车载计算平台标准化需求研究报告

全国汽车标准化技术委员会

智能网联汽车分技术委员会

2021 年 7 月

目　录

前　言

随着汽车智能化、网联化发展，汽车电子电气架构从分布式向集中式演进，同时智能驾驶需要处理的数据量和算力要求激增，传统电子控制单元或者单一的控制器已经无法满足要求，行业呼新一代的计算平台。作为智能网联汽车的“大脑”，车载计算平台是新型汽车电子电气架构的核心，是支撑自动驾驶落地的关键，也是新型智能汽车电子产业竞争的主战场。当前为车载计算平台发展初期阶段，产品尚未定型，产业生态亦在萌芽期。车载计算平台涉及汽车、电子、软件、通信等技术领域的各个环节和主体，是一项前瞻性、全局性的系统工程，正在形成新的复杂生态系统。对其认识和理解的差异，有可能导致技术路线上的分化，影响互操作性，增加部署成本。与此同时，国际国内相关领域技术标准和管理规范尚未建立，行业发展碎片化，行业应用存在一定的盲目性，不利于技术发展和应用落地。基于对车载计算平台的标准化需求的研究，梳理形成其标准体系，将对后续标准化工作进行顶层规划，有利于推动形成行业共识，明确标准化工作重点，统筹协调优势资源，加速产业链及生态的建立与完善。

本研究广泛联合整车企业、零部件供应商、自动驾驶解决方案企业、第三方研究机构，聚焦车载计算平台，充分调研国内外车载计算平台相关技术和典型产品发展现状，并对硬件技术、软件技术、连接互通、保障技术等关键技术深入分析，并在此基础上分析得出车载计算平台的标准化需求，给出相应的下一步标准制定工作的相关建议。

在此衷心感谢参加研究报告编写的各单位、组织及个人。

组织指导：汽标委智能网联汽车分标委

牵头单位：华为技术有限公司、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）、

参与单位：中国汽车技术研究中心有限公司、博世汽车部件（苏州）有限公司、惠州市德赛西威智能交通技术研究院有限公司、北京地平线机器人技术研发有限公司、国汽（北京）智能网联汽车研究院有限公司、上汽通用五菱汽车股份有限公司、联合汽车电子有限公司、大陆汽车投资（上海）有限公司、长城汽车股份有限公司、标致雪铁龙（中国）汽车贸易有限公司、北京百度网讯科技有限公司、浙江吉利汽车研究院有限公司、上海汽车集团股份有限公司技术中心。

参与人员：李宝田、吴含冰、马涛、周铮、郭盈、王伟、孟亚非、郑亮、刘晓阳、李星宇、程智锋、田思波、褚文博、唐波、罗覃月、王鑫玥、罗勇、王奕、马博、钱宏、邵学彬、方熙宇、安淑苗、王萌、冯志敏、陆睿、彭伟、卢红喜、李秋实。

1 术语定义及缩略语

1.1 术语与定义

下列术语与定义适用于本文件。

1.1.1 车载计算平台 vehicle computing platform

支撑智能网联汽车驾驶自动化功能实现的软硬件一体化平台，包括芯片、模组、接口等硬件以及系统软件、功能软件等软件，以适应传统电子控制单元向异构高性能处理器转变的趋势。也被称为车载智能计算基础平台。

1.1.2 车控操作系统 vehicle-controlled operating system

运行于车载计算平台异构硬件之上，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。

1.2 缩略语

下列缩略语适用于本文件。

AI 人工智能 Artificial Intelligence

AUTOSAR 汽车开放系统架构 Automotive Open System ARchitecture

CANBus 控制器局域网总线 Controller Area Network Bus

CPU 中央处理器 Central Processing Unit

DNN 深度神经网络 Deep Neural Network

ECU 电子控制单元 Electronic Control Unit

GPU 图形处理器 Graphics Processing Unit

IMU 惯性测量单元 Inertial Measurement Unit

MCU 微控制单元 Microcontroller Unit

SoC 片上系统 System on Chip

V2X 车联网通信 Vehicle to Everything

2 车载计算平台研究背景

2.1 概述

汽车是国民经济的重要支柱产业，带动庞大的制造业上下游，代表国家工业水平。当前汽车产业正在经历一场以“电动化、智能化、网联化和共享化”为特征的“新四化”技术革命和行业变革。车联网（智能网联汽车）作为人工智能、物联网、云计算等高新技术的重要载体，正成为汽车产业发展的热点。美国电气和电子工程师协会 IEEE 曾经做出评估预测，21 世纪中叶前，自动驾驶汽车将占据全球汽车保有量的 75%，智能网联汽车可能颠覆当前交通运输产业运作模式。美国麦肯锡公司在其发布的“展望 2025：决定未来经济的 12 大颠覆技术”研究报告中指出，智能网联汽车技术的影响力排名第六，至 2025 年，其潜在经济影响价值达到 2000-19000 万亿美元。目前，美国、欧洲、日本等汽车产业发达国家或地区已经在推动智能网联汽车产业发展方面开展了大量探索性工作，形成一定先发优势。

我国政府也高度重视车联网（智能网联汽车）的发展，相关政策标准法规研究制定进入了密集期。《国家综合立体交通网规划纲要（2021 年-2035 年）》部署了车路协同相关任务；《国家车联网产业标准体系建设指南（车辆智能管理）》、《国家车联网产业标准体系建设指南（智能交通相关）》等标准建设指南相继出台；深圳经济特区试点智能网联汽车立法，正在围绕《深圳经济特区智能网联汽车管理条

例》征求意见。《智能网联汽车生产企业及产品准入管理指南（试行）》于2021年4月发布并征求意见。

随着汽车智能化、网联化发展，汽车电子底层硬件不再是由实现单一功能的单一芯片提供简单的逻辑计算，而是需要提供更为强大的算力支持；软件也不再是基于某一固定硬件开发，而是要具备可移植、可迭代和可拓展等特性。一方面是车内网络拓扑的优化和实时、高速网络的启用，另一方面是ECU（电子控制单元）的功能进一步集成到域控制器甚至车载计算机。 作为智能网联汽车的“大脑”，车载计算平台是新型汽车电子电气架构的核心，是支撑自动驾驶落地的关键，也是新型智能汽车电子产业竞争的主战场。

2.2 研究内容

车载计算平台是支撑智能网联汽车驾驶自动化功能实现的软硬件一体化平台，包括芯片、模组、接口等硬件以及系统软件、功能软件等软件，以适应传统电子控制单元向异构高性能处理器转变的趋势。也被称为车载智能计算基础平台。

本研究广泛联合整车企业、零部件供应商、自动驾驶解决方案企业、第三方研究机构，聚焦车载计算平台，充分调研国内外车载计算平台相关技术和典型产品发展现状，并对硬件技术、软件技术、连接互通、保障技术等关键技术深入分析，并在此基础上分析得出车载计算平台的标准化需求，给出相应的下一步标准制定工作的相关建议。

2.3 研究意义

当前为车载计算平台发展初期阶段，产品尚未定型，产业生态亦

在萌芽期。车载计算平台涉及汽车、电子、软件、通信等技术领域的各个环节和主体，是一项前瞻性、全局性的系统工程，正在形成新的复杂生态系统。对其认识和理解的差异，有可能导致技术路线上的分化，影响互操作性，增加部署成本。与此同时，国际国内相关领域技术标准和管理规范尚未建立，行业发展碎片化，行业应用存在一定的盲目性，不利于技术发展和应用落地。

基于对车载计算平台的标准化需求的研究，梳理形成其标准体系，将对后续标准化工作进行顶层规划，有利于推动形成行业共识，明确标准化工作重点，统筹协调优势资源，加速产业链及生态的建立与完善。

3 车载计算平台发展情况

3.1 概述

SAE International（国际自动机工程师学会）在2018年发布的SAE J3016《Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles》中，根据不同的汽车行驶自动化程度、驾驶员介入程度和行驶场景限定程度将自动驾驶分为L0-L5共6个级别，从完全由驾驶员执行全部动态驾驶任务的人工驾驶（L0）到由自动驾驶系统在任意的连续运行环境下执行全部动态驾驶任务和功能保障而不要求任何用户进行介入的完全自动驾驶（L5）。

L3-L5级别的自动驾驶过程中需要完成大量高速计算过程以处理海量、多源、异构的数据，并需要运用人工智能、信息通信、大

数据和云计算等技术进行实时感知、决策并完成相应的车辆运动规划和控制。这大幅度提高了对自动驾驶汽车的计算能力和系统功能要求，并在实时性、可靠性、安全性等方面提出了更高要求。以 CAN 总线为基础的传统汽车分布式架构和传统的 ECU 已不能满足自动驾驶汽车的发展要求。高性能的车载计算模块与集中式的新型电子电气架构成为实现自动驾驶汽车的复杂功能、安全可靠的数据处理和决策以及大量互联信息的高效传输和管理的必需。

车载计算平台即为集中式电子电气架构中高性能车载计算模块的具体实现形态，是新型智能网联汽车的大脑，使能高级别自动驾驶功能的核心组件。车载计算平台与车内其他电子器件和系统的关系如图 1 所示，由图 1 可以看出，车载计算平台处于核心地位。车载计算平台主要完成的功能是以环境感知数据、导航定位信息、车辆实时数据、云端平台服务器数据和相关 V2X 交互数据等作为输入，融合处理多源输入数据，基于环境感知定位、智能规划决策和车辆运动控制等核心控制算法，输出驱动、传动、转向和制动等执行控制指令，实现车辆的自动驾驶功能，并结合具体应用场景向云端和其他通过 V2X 相连的设备输出有效信息，形成协作。

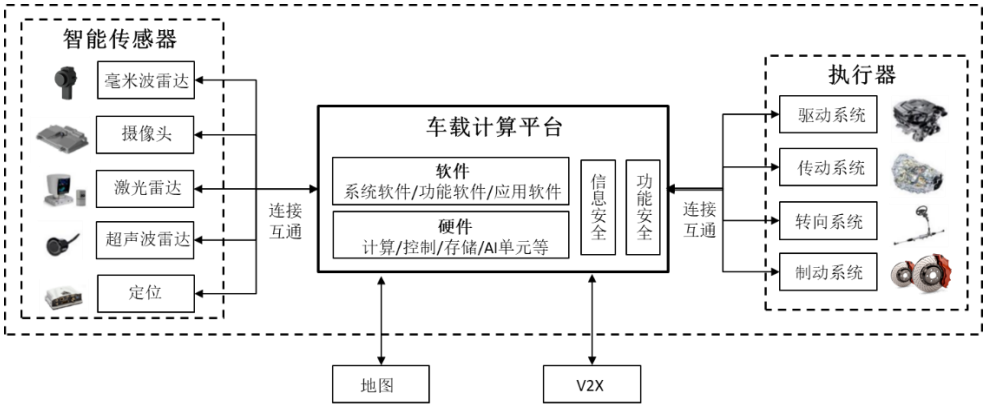

图 1 车载计算平台与其它系统的关系

国外以英伟达为代表的企业依托 GPU 领域的技术优势，不断迭代优化，推出系列产品。以英特尔为代表的企业积极研发，在努力保持技术优势的同时，通过收购大力补齐技术短板（如 Mobileye），完善相关产业结构。以特斯拉为代表的整车企业自主研发了操作系统，推出专用自动驾驶计算平台 FSD，并集成了为其自动驾驶算法开发的专用芯片，旨在实现低功耗、高性能、低成本，提高竞争门槛。国内以华为、地平线、中兴、百度等为代表的企业也在加大投入，以自身的芯片、软件、通信技术研发能力和用户资源为基础，抢占市场，并带动与整车企业深度合作加速布局。

3.2 车载计算平台产品发展情况

3.2.1 国际发展情况

（一）特斯拉 FSD

特斯拉于2019年4月发布FSD平台（Full Self-Driving Computer）。FSD 板卡上有两颗特斯拉自研 SoC 芯片，每颗 SoC 芯片主要包括 2 个负责机器学习计算的神经网络处理单元 NPU，1 个负责通用数据处理的 CPU，1 个负责图形处理的 GPU 等。每颗全自动驾驶芯片提供

72TOPS 的算力，FSD 平台的总算力达到 144TOPS，功耗为 200W。FSD 作为特斯拉的 Autopilot HW 3.0 的核心部分，已经广泛用于特斯拉的车型。特斯拉表示第二代 FSD 即 Autopilot HW 4.0 也正在研发，与博通合作设计，芯片采用台积电 7nm 工艺代工，预计 2021 年上市。

（二）英伟达 Drive 系列

英伟达在 GPU 和 AI 芯片领域占据了市场领先地位。从 2015 年开始，英伟达开始进入车载 SoC 和车载计算平台领域，为自动驾驶提供基础计算能力。目前已经推出了 4 代产品，分别是 Drive PX，Drive PX2，Drive AGX Xavier/Pegasus 以及 Drive AGX/Orin。

在 2015 年的国际消费电子展会（简称 CES）上，英伟达推出了首代车载计算平台产品 Drive PX。Drive PX 搭载了两颗英伟达 Tegra K1 芯片，算力为 2.3TOPS。在 2016 年的 CES 上，英伟达发布了第二代车载计算平台 Drive PX2，将核心芯片换为 Pascal 架构的 Tegra Parker，算力提高到 24TOPS。Drive PX2 平台曾经用于特斯拉的 Model S/X/3 车型上，直到特斯拉 2019 年推出自研计算平台。

2016 年 9 月，英伟达发布了专用于自动驾驶的 SoC 芯片 Xavier，采用新的 Volta 架构，算力达到 30TOPS，功耗 30W。在 Xavier SoC 基础上，英伟达发布了两个级别的车载计算平台产品：Drive AGX Xavier 和 Drive AGX Pegasus。Drive AGX Xavier 面向 L2/L3 级自动驾驶场景，集成了两颗 Xavier SoC，一颗作为冗余备份。这个平台已经量产上车，2020 年国内上市的小鹏 P7 电动轿车就搭载了 Drive AGX Xavier 平台，在此基础上实现了一系列 L2 级别辅助驾驶功能。Drive

