车载智能计算基础平台
参考架构 2.0
（2023 年）

中国软件评测中心（工业和信息化部软件与集成电路促进中心）

工业和信息化部装备工业发展中心

国家智能网联汽车创新中心

中国汽车工程学会

中国汽车工业协会

二〇二三年九月

顾　　问

李克强　中国工程院院士、清华大学教授

刘文强　中国电子信息产业发展研究院党委书记、副院长

瞿国春　工业和信息化部装备工业发展中心主任

张进华　中国汽车工程学会常务副理事长兼秘书长

付炳峰　中国汽车工业协会常务副会长兼秘书长

指导专家

刘法旺　工业和信息化部装备工业发展中心

高炽扬　中国电子信息产业发展研究院

安　晖　中国电子信息产业发展研究院

张文杰　国家智能网联汽车创新中心、中国汽车工程学会

王　耀　中国汽车工业协会

罗　蕾　电子科技大学

陈　渝　清华大学

许　庆　清华大学

彭　鑫　复旦大学

胡大林　北京赛目科技股份有限公司

万　蕾　华为技术有限公司

张晓先　普华基础软件股份有限公司

尚　进　国汽智控(北京)科技有限公司

丛　炜　国汽智控(北京)科技有限公司

李丰军　中汽创智科技有限公司

周时莹　中国第一汽车集团有限公司

上官云飞　远程新能源商用车集团

许　林　赛力斯汽车有限公司

孙大兴　广汽丰田汽车有限公司

王　野　合众新能源汽车股份有限公司

张　衡　东风商用车有限公司

王　恺　斑马网络技术有限公司

陈维富　黑芝麻智能科技有限公司

李玉峰　网络通信与安全紫金山实验室

刘建业　中兴通讯股份有限公司

阚志刚　北京梆梆安全科技有限公司

编写单位：

中国软件评测中心（工业和信息化部软件与集成电路促进中心）

工业和信息化部装备工业发展中心

国家智能网联汽车创新中心

清华大学

电子科技大学

网络通信与安全紫金山实验室

复旦大学

华为技术有限公司

北京赛目科技股份有限公司

黑芝麻智能科技有限公司

普华基础软件股份有限公司

合肥杰发科技有限公司

中瓴智行(成都)科技有限公司

国汽智控(北京)科技有限公司

合众新能源汽车有限公司

参研单位：

北京理工大学

合肥工业大学

中国第一汽车集团有限公司

东风商用车技术中心

上海汽车集团股份有限公司

浙江吉利控股集团有限公司

比亚迪股份有限公司

郑州宇通集团有限公司

上海蔚来汽车有限公司

赛力斯集团股份有限公司

中汽创智科技有限公司

北京经纬恒润科技股份有限公司

斑马网络技术有限公司

北京百度网讯科技有限公司

中兴通讯股份有限公司

国科础石（重庆）软件有限公司

东软睿驰汽车技术（沈阳）有限公司

北京地平线机器人技术研发有限公司

南京芯驰半导体科技有限公司

北京翼辉信息技术有限公司

易特驰汽车技术(上海)有限公司

广东为辰信息科技有限公司

上海映驰科技有限公司

中信科智联科技有限公司

智达诚远科技有限公司

目　录

第 1 章 编制背景

1.1 智能网联变革机遇期，参考架构 1.0 有效凝聚共识

车载智能计算基础平台是智能网联汽车的关键核心。智能网联汽车是决定中国汽车行业胜负的下半场。与电动化相比，智能化、网联化涉及的领域更多、程度更深、想象空间更大。智能驾驶、智能座舱、车路云一体化的快速发展，正在引发汽车创新链、技术链、产业链的重构。作为汽车的“大脑”，车载智能计算基础平台负责处理海量的异构数据、进行复杂的逻辑运算，是新型汽车电子电气架构的核心。

参考架构 1.0 为智能网联汽车研发应用创新提供了重要指引。智能网联汽车是汽车、电子信息、通信等领域跨界融合的载体和重要产物。在其发展初期，不同行业主体对汽车电子电气架构演进趋势、车载智能计算基础平台概念和架构的认识不尽相同。为推动行业凝聚共识、形成合力，2019 年，多家高校、企业、研究机构等联合制定发布了《车载智能计算基础平台参考架构 1.0（2019 年）》，为我国车载智能计算基础平台的技术创新、标准研制、试验验证、应用实践、产业生态构建等提供了参考和引导。国内已有华为、中兴、国汽智控等多家企业基于参考架构进行产品开发。2022 年中国汽车基础软件生态委员会发布《AUTOSEMO Service Framework 技术规范》，在参考架构 1.0 基础上，结合应用创新需求，构建了进一步向应用层、面向服务的架构（SOA）拓展的中间框架，通过该规范统一服务和接口，实

现整车控制器的设计与开发。

1.2 智能网联技术成长期，参考架构亟需迭代与细化

智能网联技术向更高级别自动驾驶和车路云一体化等方向迈进，参考架构需要适应发展新要求。当前 L1、L2 级自动驾驶渗透率快速增长，L3 及以上级别自动驾驶成为研发攻关的主要内容。为促进高级别自动驾驶产品的功能、性能提升，支持其商业化应用，工业和信息化部、公安部等正在筹备智能网联汽车准入和上路通行试点。北京、广州、杭州、武汉等地启动了自动驾驶“车内无人”商业化试点。多个地方的政府部门联合基础设施供应商、自动驾驶解决方案提供商、整车企业积极探索“车路云一体化”发展路线，打造技术、商业双闭环。

技术的演进、需求的丰富和认识的更新不断拓展车载智能计算基础平台的内涵和外延，参考架构需要满足发展新趋势。一是高性能车载芯片不断推出，正推进汽车电子电气架构进一步向集中化演进。英伟达雷神（Thor）、黑芝麻武当、地平线征程等系列芯片性能不断增强，满足多种跨域计算场景。二是 Linux 和 QNX 等主流车用操作系统持续增强，华为 AOS、国汽智控 ICVOS、普华 ORIENTAIS、中兴车用 OS、斑马 AliOS 等国产车用操作系统相继推出，深化了行业对车载智能计算基础平台的认识理解。三是智能驾驶、智能座舱、车路云一体化的应用场景更加具体和丰富，对车载智能计算基础平台的功能、性能、配套工具链提出更高要求。四是智能网联汽车的安全体系不断拓展和下沉，预期

功能安全、数据安全、软件升级安全等日益受到行业重视。

1.3 智能网联加速落地期，参考架构 2.0 加强前瞻引导

未来 3-5 年，智能网联汽车将创新踊跃、普及加快，对车载智能计算基础平台参考架构的需求也将更加强烈。从分域架构到“中央计算+区域控制”架构，汽车电子电气架构将继续向域集中、域融合的方向不断演进。全球高性能车载芯片、车用操作系统产业尚未发展成熟，发展格局仍未“锁定”。SOA 和空中升级（OTA）如何改变汽车软件价值链和商业模式、自动驾驶解决方案是否需要依赖高精地图和激光雷达、大模型怎样融入智能网联技术发展，都成为智能网联大规模部署所面临的热点问题。车载智能计算基础平台架构需要具备更好的包容性和技术支持能力，引导相关产品的前瞻设计和创新研发。

车载智能计算基础平台产品胜出的关键在于能否形成包括硬件平台、操作系统、应用软件、工具链在内的生态体系，构建完善的安全体系，建立技术优势和市场竞争力。这就需要统一认识理解，增强互操作性，引导提升产业生态整体水平。为此，参考架构 2.0 要在参考架构 1.0 的基础上，进一步加强前瞻性、战略性、系统性的顶层设计，在与国家标准、行业标准、团体标准术语定义保持一致的基础上，积极吸纳行业代表性研究成果，一是面向未来 3-5 年的应用需求，定义典型的应用场景，提出参考设计，指导产品研发；二是围绕高算力硬件支持、内核重构优化、系统软件构建、功能软件丰富等重点内容，引导软硬件分层解耦

的设计和开发；三是研究人工智能（AI）大模型等新兴技术，梳理构建应用生态涉及的系统软件、功能软件、工具链等需求；四是研究车载智能计算基础平台安全体系，促进智能网联汽车安全保障能力提升。

第 2 章 车载智能计算基础平台参考架构 2.0 概述

2.1 参考架构 2.0 总体框架

车载智能计算基础平台的主要目标包括，支持异构多核高算力与冗余的硬件架构、SOA 软件架构、车内高带宽主干通信网络及多种网络协议、OTA 升级等，满足高实时、多级功能安全需求、及网络安全与数据安全要求，实现软硬件的平台化、标准化，构建软硬件一体化技术体系，促进智能网联汽车的创新化、生态化发展。

