

智能汽车驾驶系统通用功能技术规范

1 范围

本文件规定了智能驾驶系统的术语和定义、功能描述、功能技术要求、预期功能安全技术要求、功能安全技术要求和信息安全技术要求。

本文件适用于整备质量不超过3500kg的载客车辆（M1，N1），其他车辆可参考执行。

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 39265—2020 道路车辆 盲区监测（BSD）系统性能要求及试验方法

GB/T 39323—2020 乘用车车道保持辅助（LKA）系统性能要求及试验方法

GB/T 39901—2021 乘用车自动紧急制动系统（AEBS）技术要求及试验方法

GB/T 34590 道路车辆 功能安全 第1-12章

GB 17675 汽车转向系 基本要求

ISO 15622 智能运输系统 自适应巡航控制系统 性能要求和试验规程（Intelligent transport systems—Adaptive cruise control systems—Performance requirements and test procedures）

ISO 21448 道路车辆 预期功能安全（Road vehicles—safety of the intended functionality）

ISO SAE 21434 道路车辆 信息安全工程（Road vehicle cybersecurity engineering）

ISO TR4804 道路车辆 自动驾驶系统的安全和网络安全、设计、验证和确认（Road vehicles—Safety and cybersecurity for automated driving systems—Design, verification and validation）

C-NCAP 2021版 中国新车评价体系

C-IASI 2020版 中国保险汽车安全指数

3 术语和定义

下列术语和定义适用于本文件。

3.1 行车系统

3.1.1

安全距离 safe distance

后方车辆为了避免与前方车辆发生意外碰撞而在行驶中与前车所保持的必要间隔距离。

3.1.2

横向距离 crosswise distance

车辆后轴中心点在地面投影点到车道线边线的垂直间距。

3.1.3

目标车辆 objective vehicle

与本车同向、同路，并在本车前方行驶的车辆。

3.1.4

路径曲率 path curvature

道路曲线某点切线方向对弧长的转动率。

3.1.5

预计碰撞时间 estimated time of collision

被试车辆与目标之间的距离除以被试车辆与目标瞬间相对车速所得出的时间。

3.1.6

车间时距 Time to collision

对于同向行驶的两连续车辆，前车尾与后车头通过道路某截面的时间间隔 t ， $t=c/v$ 。

3.1.7

稳定状态 steady state

相关参数不随时间、距离等变化的车辆运动状态。

3.1.8

车道 lane

驾驶员不需改变行驶路径的没有任何固定障碍物干扰的行驶区域。

3.1.9

设定车速 setting speed of vehicle

由驾驶员或其他控制系统设定的期望行驶速度 V_{set} ，亦即车辆在系统控制下的最高期望速度。

3.2 泊车系统

3.2.1

摄像头 camera

将周边景象转化为图像传输的影像输入设备。标清摄像头：30万像素；高清摄像头：百万级像素。

3.2.2

视场角 field of view

在光学仪器中，以光学仪器的镜头为定点，被测目标的物像可通过镜头的最大范围的两条边缘构成的夹角为视场角。视场角分为水平视场角（HFOV）和垂直视场角（VFOV）。

3.2.3

信噪比 signal to noise ratio; SNR

视频信号的大小与噪声信号（无用信号）大小的比例，以dB为单位，见公式（1）。

$$\text{SNR (dB)} = 20\lg (\text{Si/Ni}) \cdots \cdots \cdots (1)$$

式中：

Si——色块i的信号（平均像素亮度值）

Ni——色块i的噪声值（像素亮度值的标准差）

3.2.4

低照度 minimum illumination

当被摄景物的光亮度低到一定程度而使摄像机输出的视频信号低到某一规定值时的景物光亮度值。

3.2.5

动态范围 dynamic range

摄像设备能够记录的从最黑到最白之间的最大影调范围，动态范围越大说明拍摄的影像层次越分明，所有超出动态范围之外的曝光值都只能记录为黑或白。

注：动态范围实际上描述摄像设备记录影像灰阶的能力，可用灰阶测试图卡的灰阶级数表达。

3.2.6

灰阶 gray scale

摄像设备对不同光谱特性或等效光谱特性的灰度分辨能力。通常用拍摄灰阶图卡来测试。

3.2.7

全景环视主机 around view module

处理摄像头输入的图像数据，并以视频格式数据传递给设备的图像处理和控制单元。全景影像主机分为两类：系统单元和导航主机集成模组。

3.2.8

超声波传感器 ultrasonic sensor

通过超声波测量周围障碍物距离信息的输入设备。

3.2.9

标准测试杆 standard test pole

测试超声波监控范围时用于模拟障碍物的白色PVC杆，包括垂直标准测试杆和水平标准测试杆。垂直标准测试杆是指垂直放置的直径75mm，长度为1000mm的白色PVC杆。水平标准测试杆是指水平放置的直径为75mm，长度为3000mm的白色PVC杆。

3.2.10

最远探测距离 maximum detection range

监控范围内，超声波传感器能连续探测到车辆宽度2/3范围内的垂直标准测试杆的最远距离。

3.2.11

横向间距 lateral distance

自车车辆靠停车位一侧的前后轮轮胎最外侧接地点与车位外边界的距离，不含两车后视镜。

3.3 功能安全

3.3.1

安全目标 safety goal; SG

作为整车层面危害分析和风险评估结果的最高层面的安全要求。

3.3.2

功能安全要求 functional safety requirement; FSR

指定定义独立于具体实现方式的安全行为，或独立于具体实现方式的安全措施，包括安全相关的属性。

3.3.3

技术安全要求 technical safety requirement; TSR

为实现相关的功能安全要求而得出的要求。

3.3.4

故障容错时间间隔 fault tolerant time interval; FTTI

在安全机制未被激活情况下，从相关项内部故障发生到可能发生危害事件的最短时间间隔。

3.3.5

安全措施 safety measure

用来避免或控制系统性失效，探测或控制随机硬件失效，或减轻他们有害影响的活動或技术解决方案。

3.3.6

安全机制 safety mechanism

为了保持预期功能或者达到/保持某种安全状态，由电气/电子系统的功能/要素或者其他技术来实施的技术解决方案，以探测并减轻/容许故障、或者控制/避免失效。

3.3.7

汽车安全完整性等级 Automotive Safety Integrity Level;ASIL

用于定义相关项或要素需要满足的GB/T 34590中的要求和安全措施，以避免不合理的风险，其中，D代表最高严格等级，A代表最低严格等级。

3.3.8

可控性 controllability

通过所涉及人员的及时反应（可能具备外部措施的支持）避免特定的伤害或者损伤的能力。

3.3.9

严重度 severity

对潜在危害事件中可能发生的一个或多个人员的伤害程度的预估。

3.3.10

安全状态 safe state

相关项在失效的情况下，没有不合理风险的运行模式。

3.4 预期功能安全**3.4.1****预期功能 intended functionality**

为系统指定的行为，指定的行为是项目的开发者认为是标称（即无故障）功能的行为，由于所使用的组件和技术的固有特性而导致其能力限制。

3.4.2**情景 scene**

环境的快照，包括风景、动态元素、所有演员和观察者的自我表现，以及这些实体之间的关系。

3.4.3**场景 scenario**

指在特定时间空间内发生的行动，或者因车辆与人物关系构成的具体画面，是通过车辆或人物行动来表现发展关系的一个个特定过程。

3.4.4**情境 situation**

在特定时间点选择适当的行为模式。

3.4.5**误用 misuse**

人类以系统制造商不希望的方式使用系统。

3.4.6**触发事件 triggering event**

驾驶场景的特定条件，作为后续系统反应的引发剂，可能导致危险事件。

3.5 信息安全**3.5.1****资产 Asset**

具有价值或对价值有贡献的物体。

注：一项资产有一个或多个网络安全属性，其妥协可能导致一个或多个损害情况。

3.5.2**攻击可行性 Attack feasibility**

实现威胁场景的蓄意行动集。

3.5.3**攻击路径 Attack path**

实现威胁场景的蓄意行动集。

3.5.4

攻击者 Attacker

执行攻击路径的个人、团体或组织。

3.5.5

网络安全目标 Cybersecurity goal

与一个或多个威胁情景相关的概念级网络安全要求。

3.5.6

损害情况 Damage Scenario

涉及车辆或车辆功能并影响道路使用者的不良后果。

3.5.7

渗透测试 Penetration Test

网络安全测试，模拟真实世界的攻击，以确定破坏的方式。

3.5.8

威胁情况 Threat Scenario

一个或多个资产的网络安全属性受到损害的潜在原因，以实现损害情况。

3.5.9

脆弱性 Vulnerability

可作为攻击路径的一部分被利用的弱点。

4 缩略语

下列缩略语使用于本文件。

RVC 倒车监视系统 (Rear View System)

HMI 人机交互界面 (Human Machine Interface)

LVDS 低压差分信号 (Low-Voltage Differential Signaling)

AVM 全景环视系统 (Around View Monitor)

EMS 发动机控制单元 (Engine Management System)

TCU 变速器控制单元 (Transmission Control Unit)

VCU 适用于电动汽车 (vehicle Control Unit)

ESP 车身稳定系统 (Electronic Stability Program)

APA 自动泊车系统 (Auto Parking Assist)

EPS 转向系统 (Electronic Power Steering)

APP 手机连接终端 (Application)

BLE 蓝牙模块 (Bluetooth Low Energy)

5 智能驾驶系统功能描述

5.1 行车系统功能描述

5.1.1 自动紧急制动（AEB）

自动紧急制动系统通过对正前方环境的监测，当存在碰撞风险时，通过光学和声音报警提示驾驶员做出反应，当驾驶员制动过晚、制动力太小或完全没有反应时协助驾驶员制动以避免或减轻事故危害，提高行驶安全性。AEB的系统框图见图1。

