

# 人工智能驱动的智能驾舱人机交互安全性与可靠性分析

李晓海 张海涛 李亚伟

中机科（北京）车辆检测工程研究院有限公司 102100

DOI:10.12238/ems.v7i12.16436

**[摘要]** 随着智能网联汽车逐步迈入大规模商业化阶段，智能驾舱成为车内体验与信息交互的核心平台。传统以按钮、触屏为主的人机交互模式，已无法满足自动驾驶与车联网背景下的复杂需求。人工智能技术，尤其是深度学习、自然语言处理、计算机视觉与多模态融合，为驾舱提供了实时环境感知、语义理解与驾驶行为预测能力。本文围绕人工智能驱动的智能驾舱人机交互系统展开研究，从架构设计、硬件与软件方案、算法集成到安全性与可靠性测试进行系统阐述。通过构建多模态感知与融合的交互架构，提出了兼顾功能冗余、安全护栏与策略优化的设计思路，并在虚拟案例中进行了部署与验证。结果表明，该系统在语音识别延迟、注意力检测准确率与容错切换时间等关键技术参数上均实现显著改进，验证了人工智能赋能下智能驾舱交互系统的安全性及可靠性，为未来智能网联汽车的落地应用提供了参考。

**[关键词]** 人工智能；智能驾舱；人机交互；安全

## 前言：

随着智能网联汽车的快速发展，驾舱功能逐渐由单一的信息娱乐承载转变为集成化的驾驶辅助与交互中心。传统的人机交互模式主要依赖机械按键与触控屏，虽然在一定程度上满足了驾驶需求，但在自动驾驶、车联网与智能交通体系不断完善的背景下，其局限性愈发突出。尤其是在复杂交通环境中，驾驶员需要在高信息密度下快速处理任务，传统交互方式容易造成认知负荷增加与潜在安全隐患。人工智能的引入为智能驾舱的升级提供了新契机。借助语音识别、计算机视觉、手势控制、情绪分析以及多模态融合技术，智能驾舱得以实现对驾驶员状态的实时感知以及行为预测，逐渐形成“主动式”的人机协作机制，这在驾驶体验方面提供了更为自然且智能的交互方式，同时在安全性方面引入了疲劳驾驶预警、注意力监测以及紧急干预等功能，促使车辆安全性从被动防护转变为主动预防。

## 1 智能驾舱人机交互系统架构

智能驾舱人机交互系统的架构把车载计算平台当作核心，将多模态感知、智能决策以及交互呈现这三个主要环节融合在一起，它的技术本质是借助传感器网络来获取驾驶员和环境的信息，依靠人工智能算法达成语义解析以及驾驶意图预测，最后凭借语音、视觉、触控或者提高现实界面给予反馈。此架构重视实时性与安全性，还得保证有跨域协同能力，以此保证车载娱乐、辅助驾驶和安全控制功能能在同一

个平台下高效运转。

### 1.1 多模态感知与数据融合层

此层作为系统的输入端，主要依靠摄像头、毫米波雷达、红外传感器、语音采集麦克风阵列以及驾驶员监测系统即 DMS，其核心任务在于捕捉车内外的多模态数据，借助边缘计算单元开展初步的特征提取以及降噪工作，就像眼动追踪摄像头会实时采集驾驶员的注视点，语音阵列会进行方向性拾音，环境摄像头会捕捉道路场景一样。数据在这一层借助时序同步与特征融合算法比如卡尔曼滤波、多模态 Transformer 模型来达成统一建模，形成可靠的驾驶员状态参数以及环境语义描述，为上层的智能决策提供基础支持。

### 1.2 智能决策与交互逻辑层

在这一层中，人工智能算法针对感知层传递过来的数据展开深入细致的解析，形成驾驶意图识别以及交互逻辑推理，典型的技术包含基于深度神经网络的语义理解、借助强化学习驱动的策略优化，以及基于贝叶斯网络的人因状态建模，系统依靠实时预测驾驶员的操作倾向以及注意力水平，以此来决定交互方式和提示等级。比如说，当系统识别出驾驶员注意力分散的时候，就会自动调低娱乐系统音量并且触发语音提醒，这一层还内置了安全约束模块，保证所有交互逻辑不会和车辆核心安全控制发生冲突，达成“智能化但可控”的决策链路。

### 1.3 交互呈现与反馈执行层

这一层的职责是把智能决策转变为直观的人机交互体验,它主要囊括了多个维度的交互接口,像语音助手、HUD抬头显示、触控屏、AR提高现实投影以及力反馈控制器等,其关键技术在于低延迟渲染与人因工程优化,借助GPU加速达成毫秒级的UI响应,依靠自适应语音合成以及自然语调控制来提升语音交互的拟人化体验。并且为了保证安全性,系统设计了分级反馈机制,在轻度风险时运用视觉或者声音提示,在高度风险时依靠座椅震动或者方向盘力反馈实施强制提醒,这一层还和车联网以及云端平台维持通信,达成OTA更新以及持续优化,让交互体验拥有可扩展性以及长期可靠性。