AGX Pegasus 面向 L4/L5 自动驾驶场景，集成两颗 Xavier SoC 和两颗 GPU，算力达到 320TOPS，功耗 500W，目前已经在小马智行、文远知行等无人驾驶初创企业的 RoboTaxi 车队上落地。

2019 年 12 月英伟达推出了新一代 SoC 芯片 Orin，Orin 相比 Xavier，采用了新的 Amphere 架构，制程提高到 7nm，算力 200TOPS，功耗 45W。基于 Orin SoC，英伟达在 2020 年 5 月发布了第四代车载计算平台 Drive AGX Orin 和 Drive AGX RoboTaxi，Drive AGX RoboTaxi 适用于 RoboTaxi 场景，集成两颗 Orin SoC 和两块 GPU，自备达到 2000Tops，功耗 800W。Orin 和相关平台预计 2022 年量产。

（三）英特尔 Intel GO

在 CES 2017 上英特尔发布了 Intel GO，是一个针对自动驾驶汽车的开发平台。收购 Mobileye 后以“视觉优先”作为设计理念，包含了两个 Mobileye EyeQ5 芯片（一个用来进行视觉处理，另外一个用于融合/规划）以及一个英特尔的 8 核凌动芯片，分为凌动 Atom 和至强 Xeon 两个版本，采用 FPGA 做硬件加速，支持 5G。

（四）奥迪 zFAS

早在 2017 年，奥迪就宣称 2018 款奥迪 A8 具备了 L3 级自动驾驶能力，其中的关键就是名为 zFAS 的车载计算平台。奥迪与安波福、TTTech 一起设计开发了 zFAS 平台。zFAS 平台采用 Mobileye 的 EyeQ3 处理器以识别前方物体、行人和车道。采用英伟达的 Tegra K1 处理器以进行图像处理和数据整合。采用 Altera 的 Cyclone V 处理器以进行自动泊车。采用英飞凌的 Aurix TC297T 处理器以进行安全接管。

（五）博世 DASy

博世开发“DASy”是一款用于辅助与自动驾驶的、可扩展的模块化车载计算机，未来，DASy 将成为集中式车辆架构的核心组件。

灵活性是 DASy 的主要优势，可以使用基本软件和客户特定软件的组合来实现各种客户要求。标准化的数据接口可集成到各种车辆平台中。

在辅助和自动驾驶过程中，来自于车身周围的传感器信号，在传感器的控制单元中进行了预处理，并在 DASy 的微控制器中进行了整合。利用这些数据，DASy 可以生成车辆周围环境的高精度模型。集成的驾驶功能利用来自周围环境模型的信息，来决定合适的驾驶策略。之后，通过对转向，制动和动力总成系统进行有针对性的干预，即使在高速行驶时，也可以舒适，安全地执行相应的驾驶策略。它专为例如高速公路辅助在内的辅助与部分自动化功能而设计，支持达到最高功能安全 ASIL D 等级。

未来 DASy 的多种型号，将会支持适用于高速公路或城市自动驾驶出租车上的高度自动驾驶功能。DASy 的硬件包含一个硬件安全模块。加上更先进的安全措施，DASy 可以满足严格的安全和保障标准。

（六）大陆 ADC

大陆汽车推出的自动驾驶解决方案——ADC。该平台域控制器可提供多种传感器的连接支持，包括毫米波雷达，摄像头，激光雷达等。为满足整车企业不同的自动驾驶要求，ADC 平台提供了不同的配置，对于基本要求的配置，采用以瑞萨为基础的硬件架构，对于高配置，

采用以英伟达为基础的硬件架构。该平台可支持不同工况下的 L2 到 L5 级别的自动驾驶。

（七）采埃孚 proAI

2019 上海车展上，采埃孚就展示了高性能控制器 ProAIRoboThink。ProAIRoboThink 是采埃孚 ProAI 系列的第四代产品。ProAI 系列的第四代产品自带图像处理器，拥有逾 150 TOPS 的计算能力(相当于每秒 150 万亿次计算),可模块化组合最多 4 个单元，实现约 600 TOPS 的总计算能力，适用于 L4 级以上的自动驾驶解决方案。基于该系统的模块化和可扩展的特点，ProAIRoboThink 控制器可按照应用场景所需进行配置，适用场景包括 ADAS 车辆、自动驾驶车辆、商用车及工业领域，同时可为摄像头、激光雷达和雷达系统的传感器数据提供整合平台，用户可自行定制软件架构。

（八）恩智浦 Blue-Box

Blue-Box 是 2016 年恩智浦推出基于 Linux 系统的计算机平台。装备有 NXP S32V 汽车视觉处理器和 LS2088A 内嵌式计算机处理器，同时还搭载了其他为实现不同传感器节点功能的芯片，能够处理从 V2X、雷达、视觉系统、激光雷达以及车辆状态获取的信息，对传感器进行模块化管理，将多种传感器回传信息进行融合加工。按照恩智浦的计划，Blue-Box 平台提供完整汽车半导体解决方案，将推动 L4 级别自动驾驶的量产上车。

（九）伟世通 DriveCore

伟世通在 2018 CES 展上推出了 DriveCore 自动驾驶平台，主要

由 Compute、Runtime 和 Studio 三部分组成。其中 Compute 作为模块化、可扩展的硬件计算平台，运算能力覆盖 500GFLOPS-20TFLOPS（基于现有 SoC 而言），不依赖任何中央处理单元，支持英伟达、恩智浦、高通等处理器。

作为一款专门针对自动驾驶研发的、安全可靠的计算平台，DriveCore 旨在加速自动驾驶技术的开发和商业化，使汽车制造商能够以开放式协作的模式快速构建自动驾驶解决方案。2017 年底，伟世通在美国移动中心（ACM）测试场道路上首次完成了基于 DriveCore 的高速公路驾驶员系统的测试，并计划于 2020 年左右将 DriveCore 平台安装到汽车上。

（十）TTTech RazorMotion

RazorMotion 是 TTTech 推出的一款高度自动化的驾驶平台，专为高级驾驶辅助系统（ADAS）的应用开发和评估而设计。它结合了高级硬件和 MotionWise 软件框架。RazorMotion 平台和架构可支持 L2-L5 级别自动驾驶，且计划达到功能安全(ASIL-D)，在满足自动驾驶高计算性能需求的同时能够符合最高的功能安全的等级；可扩展性，失效可用，当自动驾驶达到 L4 级时，即便车辆发生故障或者部件失效，但是车辆仍能够保持一段时间内的安全运行，直到行驶到安全地方或者由人工接管。实时性，在控制层面比如紧急制动等功能方面，具有实时性。

（十一）赛灵思 ACAP

赛灵思在 2018 年推出全球首款自适应计算加速平台（ACAP）产

品——Versal 系列。ACAP 是一种高度集成的多核异构计算平台，可在软硬件两个层面随时进行更改，从而动态地适应数据中心、汽车、5G 无线等的广泛应用与工作负载需求。Versal ACAP 的体系架构从构建伊始即可支持软件可编程，拥有高度灵活的、每秒传输速率高达数兆比特的片上网络（NoC），是整合了硬件可编程逻辑单元、软件可编程处理器、以及软件可编程加速引擎的计算平台产品。

2019 年，赛灵思宣布已开始面向参与公司“早期试用计划”的多家一线客户交付 Versal™ AI Core 和 Versal Prime 系列器件。

（十二）德尔福 CSLP

德尔福与 Mobileye 联合推出自动驾驶解决方案——中央传感定位与规划自动驾驶系统（CSLP）。该系统平台采用德尔福的多域控制器并提供雷达硬件方面的支持，并整合了 Mobileye 和英特尔的软、硬件技术，其中 Mobileye 提供摄像头及相关算法的支持，而英特尔和 Ottomatika 主要提供相关软件算法的支持。分别由控制模块、感知模块、自动驾驶规划模块构成，其具有高度集成化的特性。2017 年德尔福公开其搭载中央传感定位与规划自动驾驶系统平台(CSLP 平台)的奥迪 SQ5 车型。

（十三）三星 Drvline

三星在 2018 年发布了旗下首款 Drvline 自动驾驶平台。该平台是一款模块化的可拓展平台，硬件系统包括了一块基板和一块扩展板。其中基板主要负责车辆的安全网关功能，而扩展板则提供了额外的计算力、专用的 SoC 和加速器，同时可以增加平台对更多种类和数量传

感器的支持。同时，Drvline 构建并拓展了 AUTOSAR 自适应平台，能够在任何的 POSIX 操作系统上运行。基于硬件和软件的开放性，能够满足各式各样的自动驾驶需求，从 ADAS 到 L5 均能适用。

Drvline 平台在推出后提供给汽车制造商，能够根据不同制造商的个性化需求对平台进行定制。同时三星还建立了强大的合作伙伴生态系统，比如 TTTech、AImotive、Hella Aglaia、Renovo Auto 软件合作伙伴以及 Graphcore、ThinCi、Infineon 等车载系统合作伙伴等，共同推动自动驾驶领域的技术攻关。

（十四）高通 Snapdragon Ride

高通在 2020 年国际消费电子展上发布 Snapdragon Ride 平台，包括高通的 SOC，加速器和自动驾驶软件栈。基于不同 SoC 和加速器的组合，Snapdragon Ride 平台可以匹配从 L2 辅助驾驶到 L4/L5 的全自动驾驶的场景需求，预计为 L1/L2 提供 30TOPS 的算力，为 L4/L5 提供了在 130W 功耗下的 700TOPS 算力。散热设计支持被动或风冷，以取代成本较高的水冷。预计 2022 年投入商用部署，2023 年量产上车。

3.2.2 国内发展情况

（十五）华为 MDC

针对自动驾驶对计算平台的需求，华为推出 MDC（移动数据中心，Mobile Data Center）解决方案。它集成了具有 CPU 与 AI 计算能力的 SoC 芯片，并通过底层的软硬件一体化调优，在时间同步、传感器数据精确处理、多节点实时通信、最小化底噪、低功耗管理、快速

安全启动等方面处于业界领先水平。

平台以可信架构的设计与研发，保障信息安全与功能安全，保障数据安全，消除隐私隐患，MDC 平台的操作系统能够内核通过 CC EAL 5+安全认证，MDC 平台通过 ISO 26262 的功能安全管理认证。

MDC 是一套开放的平台，具备组件服务化、接口标准化、开发工具化的特性， MDC 平台包括平台硬件、平台软件服务、功能软件平台、配置工具链及端云协同服务。MDC 的操作系统兼容主流 POSIX 标准接口和主流基础库。MDC Core 提供 Classic AUTOSAR 与 Adaptive AUTOSAR、功能安全、信息安全及 OTA 升级等 API 服务，支持主流 AI 框架及 1000 多个 AI 算子，同时提供功能软件框架及规范，定义了基本算法组件间开发接口。MDC 提供了 MDC Manifest Configurator、MDC Development Studio 等工具集，支持可视化&拖拽式操作及自动代码生成。MDC 平台的操作系统、平台软件和功能软件中间件，均以外提供标准的开放 API 与 SDK 开发包，结合工具链，助力相关企业快速开发、调测、运行自动驾驶算法与功能。

MDC 支持 L2+~L5 自动驾驶算法的平滑演进，适用于乘用车、商用车与作业车等多种应用场景。目前华为已经拥有进入量产阶段的系列化 MDC 产品，包括面向商用车作业车的 MDC300F，算力 64TOPS；面向 L2+乘用车场景的 MDC210，算力 48TOPS；面向 L4 乘用车的 MDC610，算力超过 200TOPS；面向 Robotaxi 场景的 MDC810，算力超过 400TOPS。

（十六）地平线 Matrix

地平线在 CES 2020 推出新一代自动驾驶计算平台——Matrix 2。该平台面向多层次、多场景的未来自动驾驶，搭载地平线征程 2 二代车规级芯片，具备极致性能与高可靠性，可满足 L2～L4 级别自动驾驶视觉感知需求，为自动驾驶客户提供感知层的深度赋能。

迭代后的 Matrix 2 具备更高性能、低延时、更低功耗等特点，可满足多个国家、不同场景下高级别自动驾驶运营车队以及无人低速小车的感知计算需求。相比上一代，Matrix 2 采用满足 AEC-Q 100 Grade 2 的征程 2 芯片，具备 16TOPS 的等效算力，功耗为 22W，采用被动散热方式，满足 ISO-16750 测试等级，板载支持 ASIL D 的 MCU。针对不同应用场景的传感器布置方案，提供单路和四路输入的两种选择，满足模块化需求。

在感知层面，Matrix 2 支持 23 类分割，以及 2D/3D 检测与分类，可支持包括摄像头、激光雷达在内的多传感器感知和融合。在 Matrix 2 上实现的感知算法还能够应对复杂环境，其单目前视解决方案支持在特殊场景或极端天气的情况下输出稳定的感知结果，可在低于 100 毫秒的延迟下有效感知车辆、行人、车道线、交通标识、红绿灯等多种目标，并专门针对中国道路和场景进行优化。

该平台目前已形成基于自主研发的车载 AI 芯片、参考算法和工具链的智能驾驶和智能人机交互解决方案矩阵，依托地平线 “天工开物”开发工具链，开发者和研究人员可以基于 Matrix 平台部署神经网络模型，实现开发、验证、优化和部署，可赋能 OEM/Tier1，全面满足视觉感知辅助驾驶、高级别自动驾驶、众包高精地图定位、智能

人机交互等智能驾驶场景的需求。此外，地平线将基于下一代高等级自动驾驶芯片征程 5 打造中央计算平台，AI 算力可达 512TOPS，功耗约 100W，包含芯片级功能安全。