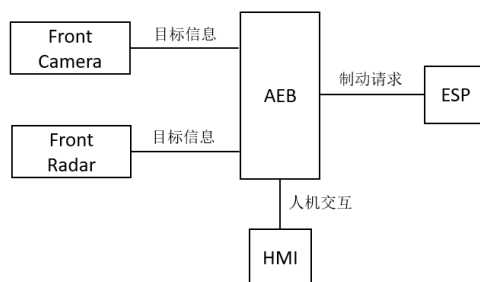


图1 AEB的系统框图

5.1.2 后碰撞预警制动（RCW）

在即将发生碰撞之前，后碰撞预警功能激活双闪以较高频率闪烁，从而吸引后方驾驶员的注意力。如果此时车辆静止，为了减少对车内乘客的伤害以及二次碰撞，执行制动。RCW的系统框图见图2。

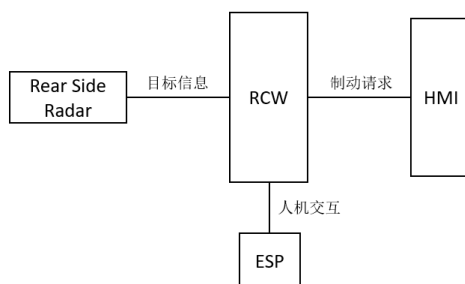


图2 RCW的系统框图

5.1.3 车道保持辅助（LKA）

通过驾驶辅助传感器实时的监控前方道路车道线情况，一旦发生无意识的车道偏离，通过电动助力转向系统辅助车辆返回本车道；当系统无法控制车辆维持在本车道时，则发出报警信息以触发车辆报警。LKA的系统框图见图3。

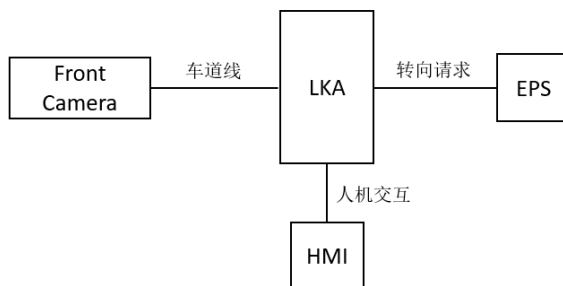


图3 LKA的系统框图

5.1.4 规避操作辅助（EMA）

在高速情况下，遇到AEB无法完成避撞风险的情况，且此时可以通过转弯避免，在驾驶员打转向无法完成完全避撞的情况下，辅助驾驶员完成转向避撞，同时通过仪表盘提醒用户。EMA的系统框图见图4。

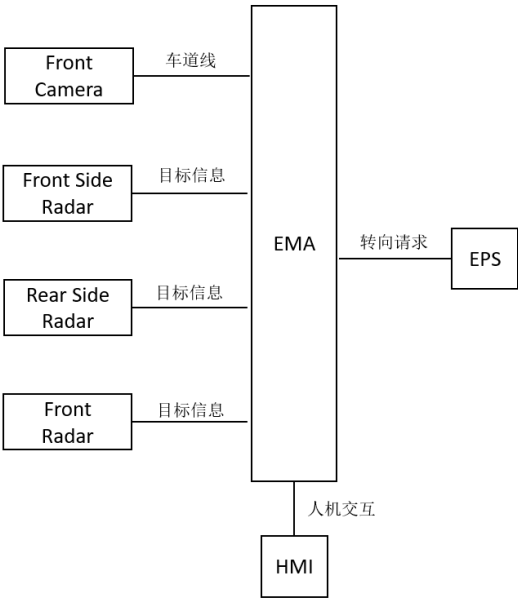


图4 EMA的系统框图

5.1.5 后方横穿交通辅助（RCTA&RCTB）

后方侧向辅助功能帮助驾驶员从停车点驶出，在驾驶员视野受阻的情况下，**当侧方来车时**，驾驶员应该被警示，如果碰撞风险很高，将执行制动，使车辆静止。如果经过的行人能够被探测到的话，RCTA也会执行报警和制动。RCTA只有在车辆在倒退或倒挡的时候被激活。RCTA&RCTB的系统框图见图5。

注：RCTA 是只有报警功能，RCTB 对应报警的同时带制动功能。

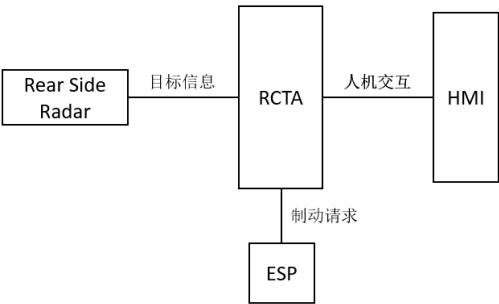


图5 RCTA&RCTB的系统框图

5.1.6 开门预警（DOW）

开门预警功能旨在阻止当驾驶员或乘客打开车门时，没有注意到后方来车从而发生碰撞。后传感器应该能够探测到相邻车道的从后方靠近的目标，从而提醒驾驶员不要打开车门。DOW的系统框图见图6。

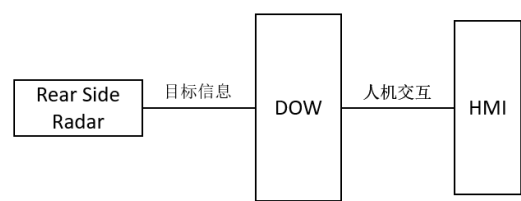


图6 DOW的系统框图

5.1.7 前方横穿交通辅助（FCTA&FCTB）

前方交叉路口预警在车辆向前行驶时能帮助驾驶员在低能见度情况下向前驶出停车位或经过交叉路口，当存在碰撞风险时，提示驾驶员做出反应，当驾驶员制动过晚、制动力太小或完全没有反应时协助驾驶员制动以避免或减轻事故危害，提高行驶安全性。FCTA&FCTB的系统框图见图7。

注：FCTA 定义功能为只有报警，FCTB 定义功能为报警的同时带制动。

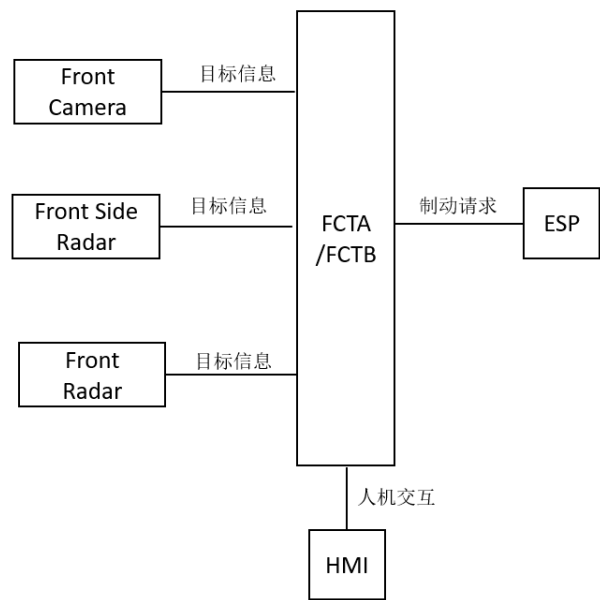


图7 FCTA&FCTB的系统框图

5.1.8 自适应巡航 ACC

自适应巡航可以实现车辆纵向控制的半自动化，是定速巡航功能的扩展。驾驶员通过设定巡航速度和车间时距在一定工作车速内实现定速控制和跟车控制：

定速控制：在没有前车情况下，自适应巡航按照驾驶员设定车速进行控制；

跟车控制：当有前车且前车车速低于设定车速时，跟随前车保持设定车间时距。

ACC的系统框图见图8。

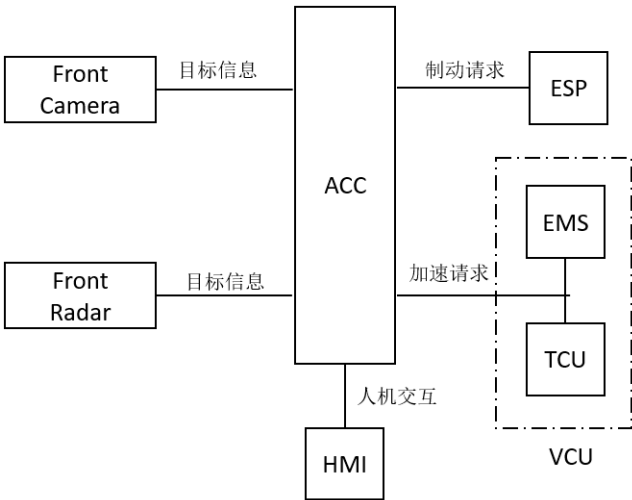


图8 ACC的系统框图

5.1.9 智慧巡航（ICC）

智能领航(ICC)是一项集车道保持，自适应巡航等功能为一体的驾驶辅助功能。可以同时的车辆进行巡航控制和方向辅助控制。系统可以根据设定车速和跟车车间时距控制自车的车速，根据左右两侧的车道线或者跟随前车进行方向盘辅助控制，脱手报警提示，全程需要驾驶员手握方向盘以便在必要时及时接管车辆。ICC的系统框图见图9。