## 2 人工智能驱动的智能驾舱人机交互系统设计

### 2.1 硬件设计

智能驾舱的人机交互系统硬件设计遵循“中央计算+多模态感知+交互输出”的整体架构。中央计算单元作为核心,需要具备高算力和实时处理能力,以支持复杂的语音识别、视觉分析和多模态融合任务。围绕中央单元,系统通过摄像头、麦克风阵列、触控屏、方向盘反馈装置等传感器与执行器构建感知与交互回路。整车采用“中央计算+区域控制”架构:中央计算平台选用车规级SoC(如NVIDIA Orin X或同档NPU $\geq 200$  TOPS, CPU 12C, GPU 2, 048 CUDA),配安全MCU(Infineon AURIX TC3xx)做A/B冗余与看门狗。感知侧配置三类传感器:①车内DMS/OMS:2 $\times$ IR全球快门摄像头(1080p@60fps, 940nm补光, FOV 68°/95°), 1 $\times$ ToF深度模组(640 $\times$ 480@30fps);②语音阵列:6麦环形阵列(48 kHz/24 bit, 波束成形SNR $\geq 20$  dB, AEC/NS前端);③环境与交互:HUD投影(12° $\times$ 3°视场,亮度 $\geq 12,000$  cd/m<sup>2</sup>), 12.8"中控触控屏(120 Hz, 触觉马达LRA), 方向盘力反馈电机(峰值扭矩 $\geq 1.8$  N $\cdot$ m)。通信总线采用以太网TSN主干(1000BASE-T1, 时钟同步 $<1$   $\mu$ s), 辅以CAN FD(2 Mbps)与LIN。

### 2.2 软件设计

软件架构的设计重点在于分层与隔离。底层系统应提供一个车规级的实时操作环境,以保障任务调度和资源分配的确定性。基础层采用AUTOSAR Adaptive + POSIX RT内核(Linux RT/QNX)混合,安全域与非安全域通过虚拟化隔离

(Type-1 Hypervisor, IPC基于共享内存+VirtIO)。中间件选择DDS(Cyclone/FastDDS)做多进程发布/订阅, QoS设为RELIABLE + DEADLINE(10 ms)保障人机回路时限;音频栈采用PA/ALSA自定义模块支持AEC/NS/AGC链路;图形渲染管线接入Wayland/WSI, UI渲染线程独立优先级(SCHED\_FIFO, prio 80), HUD走独立显示控制器+直通通道以降低合成延迟。应用层模块化为“语音助手、手势/触控、视觉关注管理、提示编排器、车机任务调度器”,通过策略引擎(YAML规则+Lua脚本)实现场景化策略热更新;全栈容器化(OCI)托管非安全应用,镜像签名与安全启动(Secure Boot/Measured Boot)。

### 2.3 算法集成设计

算法是智能驾舱的“决策大脑”,其设计应强调融合与鲁棒性。本次设计的系统采用多模态链路,多模态链路遵循“前端轻量化+后端融合推理”原则:语音链采用Conformer-RNN-T(35M参数, INT8量化,端到端ASR $<120$  ms片上延迟), NLP意图槽位BERT-Tiny蒸馏版(4L-312H), TTS使用流式Vocoder(帧延迟 $<50$  ms);视觉链DMS含瞌睡/分神/注视点估计,骨干MobileNetV3-Small + LSTM时序头,单帧 $<8$  ms;手势识别以3D-CNN(I3D-Lite)或时序关键点Transformer(4层, 8头)实现。融合层采用多模态Transformer(MM-TRM, 隐藏维512, 6层, Cross-Attention对齐音/视/触信息),时间窗1.5 s滑动,推理批大小动态自适应(1-4)。

## 3 人工智能驱动的智能驾舱人机交互安全性与可靠性测试

### 3.1 案例背景

某位于华东地区的汽车研发企业,在着手开发新一代智能驾舱之际,打算引入由人工智能驱动的人机交互系统,以此达成多模态感知、驾驶员状态监测以及语音语义交互等功能,项目研发团队挑选了一款中高端SUV原型车来开展系统验证工作,着重关注在高速行驶以及城市复杂工况下的人机交互安全性与可靠性。测试场景包含语音指令响应、驾驶员注意力检测、紧急提醒触发以及人机回路延迟等指标,鉴于该项目处于量产前验证阶段,研发团队构建了一个软硬件一体化的实验平台,依靠可量化的技术参数改进,来验证系统在多工况下的稳定性与安全性,为后续批量装