车载智能计算基础平台参考架构包含异构分布硬件架构、车控操作系统、安全体系、工具链（如图 1 所示）。

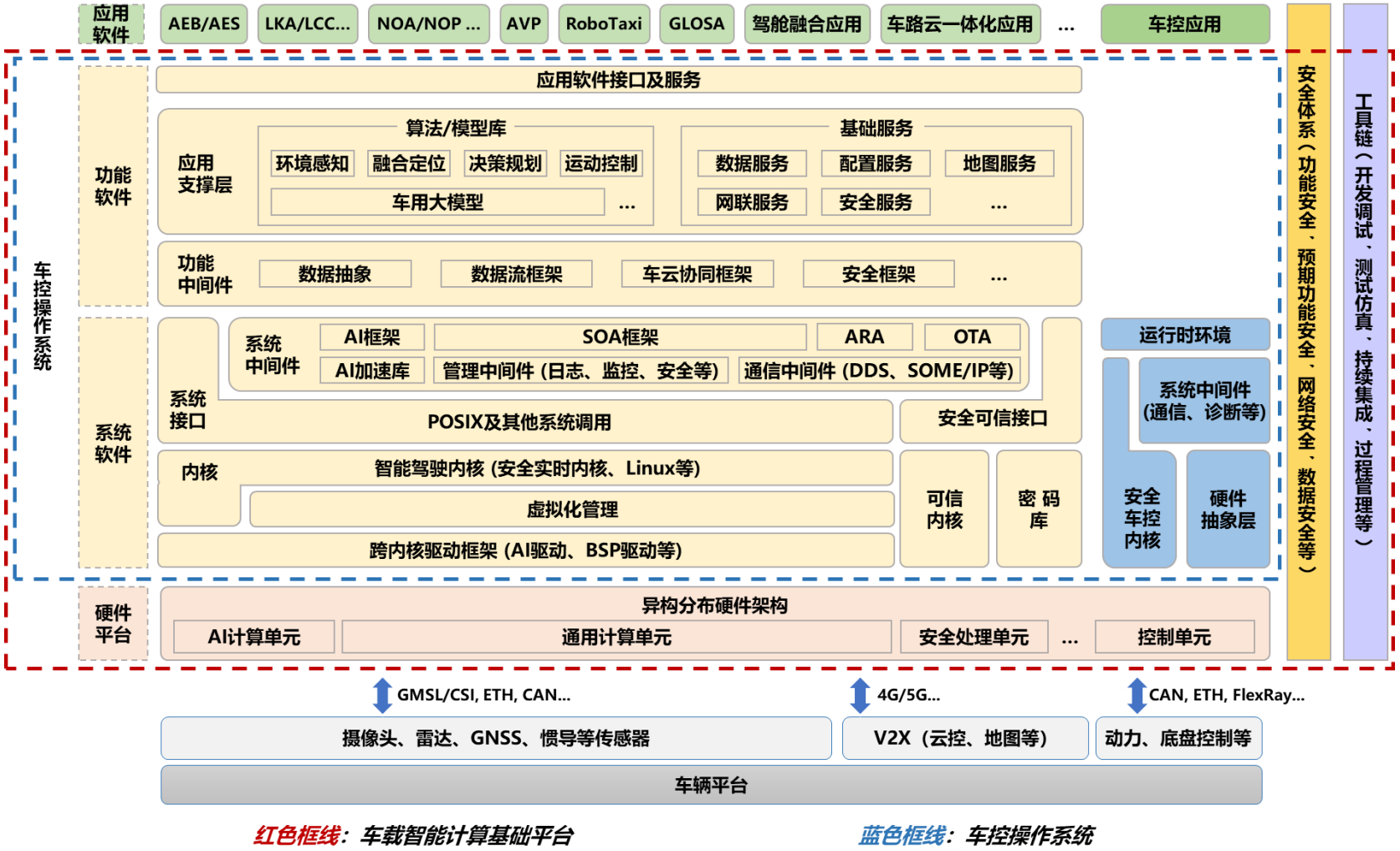

图 1　车载智能计算基础平台参考架构 2.0

异构分布硬件架构负责提供各类硬件接口和满足多方面算力需求，包括 AI 计算单元、通用计算单元、控制单元和安全处理单元等。

车控操作系统是支撑智能网联汽车驾驶自动化功能实现和安全可靠运行的软件集合。车控操作系统采用纵向分层（包含系统软件和功能软件）、横向分区（包括安全车控操作系统、智能驾驶操作系统）式架构。

——系统软件纵向分为跨内核驱动框架层、内核及虚拟化管理层、系统接口层、系统中间件层。系统软件通过标准的系统接口、系统中间件向上层提供服务，实现与功能软件的解耦；通过跨内核驱动框架（包括 AI 驱动、BSP 等各类驱动）、硬件抽象层，实现与硬件平台的解耦。

——功能软件根据各类智能驾驶功能的核心共性需求，定义和实现共性的功能组件，并通过标准的应用软件接口及服务，向上层应用软件提供服务，实现与应用软件的解耦。

安全体系保障车载智能计算基础平台的质量安全和使用安全，包括功能安全、预期功能安全、网络安全、数据安全、OTA 安全、融合安全等。

工具链为车载智能计算基础平台的开发迭代提供支撑，包括开发调试工具、测试仿真工具、持续集成工具、过程管理工具等。

车载智能计算基础平台结合传感器、V2X、动力、底盘控制乃至车辆平台，向上支撑应用软件开发。应用软件运行于车控操

作系统之上，负责智能驾驶具体功能的实现。当前 L1、L2 级智能驾驶应用已逐渐成熟普及，包括自动紧急制动（AEB）/自动紧急转向（AES）、车道保持辅助（LKA）/车道居中辅助（LCC）、自动辅助导航驾驶（NOA）/智能辅助导航驾驶（NOP）等。L3 级以上自动驾驶应用正在开发和推广之中，包括自主代客泊车(AVP)、自动驾驶出租车（RoboTaxi）、绿波车速引导（GLOSA）、驾舱融合应用及车路云一体化应用等。

2.2 参考架构 2.0 的软硬件特点

分层解耦。车载智能计算基础平台采用分层解耦的架构，既使得软件功能不依赖于底层特定硬件，更能将复杂系统划分为具有明确功能的不同层次，实现每个层次的高内聚与层次之间的低耦合，降低系统的复杂性，增加安全性、可靠性、可维护性、可移植性和可扩展性，提升开发效率，灵活实现“性能优先”和“成本优先”的差异化产品需求，更好支持不同的技术路线。

互联通信。面向人机物融合泛在计算的新模式和新场景，需要实现泛在感知与泛在互联，包括车联网（V2X）、移动通信（4G、5G）、增强的位置和导航服务、无线短距通信等。需要结合车内通信、车云通信、车人通信等业务场景，充分吸纳已有的行业标准和最佳实践，保障系统的兼容性和可移植性。

安全融合。从车载智能计算基础平台整体角度考虑安全体系建设，将功能安全、预期功能安全、网络安全、数据安全、OTA 安全有机融入到产品的设计、开发、生产、运维、报废的全过程

中。采用软硬件结合的安全技术，打造全栈内生安全体系，提升安全策略的通用性和灵活度，同时兼顾产品的性能和成本。

AI 大模型融合。探索和发挥 AI 大模型在模式识别、决策辅助等方面的提升作用，研究和把握多模态整合、多模型合并、轻量化演进等创新态势，加强 AI 大模型与车载智能计算基础平台研发、训练、应用等环节的融合，重点在数据闭环、自动标注、场景构建等云端环节使用大模型提高效率、降低成本，在智能座舱等车端环节使用大模型提供更丰富、适用的服务。

2.3 参考架构 2.0 的重点创新研究方向

车控操作系统及应用软件复杂性高、更新迭代速度快，要求车载智能计算基础平台不仅要支持基础 OTA 功能，而且要实现软硬件解耦、区域分离、接口开放、算法和软件模块可复用，满足安全性、可靠性、实时性等方面的综合需求。重点创新方向包括:

芯片与硬件平台。研究大算力实时计算、存算一体化的芯片，推动计算性能的提升。研究硬隔离技术，支持不同安全业务独立运行。研究软硬件低功耗设计，提高续航和蓄电池使用寿命。

