全措施的有效性进行了验证。至少包括：

- a) 验证对象，例如车辆型号、系统名称、软件和硬件版本等；
- b) 验证目的，例如验证功能安全概念是否得到充分实现；
- c) 验证方法及步骤概述（若通过测试开展验证，还需说明测试设备、测试环境）；
- d) 接受准则；
- e) 验证结果概述。

D.2.6.2.4 车辆制造商应具有详细系统层面的验证计划和结果以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

D.2.6.2.5 车辆制造商应提交整车层面的验证确认计划和结果总结，说明对所有影响表 D.1 中安全目标及功能安全概念的跨系统/组件集成结果、跨系统/组件接口故障及安全措施的有效性进行了验证，对

安全目标的充分性及达成效果进行了确认，至少包括：

- a) 验证和确认对象，如车辆型号、系统名称、软件和硬件版本等；
- b) 验证和确认目的，如验证系统与整车其他相关系统的安全交互要求，确认安全目标正确、完整且得到充分实现；
- c) 验证和确认方法及步骤概述（若通过测试开展验证或确认，还需说明测试设备、测试环境）；
- d) 接受准则，包括安全度量、其他接受准则（如有）；
- e) 验证和确认结果概述。

#### D. 2. 6. 3 详细功能安全验证确认计划和结果

车辆制造商应具有详细整车层面的验证确认计划和结果以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

#### D. 2. 6. 4 预期功能安全验证确认计划和结果总结

D. 2. 6. 4. 1 预期功能安全验证和确认计划总结应包含以下信息：

- a) 验证准则和确认目标：
  - 1) 解释如何选择验证及确认的场景，以保证合理覆盖 ODC 及其边界；
  - 2) 确定 ODC 合理覆盖度的方法、度量指标和目标；
  - 3) 依照 D.2.3.2 定义的验证的准则和确认目标；
- b) 验证准则的评估方法；
- c) 为选择的验证准则提供合理说明；
- d) 包含证明目标被达成的证据的验证及确认结果（例如，验证准则符合接受准则）。
- e) 防止 ADS 或自动驾驶功能退役后被重新激活的策略。
- f) 验证对象，如车辆型号、系统名称、软件和硬件版本等；
- g) 验证和确认方法及步骤概述（若通过测试开展验证或确认，还需说明测试设备、测试环境）；
- h) 根据预期功能安全验证确认计划，确定了适合的验证确认过程、资源和专业人员。