车提供可靠依据。

3.2 实施方案（400 字）

在硬件部署环节，中央计算平台选用车规级高性能 SoC，还搭载独立的安全 MCU 用于冗余监控工作，感知单元包含红外 DMS 摄像头、六麦环形阵列以及 AR-HUD 显示模组，所有设备借助车载以太网 TSN 总线达成低延迟同步，本系统明确了关键性能指标，其中语音指令响应延迟小于 300 ms，驾驶员注意力检测准确率大于 95%，交互界面渲染延迟小于 50 ms，系统端到端容错时间小于 200 ms。为达成这些指标，测试平台在硬件冷冗余和数据双通道采集的基础之上，配置实时操作系统作为安全域，Linux RT 作为非安全域，以此实现安全与娱乐的隔离运行。

展开来说，语音识别模块运用轻量化的端到端 ASR 模型，并结合噪声自适应算法，视觉检测模块采用基于卷积神经网络的疲劳检测以及眼动追踪模型，多模态融合借助 Transformer 结构达成跨模态特征对齐，策略层内部设置安全护栏机制：要是语音识别置信度低于阈值或者视觉信号丢失，系统会自动降级为简单指令提示或者直接触发物理反馈。并且 OTA 更新机制保证算法可持续优化，在测试过程中模拟了不同版本模型的迭代，以此评估系统在长期运行时的可维护性。

3.3 实施效果

具体实施测试效果如表 1 所示。

表 1 智能驾舱人机交互系统安全性与可靠性测试技术参数

指标类别	对比		
	传统方案参数	本系统参数	改进幅度
语音识别延迟（ms）	480	260	-45.80%
语音识别准确率（%）	86.5	95.4	10.30%
DMS 检测延迟（ms）	120	72	-40.00%
注意力检测准确率（%）	88.2	96.1	8.90%
UI 渲染延迟（ms）	85	42	-50.60%
系统容错切换时间（ms）	310	185	-40.30%

本系统在语音识别、驾驶员监测和交互延迟等关键指标上均有显著优化。特别是在语音与视觉双通道融合下，系统在复杂噪声和低光环境中的鲁棒性显著提升。同时，容错切

换时间缩短至 200 ms 以内，使得系统在出现异常时能快速回退至安全模式，保障驾驶安全。整体上，人工智能驱动的设计不仅提高了交互效率，也增强了系统在多工况下的稳定性与可靠性。

结语：

人工智能驱动的智能驾舱人机交互作为未来智能网联汽车的重要发展方向，既是车载信息化与驾驶安全的结合点，也是智能交通系统迈向高阶自主的关键支撑。在本研究的系统架构、设计方案与测试验证的多维分析中，可以看到技术融合所带来的双重价值：一方面，语音、视觉与触控等多模态技术的集成，使交互从被动响应转向主动感知，显著提升了驾驶体验与系统灵活性；另一方面，安全性与可靠性测试表明，算法的鲁棒性、硬件的冗余设计及软件的安全护栏能够有效降低潜在风险，实现人机之间的高效协同。未来的发展需要在开放性与安全性之间寻找动态平衡，使智能驾舱既能不断迭代功能，又能保持长期运行的稳定可控，从而真正成为智能汽车生态中安全、可信赖的中枢系统。

【参考文献】

[1]张贤, 陈波. 船舶智能驾驶舱人机交互设计研究[J]. 舰船科学技术, 2024, 46 (22): 186-189.

[2]陶建华, 龚江涛, 高楠, 等. 面向虚实融合的人机交互[J]. 中国图象图形学报, 2023, 28 (06): 1513-1542.

[3]卫宗敏. 民机驾驶舱人机交互脑力负荷预测模型[J]. 科学技术与工程, 2021, 21 (13): 5270-5274.

[4]智能座舱将重新定义人机交互[J]. 软件和集成电路, 2021, (04): 76-77.

[5]王兴宝, 雷琴辉, 梅林海, 等. 汽车语音交互技术发展趋势综述[J]. 汽车文摘, 2021, (02): 9-15.

[6]郑冬英. 基于复杂网络的战斗机驾驶舱人机交互信息网络构建分析[J]. 电脑知识与技术, 2019, 15 (09): 65-66.

[7]董勤鹏, 吴健. 基于 ARINC 661 的显控系统人机交互模拟平台的设计与实现[J]. 机电信息, 2015, (24): 136-137.

作者简介：李晓海，出生年月：1988.11，男，满族，籍贯：北京市，职称：高级工程师，学历：本科，职务：员工，研究方向：智能驾舱人机交互检测技术。