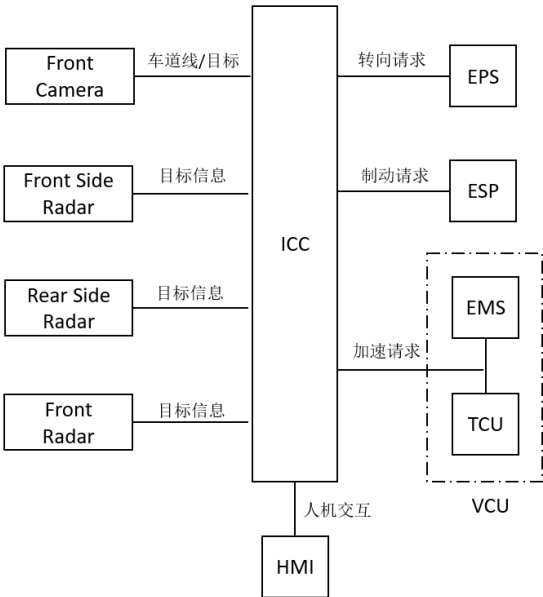


图9 ICC的系统框图

5.1.10 交通标志信息（TSI）

经过限速标志以及其它交通标志时，通过仪表盘图标提醒用户，且在超速时通过仪表盘图标闪烁以及声音报警方式提醒用户超速。TSI的系统框图见图10。

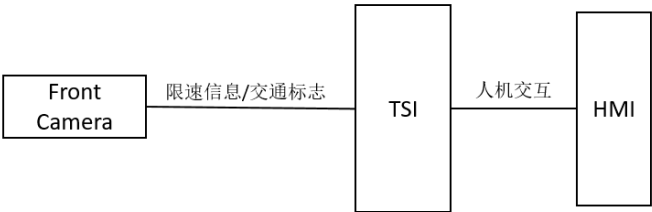


图10 TSI的系统框图

5.1.11 驾驶员状态检测（DPS）

通过摄像头采集驾驶员脸部反射的红外光去判断驾驶员是否疲劳及分心，并通过声音、光学等途径进行警示。DPS的系统框图见图11。

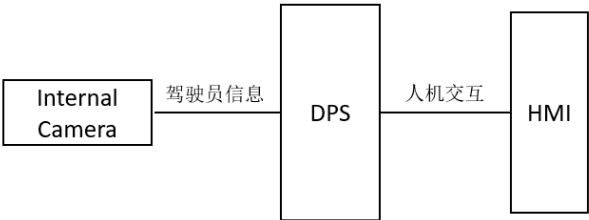


图11 DPS的系统框图

5.1.12 变道辅助（LCA）

变道辅助功能在变道时辅助驾驶员，它包括盲点监测和接近车辆报警。盲区监测（BSD）告知驾驶员在车辆盲点区域有车辆，快速来车提醒（CVW）是盲点监测的扩展，它告知驾驶员在临近车到的自车后方70m之内有车辆。这个系统是一个安全功能，对外后视镜起到增补的作用，而不是消除后视镜的需要。这个系统是一个辅助系统，并不会代替驾驶员做出操作。LCA的系统框图见图12。

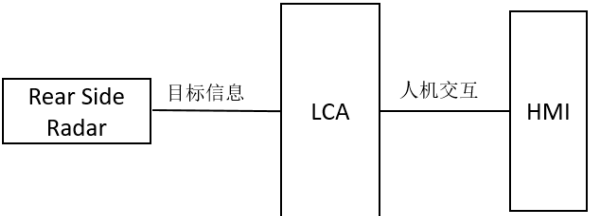


图12 LCA的系统框图

5.1.13 交通灯辅助（TLA）

道路交通灯提示功能通过前视摄像头对道路上交通信号灯的颜色及形状进行采集，通过仪表显示的方式展示给驾驶员。当交通灯颜色发生变化时，辅助声音提示。在没有交通灯的路段通过前雷达采集前车信息，在仪表上展示前车驶离的动画，提示驾驶员及时驶离。TLA的系统框图见图13。

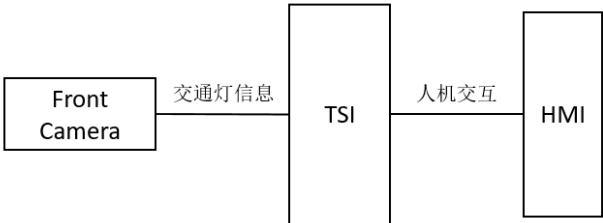


图13 TLA的系统框图

5.1.14 紧急车道保持 ELKA

通过前视摄像头和雷达识别道路边沿和相邻车道车辆有碰撞风险时，通过控制电子助力转向系统进行转向控制辅助，以便将自车控制在自车道内同时避免碰撞。ELKA的系统框图见图14。

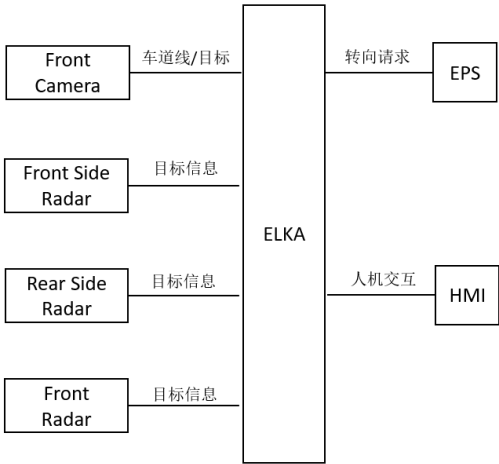


图14 ELKA的系统框图

5.2 泊车系统功能描述

5.2.1 倒车摄像头

驾驶员挂入R档时，RVC采集车辆后方的视野状况，通过LVDS视频传输至HMI，将车辆后方的道路状况提供给驾驶员，让驾驶员准确的把握车辆后方道路状况，及时规避存在的碰撞风险。倒车摄像头的系统框图见图15。



图15 倒车摄像头的系统框图

5.2.2 全景环视

通过车身前后左右4颗摄像头采集车辆周边图像，经图像拼接处理后形成一幅类似于车身上方的鸟瞰图，即：AVM。使驾驶员在HMI上可以直观的看到车辆所处位置的周围环境信息，有效的对车辆周围环境进行把控，提升低速工况下的行车安全。全景环视的系统框图见图16。

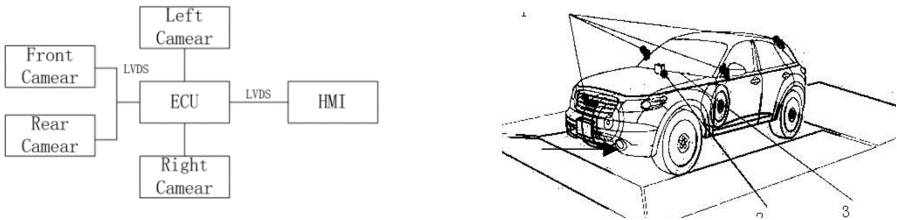


图16 全景环视的系统框图

5.2.3 超声波泊车辅助

利用超声波对障碍物的回波原理，对车辆前方/后方障碍物进行探测，并通过声音及色块的形式显示出来提醒驾驶员。超声波泊车辅助的系统框图见图17。



图17 超声波泊车辅助的系统框图

5.2.4 低速紧急制动

根据泊车辅助系统雷达传感器与摄像头探测到的障碍物融合信息，系统自动计算行驶轨迹上的碰撞风险，对车辆进行紧急制动，避免或者减轻碰撞。低速紧急制动的系统框图见图18。



图18 低速紧急制动的系统框图

5.2.5 自动泊车

自动泊车（APA）通过车辆侧边的超声波雷达或环视摄像头寻找到车位后，车辆可自主规划泊车路径，并通过控制（TCU）执行车辆的换挡，通过EMS控制车辆扭矩控制（电动车型通过VCU进行档位及扭矩控制），通过ESP控制车辆制动，通过EPS控制转向，并在HMI界面上将整个泊车过程给驾驶员提示。在遇到紧急情况时，车辆可自主刹停车辆，驾驶员也可随时干预自动泊车接管车辆。APA的系统框图见图19。

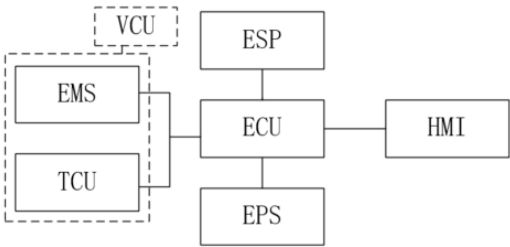


图19 APA的系统框图

5.2.6 遥控泊车

利用手机APP通过远程连接的方式，驾驶员不在车内远程遥控车辆短距离前进、后退或者完成车辆泊入车位，在遥控泊车过程中，若车辆遇到障碍物可自主刹停并提醒驾驶员车辆当前泊车状态，遇到紧急情况驾驶员也可通过手机主动中断与车辆的连接，车辆自主刹停。遥控泊车的系统框图见图20。

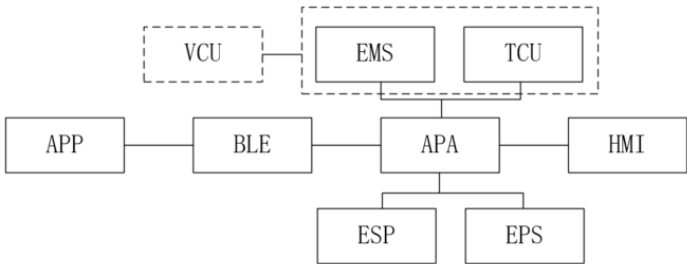


图20 遥控泊车的系统框图

6 智能驾驶系统功能技术要求

6.1 行车系统功能技术要求

6.1.1 自动紧急制动

工作目标类型：轿车、卡车、二轮车和行人。

工作车速范围：

针对移动或停止车辆目标，4km/h-150km/h；

针对静止行人：

二轮车目标，4km/h -80km/h。

驾驶员可以选择开启或关闭功能，但是功能在每个点火周期会默认开启。当功能被开启时，驾驶员可以选择开启或关闭报警，功能在车辆上电后，进行自检。自动紧急制动技术要求见表1。

表1 自动紧急制动技术要求

项目	取值
AEB/DBS 最低工作速度（静止目标）	4 km/h
AEB/DBS 最高工作速度（静止行人目标）	80 km/h
AEB/DBS 最高工作速度（运动车辆目标）	150 km/h
FCW 最低工作速度（静止目标）	30 km/h
FCW 最高工作速度（静止行人目标）	80 km/h
FCW 最高工作速度（运动车辆目标）	150 km/h
最大速度降	60 km/h
目标最小尺寸	儿童
目标类型	行人、两轮车、轿车、卡车
目标最小速度	0 km/h
误报警率	1 次每 2000 km
误预制动率	1 次每 20000 km
误全制动率	1 次每 100000 km
其他	满足 GB/T 39901 - 2021 标准

6.1.2 后碰撞预警

工作目标类型：汽车、二轮车。

工作车速范围：0-150km/h。

驾驶员可以选择开启或关闭功能，整车下线后，第一次的上电，功能默认开启。功能在车辆上电后，进行自检。后碰撞预警技术要求见表2。

表2 后碰撞预警技术要求

项目	取值
目标最小尺寸	长×宽×高：2m×0.6m×1.1m
目标最小速度	3.6 km/h
拖车模式	功能抑制
最少持续报警事件	1s
功能激活车速	$0 \leq V \leq 150 \text{ km/h (TBD)}$
功能抑制车速	$> 150 \text{ km/h}$
目标状态	非静态，相对速度 $\geq 10 \text{ km/h}$
正确报警率	$\geq 98\%$
错/误报警率	$\leq 1\%$