地平线 Matrix 自动驾驶计算平台已经与众多自动驾驶探索者达成合作：1）在 Robotaxi 领域，地平线与多家顶级自动驾驶运营公司达成合作，Matrix 被应用于近千辆的测试车队并开已开展商业运营服务；2）整车厂领域，地平线与奥迪长期在高级别自动驾驶技术研发及产品化等方面展开合作，助力奥迪在无锡获得了 L4 路测牌照，并赋能奥迪中国首次在国内实际高速公路场景进行乘用车编队 L4 自动驾驶及车路协同演示；3）在自动驾驶初创领域，地平线助力领骏突破感知瓶颈。

（十七）德赛西威 IPU03

2020 年 4 月 27 日，小鹏汽车打造的智能轿跑 P7 正式发布上市，这也意味着德赛西威全球首款基于英伟达 Xavier 自动驾驶域控制器产品 IPU03 正式量产。

IPU03 作为整车实现 L3 级自动驾驶的域控制器，能够支持高低速场景下的自动驾驶功能，通过不同传感器配置可以实现高速场景下的上下匝道、自主变道，城市道路的塞车自动跟车，低速场景下的自动泊车（APA）以及代客泊车（AVP）等功能，用同一个控制器配合不同传感器配置来实现各种场景的智能化驾驶辅助或有条件自动驾驶功能。

作为整车实现自动驾驶功能的中央处理单元，IPU03 满足车规要

求，SoC 操作系统采用 QNX Safety OS，MCU 采用包含安全组件的 AUTOSAR 操作系统，硬件设计考虑了备份冗余设计，整体满足 ISO26262 功能安全 ASIL D 要求；同时，IPU03 算力高达 30TOPS，可实时处理来自车辆雷达、摄像头、激光雷达和超声波系统的海量数据，运行感知、定位、规划和控制等算法；IPU03 支持丰富的外接设备，连接 12 路摄像头、12 路 CAN 汽车总线、2 路 LVDS、8 路千兆及 1 路万兆车载以太网等。

（十八）百度 ACU

百度自主研发的车载计算平台是基于 CPU、GPU 以及 FPGA 构建的多核异构计算架构，搭载包括激光雷达、高清摄像头、毫米波雷达，高精定位导航系统以及超声波雷达等多传感器系统，支持复杂的实时路径规划和控制的算法。其中 CPU 选取了多核架构以满足低延时的复杂逻辑控制计算需求；兼容多块 GPU 的设计可提供高达 300TOPS 以上的深度学习算力，外加支持多块可配置的 FPGA 芯片的设计使得整套系统具有强可扩展性。同时，整套系统具有在线升级(OTA)功能，通过安全网关实现安全可靠的 V2X 数据通讯，远程车辆管理和控制，以及数据流水线等云服务。为了提高系统可靠性和安全性，整套系统除了采用了更多的车规级零部件以外，还针对特定的关键功能采用了符合 ISO 26262 标准的零部件，进行了系统级功能安全设计。

百度于 2017 年 4 月发布 Apollo 自动驾驶开源平台，目前已经有超过 190 家包括车企、Tier1、政府、服务运营商，软硬件供应商等的

生态合作伙伴，是目前国际上基于自动驾驶最大的产业生态系统之一。自技术开源以来，搭载百度 Apollo 车载计算平台的车型遍布乘用车、商用车以及专用车市场，覆盖包括城市道路和固定园区在内的多种 L4 级别应用场景。搭载百度 Apollo 车载计算平台的 RoboTaxi 的已经在国内多个城市开始运营。

（十九）宏景智驾 ADCU

ADCU 是宏景智驾自主研发的车规量产级 L3/L4 车载计算平台。在技术路线上，采用以 Intel 面向 L3 等级的车规芯片 Denverton 为核心、辅以大规模 FPGA/GPU 并行计算能力而构建的多核异构计算平台架构，计算能力强、平台性好、升级性强，能够满足高速公路自动驾驶（HWP）、自主泊车（AVP）、卡车编队（Platoon）、高精度地图（HD MAP）、驾驶员监控（DMS）等多种 L3 功能。x86 CPU 作为核心计算芯片，可以满足 L3/L4 激光雷达点云、大量目标多传感器融合和复杂路径规划等算力密集程序算法的执行。图像处理等深度学习任务由大规模 GPU 或 FPGA 完成。在功能安全设计上，本身核心 CPU 所采用的 Denverton 处理器，就可以实现 ASIL C 随机硬件功能安全，同时在计算平台内部集成了 ASIL-D 级别 MCU，以实现 ASIL-D 的最高安全等级。MCU 在运行硬实时控制任务的同时还运行故障诊断算法软件，对 Denverton CPU、GPU、FPGA、网关、电源、输入输出电路、外围传感器等进行监控。在自动驾驶系统或 ADCU 故障发生时，MCU 负责执行降级处理、降速行驶或紧急停车等操作。

宏景智驾的 ADCU 高度优化其软硬件系统，整机的最高功耗不

超过 100 瓦。在整车布置优化后可以采用无风扇被动散热，进一步提高可靠性。其高效低能耗设计使其具备非常广泛的适配性，可以用于传统动力、混合动力、纯电新能源等各种车型。

（二十）黑芝麻

黑芝麻于研发计算平台 SoC，可以支持包括 CNN、RNN 在内的各种神经网络。其核心技术包括图像/视频处理、光学处理、感知理解算法、深度神经网络和融合感知系统，相当于提供一个从传感器端到应用端的全栈式感知解决方案。具体来说，这套解决方案所做的是针对车辆、行人、车道线、交通标识、信号灯等信息，通过传感器感知信号，利用控光技术把光场进行处理，使得摄像头能在各种特殊工况条件下成像，再通过毫米波雷达、超声波雷达、GPS、IMU 与摄像头融合，把这些信号传入到感知系统，再通过优化的 SoC 计算平台，把感知结果传给自动驾驶企业去做决策和控制。从计算能力的角度来说，黑芝麻在计算架构和存储架构方面做了大量优化，其计算平台的神经网络计算能力可以达到 Mobileye EyeQ5 的两倍以上，其神经网络计算的利用率能超过 85%。

黑芝麻致力于开发全球领先的人工智能车载计算平台，提供高性能、安全、可靠的车规级自动驾驶芯片，结合全天候全场景的传感器融合感知算法，配套的底层实时操作系统、完整的工具链以及软件集成开发环境，为用户开发出可量产的 L3 及以上级自动驾驶控制器提供技术支持。

3.3 车载计算平台相关标准法规现状

当前是智能网联汽车从示范验证走向量产应用的关键时期。总体而言，围绕智能网联以及自动驾驶，标准化工作已进入实质推进阶段。聚焦车载计算平台的标准化工作在智能网联汽车的标准体系中已经稳步开展，但缺少系统、完整的车载计算平台标准。

国际标准化组织(International Organization for Standardization，ISO)下属的道路车辆技术委员会(ISO/TC 22)和智能运输系统技术委员会(ISO/TC 204)负责智能网联汽车相关技术的研究和制定。其中，ISO/TC 22 侧重基于车辆自身装置而进行的信息采集、处理、决策和行为的车辆技术领域；ISO/TC 204 侧重基于道路交通设施的信息传递和交通管理信息化方面。ISO 21448 等相关标准在制定过程中。

在联合国框架下，与智能网联汽车标准化工作相关的是世界道路安全论坛(WP.1)和世界车辆法规协调论坛(WP.29)。2019 年 6 月，WP.29 通过了 GRVA 提交的《自动驾驶汽车框架文件》，旨在确立 L3 和更高级别的自动驾驶汽车安全性和相关原则，包含了自动驾驶汽车相关的工作准则、安全因素，以及 WP.29 在自动驾驶汽车法规制定与协调工作中需要优先考虑的关健性和原则性等问题。WP.29 第 181 次全体会议于 2020 年 6 月 24 日召开，会议投票表决通过了信息安全、软件升级以及自动车道保持系统 3 项智能网联汽车领域的重要法规。

美国汽车工程师学会（Society of Automotive Engineers，SAE）所制订的标准广泛地应用于汽车行业及其他行业。SAE 制定的 J3016TM《标准道路机动车驾驶自动化系统分类和定义》成为广泛认可的自动

驾驶分级标准。此外，SAE 是 ISO 相关技术委员会的重要成员，在汽车信息安全方面与 ISO 成立了联合工作组，共同制定了 ISO/SAE 21434《道路车辆信息安全》。

2019 年 10 月，ARM、博世、大陆、日本电装、通用汽车、英伟达、恩智浦、丰田宣布组成 AVCC 联盟（Autonomous Vehicle Computing Consortium，自动驾驶汽车计算联盟）。致力于集合产业链上下游力量定义用于自动驾驶功能的车载计算平台参考架构以及软件接口。

2018 年 6 月，工业和信息化部、国家标准化管理委员会共同组织制定了《国家车联网产业标准体系建设指南（总体要求）》《国家车联网产业标准体系建设指南（信息通信）》和《国家车联网产业标准体系建设指南（电子产品与服务）》系列文件，2019 年 11 月，有关单位编制完成了《国家车联网产业标准体系建设指南(车辆智能管理)》并公开征求意见。顶层标准体系虽已初步形成，但细分领域的标准仍需完善。此外，针对智能网联汽车的测试验证过程，工信部、公安部、交通运输部联合发布了《智能网联汽车道路测试管理规范（试行）》，明确上路测试的一系列要求以及交通违法处理依据。2021 年 3 月，工信部成立智能网联汽车推进组(ICV-2035)，下设法规平台、技术标准、测试应用、操作系统、网络安全、产业生态等 6 个工作小组，汇集产学研行业专家加快推进产业发展。

2018 年 4 月，汽车标准化技术委员会成立智能网联汽车分技术委员会，围绕汽车驾驶环境感知与预警、驾驶辅助、自动驾驶、信息

安全以及与资源管理与信息服务等领域，已经开展多项标准制定工作。本报告也是在智能网联汽车分技术委员会的组织和指导下编制，是首个专门针对车载计算平台标准的研究报告。

4 车载计算平台关键性技术分析

4.1 概述

车载计算平台侧重于系统可靠、运行实时、分布弹性、高算力等特点，实现感知、规划、控制、网联、云控等功能，最终完成安全、实时、可扩展的多等级自动驾驶核心功能。车载计算平台的总体架构主要包含车控操作系统和异构分布硬件架构两部分。其中，车控操作系统是基于异构分布硬件架构，包含系统软件和功能软件的整体基础框架软件。总体架构图如图 2 所示。从架构图上来说，涉及到硬件技术、软件技术、保障技术等几个方面。

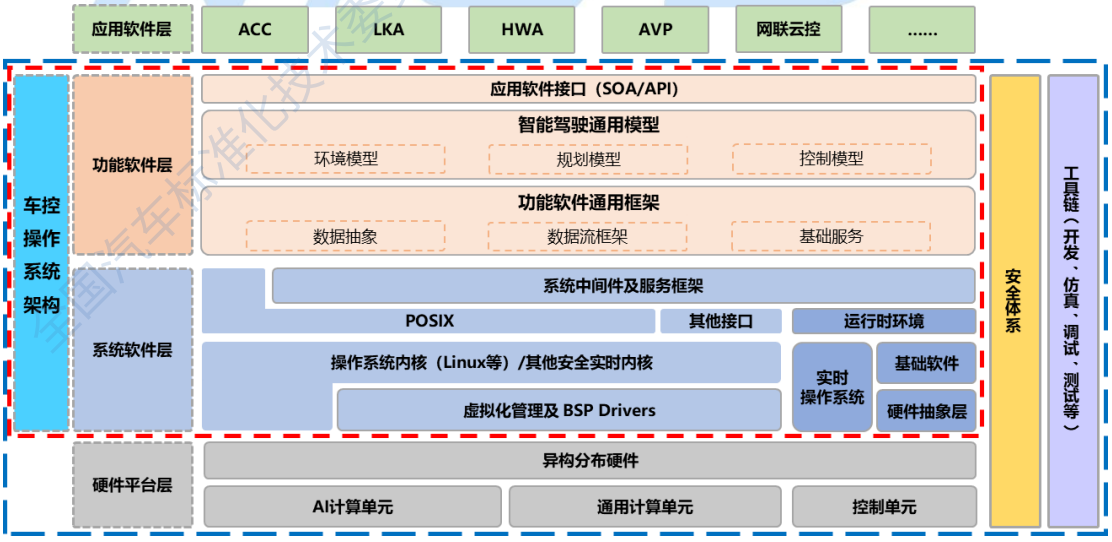

图 2 车载计算平台总体架构

4.2 车载计算平台硬件技术

车载计算平台的硬件架构为异构芯片集成化设计，对自动驾驶应

用提供运算支持和安全保障，硬件主要包括计算单元、控制单元、扩展单元、存储单元和供电单元，具有高性能、低功耗、高可靠性和易扩展等优点，图 3 是某车载计算平台硬件架构的示例。从图中可以看出，车载计算平台硬件一般包括以下几个部分：