D. 2. 6. 4. 2 应确认残余风险接受准则的达成，及试验里程与系统预期运行场景具有相同或高度相似的场景分布。

D. 2. 6. 4. 3 应采用合适的方法，开展针对 ADS 的验证和确认（例如，试验、数据驱动、分析评审等方法）。

D. 2. 6. 4. 4 试验应作为验证和确认的主要方法之一，可采用仿真试验、场地试验、道路试验等适用方法。若无法通过试验获得足够的证据，或通过试验难以符合验证和确认的全部要求时，应补充采用其他适用的方法。

示例：仿真试验中的场景生成可以使用数据回灌、数据生成等方法。

注1：数据驱动与试验相结合，以进行验证和确认。

注2：分析评审与分布式开发活动结合，以评估不可测/难测部分是否影响残余风险接受准则。

注3：若采用道路试验开展验证和确认活动，在确保交通安全的情况下，按照预期运行场景选定试验条件。

D. 2. 6. 4. 5 对于场地试验，应对静态及动态的场景元素进行选择 and 组合，用于正确复现试验场景。

D. 2. 6. 4. 6 应根据不同的风险类型或场景类型对残余风险确认目标进行分解，针对性选择合适的验证和确认方法。

注1：在符合可信度和等效性的基础上，按一定比例分配仿真试验和实车试验的目标及试验量。

注2：若采用仿真试验方法开展验证和确认活动，对试验目标及等效试验的里程或时长的合理性进行论证。

D.2.6.4.7 对于影响安全的变更，应制定回归策略，确定是否需要重新开展全部或部分验证和确认活动。

注：对于回归策略，进行文档化和追溯管理，通过评审确保其合理性和有效性。

D.2.6.4.8 验证和确认试验所使用的仿真工具链、实车测量设备、试验车辆等应符合安全验证和确认的相关要求。

注：若采用仿真试验方法开展验证和确认活动，选择合适的仿真试验工具链，以确保试验的准确性、结果的可信度及一致性。

D.2.6.4.9 对于通过数据驱动手段进行验证和确认的情况，应采用合适方法（例如，数据监测、影子模式等）。

注1：若通过构建基于场景或事件触发的数据监测和回流机制，进行不同场景或事件下的残余风险评估。

注2：若单独使用影子模式或与仿真试验相结合的方法，进行危害场景的风险评估与复测，对方法的有效性和可信度进行说明。

注3：若基于影子模式开展验证和确认活动，存在必要的机制以避免对ADS的正常工作产生干扰。

D.2.6.4.10 通过数据驱动手段进行验证和确认，应说明相关数据链路需符合的要求，包括数据采集、数据处理、数据传输、数据标注、数据挖掘等活动。

D.2.6.4.11 车辆制造商应提交预期功能安全验证确认结果总结，根据系统和整车层面开展的预期功能安全验证确认活动，以验证已知危害场景相关的功能不足已被优化改进或已被安全措施有效的覆盖，并证明已知和未知危害场景中的残余风险以足够的置信度符合接受准则，至少包括：

- a) 对已知危害场景的验证结果总结；
- b) 对已知和未知危害场景的残余风险确认结果总结。

D.2.6.4.12 应基于 D.2.5 对于触发条件的分析结果（至少涵盖表 D.2 中的触发条件），对于可能引发系统违背接受准则的触发条件及其组合，进行充分的已知危害场景的验证和确认。

注1：根据ADS的ODC定义、场景及触发条件发生的频次、严重度和相关性等因素，定性或定量地开展场景验证的重要度排序，参考GB/T 43267—2023中表B.5和表B.6的优先度子集方法。

注2：在进行危害场景生成时，考虑对ODC内、ODC边界的覆盖，根据不同触发条件类型，基于数据驱动或知识驱动，进行不同类型的场景覆盖度的定性或定量评估。

表D.2 触发条件列表

触发条件类别		触发条件	适用设计运行范围	适用自动驾驶功能类型
环境	天气	雨、雪、雾、沙尘、雾霾	任何道路	3级自动驾驶功能、4级自动驾驶功能
	光照	一天中的时间（清晨、白天、傍晚、夜晚）、光照变化（逆光、强光照、光照突然变化）	任何道路	
交互	道路类型	弯道、匝道、隧道、坡道	任何道路	
		道路交叉口、环岛	除高快速道路外的其他道路	
	道路标记	没有车道标记、断线、变浅的车道标记、有变化的多车道标记（多变少、少变多）	任何道路	
	道路设施	施工区域、交通指示灯、道路交通标志	任何道路	
		龙门架、收费站	高快速道路	



		限高架	除高快速道路外的其他道路	
	目标物类型	机动车、行人、摩托车、动物、临时障碍物（如掉落物品）、异形目标物（如洒水车、路障车等异形车辆）、低对比度目标物（如深色车辆在阴影中）	任何道路	
		自行车、电动二轮车、异形目标物（如撑伞行人、披雨衣/斗篷电动二轮车等）	除高快速道路外的其他道路	
	目标物状态	直立静止、运动、侧翻、斜置	任何道路	
	多目标物交互	遮挡、横穿、并行、对向行驶、切入、切出、紧急制动	任何道路	
用户误用		误激活、激活后误用、不接管、误接管、误退出	任何道路	

**D. 2. 6. 4. 13** 应采用适当方法进行已知危害场景的残余风险确认。对于不能接受的已知危害场景及对应的功能不足，制定并实施风险缓解措施，直至残余风险降低到合理水平。

注：根据已知危害场景的发生概率、严重度、涉险人员的可控性（如适用），评估对达成总体残余风险接受准则的影响。

**D. 2. 6. 4. 14** 已知危害场景的残余风险确认和结果认可，应判断是否符合下列条件：

- a) 已知场景导致危害行为的风险不会导致违背总体残余风险接受准则；
- b) 不存在可能导致特定道路使用者（包括用户和 ORU）面临不合理风险的已知危害场景。

注：对于短期无法修复的风险场景及对应的功能不足，通过适当措施避免不合理风险（例如，基于地理位置限制自动驾驶功能的使用）。

**D. 2. 6. 4. 15** 应对 ADS 在未知危害场景中的残余风险进行确认，以确保具有足够的置信度符合残余风险接受准则，并符合确认目标。

注1：每次ADS发生变化（例如，算法变化、驾驶策略变化、ODC变化、目标和事件探测与响应策略变化、车型变化）时，都可能带来新的未知危害场景，因而需要重新评估残余风险。

注2：识别未知危害场景的方法如真实世界数据挖掘、影子模式、场景泛化/合成/生成、专家经验、极端和边缘场景挖掘、场景敏感度分析、用户使用研究等。

**D. 2. 6. 4. 16** 对基于里程累积测试的未知危害场景残余风险确认，应根据预期运行场景选择路线，包含 ODD 可预见的相关元素（例如，道路类型和拓扑结构）、标称场景中的相关元素（例如，ORU、交通标识、交通信号）及典型的动态条件（例如，拥挤/稀疏的交通流），进而通过道路试验（例如，车辆长期测试、车队道路测试）等方式进行确认。