跨内核驱动标准化。研究虚拟化/跨操作系统驱动架构，实现一次开发驱动，多操作系统内核、多虚拟化管理兼容。研究基于标准化的虚拟驱动实现与底层异构硬件解耦、平台化，满足针对异构计算平台的硬件快速适配需求，提升生态协同效率。

操作系统内核。研究面向多核环境的新型内核架构、实时调

度、高性能 IPC（进程间通信）/RPC（远程过程调用）、内存管理、安全编程语言、内核安全模型等技术。研究高安全、强实时的微内核、单内核、多内核架构设计，实现安全实时操作系统和虚拟化管理。研究兼容 Linux 服务接口的操作系统内核，继承 Linux 生态。

基于大模型的智能驾驶技术。研究大模型的云端应用技术，降低数据标注成本，提高长尾数据挖掘效率，提高自动驾驶场景构建速度和准确度。研究大模型的车端应用技术，提升驾乘适应能力和舒适性，提高导航、娱乐、通信等方面的服务水平。研究大模型与小模型协同技术，提高海量数据预处理水平和精准利用能力，进一步提升车载智能计算基础平台及智能网联汽车的智能性，降低处理延迟，提高整体效率。

安全保障技术。研究可靠冗余设计、多层多样化监测方案、失效可运行或失效降级安全模式、场景库构建与测试评估等安全技术，降低平台随机性失效或系统性失效带来的功能安全风险。研究安全可信环境构建、纵深防御体系、网络安全监测、基于内生安全的弹性工程等防御技术，从识别风险和漏洞、安全防护、安全检测、安全响应以及快速恢复等方面综合保障网络安全。研究构建面向数据采集、传输、存储、处理、提供、公开、删除和销毁全生命周期的数据安全技术体系。

工具链。研究车载智能计算基础平台开发过程的工具链，提升研发团队开发调试能力、自动测试效率、持续集成及过程

管理水平，提升软件开发质量，实现产品高质量快速迭代、分发、升级和维护。

2.4 参考架构 2.0 的主要创新点

立足新阶段新认识，依据已经量产的应用，以及面向未来车路云及中央集中趋势，进一步明确应用软件的定义，提出典型应用场景。

总体架构方面，在延续《车载计算基础平台参考架构 1.0》基本概念的基础上，固化下沉技术主框架。

硬件平台方面，升级车载智能计算基础平台硬件架构，强调安全处理单元。

车控操作系统方面，优化概念边界，扩充、迭代、细化其功能软件及系统软件各层内各模块分工及技术栈。

安全体系方面，强化技术要求及管理要求，从企业安全管理、产品过程保障出发，涵盖网络安全、数据安全、功能安全、预期功能安全、软件升级安全及融合安全等安全要素，保障车载智能计算基础平台的质量安全和使用安全。

第 3 章 异构分布硬件架构

异构分布硬件架构提供了灵活高效的计算资源集成方式，通过集成多种不同类型的处理单元，并根据各种处理单元的特点和优势，将通用计算任务、特定类型计算任务、整体控制和协调任务等分配到最适合的处理单元上，实现更高的计算性能和能效。异构分布硬件平台通常包括 AI 计算单元、通用计算单元、控制单元以及安全处理单元等。

3.1 AI 计算单元

AI 计算单元基于并行计算架构，负责图像处理、深度学习推理等数据密集型计算。架构方面，FPGA、DSP、GPU、NPU、TPU 等专用加速器等正逐渐引入到 AI 计算单元中，并负责不同的计算任务。性能方面，随着数据量的增加、复杂模型的推理和部署、实时性要求的提高、AI 应用领域的丰富以及硬件技术的进步，对 AI 计算单元的算力需求持续增长，需要通过芯片制程升级以及内存访问、数据传输、电源管理、时钟管理、电路设计的优化提升 AI 计算单元的能效。同时，运用更灵活的任务划分和卸载机制、动态任务调度和资源管理等技术，实现通用计算单元与 AI 计算单元的协同，进一步提高处理效率。通信方面，高速串行计算机扩展总线（PCIe）、计算快速链路（CXL）、英伟达高速 GPU 互连技术（NVLink）、高带宽内存、片上网络（NoC）优化等高速互联技术加快普及应用。模型和算子方面，AI 计算单元通过通用处理器和专用加速器实现对模型和算子的支持。除

了增加定点计算的比重，AI 计算单元还为矩阵计算、卷积计算、时序计算等算子以及更复杂的 Transformer 模型等不同任务量身设计计算模组，以模块化方式提升性能、降低能耗。

3.2 通用计算单元

通用计算单元负责运行复杂的逻辑串行任务。随着智能驾驶业务和算法模型的发展，对通用算力的需求也急剧增长。通用计算单元由多个车规级多核 CPU 组成，各单核主频高、计算能力强。通用嵌入式 CPU 通常采用 ARM 架构，近年来业界也在尝试基于 RISC-V 架构进行设计。在实际应用中，需要针对具体任务进行优化和并行化，以充分利用多核 CPU 的算力。

3.3 控制单元

控制单元负责为智能网联汽车子系统提供控制功能。控制单元一般为高安全强实时的 MCU，包含实时多核 CPU、嵌入式存储单元以及必要的 I/O 与通信接口。为满足实时性要求，需对 MCU 取指令的通路、数据存取通路等特别设计，同时通过提升 MCU 核心工作频率、使用实时的软件任务调度器等，减少任务切换延迟。MCU 还需要集成 Ethernet/CAN-FD 等高速接口，提供硬件的包转发、路由等功能，减少 CPU 资源消耗，降低延迟，提供数据交换的吞吐量。

3.4 安全处理单元

安全处理单元负责安全业务的处理。在硬件设计上，根据功能安全等级需求，一般采用内建自测（BIST）电路监测电路工作

状态。对于部分执行单元，采用冗余电路设计，以实现高功能安全等级要求。在数据存储模块、数据通信链路上，采用奇偶校验编码保证端到端的数据传输安全性。在架构层面，一些大型片上系统（SoC）采用安全岛技术实现对系统内功能的监控与错误处理。

为减少 CPU 负载，对称、非对称、哈希等加解密算法加速单元被越来越多地集成到芯片之中。安全与非安全执行环境的隔离既有基于虚拟化技术的逻辑 CPU 方案，也可基于硬件电路完全隔离的硬件安全模块（HSM）技术。在系统层面，需在总线、内存接口中加入安全设计，实现系统地址空间的安全隔离要求。

第 4 章 车控操作系统

车控操作系统是车载智能计算基础平台的核心部分。

按应用领域划分，车控操作系统包括智能驾驶操作系统和安全车控操作系统。其中，智能驾驶操作系统主要面向智能驾驶领域，支持感知、定位、规划、决策等功能的实现，对安全性和可靠性要求较高。安全车控操作系统主要面向经典车辆控制领域，如动力系统、底盘系统和车身系统等，对实时性和安全性要求极高。为保证车载智能计算基础平台的安全可靠，车控操作系统一般需要满足 ASIL-B 以上等级功能安全要求（安全车控操作系统需满足 ASIL-D），并根据智能驾驶需求进行适度扩展。

按逻辑层次划分，车控操作系统包括系统软件和功能软件。系统软件创建了复杂嵌入式系统的运行环境，支持环境感知、AI 计算、通用计算和实时控制。系统软件借鉴 AUTOSAR 软件架构中的分层思想，在车控操作系统中实现 Classic 和 Adaptive 两个平台的兼容和交互。功能软件根据智能驾驶共性需求，定义和实现通用模块，以填补 AUTOSAR 架构在智能驾驶方面的不足和缺失。

4.1 系统软件

系统软件是为智能网联汽车应用场景量身定制的复杂大规模嵌入式系统运行环境。系统软件从底向上包括跨内核驱动框架、虚拟化管理、操作系统内核、系统接口与系统中间件。

4.1.1 跨内核驱动框架

跨内核驱动框架主要包含四个方面。一是架构设计。定义跨内核驱动框架的整体架构，包括驱动模型、硬件抽象、核心接口等，支持常见的宏内核、微内核、混合内核架构等。二是硬件抽象。通过定义通用的硬件访问接口，实现对不同硬件的抽象和封装，方便上层驱动的移植。三是核心接口。定义跨内核的通用驱动接口，例如文件操作接口、中断处理接口、内存管理接口等，使得驱动程序能够通过统一的接口访问不同内核。四是驱动模型。定义驱动程序的基本模型和框架，例如字符设备驱动、块设备驱动、总线设备驱动等，规范驱动程序的实现方式。