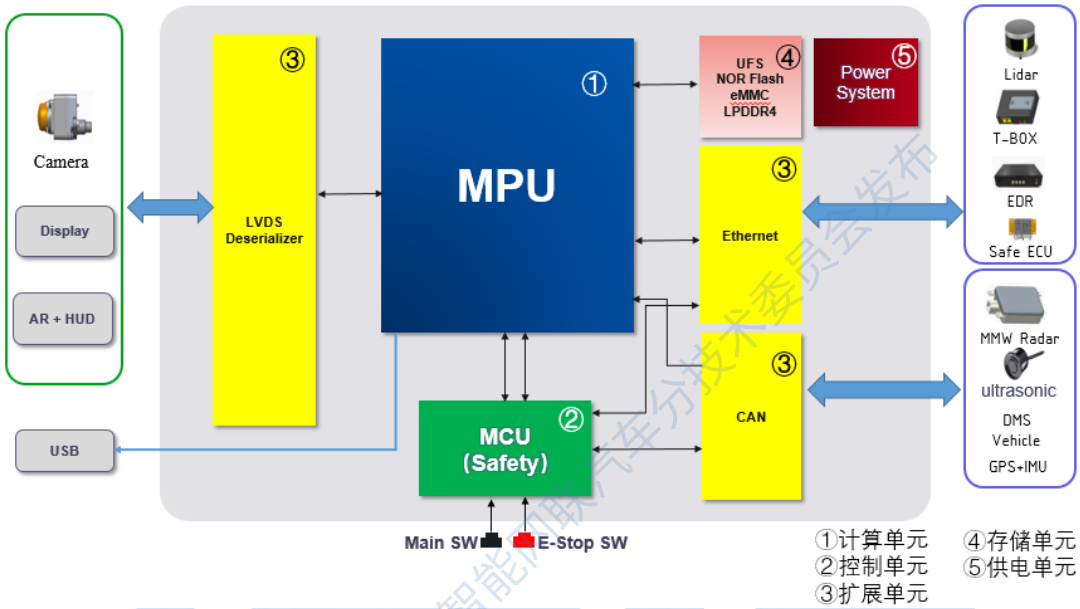

图 3 车载计算平台硬件架构示例

（一）计算单元

计算单元往往包含 CPU、AI 处理器（包括 GPU、FPGA、ASIC、DSP）等，可采用高性能的 SoC 芯片集成多个处理器。具有运算力高、功耗低、可编程等特点，可实现实时的环境感知、路径规划和决策控制等自动驾驶相关的核心算法。计算单元主要特征以及趋势如下：

1） 包含高性能多核处理器，采用异构、模块化，可扩展式架构，计算能力可配置；支持多线程处理任务等；

2） 内置独立、高性能算法处理模块，支持深度学习、神经网络、视觉融合等算法数据处理；

3） 硬件接口丰富，支持多路摄像头视频数据接入，多路以太

网设备接入，多路 CAN 接口设备计入，多路 LIN，FlexRay 的接口设备输入

4） 内置图像处理模块，随着图像分辨率的提高，摄像头尺寸小型化，散热要求增高，摄像头不适合单独增加图像处理模块，已逐渐形成往计算单元集成的趋势。摄像头图像数据的处理能力也会对算法效果造成直接影响。

5） 内置温度传感器，计算单元模块要进行大量数据运算，芯片对温度要求也比较敏感，通常内置温度传感器，当温度过高时，会输出相应信号，核心模块根据温度结果，采取对应的温度策略，以保证系统的稳定，可靠运行。

6） 计算单元至少需要满足功能安全 ASIL B 等级，在 L3 级别以上的自动驾驶场景，系统需要整体满足 ASIL D 等级要求。自检（BIST)模块,支持故障注入;片上存储器支持错误检查和纠正(ECC)保护；内置错误信号监控（ESM）模块；运行时安全诊断；支持监控电压，温度，时钟，看门狗定时器，存储器循环冗余校验（CRC）等

（二）控制单元

控制单元使用性能强大的 MCU 芯片，又称为 Safety MCU，满足功能安全 ASIL D 要求，具有强大的运算能力。有多路 CAN 总线接口和高速以太网接口，能与车身传感器连接，并接收和发送车身 CAN 总线和以太网消息，从而实现控制平台与整车其它节点进行交互。

Safety MCU 是控制平台的大脑，通过监控温度、SoC 的工作状态、供电模块状态、通信状态以及交互节点的状态，从而决定车辆横

向、纵向和制动控制的最终指令，保证行驶安全。

当检测到控制平台或配合模块出现异常时，Safety MCU 能够及时进入安全状态，及时告知驾驶员或安全停车。在一些特殊情况下，例如 SoC 异常，Safety MCU 能够根据雷达的信号计算出前方的障碍物，能够继续执行辅助驾驶，提高了辅助驾驶的舒适性。

（三）扩展单元

计算平台集成 MIPI，Ethernet，CAN 等扩展单元，计算单元和控制单元分别可以通过扩展单元对系统接口数量进行扩展，实现多路传感器同时接入计算平台，包括摄像头，角雷达，超声波雷达，惯性测量组合等，计算单元采集这些传感器数据后，进行数据融合计算。

计算单元与控制单元内置多路 CAN 接口，可以接多路 CAN 收发器，接多路 CAN 接口外部设备，如雷达模块、TBOX 模块等；

计算单元通常集成 1~3 路 MIPI CSI 接口，通过增加多路 LVDS 解串器芯片，同时扩展多路同轴接口，满足多路摄像头输入需求；

对应 Ethernet 接口设备较多的，也会通过增加 Ethernet 网关芯片，来满足多路 Ethernet 设备的需求，目前主要以百兆带宽需求为主，未来千兆带宽，万兆带宽的需求也会随之增长。

（四）存储单元

计算平台集成大容量存储单元，芯片种类主要包括 DDR、Nor-Flash 、DDR、eMMC 和 UFS，可以满足应用软件的大数据存储，如高精度地图数据、行车录像数缓存等功能，该存储单元也需要满足 ECC 保护、CRC 校验等功能安全相关的需求。

（五）供电单元

计算平台的供电单元也是整个计算平台的核心，要求提供稳定，可靠的供电网络，满足大功率用量需求；满足功能安全需求；配备专用电源管理模块给计算单元；支持 CAN 或 Ethernet 唤醒；实时监控关键的电源网络实时监控，如某路电路出现异常，反馈信号到主控单元。

4.3 车载计算平台软件技术

车载计算平台的软件架构是异构分布式操作系统协同合作的软件架构，主要分为系统软件、虚拟化系统和功能软件，具有稳定、高效和安全等优点，系统软件监控能力需满足功能安全等级要求。

（一）系统软件

车载计算平台的内核操作系统应考虑稳定安全、实时性高等性能要求，并基于当前计算平台的异构分布硬件架构进行定制化设计。异构核间的功能安全策略可以考虑采用芯片级联策略（3LSS）进行失效模式的监控。

应用于汽车电子嵌入式系统的 RTOS（实时操作系统）是功能安全策略的主要部署对象，基于 AUTOSAR 标准的 RTOS 广泛应用于汽车电子行业，得到全球汽车制造商、零部件供应商及电子半导体公司的软件系统认可，AUTOSAR 软件架构具有模块化软件设计、标准化接口设计等特点，AUTOSAR RTOS 可以满足功能安全等级要求。

嵌入式应用操作系统（例如 QNX、Linux）应具有自由裁剪、灵活移植和网络功能强大等特点。驱动程序、协议栈、文件系统、应用

程序等可以在内核以外安全保护的用户空间中运行，组件之间互不影响，满足功能安全等级要求。

（二）虚拟化系统

Hypervisor 是一种硬件虚拟化技术。它是运行在操作系统和物理硬件之间的中间软件层，对 CPU、内存和外围设备等硬件资源进行虚拟化管理，允许多个操作系统和应用共享硬件资源。Hypervisor 是实现跨平台数据共享，提高信息安全的重要途径之一。在自动驾驶应用场景中，应考虑在不同功能安全等级的操作系统中实施隔离分区管理，避免失效模式的发生，虚拟化系统策略符合功能安全等级要求。

在 Hypervisor 的基础上，建立数据分区管理模式。应用软件使用数据的时候，虚拟路由器先把外部设备数据传入安全分区（Security Partition），再由安全策略层（Security Services）进行数据的安全检查，最后数据通过检测后才输入到应用操作系统（Guest OS）中供应用软件使用。这种方式使应用软件与外部设备产生了真正的隔离，进一步提高了系统的信息安全能力。

（三）功能软件

功能软件是实现自动驾驶技术的核心共性化功能模块，包括感知、决策、规划和控制等智能驾驶核心功能的算法组件。可以分为传感器抽象功能、感知融合功能、预测功能、决策规划功能、定位功能和执行器抽象等功能模块。相关企业基于自身策略，在设计和开发功能软件时可以选择不同的功能模块和算法组件，实现拼插式功能组合，灵活构建智能驾驶系统级解决方案。

传感器抽象功能对毫米波雷达、激光雷达、摄像头、超声波雷达、GNSS、IMU 和轮速计等车载传感器的环境感知情况进行数字抽象。感知融合功能对传感器抽象模块的输入数据进行融合，结合多种传感器的特性、工况和环境信息，完成对物理世界的数字呈现。预测功能依据环境信息和交通参与者历史测量信息，对其他交通参与者的未来行驶意图和轨迹进行预测。定位功能根据高精度地图、传感器等信息输入提供自车位置，包括本车的绝对位置以及在静态动态环境中的相对位置。决策规划功能根据感知融合、自身定位和交通参与者预测等信息输入来完成自车行驶轨迹的决策和规划，并根据决策结果输出对车辆的控制命令或者告警信息。执行器抽象功能执行决策规划模块输出的车辆控制命令，驱动汽车的转向、驱动和制动等执行部件。

国汽智联、华为、中国软件评测中心、一汽、东风、长安、广汽等 16 家单位联合起草并于 2020 年 7 月 30 日联合发布了业界首个智能驾驶功能软件平台设计规范。车载计算平台功能软件架构图如图 4 所示：

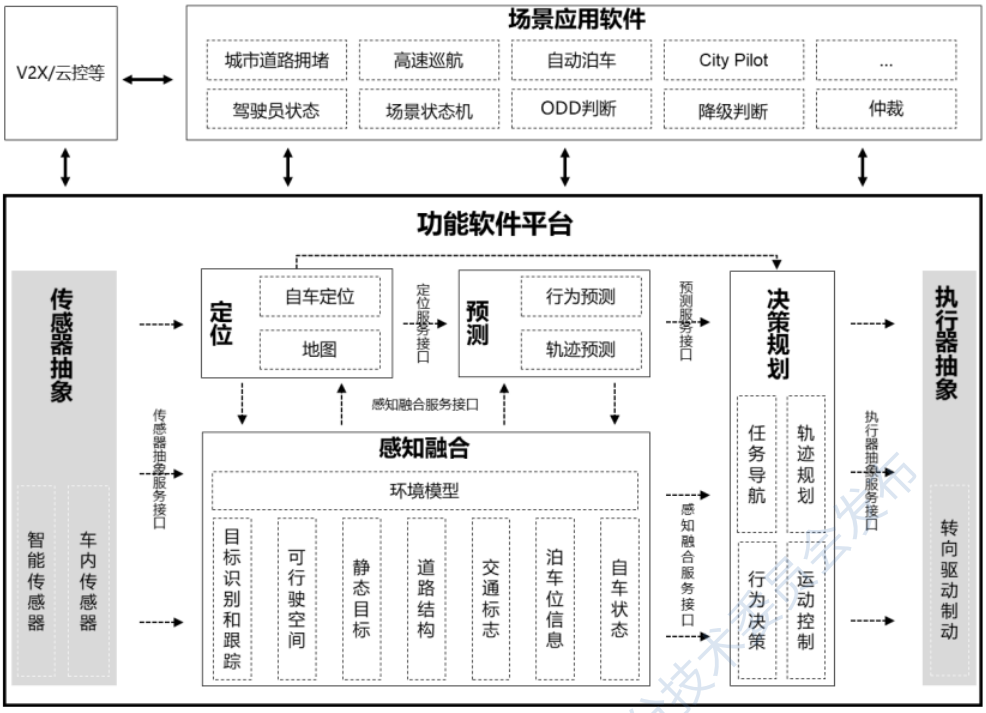

图 4 车载计算平台功能软件架构

4.3 车载计算平台保障技术

汽车网联化给乘客带来越来越多方便的同时，也埋下了信息安全隐患。大量传感器、控制器、执行器的引入使系统变得越来越复杂，同时也越发脆弱，系统故障的概率大大增加，功能安全问题同样不可忽视。所以信息安全和功能安全成为车载计算平台的关键保障技术。

4.3.1 车载计算平台信息安全技术

与传统汽车的封闭式系统不同，智能网联汽车由于其网联化程度提高，，汽车内部的参数配置、乘用人员的个人信息以及汽车内部电子电气系统的控制命令都能够被外部世界感知，不仅容易造成乘用人员的隐私泄露，还会影响到汽车的功能安全，如导致汽车功能失灵、错误判决甚至被远程操控，严重威胁乘用人员的人身和财产安全，甚至引发威胁社会安全的重大事故。

车载计算平台是智能网联汽车的大脑和实现自动驾驶功能的核心模块，也是与汽车控制域各个 ECU 直接通信并下达控制指令的计算中心，因此，车载计算平台的信息安全能力在直接影响着智能网联汽车的信息安全能力。从定位、架构、具备的功能和承载的业务上来看，平台涉及多种传感器、人工智能、端云协同，是一种涵盖物理世界和数字世界的新型混合系统。由于物理传感会影响数学世界的感知决策，感知决策又会影响物理世界的决策执行，这种相互影响的逻辑使得平台系统的设计极其复杂，同时也增大了系统的攻击面。

综上所述，车载计算平台不仅需要处理传统 ICT 领域所面临的信息安全威胁，还要解决与人身安全、社会安全相关的重大问题。因此，车载计算平台的信息安全问题需要得到足够的重视，并投入精力进行深入的研究。

4.3.1.1 车载计算平台信息安全总体架构

基于车载计算平台的架构与功能，信息安全技术可以细分为硬件安全、操作系统安全、应用安全、数据安全、隐私保护、AI 安全、通信安全几个方面。

图 5 为车载计算平台信息安全架构示意图。更细致地，硬件安全可分为芯片安全与固件安全；操作系统安全可分为操作系统加固、虚拟化安全等；应用安全则应同时考虑功能软件与自动驾驶相关应用软件的安全技术；数据安全则包括数据全生命周期中各个阶段的安全问题；隐私保护更偏重于个人数据的全生命周期合规性技术要求；AI 安全不仅应包括 AI 训练数据与训练模型的安全保护，还应该考虑 AI 算

法相关的保护技术，确保 AI 算法计算出的自动驾驶指令可靠且算法不受攻击和误导的影响。此外，通信安全应包括面向云端、面向 V2X 的对外通信安全与面向车内控制系统、车内总线的对内通信安全。