6.1.3 车道保持辅助

工作目标类型：车道线。

工作车速范围：60-160km/h。

驾驶员可以选择开启或关闭功能，当功能被开启时，驾驶员可以选择开启或关闭报警与报警方式，以及车道保持类型。整车下线后，第一次的上电，功能默认开启。功能在车辆上电后，进行自检。车道保持辅助技术要求见表3。

表3 车道保持辅助技术要求

项目	取值
最小工作车速	60 km/h
最大工作车速	150 km/h
安全边界内最大工作力矩	50N
最大功能工作横向加速度	3 m/s^2
工作弯道半径	$\geq 250 \text{ m}$
车道线长度	$> 2 \text{ m}$
车道线宽度	0.08-0.6m
车道线最大间距	10m
车道线颜色	白色，黄色
车道保持要求	维持在车道线内
其他	满足GB/T 39323—2020标准

6.1.4 紧急避让辅助

工作目标：汽车、二轮车、行人。

工作车速：50km/h-120km/h。

车辆每次上电，功能默认开启。功能在车辆上电后，进行自检。紧急避让辅助技术要求见表4。

表4 紧急避让辅助技术要求

项目	取值
最小工作车速	50 km/h
最大工作车速	120 km/h
最大功能工作横向加速度	3 m/s ²
最大附加横向位移	1m

6.1.5 后方横穿交通辅助

工作目标类型：汽车、两轮车、行人。

工作车速范围：R档，0-18km/h。

驾驶员可以选择开启或关闭功能，整车下线后，第一次的上电，功能默认开启。功能在车辆上电后，进行自检。后方横穿交通辅助技术要求见表5。

表5 后方横穿交通辅助技术要求

项目	取值
目标最小尺寸	长×宽×高：2m×0.6m×1.1m
目标最小速度	3.6 km/h
拖车模式	功能抑制
最少持续报警事件	1s
功能激活车速	≤15 km/h(TBD)
功能抑制车速	>15km/h
目标状态	3.6 km/h ≤ V ≤97.2 km/h
目标轨迹与自车轨迹倾斜角	≤30°
正确报警率	≥98%
错/误报警率	≤1%

6.1.6 开门预警

工作目标类型：汽车、两轮车、行人。

工作车速范围：0-5km/h。

驾驶员可以选择开启或关闭功能，整车下线后，第一次的上电，功能默认开启。功能在车辆上电后，进行自检。开门预警技术要求见表6。

表6 开门预警技术要求

项目	取值
----	----

目标位置	纵向范围：0.4m~90m 横向范围：0.4m~50m
静止目标	不报警
报警最小持续时间	1s
目标最小尺寸	长×宽×高：2m×0.6m×1.1m
目标最小速度	3.6 km/h
拖车模式	功能抑制
功能激活车速	0 km/h ≤V≤5km/h
功能抑制车速	>5km/h
功能抑制车速	>6.84km/h
正确报警率	≥98%
错/误报警率	≤1%

6.1.7 前方横穿交通辅助

工作目标类型：四轮车、两轮车、行人。

工作车速范围：0~40km/h。

驾驶员可以选择开启或关闭功能，整车下线后，第一次的上电，功能默认开启。功能在车辆上电后，进行自检。前方横穿交通辅助技术要求见表7：

表7 前方横穿交通辅助技术要求

项目	取值
目标最小尺寸	长宽高：2m×0.6m×1.1m
目标最小速度	3.6km/h
报警最小持续时间	1s
功能激活速度	4km/h≤V≤40km/h
功能抑制车速	>40km/h
正确报警率	≥98%
错/误报警率	≤1%

6.1.8 自适应巡航

工作目标类型：四轮车、两轮车、行人。

工作车速范围：0~155km/h。

驾驶员可以通过开关选择开启或关闭功能，通过按键设定巡航速度，通过按键设定跟车时距。功能在车辆上电后，进行自检。自适应巡航技术要求见表8。

表8 自适应巡航技术要求

项目	取值
最小执行速度	0 km/h
最大执行速度	155 km/h
最小设定速度	30 km/h
最大设定车速	150 km/h

加速度范围	纵向控制系统加速度取决于当前车速。 当车速大于20 m/s, 纵向控制平均加速度不超过2 m/s ² ; 当车速小于 5 m/s, 纵向控制平均加速度不超过4 m/s ² ; 当车速处于5 m/s -20 m/s之间, 纵向控制平均加速度在2 m/s ² - 4 m/s ² 之间线性插值;
减速度范围	当车速大于20 m/s, 纵向控制平均减速度不超过3.5 m/s ² ; 当车速小于 5 m/s, 纵向控制平均减速度不超过5 m/s ² ; 当车速处于5 m/s -20 m/s之间, 纵向控制平均减速度在5 m/s ² - 3.5 m/s ² 之间线性插值;
减速度斜率范围	车辆在20m/s以上行驶时, 减速度的平均变化率不超过2.5m/s ³ ; 车辆在5m/s以下行驶时, 减速度的平均变化率不超过5m/s ³ ; 当车速处于5 m/s -20 m/s之间, 减速度的平均变化率在5m/s ³ - 2.5m/s ³ 之间线性插值;
达到设定车速10s后, 稳态误差	≤±1 km/h
跟随停车与目标车辆的距离	(2~5) m
对于前方静止目标时, 需要跟随前方目标减速到停时, 最大允许自车车速。	≥60km/h
车辆横向加速度	参考 ISO 15622 Figure 6
在稳定环境中, 1000km目标丢失率	<5%

6.1.9 智能领航

工作目标类型：四轮车、两轮车、行人。

工作车速范围：0~155km/h。

驾驶员可以通过开关选择开启或关闭功能, 通过按键设定巡航速度, 通过按键设定跟车时距。功能在车辆上电后, 进行自检。智能领航技术要求见表9。

表9 智能领航技术要求

功能概述		项目	取值
通用指标		最小工作速度	0 km/h
		最大工作速度	155 km/h
		最小设置车速	30 km/h
		最大设置车速	150 km/h
		加速度范围	参见自适应巡航要求
		减速度范围	参见自适应巡航要求
		减速度率范围	参见自适应巡航要求
纵向控制	速度控制	达到设定车速10s后速度误差范围	≤±1 km/h
	跟车控制	跟停后和前车距离	(2~5) m
		可跟随目标类型	四轮车、两轮车、行人
	弯道控制	车辆横向加速度	参见 ISO 15622 Figure 6
横向控制	通用指标	激活前提条件	纵向功能已经激活
		车道线颜色	白色, 黄色
		车道线类型	虚线, 实线, 双实线等
		车道线宽度	(0.06~0.8)m

	横向	最大横向加速度	3m/s²
		横向控制容差	±10cm
		执行力	50N







6.1.10 交通标志信息

工作目标类型：限速交通标志，道路交通标志。

工作车速范围：0~160km/h。

驾驶员可以选择开启或关闭功能报警，但是功能在每个点火周期会默认开启。当功能被开启时，驾驶员可以选择开启或关闭报警和调教报警方式。功能在车辆上电后，进行自检。交通标志信息提醒技术要求见表10。

表10 交通标志信息提醒技术要求

项目	取值
最小工作速度	0
最大工作速度	160km/h
识别标志	直接限速标志：  解除限速标志：  条件限速标志（例.匝道，雨天，雪天，雾天，时间，距离等辅助标志）：  其他道路标志（例.注意儿童，道路施工，禁止停车，左转，右转，连续转弯，禁止超车，解除禁止超车等）   
正确识别率	≥90%
误识别/漏识别	100Km不超过3次

6.1.11 驾驶员状态监测

工作目标类型：驾驶员。

工作车速范围：>7km/h。

驾驶员可以选择开启或关闭功能，但是功能在每个点火周期会默认开启。功能在车辆上电后，进行自检。驾驶员状态监测技术要求见表11。

表11 驾驶员状态监测技术要求

项目	取值
驾驶员分心正报率	>95%
驾驶员分心误报率	<5%
驾驶员疲劳正报率	>95%

驾驶员疲劳误报率	<5%
闭眼的False positive 探测精度	<2%
闭眼的False negative探测精度	<2%

6.1.12 变道辅助

工作目标类型：四轮车、二轮车

工作车速范围：15km/h-150km/h

驾驶员可以选择开启或关闭功能。功能在车辆上电后，进行自检。变道辅助技术要求见表12。

表12 变道辅助技术要求

项目	取值
目标最小尺寸	长×宽×高：2m×0.6m×1.1m
目标最小速度	3.6 km/h
静止目标	不报警
拖车工况下	不报警
最小报警持续时间	1s
系统激活速度	15km/h≤V≤150km/h
系统抑制车速	V<15 km/h, V>150 km/h
其他	满足 ISO17387 标准 满足GB/T 39265 - 2020标准

6.1.13 交通灯辅助

工作目标类型：交通灯

工作车速范围：0-160km/h

驾驶员可以选择开启或关闭功能。功能在车辆上电后，进行自检。交通灯辅助技术要求见表13。

表13 交通灯辅助技术要求

项目	取值
最低工作速度	0 km/h
最高工作速度	150 km/h
交通灯识别最小距离	50m
圆形交通灯识别率	90%
箭头交通灯识别率	90%
交通灯类型	实心圆，左/右/直行箭头，掉头U行灯
交通灯颜色	红，黄，绿
正确识别率	>90%
正确交通灯颜色识别率	>95%
正确交通灯颜色形状识别率	>90%
误/漏识别次数，每100000km	<5

6.1.14 紧急车道保持

工作目标类型：车道线，四轮车

工作车速范围：0-160km/h

驾驶员可以选择开启或关闭功能，但是功能在每个点火周期会默认开启。功能在车辆上电后，进行自检。紧急车道保持技术要求见表14。

表14 紧急车道保持技术要求

技术要求	项目	取值
通用要求	执行力	50N
对向来车	最小工作车速	60km/h
	最大工作车速	180km/h
	最小目标车速	0km/h
	最大目标车速	130km/h
	相对速度	0-180km/h
同向来车	最小工作车速	60km/h
	最大工作车速	180km/h
	相对速度	90km/h
	道路曲率	250m
偏离道路	最小工作车速	20km/h
	最大工作车速	180km/h
VRU	最小工作车速	25km/h
	最大工作车速	110km/h