车控操作系统中的跨内核驱动框架相比面向单一内核的驱动具有四方面优势。一是可移植性强。跨内核驱动只需要开发一次，就可以工作在不同的操作系统内核上，大大提高了驱动程序的可移植性。二是开发效率高。基于通用接口和硬件抽象层，开发人员不需要了解具体内核实现，就可以更快速地开发驱动。三是维护成本低。跨内核驱动代码可以重用，不需要针对不同内核做定制化工作，大大降低了维护成本。四是兼容性好且升级方便。抽象层使得驱动能够支持多种版本内核，当内核升级时，不需要重新开发和编译驱动。

4.1.2 虚拟化管理

虚拟化管理包括 Hypervisor 和虚拟机监视器（VMM）等，利用硬件辅助虚拟化技术有效地实现系统资源的整合和隔离。虚拟化管理能够管理并虚拟化 CPU、内存、外接设备等硬件资源，

并将它们分配给运行在虚拟化管理系统软件上的多个操作系统内核。车控操作系统基于异构分布硬件架构，应用程序可能需要依赖不同的内核环境和驱动，但在物理层面上要共享 CPU 等硬件资源。虚拟化管理起到了至关重要的作用，不仅能支撑实现跨平台应用的运行，而且能显著提高硬件的使用效率。

4.1.3 操作系统内核

面向复杂驾驶场景的车控操作系统内核层需要实现多内核设计。操作系统内核主要负责管理汽车的硬件资源，并为上层软件提供进程、线程、内存、网络和安全等基础支持。这些内核可兼容 Classic AUTOSAR 和 Adaptive AUTOSAR 所规定的需求。车载智能计算基础平台异构分布硬件架构中，不同单元加载的内核应具有不同的功能安全等级：支持 AI 计算单元的操作系统内核功能安全等级为 QM~ASIL-B；支持通用计算单元的操作系统内核功能安全等级为 QM~ASIL-B；支持控制单元的操作系统内核功能安全等级为 ASIL-D。这就需要安全等级不同的多内核设计，或者单个内核支持不同功能安全等级应用的设计。

目前，应用在汽车中的实时操作系统可选择 QNX、OSEK OS、VxWorks 等操作系统内核，选择时需考虑功能安全等级和市场成熟度。由于车载智能计算基础平台的复杂性，操作系统内核必须对系统软件、功能软件以及应用软件的库进行支持并且具备可扩展性和可持续演进能力。国内企业已经推出多款自主研发的操作系统内核，部分已开源并开始商用。部分内核基于 Linux，功能

全面、高效灵活、生态健全，能广泛支持芯片、硬件环境及应用程序。部分芯片企业基于自研 SoC 芯片对 Linux 和 RTOS 进行了定制优化，在增加功能的同时注重强化安全性，实现对部分 CPU 和内存资源的保护，以满足功能安全等级要求。

在异构分布硬件架构中，独立的安全处理单元已成为芯片设计的重要方向。独立的安全处理单元可支撑运行可信内核、密码库，提供安全可信的服务功能接口。可信内核增强了对密码访问的服务支持。密码库基于硬件实现椭圆曲线密码（ECC）、高级加密标准（AES）、SM2/SM3/SM4 等密码算法，提供可并发的密码服务调用。

4.1.4 系统接口与系统中间件

系统接口是操作系统内核对上层软件提供的服务接口，支持内存分配、调度管理、I/O 处理、同步互斥等功能。系统中间件向下获取操作系统内核的系统接口服务的支持，向上支撑功能软件层提供系统中间件的服务和接口。

POSIX API 提升跨多种操作系统内核的兼容性。POSIX API 有实时扩展，包括定时器和时间管理、优先级调度互斥量和条件变量、消息队列、共享内存、异步 I/O 和同步 I/O 等。

SOA 框架通常包含模块化服务、服务注册发现、标准互操作性接口、服务编排等内容和特征。

AI 框架用于支撑自动驾驶 AI 应用和大模型应用的开发。

管理中间件中包括数据加密、身份验证、健康管理、网络与

系统安全监测等安全措施及服务，对功能软件中的安全框架和安全服务等提供支撑，提升整体车控系统的稳定性和安全性。

通信中间件具备服务发现、远程服务调用、读写进程信息等典型功能，实现车内单一节点内进程间通信或多节点间通信传输，由基于 CAN 信号向面向服务的车载以太网数据包传输过度。基于 IP 的可扩展的面向服务的中间件（SOME/IP）支持复杂车载网络的服务发现和交互。在安全性方面，SOME/IP 服务发现（SOME/IP-SD）保证了车辆网络的安全。数据分发服务（DDS）分布式通信协议可以提供灵活、可靠、实时的数据交换机制，以满足智能网联汽车中多种应用程序之间的通讯需求，并确保数据的准确性和及时性。DDS 还可以提供良好的扩展性和互操作性。

4.2 功能软件

功能软件根据智能驾驶共性需求定义和实现通用模块，是支撑智能驾驶应用生态建设的重要层级。功能软件包括功能中间件、应用支撑层、应用软件接口及服务。

4.2.1 功能中间件

功能中间件是功能软件的核心和驱动部分，由数据抽象、数据流框架、车云协同框架、安全框架组成。一方面，针对智能驾驶产生的安全和产品化共性需求，通过设计和实现通用框架模块来满足这些共性需求，是保障智能驾驶系统实时、安全、可扩展和可定制的基础。另一方面，随着高阶智驾应用的逐步实现，面对更复杂更多样的场景，可以通过车云计算框架对云端的强大算

力和存储资源进行利用，实现对大规模数据的高效处理和分析，以及利用云端的算法和模型进行更复杂和高级的决策和规划，提高智能驾驶系统的感知、决策和控制能力。

数据抽象是针对不同传感器、车辆底盘、外围硬件等的原始数据进行处理和封装，提供统一的数据格式。通过标准格式为上层的智能驾驶通用模型提供各种不同的数据源，进而建立异构硬件数据抽象，达到屏蔽硬件差异、开发平台差异，应用软件与系统软件分层解耦。

数据流框架是依托中间件技术提供标准数据接口和实时数据处理框架。数据流框架一是能够屏蔽不同硬件平台及系统软件的差异，确保功能软件之间的解耦和可靠通信；二是提供智能驾驶功能的编排、调度及部署，对各个智能驾驶系统组件和任务进行协调，提供合理的任务分配和调度机制；三是支持对智能驾驶应用和算法的数据流节点的拓扑关系进行配置，以及进行任务、计算单元、实时性等多个维度的调度管理配置；四是结合系统性能及功能安全等需求，将不同的节点配置到特定的 AI 加速单元、计算域、安全域等处理单元，在系统运行过程中能够实时调整应用和算法节点的拓扑关系及调度策略。

车云协同框架实现了智能网联车与云计算、边缘计算等关键车路云协同技术的有机融合。车云协同框架需要提供可靠的数据传输和同步机制，以确保车辆与云端之间的数据传输和同步的效率和准确性，以及提供可靠的网络通信和安全机制，同时支持车

辆端和云端之间的协同处理，将计算任务在不同的计算资源之间进行分布和协作。

安全框架提供了一系列的安全机制和措施，包括对硬件设备、操作系统、应用程序等进行实时监测，在发现相关故障时及时处理，防止故障蔓延，进而影响整个系统的运行。其中，安全监控模块包括设备监控、资源监控、应用程序监控等，在检测到异常状态时，通过安全监控及时上报，由安全监控服务程序根据系统配置进行决策处理。

4.2.2 应用支撑层

应用支撑层使用 SOA 服务等方式为智能驾驶功能提供支持，主要包含算法/模型库和基础服务。算法/模型库提供智能驾驶应用的可拆解重组的算法模块和原子组件库，支持组件式开发，并可自由扩展和引入第三方单元可插扩算法模块，快速实现环境感知、决策规划、车辆控制等算法开发。随着深度学习和神经网络、多模态感知、强化学习等技术发展，模型库提供的算法模块需要不断丰富扩展，借助新技术，以适应更复杂、更广泛的智驾应用场景。基础服务为智能驾驶系统提供必要的功能和支持，支持智能驾驶系统的安全、可靠和高效运行，随着智能驾驶技术的发展，数据安全和网络安全将成为更加关键的问题，功能要求更加全面和智能化，基础服务需要具备可扩展性，不断演进和创新，以应对智能驾驶技术的挑战和需求。

1）算法/模型库

算法/模型库由多个独立的算法模块及模型组成，用户可通过对这些模块的直接或组合使用,形成智能驾驶系统中不同的功能。智能驾驶算法库主要为支撑智能驾驶算法进行高效开发，提供智能驾驶应用的可拆解重组的算法模块和原子组件库，支持组件式开发，并可自由扩展和引入第三方单元可插扩算法模块，快速实现环境感知、决策规划、车辆控制等算法开发。