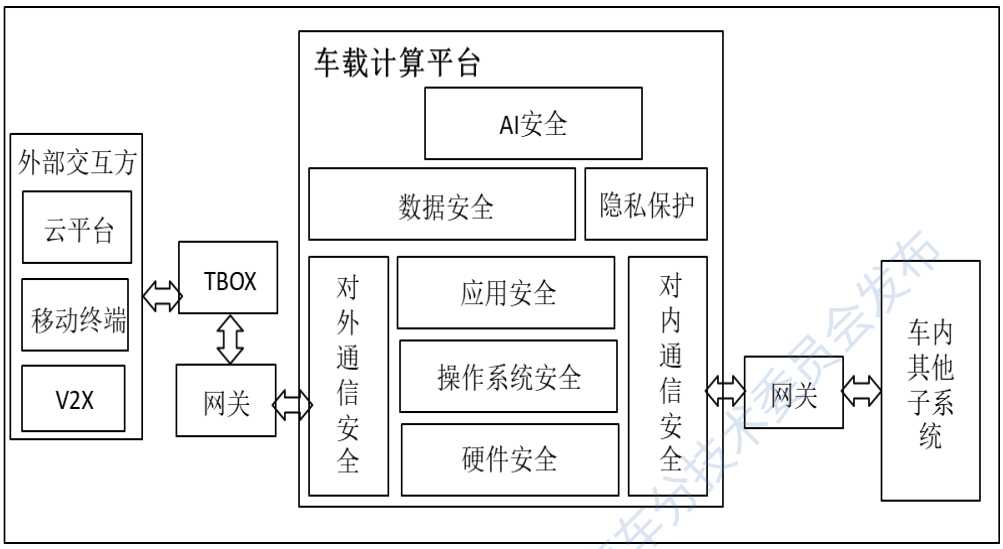

图 5 车载计算平台信息安全架构

4.3.1.2 车载计算平台信息安全威胁的影响

智能网联汽车的发展带来了便利，但也暴露了易被远程攻击、恶意控制的安全隐患，智能网联汽车目前面临的主要风险威胁包括 4 个层面：

一车端安全威胁，主要是指车内各个零部件和车内网络面临的安全威胁，包括车载计算平台的安全威胁。

二，网络传输安全威胁，主要是指车辆与云平台、与其他车辆、与基础设施的数据传输安全威胁。

三，云平台安全威胁，主要是指智能网联汽车连接的云平台的安全威胁。

四，外部互联生态安全威胁，主要是指与车辆互联的移动 APP 和充电桩等面临的安全威胁。

其中对具备智能驾驶功能的车辆来说，车载计算平台是智能驾驶的“大脑”，具有核心地位。

车载计算平台的安全威胁来自几方面：

一，接口安全威胁，攻击可能来自 Cloud/V2X 接口，诊断接口，传感器接口、调试接口等。

二，通信安全威胁，攻击可能包括重放、劫持、篡改等。

三，软件安全威胁，攻击可能包括恶意软件植入、恶意软件升级、软件漏洞、敏感信息泄露、拒绝服务攻击等。

四，硬件安全威胁，攻击可能包括侧信道攻击，物理侵入攻击等。

五，AI 安全威胁，攻击可能包括后门攻击、药饵攻击、模型窃取攻击、闪避攻击等。。

此外，车载计算平台的安全威胁不仅影响信息安全本身，也影响功能安全。

此外，SAE 在其 2016 年发布的 J3061 《Cybersecurity Guidebook for Cyber-Physical Vehicle Systems》中对信息安全和功能安全之间的关系进行了研究，认为功能安全关键系统（Safety-Critical Systems）是信息安全关键系统（Cybersecurity-Critical Systems）的一个子集，即部分信息安全关键系统出现的问题会最终导致功能安全问题，如图 6 所示。基于车载计算平台在车内电子电气架构中的位置与功能，以及对与其进行交互的车内外组件进行威胁分析，可以得出表 1。

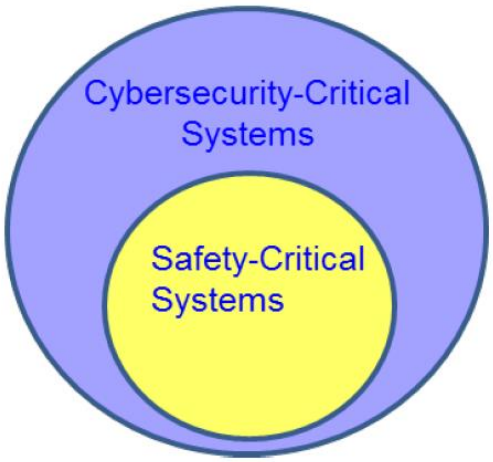

图 6 信息安全关键系统与功能安全关键系统的关系(来源 J3061)

表 1 车载计算平台安全威胁的影响分析

目标	攻击途径/手段		影响
云端服务器	攻破车载计算平台	利用车载计算平台登录云端服务器	云端存储的机密信息、汽车用户个人隐私数据被窃取，造成汽车用户与云端用户隐私泄露。
车载娱乐系统		通过车载计算平台与 HMI 交互	HMI 中存储的机密信息、汽车用户个人隐私数据被窃取，威胁与汽车用户关联的账户安全，带来隐私泄露和经济损失风险。
其他汽车		利用 V2X 通信向路基或其他汽车发送欺骗信息	其他车辆自动驾驶模块决策受干扰和误导，可能发出错误的控制指令，导致汽车行驶出现异常，对汽车乘用人员造成人身伤害威胁。

车身控制		通过车控网络，利用车载计算平台向车控模块 ECU 发送控制指令	车身控制系统如后视镜、车灯、车门、座椅调节等模块被攻击者控制，对汽车乘用人员造成人身伤害威胁。
底盘系统			底盘系统如转向模块等被攻击者控制，造成转向失灵或不可控，对汽车乘用人员造成人身伤害威胁。
制动系统			制动模块如动力、刹车模块被攻击者控制，造成制动异常，对汽车乘用人员造成人身伤害威胁。

从表 1 中可以看出，车载计算平台的信息安全问题不仅会造成传统的信息安全威胁，如机密信息获取、个人隐私泄露和经济财产损失，还会造成功能安全问题，威胁汽车乘用人员的生命安全。综上可得，车载计算平台是一个信息安全关键系统，同时也是功能安全关键系统。因此，在分析车载计算平台的信息安全问题时，需考虑其对功能安全的影响。

4.3.1.3 车载计算平台 AI 安全挑战

车载计算平台需要支撑智能驾驶功能，离不开 AI 计算。AI 的安全是车载计算平台区别于其它平台的特殊需求，目前 AI 安全的挑战包括：

- 软硬件的安全

在软件及硬件层面，包括应用、模型、平台和芯片，编码都可能存在漏洞或后门；攻击者能够利用这些漏洞或后门实施高级攻击。在AI模型层面上，攻击者同样可能在模型中植入后门并实施高级攻击；由于AI模型的不可解释性，在模型中植入的恶意后门难以被检测。

- 数据完整性

在数据层面，攻击者能够在训练阶段掺入恶意数据，影响AI模型推理能力；攻击者同样可以在判断阶段对要判断的样本加入少量噪音，刻意改变判断结果。

- 模型保密性

在模型参数层面，服务提供者往往只希望提供模型查询服务，而不希望曝露自己训练的模型；但通过多次查询，攻击者能够构建出一个相似的模型，进而获得模型的相关信息。

- 模型鲁棒性

训练模型时的样本往往覆盖性不足，使得模型鲁棒性不强；模型面对恶意样本时，无法给出正确的判断结果。数据隐私： 在用户提供训练数据的场景下，攻击者能够通过反复查询训练好的模型获得用户的隐私信息。

针对车载计算平台的安全攻击方式有以下几种：

- 闪避攻击

通过修改输入，让AI模型无法对其正确识别。研究表明深度学习系统容易受到精心设计的输入样本的影响。这些输入样本就是学术界定义的对抗样例或样本，即Adversarial Examples。它们通常是在正

常样本上加入人眼难以察觉的微小扰动，可以很容易地愚弄正常的深度学习模型。

除了对数字的图片文件加扰， 有人对路标实体做涂改，使 AI 路标识别算法将“禁止通行”的路标识别成为“限速 45”。它与数字世界对抗样本的区别是，物理世界的扰动需要抵抗缩放，裁剪，旋转，噪点等图像变换

生成对抗样本需要知道 AI 模型参数，但是在某些场景下攻击者无法得到模型参数。 有人发现对一个模型生成的对抗样本也能欺骗另一个模型，只要两个模型的训练数据是一样的。这种传递性（Transferability）可以用来发起黑盒攻击，即攻击者不知道 AI 模型参数。其攻击方法是，攻击者先对要攻击的模型进行多次查询，然后用查询结果来训练一个“替代模型”，最后攻击者用替代模型来产生对抗样本。产生出来的对抗样本可以成功欺骗原模型。

- 药饵攻击

AI 系统通常用运行期间收集的新数据进行重训练，以适应数据分布的变化。 例如，入侵检测系统（IDS）持续在网络收集样本，并重新训练来检测新的攻击。在这种情况下，攻击者可能通过注入精心设计的样本，即药饵，来使训练数据中毒（被污染），最终危及整个 AI 系统的正常功能，例如逃逸 AI 的安全分类等。

- 后门攻击

AI 模型也可以被嵌入后门。只有制造后门的人知道如何触发，其他人无法知道后门的存在，也无法触发。与传统程序不同的是，神

经网络模型仅由一组参数构成，没有源代码可以被人读懂，所以后门的隐蔽性更高。攻击者通过在神经网络模型中植入特定的神经元生成带有后门的模型，使得模型虽然对正常输入与原模型判断一致，但对特殊输入的判断会受攻击者控制。

- 模型窃取攻击

模型/训练数据窃取攻击是指攻击者通过查询，分析系统的输入输出和其他外部信息，推测系统模型的参数及训练数据信息。

4.3.1.4 车载计算平台信息安全防护体系

建立车载计算平台的信息安全防护体系，可从如下两个维度开展：

（1）车载计算平台的产品信息安全生命周期保护

关注车载计算平台全生命周期内的信息安全防护，包括设计开发、生产、使用运维、报废等过程。

首先，在设计开发阶段，基于产品的应用场景，从产品生命周期的视角来识别信息安全威胁，并针对性地设计信息安全防护方案。在零部件开发过程中，将信息安全防护方案落地实施。

其次，在零部件和整车生产阶段，需要做到产品下线之初便预置产品的安全信任根，例如，注入了产品的根证书和密钥等。

接着，在使用运维阶段，关注产品的信息安全状态和信息安全事件，做好信息安全事件监控、产品信息安全漏洞管理和应急响应工作。

最后，在产品报废阶段，需要清理产品中的机密数据，避免敏感信息的泄露。

（2）车载计算平台的产品信息安全防护技术体系。

建立车载计算平台的纵深防护体系，即从多方面设计和部署信息安全防护措施，做到全方位的信息安全保护。

（a）硬件安全防护

首先，应通过禁用调试接口、减少芯片管脚暴露、采用内层布线隐藏通信线路等措施，减少硬件上的攻击面。其次，利用硬件安全模块来保障车载计算平台的信息安全基本属性，例如，HSM、SE 和 TrustZone 等技术，并基于硬件安全模块，实现如下功能：

- 充当硬件信任根

通过验证数字签名和产品密钥，检查引导加载程序和关键操作系统文件是否被篡改。无效文件在攻击或感染系统之前被阻止运行，从而为车载计算平台提供信任基础。

- 创造隔离的可信执行环境

如受信任的处理器模块：使用加密技术为每个已批准的组件创建唯一标识符，从而将启动环境的元素与已知良好的源进行精确比较，阻止不匹配的代码启动。

- 实现安全存储

利用硬件安全模块存储产品密钥、证书等重要数据，避免攻击者对敏感数据进行非授权访问。

- 实现密码学运算加速

利用硬件电路对密码学运算进行提速，提高密码运算性能，以应对业务场景中对密码运算的高实时性要求。

（b）软件安全防护

除了在硬件上部署信息安全防护措施，还需要软件信息安全防护措施的配合，包括操作系统和应用软件两个维度。

- 实现安全启动

与硬件信任根配合使用，确保被加载的软件组件真实有效，为软件运行提供信任根。

- 隔离可信执行区和不可信执行区

在硬件可信执行环境的基础上，进一步根据系统中软件属性，划分成可信执行区和不可信执行区。通过隔离不同的进程或应用功能，实现系统的信任隔离。

- 部署程序安全升级措施

对于需要执行程序升级的应用场景，系统需要具备校验程序包机密性和完整性的措施，确保被升级的程序包来自可信的发布方，杜绝系统软件被非法篡改的情况出现。

- 部署日志记录服务

提供日志记录功能接口，系统重要应用能够调用该接口记录运行日志，通过导出该日志可以对应用运行状态进行分析。

（c）通信端口防护

面向自动驾驶应用场景，车载计算平台将包含多种通信接口，例如，CAN、Ethernet 等，实现车内和车外的数据交互。对于通信接口上部署的安全防护措施，需要保证交互数据的真实性、可用性和完整性，同时确保数据交互过程的实时性和可靠性。部署的信息安全防护措施包括：

- 关闭后门端口

通信接口上不允许存在未声明或未使用的后门端口，避免攻击者通过这些端口对系统进行攻击。

- 进行交互数据的过滤

对通信端口上交互的数据进行信号过滤，过滤异常的通信数据和信号，例如，部署防火墙措施和入侵检测措施。此外，还需要验证数据是否来自合法的数据源，保证交互数据的真实性和完整性。