6.2 泊车系统功能技术要求

6.2.1 倒车摄像头

倒车影像系统主要参数见表15。

表15 倒车影像系统主要参数要求

序号	技术要求描述	技术要求参数
1	摄像头启动时间	≤3s
2	视场角	水平（HFOV）≥180° 垂直（VFOV）≥110°
3	信噪比	≥42dB
4	低照度	≤1lux
5	动态范围	≥120dB
6	广角视图中车身占比	5%~15%
7	后方盲区距离	≤25 cm
8	检测帧率	≥25 fps
9	光轴精度	≤1°

6.2.2 全景环视

全景环视系统主要参数见表16。

表16 全景环视系统主要参数要求

序号	技术要求描述	技术要求参数
1	俯视图下前方显示距离	$\geq 2.5\text{m}$
2	俯视图下后方显示距离	$\geq 2.5\text{m}$
3	俯视图下左、右显示距离	$\geq 2\text{m}$
4	俯视图下前方盲区距离	$\leq 20\text{cm}$
5	俯视图下后方盲区距离	$\leq 25\text{cm}$
6	俯视图下左侧盲区距离	0mm
7	俯视图下右侧盲区距离	0mm
8	前视图中车身占比	5%~10%
9	后视图中车身占比	5%~15%
10	前广角视图中车身占比	5%~10%
11	后广角视图中车身占比	5%~15%
12	前两侧视图中车身占比	5%~15%
13	后两侧视图中车身占比	5%~15%
14	左视图中车身占比	5%~15%
15	右视图中车身占比	5%~15%
16	轨迹线位置精度(纵向)	真实运动轨迹 1m 内误差小于 5%，1m 外小于 10%
17	轨迹线位置精度（横向）	真实运动轨迹 1m 内误差+5cm 以内，1m-3m 误差+10cm 以内，3m-5m 误差+15cm 以内；
18	轨迹线本身精度	<10%

6.2.3 超声波泊车辅助

超声波系统主要参数见表17。

表17 超声波系统主要参数要求

序号	技术要求描述	技术要求参数	备注
1	PDC盲区（m）	$\leq 0.1\text{m}$	—
2	探测分辨率（mm）	$\leq 10\text{mm}$	针对标准测试杆
3	系统探测精度（mm）	5%	比如当障碍物距离为1m时，精度为5cm
4	障碍物检测准确率	95%	—
5	障碍物检测误报率	0	在无外界噪音，且路面平整
6	第一次探测时间（ms）	$\leq 500\text{ms}$	—
7	接近障碍物时数据更新时间（ms）	$\leq 80\text{ms}$	—
8	远离障碍物时数据更新时间（ms）	$\leq 240\text{ms}$	—
9	功能使能最大车速	$\geq 12\text{ km/h}$	—
10	特殊障碍物识别	可识别	1. 0.15m, 0.25m(路沿) 2. 圆柱型物体，高度1m，直径75mm 3. 孔径为3cm，丝直径4mm的铁丝网

6.2.4 低速紧急制动

低速紧急制动主要参数见表18。

表18 低速紧急制动主要参数要求

序号	技术要求描述	技术要求参数
1	PD探测距离（m）	8m
2	3DOD识别距离（m）	8m
3	摄像头精度（m）	障碍物与摄像头的距离的±10%，比如距离为1m时，精度为 ± 10 cm
4	安全距离（m）	0.25±0.05
5	障碍物识别高度	高于后保最低点
6	最大制动减速度	≤-g
7	不会引起误报的最小坡度	≤10%
8	障碍物识别要求	高度为1m，直径为75mm的圆柱物体 边长25cm的立方体，并且色差明显 高度为1m，直径为250mm的圆柱物体 身高高于0.8m的儿童和成人 自行车和摩托车 小型汽车 中大型汽车和卡车

6.2.5 自动泊车

自动泊车主要参数见表19。

表19 自动泊车主要参数要求

序号	技术要求描述	技术要求参数
1	APA使能最大车速	≤30km/h
2	支持车位类型	水平车位、垂直车位、斜列车位
3	弯道车位最小曲率半径	≥40m
4	可检测车位线宽度	8-30cm
5	车位探测误差	≤20cm
6	车位记忆距离	≥30m
7	水平车位通道宽度阈值	≥3.8m
8	垂直车位通道宽度阈值	≥5m
9	水平/弯道车位长度要求	车长L+0.7m
10	水平/弯道车位宽度要求	车宽D+0.2m
11	垂直/斜列车位深度要求	车长L+0.5m
12	垂直/斜列车位宽度要求	车宽D+0.6m
13	视觉水平车位	车长L+0.6m
14	视觉垂直车位	车宽D(不含后视镜)+0.3m
15	视觉最大车位宽度	3.5m
16	视觉最大车位长度	7m
17	车位识别率	≥85%

18	车位误识别率	2%
19	最大支持泊车坡度	≤15%

6.2.6 遥控泊车

遥控泊车主要参数如表20。

表20 遥控泊车主要参数要求

序号	技术要求描述	技术要求参数
1	手机APP连接距离	≥10m
2	手机APP连接时间	≤2s

7 智能驾驶系统功能安全技术要求

根据行车系统的功能进行技术安全需求分解，将FTTI定义为故障发生开始到控制器发出指令结束的时间段，从而脱离各车型的不同特性系统的影响，进行通用适配。

根据TSR的通用设计规范，E2E均使用于ASILB及以上等级的信号交互需求中，本处不进行一一对应罗列，只进行主要信号需求定义，信号名随不同通信矩阵进行适配。

各行车功能的技术安全需求的不重复性：如果ADAS功能有基础功能依赖，则，安全需求分析中，默认已符合基础功能的安全需求，只做增加特征功能的需求分析。

7.1 行车系统功能安全技术要求

7.1.1 行车系统功能安全分布

行车系统整体最高功能安全等级划分见表21。

表21 各行车系统最高功能安全等级

行车系统名称	功能安全最高ASIL等级
自动紧急制动 AEB	ASIL B
前碰撞预警 FCW	无
后碰撞预警 RCW(制动)	ASIL B或A
车道保持辅助 LKA	ASIL B
规避操作辅助 EMA	ASIL B
后方横穿交通辅助 RCTA	无
后方横穿交通辅助制动 RCTB	ASIL B或A
开门预警 DOW	无
前方横穿交通辅助 FCTA	无
前方横穿交通辅助制动 FCTB	ASIL B或A
自适应巡航 ACC	ASIL A
智慧巡航 ICC	ASIL B
交通标志信息 TSI	无
驾驶员状态检测 DPS	无

变道辅助 LCA	无
交通灯辅助 TLA	无
紧急车道保持ELKA	ASIL B

7.1.2 行车系统技术安全需求

7.1.2.1 自动紧急制动技术安全需求

自动紧急制动相关技术安全需求见表 22。

表22 自动紧急制动技术安全需求

TSR编号	ASIL等级	故障时间间隔FTTI	安全状态	需求描述
ADAS_AEB_TSR_01	B	300ms	AEB减速请求发无请求	如果油门踏板开度大于85%，ADAS不应将AEB减速请求信号置为有效 ^a
ADAS_AEB_TSR_02	B	500ms	AEB减速请求发无请求	只有当ESC无故障或ESC功能关闭时，ADAS才可通过将AEB加速请求信号置为有效来请求AEB减速 ^b
ADAS_AEB_TSR_03	B	300ms	DBS减速请求发无请求	当DBS状态为激活时，ADAS不应将减速度请求值设置到大于3倍的驾驶员减速请求值 ^c
ADAS_AEB_TSR_04	B	300ms	AEB减速请求发无请求	除非识别出自车与感知融合探测的物体间存在碰撞风险，ADAS不应通过将AEB减速请求信号置为有效以请求AEB减速 碰撞风险基于： <ul style="list-style-type: none"> • 自车纵向车速 • 自车偏航率 • 自车纵向加速度 • 物体位置 • 物体探测时间等 该物体应在50ms内由雷达或摄像头报告
^a 如果油门踏板开度变化率大于85%，且AEB减速请求信号有效时，应通过将AEB减速请求置无效以中止正在进行的减速操作。 ^b 如果在AEB激活控制减速的过程中，ESC故障，AEB发退出请求，并报警提醒驾驶员，记录DTC。 ^c DBS是驾驶员踩着一定的制动，有一点的刹车踏板开度。				

7.1.2.2 后碰撞预警技术安全需求

后碰撞预警相关技术安全需求见表23。

表23 后碰撞预警技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_RCW_TSR_01	B	500ms	RCW制动请求发无请求	只有当自车运动状态信息为有效时，ADAS才可将RCW制动请求置为有效。（根据减速度不同，将ASILB降为ASILA）
注：自车状态信息基于轮速传感器和车辆运动状态信息，提供有关车辆静止和车辆前进方向的信息。				

7.1.2.3 车道保持辅助技术安全需求

车道保持辅助相关技术安全需求见表 24。

表24 车道保持辅助技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_LKA_TS_R01	B	300ms	横向控制模式请求发无请求	只有当ESC无故障时，ADAS才可将横向控制模式请求信号置为LKA横向干预

7.1.2.4 规避操作辅助技术安全需求

规避操作辅助相关技术安全需求见表25。

表25 规避操作辅助技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_EMA_TS_R01	B	300ms	横向控制模式请求发无请求	只有当ESC无故障时，ADAS才可将横向控制模式请求信号置为EMA横向干预
ADAS_EMA_TS_R02	B	300ms	横向控制模式请求发无请求	只有当车速信号指示车速低于120km/h时，ADAS才允许将横向控制模式请求置为EMA横向干预
ADAS_EMA_TS_R03	B	500ms	横向控制模式请求发无请求	只有当主动转向信号有效时，ADAS才可将横向控制模式置为EMA横向干预
ADAS_EMA_TS_R04	B	500ms	横向控制模式请求发无请求	ADAS应根据偏航率判断发送的附加转向力矩请求信号方向与驾驶员转向方向相同