环境感知是对车辆周围的环境和道路条件进行感知和理解，帮助智能驾驶系统决策规划。感知算法模型库提供预置的可拆解重组的感知算法原子组件，包含基于 Transformer+BEV 技术下的多模态多种传感器下的端到端感知模型组件化和配置化开发。支持使用各种传感器（如摄像头、毫米波雷达、激光雷达等）获取车辆周围环境的信息，通过 V2X 通信接收来自其他车辆、交通信号灯以及交通管理中心的实时信息，将来自不同传感器的数据与 V2X 实时交互信息进行融合，使智能驾驶系统获得更加准确和完整的环境感知结果。

融合定位是指利用多种传感器技术对车辆位置和环境信息进行综合处理，以实现精确的定位和导航功能。融合定位模型库提供预置的可拆解重组的融合定位算法原子组件。通过将不同传感器的数据进行融合，可以提高定位的准确性和鲁棒性，从而更好地支持智能驾驶系统对车辆的控制和决策。融合定位技术在智能驾驶领域具有重要的应用价值，可以提高车辆的定位精度、抗干扰能力和安全性，为实现可靠的智能驾驶提供基础支持。

决策规划是基于感知和预测结果进行路线与轨迹的决策规划。规划模型库提供预置的可拆解重组的规划算法原子组件，包括通用 AI 和规则的决策规划算法组件化和配置化开发，实现对道路环境进行全面、精细的建模和理解，对交通参与者的行为和意图进行准确的预测和分析，制定出最优的行动策略。

运动控制是根据决策规划的输出结果，对车辆的横纵向进行控制。运动控制模型库提供预置的可拆解重组的控制算法原子组件，包括主流的横纵向控制算法组件化和配置化开发，实现根据决策规划结果，对车辆进行精确的操控和控制策略的实施。

车用大模型是指在智能驾驶系统中应用大型的深度学习模型来处理感知数据、做出决策以及规划行车路径等任务。利用车用大模型，将环境信息输入到神经网络中进行特征提取和识别，决策阶段将感知结果作为输入，经过神经网络的推理和判断，输出对车辆行为的预测和路径规划，控制阶段将决策结果转化为车辆的具体控制指令，如转向、加速、制动等。使用车用大模型可以显著提升智能驾驶系统的感知、理解和决策能力，使得车辆能够更加准确地识别和适应各种复杂的交通环境。

2）基础服务

基础服务支持智能驾驶系统的安全、可靠和高效运行，包括数据服务、软件升级服务、安全服务、网联服务、地图服务等。这些基础服务在智能驾驶操作系统中起着关键的作用，支持智能驾驶系统的安全、可靠和高效运行。它们相互协作，为智能驾驶

系统提供必要的功能和支持。

数据服务为智能驾驶车辆提供数据采集和处理的服务。需要支持数据的采集、触发、回传等能力。采集服务负责采集任务的生命周期管理，包括任务建立，收集数据、放入缓存。需要在资源有限的情况下做数据采集，采集对象为结构化数据和非结构化数据。可以通过相关的配置，对采集的数据、频率、策略以及存储策略等进行定制化管理和限制。

配置服务对外提供统一的配置接口，支持进行外部链接，获取用户配置设定，以及返回配置后的结果。可以依据需求通过动态库和配置来进行加载和使用。在与各种用户界面（UI）进行交互时，配置服务应提供统一的数据获取与数据发送的方式，便于各种 UI 进行相关的适配。配置服务还应负责处理和缓存所有的数据，保证数据的一致性，并统筹处理命令冲突的决策。

地图服务提供高精度、实时的地图数据，以支持智能驾驶系统的定位、路径规划和决策制定。实现系统与不同厂商的高精地图数据接入，支持高级驾驶辅助系统（ADAS）功能获取地图相关的感知数据，支持基于高精地图的定位服务。地图服务提供了包含 EHP（电子地平线提供者）、EHR（电子地平线解析者）在内的一系列模块，并对外提供统一的接口获取数据。

网联服务是指智能驾驶技术和网络技术相结合，使车辆通过互联网实现数据交换和通信。可通过网联服务实现车辆间交通信息共享和云端控制等。为智能驾驶系统提供远程监控、数据上传

和指令下发等功能，可以实时获取实时交通信息、车辆的状态、位置、传感器数据等信息，进行数据分析和处理，并根据需要下发指令给车辆，以实现远程控制和协同操作。同时，可实现对智能驾驶车辆的协同管理和智能决策。

安全服务包括数据安全、网络安全、AI 安全等，为智驾系统提供基础安全服务。为车辆数据和个人隐私提供了全生命周期的安全防护机制，并保护智能驾驶系统免受未经授权的访问、篡改和破坏。采用不同的防护手段，以数据安全分级为基础，按照一定的规则和策略实现对数据进行全生命周期的管控，包括对数据建立分类分级处理机制、对敏感个人信息进行加密、提供安全的数据传输通道、对车外个人信息进行脱敏等。对车载智能计算基础平台的系统完整性保护、机密性保护、身份和访问权限控制、安全管理和安全隔离，边界和通信安全，智能驾驶应用安全等。提供模型加密、模型完整性验证等方式确保模型的安全性，避免遭受对抗性样本攻击，模型篡改等问题。

4.2.3 应用软件接口及服务

应用软件接口及服务是车控操作系统为应用软件开发所提供的封装程序，降低技术门槛，提升开发效率。应用软件接口主要包括配置接口、加载接口和数据交换接口。配置接口主要为传感器和执行器的适配和标定提供相应接口；加载接口主要为开发模板及组件的加载提供相应接口，可实现自定义组件的定制化开发，以及数据流框架的节点编排、部署和调度；数据交换接口实

现应用软件与功能软件之间、功能软件内部算法之间的数据交换，应包括传感器接口、执行器接口、自车状态接口、地图接口、感知融合接口、定位接口等。用户可基于接口开发应用软件，依靠拆解可重组算法库的开发方式，使运行时调度和函数级服务更加自主灵活，不同应用之间的功能软件组件可高度复用；同时，可通过服务配置和接口，进行功能服务差异化配置和扩展性开发，支撑软件灵活迭代，为用户提供千人千面的用户体验。这些接口和服务共同为智能网联汽车系统的开发和应用提供了支持和便利。

第 5 章 工具链

完善的工具链对车载智能计算基础平台产品快速开发迭代、高质量交付具有关键作用。工具链为汽车软件开发过程(V 模型、敏捷开发等)的各阶段提供安全、易用、可扩展的支撑。软件开发过程一般包含需求、架构、开发、测试、集成、验证等环节，环节之间需要通过工具链建立数据流或工作流的链接，实现研发的数据统计和过程追溯。各环节可使用独立的工具，也可使用一套工具支撑多个环节甚至整个产品的开发过程。企业可根据技术和成本等因素选择一体化工具链、多来源组合工具链或自研工具链。工具链应具备开放性、兼容性和互操作能力，能够适应各类业务场景，形成无缝协同的一体化平台，支持软件模块的复用，降低开发成本，提升开发效率。

5.1 开发调试工具

开发调试工具是进行软件开发、配置、编译、调试、源码管理、版本管理和软件发布的可视化集成开发环境。开发调试工具需要支持的编程语言包括 C/C++、Rust、Python、Java 等。

5.1.1 开发工具

开发工具用于处理开发过程中架构设计、模块定义以及通信模式搭建等任务。在架构设计阶段，开发工具以图形化的方式创建和修改架构，通过配备丰富的模板支持快速创建和定制各种系统元素，简化系统架构设计的复杂性。在模块定义阶段，开发工具提供模块和接口的定义、配置功能，提高系统的可维护性和稳

定性。在通信模式搭建阶段，开发工具支持多种通信协议和标准，能够设计和验证通信路径。开发工具支持自动驾驶应用场景库扩展，覆盖算法从训练到推理的研发过程，具备采集、回放、清洗、标注的数据闭环能力。

5.1.2 配置工具

配置工具辅助实现软硬件抽象，屏蔽软硬件的差异性、复杂性，支撑产品模块化、标准化。配置工具一般包括基础软件配置工具和应用软件配置工具，支持模块化、标准化代码生成和验证。基础软件配置工具强调硬件抽象，使得基础软件能够屏蔽硬件的复杂性，为上层应用提供统一的接口，简化软件开发过程。应用软件配置工具支持对软件组件进行模块化设计和配置，使得开发人员能更加专注于应用层功能。