- 管理访问控制权限

根据“最小权限”原则，对通信端口上的访问控制器进行管理，根据通信端口上的访问用户类型划分其对应的访问权限和控制访问策略。

（d）AI 安全防护

针对 AI 的闪避攻击，安全防护技术包括：在数据收集阶段采用对抗样本生成方法；在模型训练阶段采用网络蒸馏和对抗训练方法；在模型使用阶段采用对抗样本检测、输入重构和 DNN 模型验证方法。

针对 AI 的药饵攻击，安全防护技术包括：在数据收集阶段采用训练数据过滤和回归分析方法；在模型训练阶段采用集成分析方法。

针对 AI 的后门攻击，在模型训练阶段采用模型剪枝方法；在模型使用阶段采用输入预处理方法。

针对 AI 的窃取攻击，在模型训练阶段采用差分隐私方法；在模型使用阶段采用隐私聚合教师模型 PATE 和模型水印方法。

4.3.2 车载计算平台功能安全与预期功能安全技术

功能安全的融入是车载计算平台产品研发生产和技术发展的客观要求。功能安全在自动驾驶系统的全生命周期中起着指引、规范、控制的作用。明确的功能安全要求、技术方案和规范的功能安全开发流程可以降低和避免来自系统性失效和随机硬件失效的风险。车载计算平台在运行过程中出现故障时，也依赖于功能安全机制确保系统进入安全状态。

道路车辆功能安全的提出主要是降低汽车电子电气系统的功能异常表现引起的危害而导致的不合理风险。电子电气系统的失效包括硬件自身的随机失效及研发过程中引入的系统性失效（软件失效属于系统性失效）。车载智能计算平台实现自动驾驶功能，需要具备可靠冗余的安全设计，其核心系统须达到功能安全相关标准的要求，如ISO 26262:2018、GB/T 34590-2017 等。

目前，针对功能安全要求主要采用 ISO 26262 标准，该标准详细地描述了电子电气系统的硬件随机失效，以及潜在、多点故障失效，软件故障注入测试等内容。电子电气系统的故障可分为随机硬件故障和软件或流程原因导致的系统性故障。通过实施功能安全，以危害分析和风险评估后得到的安全目标及汽车安全完整性等级（ASIL 等级）为导向，开发和落实相关安全要求，能有效降低系统功能失效导致的风险。例如，为了达到自动驾驶功能安全等级 ASIL D 的要求，目前一般采用主从两个主控器，实现故障检测与冗余控制等。这种冗余设计不仅包含系统软件和功能软件，也兼顾传感器、车辆网络、芯片、

硬件平台等，可以高效完备地实现车载计算平台的车规级功能安全。

具有自动驾驶功能的汽车是一项极其复杂的系统，要证实系统可以完成设定的目标，即所说的预期功能安全 SOTIF（Safety Of The Intended Function），是一项非常具有挑战性的工程。SOTIF 针对的系统功能局限可分为 3 类：感知——目标使用场景考虑不周全，导致系统不能准确识别环境要素；决策——功能仲裁逻辑不合理，导致运动控制偏离预期等；控制——执行器功能局限导致与理想目标偏差。

车载计算平台承担着自动驾驶中至关重要的决策工作，因此必须满足预期功能安全要求，最新补充的 ISO/PAS 21448 预期功能安全要求将成为重要参考。

在车载计算平台中，理想的状态下对其输入确定数值，即可期望相同的结果，但车辆的运行场景往往是多变的，静态和动态因素同时存在于驾驶场景之中，这种连续或离散变化的状态对于感知来说的输入变量是不可量化和计算的，因此很难保证系统输出的稳定性和鲁棒性，直接导致系统的设计不能满足目标市场的实际需求。

功能局限产生的本质原因就是设计开发时系统功能定义不能充分覆盖目标市场的使用需求。为此，需要充分搜集预期使用场景的数据，作为功能设计输入，同时要求进行大量的验证工作，包括实地实车测试，以尽可能涵盖全部使用工况，并在广泛相异的情形以及天气情况下实现安全目标。福特汽车的安全报告中就提到，在产品开发的早期就开始做软件在环、硬件在环和大批量的车辆测试，通过虚拟测试和路试的方法积累尽可能多的 Scenario 数据库，以测试驱动开发的

敏捷开发形式快速进行算法迭代，保证目标市场的投放稳定可靠。

5 车载计算平台标准化研究

基于车载计算平台技术及产业的发展现状，其标准化需求主要集中在参考架构、连接互通、保障能力、性能要求等几个方面。

5.1 车载计算平台参考架构标准化

发展车载计算平台，既要突破关键基础共性技术，还要突破现有供应链体系和商业模式，涉及面广，实施难度大。车载计算平台涉及汽车、软件、芯片、信息通信等技术领域的各个环节和主体，是一项前瞻性、全局性的系统工程。当前，定义、术语尚未明确，车载计算平台、车载智能计算平台、车载智能计算基础平台、高性能计算平台、智能计算平台等概念较为混乱，面向的应用场景、驾驶自动化等级等边界不清，关键核心技术发展重点存在分歧。对其认识和理解的差异，有可能导致技术路线上的分化，影响互操作性，增加部署成本，进而影响了产品的产业化和商业模式拓展。与此同时，当前正处于车载计算平台发展初期阶段，国际国内相关领域技术标准和管理规范尚未建立，行业发展碎片化，行业应用存在一定的盲目性，不利于技术发展和应用落地。

推动参考架构的研究梳理和标准化工作，可以为我国车载计算平台的技术创新、试验验证、应用实践、产业生态构建等提供参考和引导。另一方面，推动参考架构的研究梳理和标准化工作需要广泛调研相关行业企业需求，避免限制企业个性化技术创新的发展要求，同时注意与国际国内已有或正在研制的标准规范的协同。因此，应基于前

期研究工作基础，进一步深化研究，完善后续参考架构标准化工作。

车载计算平台参考结构自底向上可以划分为硬件平台、系统软件、功能软件和应用软件等四层。功能软件层包含感知融合、定位、预测和决策规划等核心功能和算法模块，是驾驶自动化系统的核心部分。通过构建一个标准化的功能软件平台，定义功能软件层的系统架构以及功能模块和算法组件的逻辑服务接口，可以明确产业分工和边界，缩短智能驾驶系统的开发周期并降低系统集成成本。

5.2 车载计算平台连接互通标准化

5.2.1 连接器接口标准化

根据目前及未来的智能驾驶发展方向，计算平台可能存在的接口有以太网接口、CAN/CAN FD 接口、视频接口（如差分或同轴电缆）、USB 接口、串行接口及外置存储接口等。关于各功能接口目前无针对标准进行规范，通用型接口标准有《QC/T 1067 汽车电线束和电器设备用连接器》、《QC/T 29106 汽车电线束技术条件》、《QC/T 417 车用电线束接插器》、《QC/T 29009 汽车用电线接头技术条件》、《GMW3191 CONNECTOR TEST AND VALIDATION SPECIFICATION》等均规定了车用接插件的形式、设计规范及测试标准。

5.2.2 通信网络标准化

在汽车智能化的今天，新的应用对车载通信网络带宽提出了更高的要求，车载以太网也便应运而生。但是整个汽车工业不会全部都转换为以太网，现用的 CAN 网络及其升级版 CAN-FD/CAN-XL LIN 还

会沿用。可以预见未来会以混合网络的形式存在，网络拓扑简图如 4-4-3 所示，各个子网之间通过网关进行通信，子网内兼容现有的网络通信。

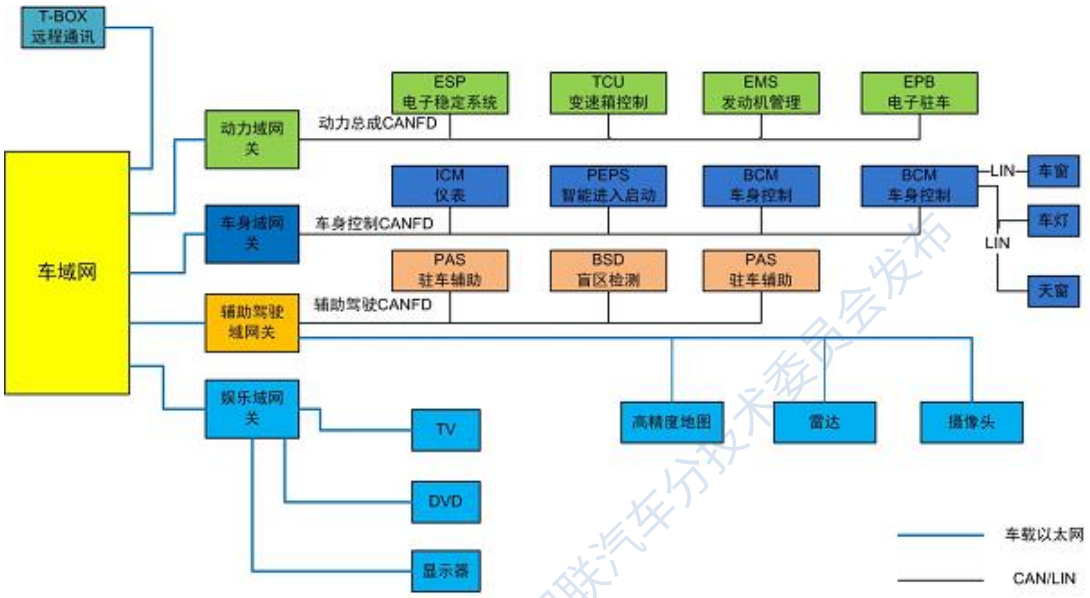

图 7 车内混合通信网络示意图

（1）LIN

LIN 是一种低成本的通用串行通信网络，只需要单个线缆，成本低，最大传输速度为 20kb/s,总线电平一般为 12V，主要应用在车门，天窗，座椅控制领域，对传输速度、性能和容错功能要求不高的应用场景。

在未来的汽车工业应用中，LIN 网络仍然可以做为 CAN 或者其他网络的一种有效的补充，应用在低速通讯的场景中。

（2）CAN

CAN 经过数十年的发展，已经形成的完善的标准体系 ISO-11898，兼容性高，有完善的开发工具链体系和生态应用。

CAN 是总线式通讯，具有高实时性，传输距离远，抗电磁干扰能力强等优点，成本低，能够很好的适应传统车载 ECU 间的控制数据传输需求，通过双绞线或者同轴电缆进行信号传输，适用于大数据量短距离或者长距离小数据量的传输，通讯距离最远可达到 10 千米(速率低于 5kbps),最大传输速率 1Mbps(距离小于 40 米)，易扩展，网络内的节点个数理论上不受限制。可靠性极高。CAN 具有完善的通信协议，可由 CAN 控制器芯片机器接口芯片来实现，开发难度低，开发周期短。

CAN-FD 是第二代 CAN 通信技术，是 CAN 协议的升级版，物理层与 CAN 一致，跟传统 CAN 能很好的兼容，开发成本也跟 CAN 相差不大,一帧数据最长为 64 字节,速率可变,仲裁速率最高 1Mbps，与 CAN 相同,数据速率最高为 8Mbps,同时帧格式也做了一些扩展。

CAN-XL 是 2020 年起草的第三代 CAN 通信技术，保持 CAN 协议的优势，为高达 10Mbps 速率的通信提供解决方案，填补 CAN-FD 与以太网之间的空白，可以和 CAN-FD 互操作，实现 CAN-FD/CAN-XL 混合网络。物理层仍然在开发的过程中。

（3）FlexRay

FlexRay 联盟成立于 2000 年，于 2009 年解散，是一种具备故障容错的高速车载总线系统，有两个信道组成，单个通道速率高达 10Mbps，能更好的实现冗余，当两个信道传递不通数据时，数据速率高达 20Mbps。

（4）车载以太网通信

100BASE-T1 是 IEEE 针对 100Mbps 汽车以太网的规范，也称为 IEEE802.3bw,它通过使用一对非屏蔽双绞线可实现 100Mbps 的全双工数据传输，同时在两个方向上传输，通信距离 15m 以上。通讯速率快。将车载生态系统标准化为一种网络架构(如附图 4-4-3 所示)，从而简化了 ECU 之间的整体通信，甚至可能消除对 MOST/FlexRay 的需求，为车内音视频的多媒体应用提供了可能。

1000BASE-T1 是 IEEE 针对 1000Mbps 汽车以太网规范，也称为 IEEE802.3bp,也是使用一对双绞线进行全双工通信，通信距离在 40m 以上。

10Gbps，以太网规范 IEEE 802.3ae，为高带宽需求的车载应用开发成为可能，自动驾驶系统中会在汽车周围安装多个摄像头，无损的图像数据可以经过千兆/万兆以太网传输到车载电脑存储，便于后期备份，仿真使用，满足相关法律法规的要求。

随着自动驾驶的持续推进，百兆网/千兆网，甚至万兆网，将大规模的应用于自动驾驶系统内，为大数据量的感知计算提供高速可靠的通讯服务。

（5）短距离无线通信

蓝牙技术已经应用在汽车上，如蓝牙钥匙控制车窗、蓝牙电话等，通讯距离 10 米以内，使用 IEEE802.15 协议，全双工传输，传输速率 1Mbps，考虑到功能安全，应用场景还比较有限。

除了蓝牙技术以外，新一代专门为车内场景设计的短距离无线通信技术也开始出现，例如，2020 年 9 月 22 日，星闪联盟（SparkLink

Alliance）正式在北京成立，目标是推动新一代无线短距通信技术创新和产业生态，在低时延、高可靠、多并发、精同步等方面发展性能优势，承载智能汽车、智能家居、智能终端和智能制造等场景应用并满足极致性能需求。

未来的车载网络将会是CAN/LIN/以太网混合网络形式存在，LIN用来控制车窗、车门之类的低速通讯场景，CAN 仍然会用来控制底盘相关服务，数据量大的影音娱乐需求、高分辨率摄像头图像数据及其他传感器数据传输将用以太网来完成，同时车载短距无线也由于其部署的灵活性在座舱娱乐、胎压监测、电池管理等领域逐渐得到更加广泛的应用。