7.1.2.5 后方横穿交通辅助技术安全需求

后方横穿交通辅助相关技术安全需求见表26。

表26 后方横穿交通辅助技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_RCTB_TSR01	B	500ms	RCTB制动请求信号发无请求	只有当自车运动状态信息表示为后退时，ADAS才可将RCTB制动请求信号置为有效
ADAS_RCTB_TSR02	B	300ms	RCTB制动请求信号发无请求	当油门踏板开度大于85%时，ADAS不应将RCTB制动请求信号置为有效 注意：如果RCTB制动请求信号已置为有效时，油门踏板开度大于85%，则应通过将RCTB制动请求信号置为无请求来中止减速
ADAS_RCTB_TSR03	B	500ms	RCTB制动请求信号发无请求	只有当车速信号指示为低于18km/h时，ADAS才能被允许将RCTB制动请求信号置为有效

7.1.2.6 前方横穿交通辅助技术安全需求

前方横穿交通辅助相关技术安全需求见表27。

表27 前方横穿交通辅助技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_FCTB_TSR01	B	300ms	减速请求发无请求	当油门踏板开度大于85%时，ADAS不应通过将FCTB制动请求信号置为有效来请求FCTB减速 ^a
ADAS_FCTB_TSR02	B	500ms	减速请求发无请求	只有当车速信号指示当前车速低于18km/h时，ADAS才可通过将FCTB制动请求信号置为有效来请求FCTB减速
ADAS_FCTB_TSR03	B	300ms	减速请求发无请求	只有当ESC无故障时，ADAS才可通过将FCTB制动请求信号置为有效来请求FCTB减速

^a 当FCTB制动请求信号有效时，如果油门踏板开度变化大于85%，则应通过将FCTB制动请求信号置为无效以中止正在进行的减速。

7.1.2.7 自适应巡航技术安全需求

自适应巡航相关技术安全需求见表28。

表28 自适应巡航 ACC 技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_ACC_TS_R01	A	500ms	ACC功能禁止	ASDM 监控驾驶员侧车门状态信号，如果此信号故

				障，ACC功能停用
ADAS_ACC_TS R02	A	500ms	ACC功能禁止并提醒驾驶员	如果车速 > 15 km/h，当ESC失效时，ASDM 应该发送纵向控制状态失效信号，ACC功能停用
ADAS_ACC_TS R03	A	500ms	ACC功能禁止并提醒驾驶员	ASDM 应检测 ESC 状态的通信故障，如果检测到通信故障，将停用正在进行的 ACC 功能
ADAS_ACC_TS R04	A	500ms	ACC功能禁止并提醒驾驶员	ASDM 应该监控车门状态信号，如果车门是开着的，ACC应该退出
ADAS_ACC_TS R05	A	300ms	ACC保持纵向控制禁止	当车辆保持停止状态超过10s，ACC功能恢复按钮未被驾驶员按下且加速踏板未被踩下，ASDM不应该发送驾驶员驶离请求有效 注：同样适用于车辆被保持停止后，计时器从0s开始计时，10s内，ACC功能恢复按钮被按下或加速踏板位置被踩下，计时器再次从0s重新开始计算的情况

7.1.2.8 智慧巡航技术安全需求

智慧巡航相关技术安全需求见表29。

表29 智慧巡航 ICC 技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_ICC_TSR 01	A (D)	300ms	报警并提醒驾驶员接管	当 ICC 处于激活状态时，ASDM 不应由于ASDM产生的减速请求导致减速度变化率超过安全限制 (5 m/s ³) 注：正常减速0.45g
ADAS_ICC_TSR 02	A (D)	300ms	报警并提醒驾驶员接管	当 ICC 处于激活状态时，ASDM 不应产生减速请求超过安全限制 (4.5 m/s ²)。
ADAS_ICC_TSR 03	B (D)	200ms	报警并提醒驾驶员接管	ASDM应该避免发送非预期的转向角度请求信号到转向系统

7.1.2.9 紧急车道保持技术安全需求

紧急车道保持相关技术安全需求见表30。

表30 紧急车道保持 ELKA 技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_ELKA_T SR01	B	500	横向控制模式请求发无请求	只有挡ESC无故障时，ADAS才可通过将横向控制模式请求信号置为ELKA
ADAS_ELKA_T SR02	B	300	减速请求发无请求	只有当ESC无故障时，ADAS才可通过将ELKA制动请求信号置为有效来请求减速
ADAS_ELKA_T SR03	B	300	减速请求发无请求	当油门踏板开度大于85%时，ADAS不应通过将ELKA制动请求信号置为有效来请求减速 注意：当ELKA制动请求信号有效时，如果油门踏板开度变化大于85%，则应通过将ELKA制动请求信号置为无效以中止正在进行的减速。

7.2 泊车系统功能安全技术要求

7.2.1 泊车系统功能安全分布

泊车系统整体最高功能安全等级划分见表31。

表31 各泊车系统最高功能安全等级

泊车系统名称	功能安全最高ASIL等级
倒车影像 RVC	无
全景环视 AVIM	无

超声波泊车辅助 PDC	无
低速紧急制动 PEB	无
遥控泊车 RPA	ASILB
自动泊车APA	ASILA

7.2.2 泊车系统功能安全需求

7.2.2.1 遥控泊车功能安全需求

遥控泊车相关技术安全需求见表32。

表32 遥控泊车 RPA 技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_RPA_TSR_01	B	300ms	车辆刹停并报警	泊车系统将手机APP计算结果与标准答案进行比较及正确性检查。如果比较结果不一致，泊车模块将发送刹车的请求
ADAS_RPA_TSR_02	B	300ms	车辆刹停并报警	泊车控制系统应在300ms内判断EPB控制请求的正确性（判断条件XX）
ADAS_RPA_TSR_03	B	300ms	车辆刹停并报警	泊车控制系统应在300ms内判断泊车车速控制相关信号的正确性（判断条件XX）
ADAS_RPA_TSR_04	B	800ms	车辆刹停并报警	泊车控制系统应检测前轮速信号的正确性（判断条件XX）
ADAS_RPA_TSR_05	B	800ms	车辆刹停并报警	泊车控制系统应检测后轮速信号的正确性（判断条件XX）
ADAS_RPA_TSR_06	B	800ms	车辆刹停并报警	泊车控制系统应检测车速信号的正确性（判断条件XX）
ADAS_RPA_TSR_07	A	800ms	车辆刹停并报警	ADAS控制系统应在800ms内正确判断USS的数据(判断条件XX)
ADAS_RPA_TSR_08	B(D)	100ms	禁止泊车功能激活	当车速大于3km/h时，泊车控制系统应在100ms内正确检查握手请求信号和RPA状态机故障
ADAS_RPA_TSR_09	B	300ms	车辆刹停并报警	泊车流程完成后，泊车控制系统需要检查来自底盘控制系统的EPB状态信号，以确认EPB是否成功触发（channel1） 对于SAF_RPA_TSR_09和SAF_RPA_TSR12，当其中一个满足(应用EPB或P-lock)时，泊车控制器可以完成停车并退出
ADAS_RPA_TSR_10	B	300ms	禁止泊车功能激活	泊车控制系统应检查手势原始数据。将手机APP计算结果与标准答案进行比较及正确性检查。如果比较结果不一致或手势状态错误，泊车控制系统将发送刹车的请求
ADAS_RPA_TSR_11	B	300ms	禁止泊车功能激活	泊车控制系统应在300ms内判断目标挡位信号的正确性(判断条件XX)
ADAS_RPA_TSR_12	B	300ms	禁止泊车功能激活	泊车控制系统应检查车辆当前挡位信号以确认完成停车后挡位成功挂入P档。 对于SAF_RPA_TSR_09和SAF_RPA_TSR12，当其中一个满足(应用EPB或P-lock)时，泊车控制器可以完成停车并退出。
ADAS_RPA_TSR_13	A(B)	300ms	车辆刹停并报警	泊车控制系统应限制远程泊车操作时间不超过3分钟
ADAS_RPA_TSR_14	A(B)	300ms	车辆刹停并报警	泊车控制系统应从底盘控制系统正确接收EPB状态信号。（channel2）
ADAS_RPA_TSR_15	A(A)	800ms	车辆刹停并报警	泊车控制系统应检查USS雷达的故障(判断条件XX)
ADAS_RPA_TSR_16	A(A)	600ms	车辆刹停并报警	USS雷达应该正确地将数据发送给泊车控制系统(设计条件XX)

ADAS_RPA_TSR 17	A	800ms	车辆刹停并报警	泊车控制系统应从制动控制系统正确接收底盘控制状态信号(设计条件XX)
ADAS_RPA_TSR 18	B	300ms	禁止泊车功能激活	泊车控制系统应接收来自底盘控制系统的坡度信号(设计条件XX)
ADAS_RPA_TSR 19	B	150ms	禁止泊车功能激活	泊车控制系统应正确发送目标挡位信号(P档)(设计条件XX)
ADAS_RPA_TSR 20	B(D)	300ms	车辆刹停并报警	泊车控制系统应在300ms内判断握手请求信号的准确性(判断条件XX)
ADAS_RPA_TSR 21	B(D)	100ms	禁止泊车功能激活	当车速大于3km/h时,泊车控制系统应在100ms内通过比较轮速和车速,正确检查EPB控制请求信号的故障
ADAS_RPA_TSR 22	B	100ms	关闭RPA功能,向刹车控制系统发送刹车请求并报警	泊车控制系统应监测车辆速度值。如果实时车速超过3km/h超过1秒(待定),泊车控制系统应停用该功能,并向底盘控制系统发送紧急制动请求