5.1.3 调试工具

调试工具可支撑实时或离线的故障定位和问题分析，提高车载智能计算基础平台调试效率。调试工具主要包括标定工具、运行监控工具、数据录制与回放工具等，可以将产生的边角案例（Corner Case）保存下来，用于支撑自动驾驶场景系统失效故障分析。

5.1.4 集成工具

集成工具可将多个开发环境跨平台整合到一个工具环境中，提供无缝集成的软硬件基础设施和标准化接口。集成工具包含编辑器、编译器、调试器和构建工具的应用程序，具备模块化设计、

代码自动生成、组件配置和参数管理等功能，支持可扩展的自动驾驶应用场景库、车云一体化的敏捷集成开发模式。

5.2 测试仿真工具

测试仿真工具可支撑算法、软件的测试验证，以保证车载智能计算基础平台的质量和可靠性。测试仿真在保障软硬件功能符合需求定义的基础上，进一步满足功能安全、预期功能安全、网络安全等要求。

5.2.1 测试工具

测试工具具备测试用例自动化执行，测试流程标准化管理和报告生成等功能。测试工具用于单元测试、集成测试、系统测试等关键环节，支撑验证软硬件的功能、性能、安全和可靠等测试内容，帮助规范测试方法和测试流程。

5.2.2 仿真工具

仿真工具用于模拟自动驾驶运行场景及软硬件环境。仿真工具包括虚拟仿真工具和物理系统在环仿真工具，可以模拟车辆控制、静态场景、动态交通流、感知传感器等，支持自动驾驶设计运行场景及响应测试。仿真工具具备多种核心能力，包括测试场景库建设能力、仿真场景生成能力、场景孪生测试能力、云端大规模并行加速测试能力等。仿真测试根据不同阶段可分为模型在环、软件在环、处理器在环、硬件在环、车辆在环等。

5.3 持续集成工具

持续集成工具具有自动化的检出代码、编译构建、运行测试、

结果记录、测试统计等功能，是实现车载智能计算基础平台敏捷开发流程的重要支撑。车载智能计算基础平台不仅包含了传统的软件代码，而且包含了数据驱动的智能模型。持续集成工具进行自动编译、发布、测试和监控，通过周期性自动化测试，实现高效敏捷开发流程，提高软件、模型开发部署的效率。

5.3.1 开发运维一体化（DevOps）工具

DevOps工具可用于执行智能驾驶算法和软件构建过程中的代码仓库管理、依赖管理、代码编译、代码分析、安全测试等任务。DevOps 工具解决了研发维护成本高，缺少数据共享平台、权限共享机制等问题，可以减小算法集成与灌装上车的交付风险，缩短产品迭代周期，加强过程保障。

5.3.2 模型运维一体化（ModelOps）工具

ModelOps工具用于执行对自动驾驶AI模型的搜索、转换、压缩、测试与训练任务。ModelOps 工具可以提升模型质量及其开发速度，分配计算资源，提升模型的推理响应速度，减少资源消耗，确保数据安全和隐私。

5.4 过程管理工具

过程管理工具可以全面地规约车载智能计算基础平台相关软件过程的需求、复用过去的过程经验，减少过程开发和改进中的重复劳动。过程管理工具可为软件质量管理体系提供基于软件开发数据的客观证据，使产品研发过程满足 IATF16949、ASPICE、GB/T 34590、ISO 21434 等标准要求。

5.4.1 需求规约与管理工具

需求规约与管理工具进行涉众需求获取、分析、管理，保证需求的一致性和可追踪性。需求规约与管理工具包含需求获取工具、需求分析与规约工具、需求评审工具、需求管理工具，具备协作功能，可以实现多人在线协同。

需求获取工具可以适应不同项目、层次、类型的需求，支持包括汽车软件功能、性能效率、安全性、可靠性等需求内容的收集。需求分析与规约工具面向不同类型汽车软件原始用户需求，制定系统需求，生成软件需求，形成符合规范的规约描述。需求评审工具具备自动化分析和验证需求的能力，通过模型检查、形式化验证或其他技术自动化检测需求之间的冲突、不一致性或遗漏，提供相应的反馈和建议。需求管理工具支持需求追踪、需求变更，可以可视化追踪关系，扩展并维护追踪关联，根据需求标识符或名称定位需求，获取需求的状态、开发进度等信息。需求管理工具可以生成报告或报表，为决策与规划提供依据。

5.4.2 任务和缺陷管理工具

任务管理工具提供各类开发任务的建立、分配、状态和进度管理、历史查询分析等功能。任务管理工具与代码版本管理工具之间需要建立任务与代码提交操作的关联关系，支撑对代码修改原因的深入回溯分析。缺陷管理工具为软件中发现的缺陷提供全生命周期的管理，覆盖从缺陷提出到修复验证的整个缺陷生命周期，实现缺陷的快速发现、全程追踪、及时消除和主动预防。

5.4.3 代码分析与追溯工具

代码分析与追溯工具用于跟踪、评估、优化代码质量，确保交付高质量、可追溯的软件产品。代码分析与追溯工具包括静态分析工具、动态分析工具和源代码演化追溯工具。模型或代码静态分析通过程序分析等技术识别代码中的潜在缺陷。模型或代码动态分析有助于发现代码中的潜在错误、漏洞和异常情况，通过持续监测和代码测试，确保代码符合开发规范，减少缺陷数量，规避已知漏洞。源代码演化追溯工具用于实现对软件代码变化历史的细粒度分析，呈现代码质量问题引入、发现和修复的过程，进一步根据代码依赖关系，对可能处于受影响范围内的代码进行质量回溯，最大限度地从源代码级别识别出质量问题的原因。

5.4.4 软件供应链安全工具

软件供应链安全工具用于检测商业或开源软件安全漏洞、许可证合规性等问题。车载智能计算基础平台上运行的软件往往来源于不同的供应商，包含大量开源组件，可能存在安全漏洞、许可证不合规、版本更新不及时等问题。软件供应链安全工具可以实现软件组件级、源码级和二进制级的组成成分分析，构建软件物料清单，在此基础上实现安全风险分析、许可证合规分析、维护风险分析。

第 6 章 安全体系

车载智能计算基础平台是整车的计算核心和智能驾驶的功能载体，也是整车安全保障的基础关键和核心要地。安全体系保障车载智能计算基础平台的质量安全和使用安全，包括功能安全、预期功能安全、网络安全、数据安全、OTA 安全、融合安全等。

6.1 功能安全

车载智能计算基础平台需要根据 GB/T 34590 相关标准规范，降低随机性失效或系统性失效带来的风险。加强功能安全，可以从监测方案、安全模式、安全测试用例库、产品过程管理、人工智能安全等五方面考虑。

6.1.1 多样化监测方案

车载智能计算基础平台可采用多样化监测方案，对于重要输入数据采用循环冗余校验（CRC）、范围校验等多重校验方式，验证输入数据的正确性、有效性；对于重要输出数据采用多种计算方式，设置安全机制，优先使用安全保障程度更高的数据或通过仲裁等方式判断最终输出；对于重要模块或单元采用程序流监控等方式监控其运行状态。

6.1.2 失效可运行或失效降级安全模式

车载智能计算基础平台重要硬件需考虑冗余设计，确保发生故障时能够快速切换到备用模块。软件采用分层架构，各层之间通过定义接口进行交互，降低耦合度，保证软件模块的独立性；重要的软件功能模块设计冗余机制；加强软件各层的容错处理，

发生故障时可以自动重启、重试或开启备用模块，避免整体系统失效。

6.1.3 安全测试用例库

构建标准化的功能安全测试用例库，测试用例有明确的预期结果和合格判断标准，支撑开展面向多样化复杂场景的仿真测试与实车测试；注重构建持续的数据收集和反馈机制，软件运行过程中持续监控返回的数据，不断丰富和完善测试用例，积极推动功能安全测试由经验驱动向数据驱动转变。

6.1.4 产品过程管理

充分集成并严格优化现有安全工程流程，实施贯穿“概念、研发、生产、运维、报废”全流程的安全管理，确保功能安全可覆盖产品全过程。

6.1.5 人工智能安全

保证自动驾驶通用模型算法的开发流程严格遵守功能安全要求；确保模型经过足量学习训练且通过测试验证，在真实场景下具备良好鲁棒性和容错性；确保 AI 计算单元、通用计算单元等硬件的随机失效率满足安全要求。