5.2.3 逻辑接口标准化

车载计算平台在功能上需要传感器输入数据，需要将车控指令发往底盘执行器（驱动、转向、制动等系统）。因此车载计算平台与传感器和执行器之间除了有网络连接外，还需要定义语义层面的逻辑接口标准，以方便车载计算平台与传感器和执行器的双向兼容，使得车载计算平台既能够识别传感器输入的数据和执行器反馈的数据，同时车载计算平台也能够发送控制指令控制不同的传感器和执行器。

在车载计算平台与传感器的逻辑接口方面，ISO 组织制定了标准《ISO 23150:2020 Road vehicles — Data communication between sensors and data fusion unit for automated driving functions — Logical interface》，定义了毫米雷达、激光雷达、摄像头等传感器所识别对象的特征和格式。目前国内正在研究以 ISO 23150 为蓝本制定中传感器逻辑接口国

家标准。

在车载计算平台与执行器的逻辑接口方面，中国汽车工程学会正在制定《线控转向及制动系统通讯协议要求及测试规范》，标准定义了车载计算平台与制动和转向系统的控制反馈信号，明确信号的长度、范围、精度、单位、必要性等。

5.3 车载计算平台保障能力要求标准化

5.3.1 信息安全标准化

工信部、发改委印发的《扩大和升级信息消费三年行动计划（2018-2020 年）》提出，要推进车载智能芯片、自动驾驶系统、车载智能算法等关键技术产品研发，构建一体化智能车辆平台，培育多元化应用。到 2020 年，建立可靠、安全、实时性强的智能网联汽车计算平台，形成平台相关标准，支撑高度自动驾驶（HA 级）。因此，车载计算平台的信息安全标准化需求非常迫切。

车载计算平台在自动驾驶中起着关键作用，一方面接收不同传感器采集的环境感知信息，另一方面，通过解释和处理接收到的环境感知信息，决定应该如何控制车辆，并把相应的控制指令传递给车辆执行单元。

鉴于车载计算平台在自动驾驶系统中的关键性，保证其安全性是自动驾驶极其重要的目标。同时，由于驾驶员已经不在自动驾驶的控制闭环中，自动驾驶系统的失效不能够依赖于驾驶员作为额外的后续处理冗余。这就要求车载计算平台本身是可信任的，且能够抵御外界入侵。

除此之外，车载计算平台也会涉及用户信息，以及其他方面的隐私或保密信息，例如自动驾驶的黑匣子功能，因此，车载计算平台也需要考虑个人信息的隐私保护。

鉴于自动驾驶对于冗余系统的需求，车载计算平台的信息安全保护也需要基于纵深防御的思想。这其中包括车载计算平台自身硬件、操作系统、软件的信息安全措施；对于环境感知信息的交叉验证；以及对各关键节点通讯的有效保护。此外，鉴于技术上和成本上的限制，我们无法完全排除车载计算平台受攻击的可能性。在发生攻击事件后，车载计算平台必须考虑合适的后续处理或降级措施，在不依赖驾驶员处理的情况下，仍能够保证车辆的安全。

随着时间的推移或者自动驾驶功能的不断迭代，可能会出现新的漏洞或攻击方式。这就要求车载计算平台能够提供合适的更新机制，能够升级本身的信息安全措施，来保证整个车辆生命周期的信息安全。

总之，车载计算平台信息安全应考虑通信层面，包括环境感知、控制指令；自身的软硬件信息安全和隐私安全；攻击发生后的处理措施以及全生命周期的信息安全保障几个方面的内容。标准化需求应包括硬件安全技术要求、通信协议与接口安全技术要求、操作系统安全技术要求、固件安全技术要求、应用软件安全技术要求、数据安全技术要求及与之对应的信息安全测试方法。

5.3.2 功能安全与预期功能安全标准化

功能安全主要针对车载计算平台系统产生漏洞、发生故障时产生失效行为的问题。当检测到潜在危险情况时，启动保护或纠正装置，

以防止发生危险事件或通过缓解措施来减少危险事件的后果。对于智能网联汽车来说，实现功能安全最根本的目的在于提升汽车的安全性，此外，执行功能安全能够提供安全开发证据，并且提供了合作方之间相互理解的平台。

ISO 26262 是针对电子电器架构的汽车功能安全标准，主要定位在汽车行业中特定的电器件、电子设备、可编程器件等专门用于汽车领域的部件。车载计算平台实现自动驾驶功能，应对产品的整个生命周期进行评估，根据需求进行分解，确定每一条需求的 ASIL 等级要求，其核心系统必须达到功能安全 ASIL-D 级别。此外，还应对概念设计、软硬件设计、以及最后的生产、操作环节进行严格要求。同时考虑软硬部件失效、功能受限以及应用场景不完备情况下的分析流程和设计需求，以确保车载计算平台的功能性失效不会造成危险的发生。

除此以外，国外功能安全标准还包括 SAE J2980, UL4600，ISO TR4804。SAE（SAE International，国际自动机工程师学会）发布了 SAE J2980 Considerations for ISO 26262 ASIL Hazard Classification（ISO 26262 ASIL 危险分类的注意事项)标准，用于指导 ASIL 定级。SAE J2980 标准基于 ISO 26262 的既有定义，在 S（Severity，严重度）、E（Exposure，暴露率）、C（Controllability，可控性）三个指标的评估方面做了更详细的说明，为整车及零部件企业功能安全开发提供参考。

UL 4600 自动驾驶安全评价标准由 UL（Underwriters Laboratories，美国保险商实验室）与 Edge Case Research（自动驾驶研究机构）合作开发，是针对自动驾驶系统的安全评估标准。该标准旨在为自动驾

驶设计提供完整的安全评价原则和体系，为机器学习、感知操作环境和自动驾驶所需的硬件和软件提供安全性及可靠性评估。UL 4600 根据自动驾驶系统的当前状态和对其操作环境的感知，评估自动驾驶系统在无人为干预的情况下安全地执行预期功能的能力，帮助厂商梳理所有与自动驾驶安全相关的领域，标明所有必需测试的项目，从而建立系统的方法，确保设计团队不会遗漏某个可合理预见的问题。

2019 年，由宝马发起，安波福、奥迪、百度、宝马、大陆、戴姆勒、克莱斯勒、HERE、英飞凌、英特尔、大众等 11 家公司共同发布了《自动驾驶 安全第一》白皮书，阐述了如何在自动驾驶系统上综合运用功能安全、预期功能安全和信息安全的方法论。ISO（International Organization for Standardization，国际标准化组织）基于这份白皮书，将发布全球第一个专门针对自动驾驶的应用安全标准 ISO TR4804 Road vehicles - Safety and cybersecurity for automated driving systems - Design, verification and validation（道路车辆—自动驾驶系统的功能安全和网络安全—设计、验证和确认）。

GB/T 34590 是中国汽车行业功能安全的设计标准。作为自动驾驶关键性的控制单元，车载计算平台的设计过程中，应该充分考虑符合 GB/T 34590 的要求。

鉴于自动驾驶功能的不断演进，以及不同车辆上自动驾驶功能的多样性，车载计算平台应该充分考虑当前和未来所支持的功能的最高的功能安全等级，并且从整体的软件和硬件架构设计上满足对应的功能安全等级。对于对外的接口应该设计足够的安全措施，以确保通信

过程的稳定性，可靠性和及时性。同时应该考虑和周边系统交互需求的协调性，包括车内其他系统，以及车外系统，例如云，地图或路端设施等等。

除了对于产品本身的软硬件的技术要求，GB/T 34590 对于系统开发其他方面的要求，也应该应用于车载计算平台的开发设计过程中，包括开发流程以及开发工具。开发工具应该都具备对应的资质，以确保对于开发产品没有影响。

由于智能网联汽车的发展趋势，车载计算平台必然会引入越来越多信息安全的保障措施。在满足信息安全要求的同时，不能违背对应的功能安全目标及相应的安全状态。

自动驾驶功能需要有大量的数据处理，车载计算平台应该具备强大的运算能力和运算速度，以确保整体功能在表现不会违背任何的安全要求和设计。同时，需要保证不同场景下对应功能的切换以及降级过程能够实现有效的安全状态，譬如系统失效后紧急状态的切换。

最后，针对于自动驾驶场景的复杂性，车载计算平台应该设计有效的验证方法和策略，并在开发中确保该验证的实施。

功能安全主要针对车载计算平台系统产生漏洞、发生故障时产生失效行为的问题。当检测到潜在危险情况时，启动保护或纠正装置，以防止发生危险事件或通过缓解措施来减少危险事件的后果。对于智能网联汽车来说，实现功能安全最根本的目的在于提升汽车的安全性，此外，执行功能安全能够提供安全开发证据，并且提供了合作方之间相互理解的平台。

信息安全关注于与安全相关的威胁，功能安全关注于与安全相关的失效，而 ISO/PAS 21448《Road vehicles — Safety of the intended functionality》中引入的预期功能安全（SOTIF）要求，则关注由功能不足，或者由可合理预见的人员误用所导致的危害和风险。预期功能安全需要确保自动驾驶汽车在正常运行期间的功能和安全。因此，车载计算平台预期功能安全保障应涵盖自动驾驶设计概念的细节、预期功能安全标准评估、降低预期功能安全相关风险方法以及预期功能安全相关风险的检查和验证。

此外，对于场景的评估也是保障预期安全功能的一大要素，应确保当前场景和用例的完整合理性。对不同环境场景进行前期概念分析和后期验证，通过不同场景的资料、这些场景的安全分析、安全场景验证、触发事件验证、以及在环境中验证车辆搭载的安全系统来保障车载计算平台的预期功能安全。

5.4 车载计算平台性能要求标准化

车载计算平台的性能主要考察逻辑算力、AI 算力、能效比等几方面。其中逻辑算力测试主要针对 CPU，AI 算力可针对 GPU、ASIC 芯片或 FPGA 等。能效比指标计算前，需要测量出每种算力测试进行时计算平台的功耗。

5.4.1 算力测试方法

（1）CPU 测试

在嵌入式系统行业用于评价 CPU 性能指标的标准主要有三种：DMIPS（Dhrystone Million Instructions Per Second，每秒处理的百万级

的机器语言指令数）、Whetsone MIPS、CoreMark，其中 Dhrystone 是一种古老的却历时 30 年而不衰的嵌入式系统处理器测试基准，至今仍为各大处理器生产厂商所采用。其中 CoreMark 是一种新兴流行的嵌入式系统处理器测试基准，被认为是比 Dhrystone 和 MIPS 更具有实际价值的测试基准。

（2）AI 算力性能测试

车载计算平台是否能够保障自动驾驶的安全，有两个重要影响因素：一是计算平台本身软硬件的设计是否足够支撑汽车在极端场景下的自动化功能正常运作；二是其中包含的车载 AI 芯片本身的算力和对应的算法是否足够支持汽车具备准确且实时的感知能力，保障自动驾驶汽车的行车安全。以感知为例：自动驾驶车辆需要对车身 360°范围内的环境进行感知，包括对移动物体的识别、跟踪、预测、对于驾驶环境的语义分割、建模、定位，其感知的范围非常广，而且还要在不同的天气情况、光照条件下可靠地工作，这对于车载计算平台的 AI 算力以及对应的感知算法的可靠性、准确性提出了极其苛刻的要求。

AI 芯片面临的一大挑战，是算法演进速度远超硬件改进速度，车规级 AI 芯片的迭代周期一般需要 2 到 3 年，而软件算法的迭代周期则是几个月，AI 芯片的算法演进则更快，两者演化周期的不匹配，致使评估芯片 AI 性能的方法与算法发展之间存在脱节的现象，对任何开发从事 AI 芯片以及对应解决方案的算法公司都是一个巨大的挑战，AI 芯片与算法要实现软硬件协同发展。

目前业界尚缺乏一个与时俱进的，能有效评估 AI 性能的标准。业界惯常使用的评测标准有两种，一是峰值算力，但峰值算力只反映车载计算平台理论上的最大 AI 计算能力，而非在实际 AI 应用场景中的处理能力，具有很大的局限性；二是目前行业较为知名的基准测试组织 MLPerf，其采用的模型少且更新速度滞后于算法演进的速度，无法及时反映算法效率的提升以及各种精度下芯片能够达到的计算速度，因而无法描述 AI 性能的全貌。

例如特斯拉 HW3.0 计算平台采用自研 FSD 芯片，AI 算力 72TOPS，其前代 HW2.5 平台采用的芯片为英伟达 DRIVE AGX Xavier，AI 算力为 24TOPS，如果单纯从 AI 算力角度衡量性能是 3 倍关系，但从图像处理帧率来看，实测性能是 21 倍的差别。算力不是评估自动驾驶性能的唯一指标，更应关注真实性能，即处理 AI 任务时的真实处理能力。

评估车载计算平台 AI 性能，应关注真实的用户价值，本质上应该关注做 AI 任务的速度和精度，即‘多快’和‘多准’两个关键维度。在体现真实 AI 性能的同时留有最大的优化空间，指引用户以最优方式使用芯片。

国内外多个行业组织机构都在推出相关的 AI 性能评测标准，包括 MLPerf，苏黎世理工学院的 AI benchmark 等等，这类评测的特点多数属于基准测试的范畴，效果依赖于模型的数量和更新速度。由于芯片算法演进速度远超硬件改进速度，致使评估 AI 性能的方法与算法发展之间存在脱节的现象，智能网联汽车产业尚缺乏与时俱进、能

够有效评估 AI 性能的标准。

针对当前 AI 性能评测存在的问题，MAPS(Mean Accuracy-guaranteed Processing Speed，精度保持下平均帧率）评测方法针对应用场景的特点，在精度有保障的前提下，包容所有与算法相关的选择，评估芯片对数据的平均处理速度，以此为业界提供一个评估芯片真实性能的全新视角。MAPS 评测方法能够直观、量化视觉感知计算芯片的真实性能，提供清晰的评价结果，牵引面向真实场景的芯片性能优化方向，帮助业界更全面地了解每款芯片的视觉感知计算能力，找到最适宜的视觉感知落地方案。