注：由于真实世界中未知危害场景的随机分布特性，开展统计学的分析和论证以支持基于里程的确认。

#### D. 2. 6. 5 详细预期功能安全验证确认计划和结果

车辆制造商应具有详细预期功能安全验证确认计划和结果以备查，并提供相关的企业名称、文件名、版本、状态、日期、储存位置等基本信息。

#### D. 2. 7 安全评估发布报告总结

车辆制造商应提交安全评估发布报告总结，评估所有安全相关活动实现情况，以及每项工作成果的完整性、正确性和一致性，评估安全验证和确认活动中对系统预期运行场景的覆盖性、残余风险与接受准则的符合性，应包括：

- a) ADS 在每个测试场景下的 DDT 执行是否符合行为能力（危害行为接受准则）的要求的评估；
- b) 考虑全部功能安全和预期功能安全活动中识别的风险后，ADS 能力是否足以保障用户安全及 ADS 的使用安全，总体残余风险是否符合接受准则的评估；

注：功能安全方面评估系统实现了安全目标，且无导致违背安全目标的问题或存在的问题风险可接受。

- c) 功能安全和预期功能安全评估发布的结论；
- d) 运行阶段的功能安全和预期功能安全监测及保障措施总结，以有效识别系统运行阶段的残余风险，并针对不合理的残余风险问题及时实施保障措施。

### D.3 声明、论据和证据

#### D.3.1 一般要求

##### D.3.1.1 安全档案应包括一系列声明，至少应：

- a) 每项声明至少有一项论据支持；
- b) 每项论据至少有一项证据支持；
- c) 每项声明、论据和证据应有唯一的标识。

注：一项证据可能支持不止一项论据。

##### D.3.1.2 以下要求均应至少对应一项声明：

- a) D.3.1.3 涉及章节中规定的各项要求；
- b) D.3.1.4、D.3.1.5 规定的各项要求；
- c) 车辆制造商自行规定的各项要求（如有）。

注：若一项宽泛的声明不充分或需要额外的解释，则可能创建多项子声明，只要子声明符合逻辑连贯性且声明间的关系说明在总结文档中被包括。

##### D.3.1.3 声明、论据和证据应易被理解、符合逻辑、正确和稳健，并证明：

- a) ADS 对用户及 ORU 不会造成不合理的风险；
- b) ADS 符合本文件的以下要求：
  - 1) DDT 执行要求（5.1）；
  - 2) 人机交互要求（5.2）；
  - 3) 用户告知要求（5.3）；
  - 4) 其他要求（5.4）。

##### D.3.1.4 声明、论据和证据应描述如何将 SMS（6.1）应用于 ADS 全生命周期的安全管理。

##### D.3.1.5 声明、论据和证据应证明所采用的试验方法适用于安全档案以及性能或功能要求的符合性证明。

##### D.3.1.6 声明、论据和证据应提供以下总结信息：

- a) 确定声明及其支持论据和证据之间关系；
- b) D.3.1.2 涉及的每项要求都被识别且符合。

##### D.3.1.7 与声明、论据和证据相关的各项相关假设均应说明。

##### D.3.1.8 支持声明的每项论据都应提供背景信息和支持信息，解释如何根据一系列适当的证据符合声明。

##### D.3.1.9 支持论据的证据应包括试验结果或分析（例如，系统布局及示意图、图片、所需文档等）。

#### D.3.2 生成证据的试验活动要求

### D.3.2.1 生成证据的试验条件要求

D.3.2.1.1 用于生成证据的仿真试验条件应符合 6.2.1 的要求，安全档案中的仿真试验条件描述应至少包括：

- a) 仿真试验的预期用途及其在整体试验方案中的作用；
- b) 考虑 6.2.1.7 要求的关键性分析结果，以提供支撑安全档案的证据并用于评估 ADS 是否符合功能要求或用户要求；
- c) 仿真工具链及其组件；
- d) 仿真工具链的限制、假设以及可能影响结果的不确定性来源（6.2.1.5）；
- e) 仿真工具链的适用范围（6.2.1.6）；
- f) 确认仿真工具链的方法（6.2.1.9.7）；
- g) 验收试验（6.2.1.9.3）和验收准则（6.2.1.9.4），用于确认仿真工具链能生成支撑安全档案所需的证据（6.2.1.9.2、6.2.1.9.8）。