6.2 预期功能安全

以失效风险预防、探测、消除为核心的传统功能安全体系已无法满足自动驾驶车辆的安全保障需求，需要聚焦因设计不足或性能局限风险的预期功能安全（SOTIF）。为最大限度保障汽车预期功能安全，车载智能计算基础平台应符合 ISO 21448 和

ISO/AWI PAS 8800 相关要求，综合应用功能优化、性能提升、风险监测防护、异构冗余设计等多种安全保障手段，在设计开发、分析评估、验证确认、测试评价、功能改进、发布等环节予以全面保障。

6.2.1 功能性能提升

为适配新型外部传感器、处理大流量实时数据，在感知定位、决策规划、控制执行领域进行软硬件优化。软件层面，面向各类感知决策算法，从模型选择、网络结构、训练策略、数据质量等方面优化调整，重点考虑车用大模型、对抗训练、迁移学习、高效数据清洗、数据增强等技术。硬件层面，应进一步优化硬件单元的计算及处理性能和能效，综合提升车载智能计算基础平台处理的可移植性、准确性、鲁棒性、实时性。

6.2.2 风险监测防护

聚焦 SOTIF 场景长尾效应导致的未知风险，建立感知定位、决策规划、控制执行相关风险监测模型。综合利用外部感知信息和车辆动力学信息，分析汽车所处环境与设计运行域关系，提高预期功能安全风险综合认知能力，及时通过功能限制或请求驾驶员接管以降低风险。注重基于关键场景数据反馈的系统更新优化机制,加强数据驱动下的持续迭代学习，依托 OTA 等远程升级技术共同构建具备自学习、自适应的 SOTIF 风险防护体系。

6.2.3 多层级异构冗余设计

针对单一软硬件的局限性及设计不足，考虑关键部件、关键

系统的异构冗余设计。感知层面，应采用多传感器融合方案，综合各类传感器在不同场景下的优势，分别在数据级、特征级及目标级实现融合，提高环境要素识别完整性。决策层面，应考虑规则驱动与数据驱动相结合的混合决策机制，以提高决策过程及结果的可靠性、可解释性。控制层面，应注意完善面向中、高风险工况的冗余控制方案。系统层面，可考虑“高阶+低阶”的自动驾驶系统冗余配置方案,避免单一风险导致整体安全问题，同时可通过多组件间的互补提高整体功能性能。

6.2.4 测试评估

为确保预期功能安全风险可接受，应推行基于优先场景库的高效自动驾驶测试方法，并遵循 SOTIF 双层安全接受准则开展量化评估。测试方面，应注意场景要素的合理解耦，依据要素敏感性、严重度、暴露频次等综合评估筛选出场景优先度子集，建立优先场景库；构建高效高保真的仿真模型，开展基于优先场景库的自动驾驶仿真测试，提高自动驾驶测试效率，用更少的测试里程达到更充分的验证效果。评估方面，应严格遵循危害行为事件接受准则、总体安全风险接受准则、自动驾驶里程累积测试终止原则等基本原则，通过可控性、SOTIF 信心度等安全度量指标，量化评估自动驾驶车辆预期功能安全水平。

6.3 网络安全

网络安全旨在保障平台网络系统软硬件及数据不因偶然或恶意原因被破坏、更改、泄露，是智能网联汽车设计、开发、生

产、应用、运营、维护全生命周期中不可或缺的关键要素。网络安全保障应遵循最小权限设计、周期性安全测试、攻击面收敛等原则，同时需坚持整体安全观，综合考虑安全风险识别、安全防护、安全响应以及韧性抗毁等方面。

6.3.1 安全风险识别与管理

为提升网络安全防护的精准性和高效性，应加强对安全风险的识别、共享和规范管理。安全风险识别方面，应开展平台网络安全检测，从传感器干扰欺骗、AI 对抗攻击、越权访问、软件漏洞、系统后门等安全风险入手，结合其危害性和延续性，综合评估风险等级。依据优先级实施风险应对措施。推动共享网络安全信息情报，落实已知漏洞和网络威胁对策，构建威胁数据及防护产品标准库。网络安全风险管理方面，应强调构建全过程的网络安全保障能力，建立平台供应链网络安全责任共担机制，将操作系统等重点防护和平台整体防护相结合。

6.3.2 安全可信基础能力建设

为了确保车载智能计算基础平台基础能力的安全可靠性，需要强化安全可信基础能力建设。综合运用硬件安全模块（HSM）、可信执行环境（TEE），建立信任锚点，构建跨域认证机制，形成车载智能计算基础平台的安全可信基础能力。需要融合身份认证、网络安全监护、数据加密、实名注册等安全措施，同时兼顾车载模块资源紧缺因素，建议采用轻量化防护措施，提升车载智能计算基础平台安全可信的能力。需要加强车载智能计算基础平台设

计、建设、运行、维护等服务实施安全管理，采购安全可信的网络产品和服务，确保供应链安全。此外，需要制定车载智能计算基础平台相关技术标准、管理标准和过程标准等，为保障其基础能力安全可控提供标准化参考准则。

6.3.3 纵深防御体系构建

车载智能计算基础平台需要建立具备纵深防御、长期监控和全生命周期的网络安全防护体系。需考虑平台与外部环境、平台与车内网络各节点的访问隔离及网络层安全；需要考虑从硬件、固件、系统软件到功能软件的全栈软硬件防护，并建议将加密认证、防火墙、异常检测等防护标准化、模块化，以方便供给侧实现；需要考虑与车内网其他节点以及 V2X 节点和云端的传输安全。车载智能计算基础平台也要求其内部多域之间的访问控制和监控、与执行器传输的高等级认证和加密要求、更多代码安全、海量数据的存储安全如防泄漏功能，以及相应的 OTA 升级支持等等。同时，需对车载智能计算基础平台运行状态、产生输出的数据、车载网络流量等方面进行实时监测和风险评估，强化车载通信端口与路侧通信设备、服务云平台等节点网络通信的监测能力，防范网络侵入、数据窃取、远程控制等安全风险，防止车载智能计算基础平台隐私数据泄漏、重要数据非法出境等异常情况。

6.3.4 网络弹性赋能

为了提升对已知/未知网络攻击威胁的容忍能力，传统网络安全范畴需要向网络弹性赋能方向演进发展。智能网联汽车作为

复杂物理信息系统，容易遭受各类已知/未知的网络攻击威胁。传统网络安全侧重从预防、抵御两方面制定防护目标及措施，难以提升智能网联汽车应对未知网络攻击的快速恢复、主动适应的能力。因此，需要建立涵盖预防、抵御、恢复和适应等安全能力。车载智能计算基础平台需要建立能够感知抵御已知/未知威胁的弹性防护能力。强调构建、设计、开发、实施、维护和维持平台的可信度。实施融合安全策略，运用内生安全、动态防御、安全监控等技术，使平台具有预测、感知、承受、恢复和适应不利条件和攻击的能力。

6.4 数据安全

车载智能计算基础平台是整车数据的汇集和处理核心，须充分重视数据安全。车载智能计算基础平台在数据的开发利用上要依法依规开展，满足合规要求。国际层面，以欧盟通用数据保护条例（GDPR）为代表；我国为规范数据处理活动，保障数据依法有序自由流动，发布了《数据安全法》、《个人信息保护法》，并以此为基础，不断推出和完善关于智能网联汽车数据安全的政策法规、标准体系，为数据安全保障提供了具体指引和实施参考。

车载智能计算基础平台要建立以数据为中心、面向业务数据流转、按需防护的数据安全管理体系。对平台设计、研发、生产、运维、报废等过程中涉及的数据分级分类，明确数据分类分级的安全技术保护要求。构建以数据收集、存储、使用、传输、删除和出境安全为核心的数据安全技术体系。数据安全保障措施应与

车载智能计算基础平台产品同步规划、同步建设、同步使用，围绕数据处理的各个场景，实现数据全过程保护。

6.5 软件升级安全

设计并建立车载智能计算基础平台软件升级安全防护体系，不仅是智能网联汽车安全性要求，也是影响车辆系统基础功能稳定运行的关键因素。软件升级是使系统保持具备最新功能和更高安全性的根本途径，但是软件升级环节也面临较为严重的安全威胁，针对软件升级包和升级过程的篡改、破坏、窃取、伪造等攻击手段给系统以及行车安全带来巨大风险和安全隐患。

车载智能计算基础平台需遵照各类政策法规与标准要求建立可靠的软件升级安全保障体系。针对车辆软件升级，国际上出台了 R156 法规，即《关于就软件更新与软件更新管理系统批准车辆的统一规定》，我国的强制性国标《汽车软件升级通用技术要求》已进入审查阶段，用以支撑对汽车生产企业的软件研发管理体系以及车辆升级功能的监管与规范。