7.2.2.2 自动泊车功能安全需求

自动泊车相关技术安全需求见表33。

表33 自动泊车 APA 技术安全需求

TSR编号	ASIL	FTTI	安全状态	需求描述
ADAS_APA_TS R01	A	800ms	车辆刹停并报警	ADAS应该在200ms内要正确的判断泊车车速信息
ADAS_APA_TS R02	A	800ms	车辆刹停并报警	ADAS应该在200ms内通过实际车速和整车期望车速来检测车速信号的正确性
ADAS_APA_TS R03	A	800ms	车辆刹停并报警	ADAS应该校验前轮轮速脉冲信号的正确性
ADAS_APA_TS R04	A	800ms	车辆刹停并报警	ADAS应该校验后轮轮速脉冲信号的正确性
ADAS_APA_TS R05	A	800ms	车辆刹停并报警	ADAS应该校验目标车速的正确性
ADAS_APA_TS R06	A	600ms	车辆刹停并报警	ADAS应该在600ms内判断整车侧边超声波雷达数据的正确性(如:回波超出最大的可测量范围)
ADAS_APA_TS R07	A	600ms	车辆刹停并报警	ADAS应该在600ms内判断整车前超声波雷达数据的正确性(如:回波超出最大的可测量范围)
ADAS_APA_TS R08	A	600ms	车辆刹停并报警	ADAS应该在600ms内判断整车后方超声波雷达数据的正确性(如:回波超出最大的可测量范围)
ADAS_APA_TS R09	A(D)	100ms	禁止泊车激活	当车速高于5km/h时,ADAS需要在100ms内校验泊车状态的正确性(APA, RPA)
ADAS_APA_TS R10	A	300ms	禁止泊车激活	ADAS应该校验挡位信息正确性(如:1、R档和D档需达ASILB,2、分别校对车辆运动与目标物距离情况判断当时的真实档位方向)
ADAS_APA_TS R11	A(D)	100ms	禁止泊车激活	当整车车速大于5km/h时ADAS在100ms内应该通过车轮速度和整车速度比较来校验ADAS目标速度的正确性
ADAS_APA_TS R12	A	800ms	车辆刹停并报警	ADAS应检查超声波雷达故障(如:余振、断路、短路、阈值无法配置)
ADAS_APA_TS R13	A	300ms	禁止泊车激活	ADAS应在300ms内判断泊车状态信息(APA, RPA)和APA工作状态信息的正确性

8 智能驾驶系统预期功能安全技术要求

8.1 系统预期功能安全分布

对系统进行预期功能安全考量时,通过系统较高级功能往下覆盖低级功能,系统涉及到预期功能安全需求的功能可参考表34。

表34 预期功能安全功能分布

系统	功能
行车	自适应巡航ACC
	智慧巡航ICC
	车道保持辅助LKA
	变道辅助LCA
	规避操作辅助EMA
	自动紧急制动AEB
	紧急车道保持ELKA
泊车	全自动泊车APA
	遥控泊车RPA（包括了APA，APA少一些需求）

8.2 系统预期功能安全需求

8.2.1 行车系统预期功能安全需求

行车系统的预期功能安全需求见表35。

表35 行车系统预期功能安全需求

Requirement ID	allocated	Requirement description
SR_driving_001	感知融合	感知融合对于前方车辆目标物最远识别距离至少应达到200m
SR_driving_002	感知融合	感知融合对于后方车辆的最远识别距离至少应大于80m
SR_driving_003	感知融合	感知融合应至少提前100m识别到有人工改道、限速标志，车道线等
SR_driving_004	感知融合	感知融合的目标识别准确率应>98% ^a
SR_driving_005	感知融合	感知融合对车辆目标的漏识别率应<1%
SR_driving_006	感知融合	感知融合对车辆目标的误识别率应<1%
SR_driving_007	感知融合	感知融合在纵向距离30m内的距离精度应<0.1m
SR_driving_008	感知融合	感知融合在横向距离30m内的距离精度应<0.15m
SR_driving_009	感知融合	感知融合的目标物速度精度偏差不得超过0.1m/s
SR_driving_010	感知融合	感知融合对弯道曲率的拟合与计算准确率应>85%
SR_driving_011	规划决策	对目标对象的轨迹预测不得小于3-5s
SR_driving_012	规划决策	路径规划的一致性>95%
SR_driving_013	规划决策	系统决策时需要将相关环境参数作为车速限制的condition. 例：弯道曲率，路面附着系数，坡度，横向坡度，lead vehicle车速，路径规划，限速标志，当前位置（收费站，窄道）
SR_driving_014	规划决策	系统应根据道路设计定义的车速与曲率对应关系进行车速适配：
SR_driving_015	规划决策	应保证车辆在本车道内，车辆居中偏移量不得超过±0.15m
SR_driving_016	规划决策	对于Eadp感知到的目标进行决策控制的响应时间应<100ms
SR_driving_017	规划决策	自动变道功能激活后，需根据当前车速请求方向盘转角值
SR_driving_018	规划决策	自动变道的最大车速应≤130km/h

SR_driving_019	规划决策	当自车在前方道路距离小于一定值，仍无法进行并道或汇入动作时，应提示驾驶员接管： 车速为130km/h时接管提示距离应至少为123m 车速为100km/h时接管提示距离应至少为95m 车速为80km/h时接管提示距离应至少为77m 车速为60km/h时接管提示距离应至少为60m 注：无法进行并道或汇入动作是指，剩余距离内无法规划出可进行并道的路径轨迹。
SR_driving_020	规划决策	外部因素导致横向控制不可用时，ASM系统需在100ms内发出驾驶员接管提示
SR_driving_021	规划决策	ASM有请求指令，超时未接管时ASM请求HMI语音提示驾驶员
SR_driving_022	规划决策	预测到车辆有变道意图(有转向灯或偏向车道线移动位移)，且有碰撞风险时，应至少提前0.5s(TBD)开始减速
a 不同目标类型、不同距离还需分情况讨论。		

8.2.2 泊车系统预期功能安全需求

泊车系统的预期功能安全需求见表36。

表36 泊车系统预期功能安全需求

Requirement ID	allocated	Requirement description
SR_parking_001	感知融合	对5m内的目标物探测准确率应>99%
SR_parking_002	感知融合	对目标探测的漏识别率应<0.5%
SR_parking_003	感知融合	至少应识别到高度0.2m以上的行人（包括站、坐、躺的成人和小孩）
SR_parking_004	感知融合	对目标的距离探测精度应<0.1m
SR_parking_005	规划控制	泊车过程中车速应至少小于1m/s
SR_parking_006	规划控制	坡度>15%时应退出泊车控制
SR_parking_007	规划控制	车速高于泊车设定速度时，应退出泊车控制
SR_parking_008	规划控制	ODD不满足导致泊车退出时，档位应切换至P档，并执行制动
SR_parking_009	规划控制	无法接收到手机控制信号时，应在100ms内报警并执行制动 ^a
SR_parking_010	其他需求	遥控泊车过程中，驾驶员距离车辆的距离不得超过5m ^b
a 遥控泊车		
b 遥控泊车		

9 智能驾驶系统信息安全技术要求

9.1 智能驾驶系统功能层信息安全技术要求

行车及泊车系统功能信息安全映射关系，见表37：

表37 系统功能信息安全映射关系

系统功能	处理方案						
	数据安全	需要保护的信息安全性质					
		保密性	完整性	认证/鉴定	可用性	抗抵赖性	授权
车道保持辅助	Y	Y	Y		Y		

紧急避让辅助	Y	Y	Y	Y	Y		Y
后方横穿交通辅助	Y	Y	Y	Y	Y		
前方横穿交通辅助	Y	Y	Y		Y		
自适应巡航	Y	Y	Y		Y		Y
交通标志信息	Y	Y	Y	Y	Y		
变道辅助	Y	Y	Y		Y	Y	Y
交通灯辅助TLA	Y	Y	Y	Y	Y		
紧急车道保持ELKA	Y	Y	Y	Y	Y		Y
倒车影像RVC	Y	Y	Y		Y		Y
全景环视AVM	Y	Y	Y	Y	Y		Y
超声波泊车辅助PDC	Y	Y	Y	Y	Y	Y	
低速紧急制动PEB	Y	Y	Y		Y	Y	
自动泊车APA	Y	Y	Y		Y		Y
遥控泊车 RPA	Y	Y	Y	Y	Y	Y	Y

根据表 37 进行各功能的信息安全技术要求分解。

9.1.1 横向与纵向行车控制功能信息安全技术要求

横向与纵向行车控制功能包括：车道保持辅助/紧急避让辅助/自适应巡航/变道辅助/紧急车道保持/前后横穿交通辅助。

对横向与纵向行车控制功能的信息安全技术要求见表 38：

表 1 横向与纵向行车控制功能的信息安全技术要求

用例描述：		评论意见
车道保持辅助	CSR01: LKA 激活状态下，由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR02: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR03: LKA 激活状态下，由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	—
	CSR04: LKA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号需加密	例如：CAN 网络 AES128
	CSR05: LKA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR06: LKA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号保证可用	—
	CSR07: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如：AES128
	CSR08: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如：消息验证码或哈希值校验
	CSR09: LKA 激活状态下，由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
紧急避让辅助	CSR10: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR11: EMA 激活状态下，由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	—
	CSR12: EMA 激活状态下，由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR13: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如：AES128

	CSR14: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如: 消息验证码或哈希值校验
	CSR15: EMA 激活状态下, 由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
自适应巡航	CSR16: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR17: ACC 激活状态下, 由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	例如: CAN 网络消息验证码或哈希值校验
	CSR18: ACC 激活状态下, 由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR19: ACC 激活状态下, 驾驶员监控摄像头传输至自动驾驶域控制器的信号需加密	例如: CAN 网络 AES128
	CSR20: ACC 激活状态下, 驾驶员监控摄像头传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR21: ACC 激活状态下, 驾驶员监控摄像头传输至自动驾驶域控制器的信号保证可用	—
	CSR22: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如: AES128
	CSR23: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如: 消息验证码或哈希值校验
	CSR24: ACC 激活状态下, 由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
变道辅助	CSR25: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR26: LCA 激活状态下, 由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	—
	CSR27: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如: AES128
	CSR28: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如: 消息验证码或哈希值校验
	CSR29: LCA 激活状态下, 由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
紧急车道保持	CSR30: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR31: ELKA 激活状态下, 由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	—
	CSR32: ELKA 激活状态下, 由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR33: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如: AES128
	CSR34: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如: 消息验证码或哈希值校验
	CSR35: ELKA 激活状态下, 由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
前后横穿交通辅助	CSR36: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR37: RCTA/FCTA 激活状态下, 由前视毫米波雷达传输至自动驾驶域控制器的信号需保证可用	—
	CSR38: 由自动驾驶域控制器与底盘域控制器的信号需加密	例如: AES128
	CSR39: 由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如: 消息验证码或哈希值校验
	CSR40: RCTA/FCTA 激活状态下, 由自动驾驶域控制器与底盘域控制器的信号需保证可用	—