D.3.2.1.2 用于生成证据的场地试验条件应符合 6.2.2 的要求，安全档案中的场地试验条件描述应至少包括：

- a) 预期用途及其在整体试验方案中的作用；
- b) 体现 ODC 和预期运行工况的静态和动态元素。

D.3.2.1.3 用于生成证据的道路试验条件应符合 6.2.3 的要求，安全档案中的道路试验条件描述应至少包括：

- a) 预期用途及其在整体试验方案中的作用；
- b) 所选试验路线及其路线选择策略。

### D.3.2.2 生成证据的试验场景及其管理的要求

D.3.2.2.1 用于得出与 ADS 的 ODC 及安全档案相关的 ADS 行为能力采用的过程应适当。

D.3.2.2.2 识别和生成场景的方法应符合 D.2.5.2.7 的要求。

D.3.2.2.3 生成和识别的场景集应适用于证明安全档案并能涵盖 ADS 在实际运行中可能遇到的可合理预见的场景和条件。作为支持安全档案的证据所选择的场景集应至少包括以下内容：

- a) 触发 ADS 后援响应的场景（例如，不符合 ODC）；
- b) 可合理预见且不可预防的场景（例如，ORU 的不安全行为或基础设施故障）。

D.3.2.2.4 选择具体场景时应采用适当的技术来探索参数空间。

### D.3.2.3 生成证据的试验过程的要求

D.3.2.3.1 生成证据的试验过程应符合 D.2.6.1.2 的要求。

D.3.2.3.2 生成证据的试验过程应适当且符合以下要求：

- a) 识别需要采用不同试验方法开展试验的场景；
- b) 验证所采用的不同试验方法之间试验结果的一致性。

### D.3.2.4 试验结果的要求

D.3.2.4.1 试验结果应包括适当的验收准则。

注：试验结果可能单独提供或汇总提供。

D.3.2.4.2 试验结果应能证明 ADS 在执行 DDT 时的行为能力，至少证实了安全档案中以下情况的声明和论据：

- a) 在标称场景、风险场景和失效场景下；

- b) 从符合到不符合 ODC 时；
- c) 在无法避免与 ORU 发生碰撞的情况下。

D.3.2.4.3 每项试验应包括足够的信息，或以可根据要求复现的方式记录（例如，相同的软件/硬件版本、相同的工具版本、相同的场景、相同的参数等）。为便于复现该证据，车辆制造商应为必要的工具和分析软件提供获取和执行条件。

#### D.3.2.5 试验证据的要求

D.3.2.5.1 试验证据应来源于经过充分描述的仿真试验、场地试验和道路试验的组合，并表明试验方法间结果的一致性。

D.3.2.5.2 仿真试验证据应至少包括风险场景及低概率事件。风险场景应至少包括可能导致碰撞的场景。

D.3.2.5.3 场地试验证据的场景中应至少包括可导致碰撞的风险场景。

D.3.2.5.4 道路试验收集的证据应至少符合：

- a) 涵盖 ADS 在实际运行中可能遇到的各种场景和条件，覆盖预期运行的道路类型；
- b) 若 ADS 在道路试验过程中遇到风险场景或失效场景，结合场地试验和仿真试验的结果考虑 ADS 的响应，包括与标称场景下 DDT 执行要求的任何差异。

D.3.2.5.5 与交互相关的特定试验用例应符合：

- a) 参与试验的人群能够代表预期的用户群体以及 ORU 群体（如适用）；
- b) 所获数据结果具备统计显著性。

#### D.4 车辆制造商安全档案内审要求

D.4.1 作为符合6.1.4的要求的部分证明，车辆制造商应在型式批准之前评审其安全档案。

注：建议在开发过程中实现。

D.4.2 内审员应保持独立性，不应受任何可能威胁其公正客观评审安全档案能力的影响。

注：内审员可能是车辆制造商的内部或外部人员。

D.4.3 内审应被记录、可供查验，包括：

- a) 内审员或内审团队的资格；
- b) 内审日期或周期；
- c) 被内审的安全档案、工具和 ADS 的版本；
- d) 用于内审安全档案的方法；
- e) 任何可复现的证据清单；
- f) 已识别的偏差项、问题、置信度较低的部分或尚不明确的部分。

D.4.4 车辆制造商应在每次内审后合理的时限内，将针对所发现问题的整改或完善措施（例如，版本发布说明）纳入内审文档。

## 参 考 文 献

- [1] GB/T 34590—2022 道路车辆 功能安全（所有部分）
  - [2] GB/T 40429—2021 汽车驾驶自动化分级
  - [3] GB/T 43267—2023 道路车辆 预期功能安全
-