车载智能计算基础平台软件升级安全，需在软件发布和升级使用中通过有效的安全建设方法和技术手段，确保软件升级的安全可靠。整车企业要建立软件升级管理体系，并加强软件升级安全测试体系与安全基础保障能力，在已有技术要求与管理机制基础上，参考网络安全与数据安全体系架构，梳理智能网联汽车安全相关标准、规范，以标准属性作为分类维度构建体系框架，逐步健全和完善系统软件升级全流程管控体系。软件升级包的真实

性和完整性应受到保护，以合理方式防止软件包被破坏并阻止无效的软件更新，设备端需部署保护机制，确保仅可执行经过安全认证和完整性校验的软件升级包。在用户安全与合法性层面，须制定可靠的软件升级策略，特别对于 OTA 升级，须按规定要求进行备案，并且无论采用 OTA 模式还是传统有线升级模式，在软件升级前后务必尽到用户告知义务，并在功能层面禁止非驻车模式、电量不足等情况下的软件升级，避免安全隐患。对于可能出现的升级失败场景，部署自动回滚机制，确保设备系统始终可恢复至安全状态。最后，设备系统需具备记录升级过程的能力，对于每次软件升级，按规范要求记录数据信息并保存规定时限，以供安全审计使用。

6.6 融合安全

数据安全、网络安全、功能安全和预期功能安全在智能网联汽车身上并不是孤立存在的，它们相互影响，甚至特定条件下相互转化，产生了严重的融合安全问题。面对融合安全问题，依靠单方面安全已无法保障系统安全，亟需进行功能安全、预期功能安全、网络安全及数据安全的协同研究，突破各类安全领域的共性技术问题，更加系统地保障智能网联汽车产品安全。

依托 V 型开发流程，从融合安全风险辨析、一体化防护、协同联动测试、综合论证评估及全生命周期监测五个阶段开展：在融合安全风险辨析阶段，重点研究融合安全特征及风险传递机理、协同相关项定义、威胁/危害识别及融合安全目标分类分级的相

关内容；在融合安全一体化防护阶段，重点考虑协同优化设计、一体化安全架构及安全机制冲突解决等内容；在融合安全协同联动测试阶段，重点关注基于“三支柱”的联动测试方法及在具体测试过程中，测试对象、人员、场景、用例与工具等的协同；在融合安全综合论证评估阶段，构建融合安全多层级评价指标系统，依托全面的安全体系进行系统安全确认。面向全生命周期开展融合安全监测，包含融合态势感知、异常监测预警相关内容。

第 7 章 发展建议

车载智能计算基础平台是实现汽车智能化的创新底座，也是保障智能网联汽车供应链安全的基础核心。国内外企业积极布局车载智能计算基础平台研发，已取得丰硕成果。建议集中资源，凝心聚力，打造架构统一、生态完善、具有产品竞争力的车载智能计算基础平台。

7.1 凝聚发展思路，统筹协作竞争

凝聚行业共识，明确车载智能计算基础平台的发展目标、参考架构、关键核心技术和重点攻关任务。统筹不同的技术路线，突破关键共性技术。鼓励联合攻关和合作开发，鼓励开源开放，降低开发成本，提升开发效率。支持企业在具体技术实现、应用场景、商业模式等方面持续深耕，挖掘细分领域市场，开展差异化良性竞争，充分发挥企业比较优势。

7.2 鼓励技术攻关，加快生态构建

围绕车载智能计算基础平台参考架构，攻关车规级计算芯片、车控操作系统、核心算法、开发测试工具链等核心技术。充分发挥专精特新、揭榜挂帅、科技专项等政策机制引导作用，构建协同开放型技术创新体系，政府、行业、企业联动，打通“基础前沿—重大共性关键技术—应用示范研究”的技术创新全链条。鼓励整车企业构建多元化产业应用生态，以整车带动核心零部件集成应用；建立开放型产业链协同创新环境，繁荣智能网联汽车生态。

7.3 完善标准体系，探索开发实践

聚合行业优势资源，同步推动相关接口标准的规范化建设，推动实现软硬件分层解耦以满足底层操作系统与芯片的高效适配。通过编制完善产业发展指导性文件以及国家、行业、团体标准体系，增强解决方案的通用性与可移植性，促进产业链的精细化分工与密切配合，提升产业链协同开发效率。探索基于参考架构和标准的开发实践，强化标准牵引能力。

7.4 加强检测认证，强化安全保障

建设第三方检测认证体系，涵盖车载智能计算基础平台关键质量特性、软硬件接口、安全合规等。一方面可以通过建立基础门槛，以加强产品质量保障；一方面可以更好地促进上下游之间的沟通互信。跟踪国际国内最新的安全技术研究成果和法律法规，鼓励检测机构提升软硬件检测能力，重点完善功能安全、预期功能安全、网络安全、数据安全、软件升级检测认证体系。以测促研，以评促用，加快推动产品研发和试点示范。鼓励数据共享与检测认证结果互认。

附件：缩略语

缩略语	英文名称	中文名称
ADAS	Advanced Driving Assistance System	高级驾驶辅助系统
AEB	Autonomous Emergency Brake	自动紧急制动
AES	Automatic Emergency Steering	自动紧急转向
AES	Advanced Encryption Standard	高级加密标准
AI	Artificial Intelligence	人工智能
ARA	AUTOSAR Runtime Adaptive	AUTOSAR 自适应平台运行时
ASIL	Automotive Safety Integrity Level	汽车安全完整性等级
ASPICE	Automotive Software Process Improvement and Capacity dEtermination	汽车软件过程改进及能力评定
AUTOSAR	AUTomotive Open System Architecture	汽车开放系统架构
AVP	Automated Valet Parking	自主泊车辅助
BEV	Bird's Eye View	鸟瞰图
BIST	Built In Self Test	内建自测
BSP	Board Support Package	板级支持包
CAN	Controller Area Network	控制器局域网总线
CAN-FD	CAN with Flexible Data rate	可变速率 CAN
CPU	Central Processing Unit	中央处理器
CRC	Cyclic Redundancy Check	循环冗余校验
CXL	Compute Express Link	计算快速链路
DDS	Data Distribution Service	数据分发服务
DSP	Digital Signal Processing	数字信号处理
ECC	Elliptic Curve Cryptography	椭圆曲线密码学
ECU	Electronic Control Unit	电子控制单元

缩略语	英文名称	中文名称
EHP	Electronic Horizon Provider	电子地平线提供者
EHR	Electronic Horizon Reconstructor	电子地平线解析者
ETH	EtherNet	以太网
FPGA	Field Programmable Gate Array	现场可编程逻辑门阵列
GDPR	General Data Protection Regulation	通用数据保护条例
GLOSA	Green Light Optimal Speed Advisory	绿波车速引导
GMSL	Gigabit Multimedia Serial Links	千兆多媒体串行链路
GPU	Graphics Processing Unit	图形处理单元
HSM	Hardware Security Module	硬件安全模块
I/O	Input/Output	输入/输出
IPC	Inter-Process Communication	进程间通信
LCC	Lane Centering Control	车道居中辅助
LKA	Lane Keeping Assist	车道保持辅助
MCU	Microcontroller Unit	微控制单元
NOA	Navigate On Autopilot	领航辅助驾驶
NoC	Network on Chip	片上网络
NOP	Navigate On Pilot	领航辅助
NPU	Neural network Processing Unit	神经网络处理单元
OTA	Over the Air	空中升级
PCIe	Peripheral Component Interconnect Express	高速串行计算机扩展总线标准
POSIX	Portable Operating System Interface of UNIX	可移植操作系统接口
QM	Quality Management	质量管理
RISC	Reduced Instruction Set Computer	精简指令集计算机

缩略语	英文名称	中文名称
RoboTaxi		自动驾驶出租车
RPC	Remote Procedure Call	远程过程调用
RTOS	Real Time Operating System	实时操作系统
SOA	Service-Oriented Architecture	面向服务的架构
SoC	System on Chip	片上系统
SOME/IP	Scalable Service-Oriented Middleware over IP	基于 IP 的可扩展的面向服务的中间件
SOTIF	Safety of the Intended Functionality	预期功能安全
TEE	Trusted Execution Environment	可信执行环境
Tier 1		汽车零部件一级供应商
TPU	Tensor Processing Unit	张量处理单元
UI	User Interface	用户界面
V2X	Vehicle to Everything	车用无线通信技术
VMM	Virtual Machine Monitor	虚拟机监控器