9.1.2 交通标志信息 TSI 和交通灯辅助 TLA 的信息安全技术要求

对交通标志信息TSI和交通灯辅助TLA的信息安全技术要求见表39:

表 2 交通标志信息 TSI 和交通灯辅助 TLA 的信息安全技术要求

用例描述:		评论意见
交通标志信息	CSR53: 导航定位地图系统传输至自动驾驶域控制器的信号需加密	例如: CAN 网络 AES128
	CSR54: 导航定位地图系统传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR55: TSI 激活状态下, 导航定位地图系统与自动驾驶域控制器的信号需保证可用	—
	CSR56: TSI 激活状态下, 由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
交通灯辅助	CSR57: 导航定位地图系统传输至自动驾驶域控制器的信号需加密	例如: CAN 网络 AES128
	CSR58: 导航定位地图系统传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR59: TLA 激活状态下, 导航定位地图系统与自动驾驶域控制器的信号需保证可用	—
	CSR60: TLA 激活状态下, 由前视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR61: 由前视毫米波雷达传输至自动驾驶域控制器的信号需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR62: TLA 激活状态下, 由前视毫米波雷达传输至自动驾驶域控制器的信号须保证可用	—
数据安全要求	DSR06: 激活(如首次使用, 撤销同意后再次使用)本自动驾驶功能时, 提供同意界面供用户点击同意 DSR07: 针对图像视频类脱敏, 方法可参考法规《汽车传输视频及图像脱敏技术要求与方法》 DSR08: 自动驾驶域控制器须关闭摄像头拍摄功能, 如果定位系统已确认己车处于重要敏感区域。(重要敏感区域由测绘资质的图商进行识别)	人脸图像脱敏 车牌图像脱敏 重要地理位置脱敏 人脸脱敏 车牌脱敏

9.1.3 倒车影像和全景环视信息安全技术要求

对倒车影像和全景环视的信息安全技术要求见表40:

表 3 倒车影像和全景环视的信息安全技术要求

用例描述:		评论意见
倒车影像/全景环视	CSR69: RVC/AVM 激活状态下, 由环视摄像头传输至自动驾驶域控制器的信号需保证可用	
	CSR70: RVC/AVM 激活状态下, 数字视频录像机传输至自动驾驶域控制器的图片需加密	例如: CAN 网络 AES128
	CSR71: RVC/AVM 激活状态下, 数字视频录像机传输至自动驾驶域控制器的图片需防篡改	例如: CAN 网络消息验证码或哈希值校验
	CSR72: RVC/AVM 激活状态下, 数字视频录像机传输至自动驾驶域控制器的图片需保证可用	—
数据安全要求	DSR12: 倒车影像/全景环视的人脸、车牌等个人敏感数据, 脱敏方法可参考法规《汽车传输视频及图像脱敏技术要求与方法》 DSR13: 自动驾驶域控制器须关闭摄像头拍摄功能, 如果定位系统已确认己车处于重要敏感区域。(重要敏感区域由测绘资质的图商进行识别) DSR14: 倒车影像/全景环视的人脸、车牌等个人敏感数据, 数据分区存储: 一般数据 Flash/ROM 存储中, 存储时间: 输入具体参数, 并告知用户 DSR15: 倒车影像/全景环视的人脸、车牌等个人敏感数据, 需要设置安全访问 DSR16: 倒车影像/全景环视的安全日志; 数据安全存储的日志; 安全访问的日志; 数据敏感判断日志; 数据命令信号日志等 DSR17: 倒车影像/全景环视的人脸、车牌等个人敏感数据需要通过 AES128 解密 DSR18: 倒车影像/全景环视的人脸、车牌等个人敏感数据通过 SHA1 做	—

	完整性校验	
--	-------	--

9.1.4 泊车功能的信息安全技术要求

泊车功能包括：超声波泊车辅助/自动泊车/遥控泊车/低速紧急制动PEB。
对泊车功能的信息安全技术要求见表41：

表 4 泊车功能的信息安全技术要求

用例描述		评论意见
超声波泊车辅助信息安全需求	CSR73：由超声波传输至自动驾驶域控制器的信号需防篡改	例如：消息验证码或哈希值校验
	CSR74：PDC 激活状态下，由超声波传输至自动驾驶域控制器的信号需保证可用	—
自动泊车/遥控泊车	CSR75：导航定位地图系统传输至自动驾驶域控制器的信号需加密	例如：CAN 网络 AES128
	CSR76：导航定位地图系统传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR77：APA/RPA 激活状态下，导航定位地图系统与自动驾驶域控制器的信号保证可用	—
	CSR78：APA/RPA 激活状态下，由环视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR79：APA/RPA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号需加密	例如：CAN 网络 AES128
	CSR80：APA/RPA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR81：APA/RPA 激活状态下，驾驶员监控摄像头传输至自动驾驶域控制器的信号保证可用	—
	CSR82：由超声波传输至自动驾驶域控制器的信号需防篡改。	例如：消息验证码或哈希值校验
	CSR83：APA/RPA 激活状态下，由超声波传输至自动驾驶域控制器的信号需保证可用	—
	CSR84：由自动驾驶域控制器与底盘域控制器的信号需加密	例如：AES128
	CSR85：由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如：消息验证码或哈希值校验
	CSR86：APA/RPA 激活状态下，由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
低速紧急制动	CSR116：导航定位地图系统传输至自动驾驶域控制器的信号需加密	例如：CAN 网络 AES128
	CSR117：导航定位地图系统传输至自动驾驶域控制器的信号需防篡改	例如：CAN 网络消息验证码或哈希值校验
	CSR118：PEB 激活状态下，导航定位地图系统与自动驾驶域控制器的信号保证可用	—
	CSR119：PEB 激活状态下，由环视摄像头传输至自动驾驶域控制器的信号需保证可用	—
	CSR120：由自动驾驶域控制器与底盘域控制器的信号需加密	例如：AES128
	CSR121：由自动驾驶域控制器与底盘域控制器的信号需防篡改	例如：消息验证码或哈希值校验
	CSR122：PEB 激活状态下，由自动驾驶域控制器与底盘域控制器的信号需保证可用	—
数据安全要求	DSR19：自动泊车/遥控泊车/低速紧急制动 PEB 的人脸、车牌等个人敏感数据，方法可参考法规《汽车传输视频及图像脱敏技术要求与方法》	—
	DSR20：自动驾驶域控制器须具备关闭摄像头拍摄功能，如果定位系统已确认已车处于重要敏感区域。（重要敏感区域由测绘资质的图商进行识别）。	

9.2 功能层与零件层信息安全映射关系

功能层与零件层的信息安全映射关系见表42。

表 5 功能层与零件层信息安全映射关系

系统功能	处理方案											
	域ECU	通信	导航 定位 地图 系统	毫米 波雷 达	激光 雷达	单目 前视 摄像 头	多目 前视 摄像 头	环视 摄像 头	驾驶 员监 控摄 像头	红外 传感 器	超声 波传 感器	数字 视频 录像 机 DVR
倒车影像RVC		Y						Y				Y
全景环视AVM								Y				Y
超声波泊车辅助PDC	Y	Y									Y	
低速紧急制动PEB	Y	Y	Y			Y		Y				
自动泊车APA	Y	Y	Y					Y	Y		Y	
遥控泊车RPA	Y	Y	Y					Y	Y		Y	
车道保持辅助	Y	Y		Y		Y			Y			
紧急避让辅助	Y	Y		Y		Y						
后方横穿交通辅助	Y	Y		Y								
前方横穿交通辅助	Y	Y		Y								
自适应巡航ACC	Y	Y		Y		Y			Y			
智能领航ICC (HWA/ALCA)	Y	Y	Y	Y		Y			Y			
交通标志信息TSI	Y	Y	Y			Y						
驾驶员状态检测	Y	Y							Y	Y		
变道辅助LCA	Y	Y		Y								
交通灯辅助TLA	Y	Y	Y	Y		Y						
紧急车道保持ELKA	Y	Y		Y		Y						

9.3 智能驾驶系统零件层信息安全技术要求

以自动驾驶系统常见零件需要的安全措施为例，常用信息安全映射关系见表43：

表 6 零件层信息安全映射关系

传感器及模块	处理方案					
	01_脱敏	02_基础密 钥保护	03_随机数 生成	04_网络入侵检 测与防范系统	05_硬件强制安全	06_增强的系统强 化
域ECU	Y	Y	Y	Y	Y	Y
通信				Y		
毫米波雷达			Y			Y
激光雷达			Y			Y
单目前视摄像 头	Y	Y	Y			Y
双目前视摄像 头	Y	Y	Y			Y
环视摄像头	Y	Y	Y			Y

驾驶员监控摄像头	Y		Y		Y	Y
红外传感器			Y			Y

表 7 零件层信息安全映射关系（续）

传感器及模块	处理方案						
	07_安全启动	08_安全调试	09_通用软件认证	10_系统强化	11_程序隔离	12_安全访问	13_安全审计日志
域ECU	Y	Y	Y	Y	Y	Y	Y
通信			Y			Y	Y
毫米波雷达		Y	Y	Y	Y	Y	
激光雷达		Y	Y	Y	Y	Y	
单目前视摄像头		Y	Y	Y	Y	Y	
双目前视摄像头		Y	Y	Y	Y	Y	
环视摄像头		Y	Y	Y	Y	Y	
驾驶员监控摄像头	Y	Y	Y	Y	Y	Y	Y
红外传感器		Y	Y	Y	Y	Y	

注1：Y指代该器件模块必须具备对应信息安全机制。

注2：表格中所列信息安全机制或不是全部，仅代表常见的机制。