MAPS 评测方法为：在不同精度点上选择最优的 FPS 值，将这些点绘制在以帧率为横坐标，精度为纵坐标的坐标系内，顺序连接这些最优 FPS 对应点，绘制出一条曲线。

MAPS 计算公式为：

$$\left\{\sum_{i=1}^{N}\frac{1}{2}(fps_{i-1}+fps_i)*(acc_i-acc_{i-1})\right\}/(acc_n-acc_0)$$

假设落在指定精度范围内获得了 N 个最高的 FPS 值，设定：

1）第 i 个点对应的帧率$\mathrm{fps_i}$，对应的精度为$\mathrm{acc_i}$；

2）第 i-1 个点对应的帧率$\mathrm{fps_{i-1}}$，对应的精度为$\mathrm{acc_{i-1}}$，则第 i 点和第 i-1 点之间的连线与纵坐标围成的面积为：$1/2(\mathrm{fps_{i-1}}+\mathrm{fps_i})*(\mathrm{acc_i}-\mathrm{acc_{i-1}})$；

3）整个曲线与纵坐标围成的总面积则为分段面积总和，即：$\sum_{i=1}^{N}1/2(\mathrm{fps_{i-1}}+\mathrm{fps_i})*(\mathrm{acc_i}-\mathrm{acc_{i-1}})$；

4）测试结果中落在指定精度范围内获得的最高精度为$\mathrm{acc_n}$，最底

精度为acc_0；则精度区间为$acc_n - acc_o$；

5）根据 MAPS 定义可知：MAPS = 曲线所围面积/(精度区间)，即：$\{\sum_{i=1}^{N} 1/2(fps_{i-1} + fps_i) * (acc_i - acc_{i-1})\}/(acc_n - acc_o)$。

MAPS 测评方法如下图所示：

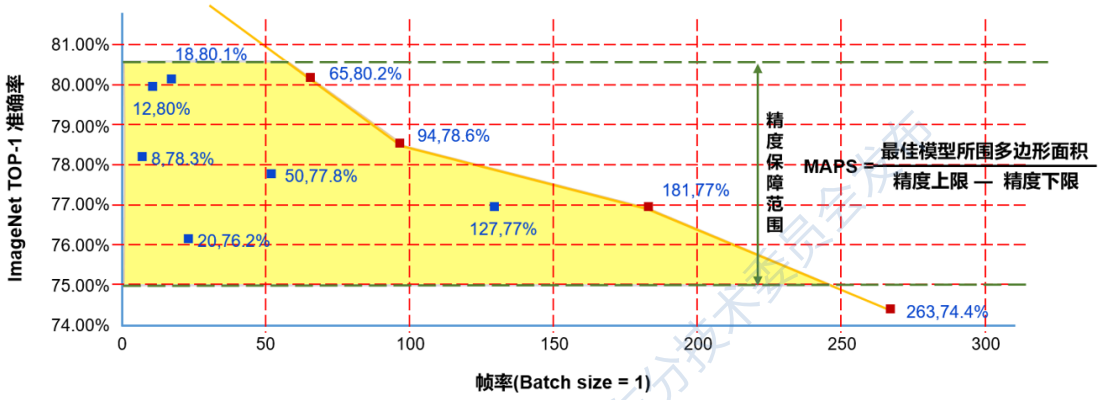

图 8 MAPS 测评方法图

具体方法如下：

1）将某算法模型运行得到的处理速度和精度用一个点表示在二维坐标系，如上图所示，其中横坐标表示处理速度即帧率，单位为 FPS，纵坐标表示模型精度，即在 IamgeNet 数据集下 TOP-1 分类精度（不同类型模型的精度单位不同，如：分类模型精度为 ACC，检测模型精度为 mAP 等），尝试多种不同的选择，生成多个点。

2）以精度为纵轴，以 fps 为横轴的坐标系下，选择最优的 FPS 点形成的包络线，最优 FPS 点选取规则：以最高精度点为起点，沿纵轴递减方向，第一个 FPS 大于当前 FPS 的点即为下一连接点

3）与纵轴围成的面积除以精度范围，即可得到该芯片的 MAPS 值，单位仍是 FPS，表示在此精度保障范围内的平均处理速度，其公式为 MAPS = 所围多边形面积 /（最高精度-最低精度）

5.4.2 功耗测试与能效比

（1）功耗测试

计算平台运行不同测试时功耗不同，所以需要对每一项算力测试的功耗分别进行测试，功耗测试采用功率分析仪。计算平台进行测试过程中开启功率测试功能，同时连续采集一定数量的功耗数据并进行保存。

（2）能效比计算

能效比即算力能效比，定义为计算平台最大算力与功耗比值，其单位为 TOPS/W，在利用 MAPS 评测方法时单位为 FPS/W。

5.4.3 计算性能评测方法

（1）单项指标

测试计算平台算力性能，与计算有关的考核指标主要有以下几点：

GPU 最大算力；GPU 最大算力功耗比；CPU 单核 CoreMark/Hz 指标；CPU 最大运行频率；CPU 内核数量；AI 算力 MAPS 值；内存/存储大小等。

以上几种指标绝对数值差异较大，无法将各方面性能做综合处理进行横向对比。

（2）综合评价举例

可以参考每个计算平台各项指标和成熟应用的 Jetson TX1 模块相应指标进行对比，将各项结果加权处理，以得到计算平台综合性能指标，用以评价计算平台的总体性能。

英伟达公司 2016 年发布的 Jetson TX1 是首款针对深度学习神经

网络设计的嵌入式超级计算平台，目前广泛应用于无人机、自主机器人系统、先进驾驶辅助系统（ADAS）、移动医学成像等领域。NVIDIA Jetson TX1 基于 Tegra® X1 处理器打造，采用和超级计算机完全相同的 Maxwell 架构 256 核心 GPU，可提供高达 1TFlops 的强大计算性能并完整支持 NVIDIA® CUDA®技术。参考官网数据，Jetson TX1 模块的参数信息见下表：

表 2 Jeston TX1 考核指标与权重表

项目	指标	比例（%）
GPU	矩阵卷积运算最大算力	45
	矩阵乘法最大算力	20
CPU	CoreMark/MHz	5
	最大运行频率	5
	内核数量	10
Memory	内存大小	10
能耗	最大算力功耗比	5

判定指标可分为四项：AI 能力、CPU 能力、内存大小和能效比。计算平台的 AI 性能主要由 GPU 提供，以算力优先的方式进行划分可分为：GPU 分配 65%权重，CPU 分配 20%权重，内存分配 10%权重，效能分配 5%权重，具体见下表。此处需要说明的是，后续随着不同种类的计算平台测试结果的积累，可以对各个权重进行调整，以适配市面上绝大多数计算平台，使评价结果更客观。

设定 Jetson TX1 计算平台为 100 分，其它计算平台逐项与 Jetson

TX1 进行对比，按照表 3 中的权重进行计算，将各项分相加可得到综合评分。以英伟达 Xavier 为例（指标是参考官方数据估值），计算见下表。其他计算平台采用此方法评价性能时，方法和步骤类似。

表 4 Xavier 评分表

项目	Jetson TX1	Xavier	权重	过程及得分
GPU	2TOP（INT8）	22TOPS（INT8）	0.45	$100\times(22\div2)\times0.45=495$
	60GFLOPS	140GFLOPS	0.2	$100\times(140\div60)\times0.2=46.7$
CPU	3.8	8	0.05	$100\times(8\div3.8)\times0.05=10.5$
	1730	2270	0.05	$100\times(2270\div1730)\times0.05=6.6$
	4	8	0.1	$100\times(8\div4)\times0.1=20$
Memory	4GB@64-bit	32GB@256-bit	0.1	$100\times(32\div4)\times0.1=80$
能效比	0.2 TOPS/W	0.5 TOPS/W	0.05	$100\times(0.5\div0.2)\times0.05=12.5$
总分	$495+46.7+10.5+6.6+20+80+12.5=671.3$			

6 车载计算平台标准化建议

6.1 车载计算平台信息安全标准化建议

车载计算平台作为汽车自动驾驶过程中完成海量、多源数据处理的核心部件，承担着决策并完成相应的车身控制的重任，同时作为自动驾驶相关数据信息在云端、路端和车端交互的核心纽带，应用前景广阔，车载计算平台的信息安全问题不仅会造成传统的信息安

全威胁（诸如信息篡改、泄露），还会造成功能安全问题（由车载计算平台决策错误引发的非预期车控行为威胁驾乘人员的生命安全）。

此外，运行于车载计算平台上的AI应用是确保自动驾驶功能安全有效运行的决定性因素，也是车载计算平台区别于其他智能网联汽车部件的明显特征。因此，车载计算平台需要更高级别的信息安全防护，应针对车载计算平台制定专门的信息安全标准。

当前车载计算平台信息安全技术研究和开发水平上存在参差不齐的情况，通过车载计算平台相关标准工作，可提升行业的整体研究和开发能力。汽标委对于网关、车载信息交互系统、车载充电系统等关键部件/系统均已制定了单独的技术标准，但车载计算平台仍处于空白，直接导致厂商在定义安全需求或执行开发工作时缺乏相应标准的约束和指导。规范智能网联汽车车载计算平台的信息安全技术要求和试验方法，有利于保障车载计算平台的信息安全水平，同时降低自动驾驶汽车由于信息安全带来的功能安全威胁。

表 5 车载计算平台信息安全标准化建议

标准化对象	必要性	可行性	启动建议
硬件安全技术要求及测试方法	硬件具备防侧信道攻击、防物理攻击、防注入攻击； 支持芯片国密加密算法以及国密安全等级； 具备硬件高安全模块，并达到公认的安全等级（如国密认证、CC认证）；	体现了车载计算平台相比其他部件更高级别的安全防护要求，有标准化基础	建议启动
通信协议与接口安全技术要求及测试方法	计算平台与外部传感器（摄像头、Lidar、Radar、USS、GNSS）间进行身份认证，确保传感器身份的真实性，间接证明其客观上满足性能	体现了车载计算平台相比其他部件依赖更多信	建议启动

	要求，同时防止遭到中间人攻击； 传感器数据加密；	息源输入进行最终决策的特殊性，有标准化基础	
AI 安全技术要求及测试方法	AI 模型自身保护（AI 模型不被窃取，需要安全执行环境进行安全存储）； AI 冗余，部署多个模型，在信息安全导致单个模型出现错误时不影响智能驾驶最终决策，在遭受攻击时，降低系统全面被攻克的可能性，提升系统的健壮性； AI 隔离（不该用 AI 的时候不让用，不具备应用权限时不让用），AI 能力和 AI 能力之间也要隔离，只有经过授权认证的 AI 指令才能执行； AI 熔断，整车在 AI 控制下（L3~L5），发生异常时，能确保车回归到人工控制下； AI 检测，检测对抗样本、恶意数据、恶意调用	体现了车载计算平台相比于其他部件依赖 AI 实现安全自动驾驶功能的特殊性，有标准化基础	建议启动
操作系统安全技术要求及安全测试方法	操作系统高安模块安全等级应达 CC EAL5+； 高安隔离引擎，多域安全隔离； 应能支持 L2~L5 级智能驾驶安全要求；	车控操作系统已有信息安全标准化规划	建议启动，纳入车控操作系统标准体系
应用软件安全技术要求及安全测试方法	如对应用软件代码使用签名机制、为应用软件所分配的访问权限安全等；	突出车载计算平台对应用软件的安全要求	建议启动
数据安全技术要求及安全测试方法	考虑全生命周期下（采集、存储、传输、销毁等）数据的安全合规保护等	突出车载计算平台的对关键数据的	建议启动

		安全要求	

6.2 车载计算平台功能安全标准化建议

目前，车载计算平台的功能安全尚未形成行业共识。当前，功能安全在 ADAS 领域的实践已形成一定的共识，但主要由 Tier 1（汽车零部件一级供应商）巨头企业主导。而对于国内的整车企业、零部件供应商以及自动驾驶解决方案提供商，功能安全在 L3 及以上自动驾驶领域的具体实践仍在探索推进，行业共识尚未形成，影响了车载计算平台产品的功能安全开发及实车应用。基于 GB/T 34590 和 ISO 26262，对车载计算平台的功能安全进一步深化研究和探索实施，在实施方案固定、成熟后，以最佳实践等形式推出研究成果，可以加快行业共识的形成。建议推迟启动。

表 6 车载计算平台功能安全标准化建议

标准化对象	必要性	可行性	启动建议
车载计算平台功能安全基本要求及测试规范	明确关键模块的功能安全等级要求，规范软件单元测试验证、软件集成验证、嵌入式软件测试等方面工作	车载计算平台的功能安全具体实践仍在探索，行业共识未形成，暂不具备标准化基础	推迟启动

6.3 车载计算平台参考架构标准化建议

车载计算平台在产品形态、技术方案、功能要求等方面尚未收敛，相关企业的具体产品架构设计各有不同，且仍在不断迭代更新中。具体架构和技术方案标准化工作基础不足，建议推迟启动。

建议启动车载计算平台术语定义标准化工作，可纳入智能网联汽

车的整体术语和定义标准。

6.4 车载计算平台连接互通标准化建议

在第 5 章的研究分析中可以看出，目前车载计算平台的连接器、通信网络和逻辑接口已有相关标准，可以考虑在以下方面进行标准化：

1）针对高等级自动驾驶，多摄像头之间时间同步精确同步机制：当前摄像头图像时间戳是从 ISP 送入，SoC 中加入，存在一定延迟，当高帧率情况下建议摄像头数据中自带时间戳，涉及硬件、协议等细节标准化需求。

2）板级接口：参考 PCIe 等接口规范，建立车载计算平台的计算板卡标准化接口，其关系如同 PC 与 PCIe 卡的关系类似，从而使得车载计算平台算力可扩张，硬件可更新。

车载计算平台连接互通相关标准化建议如下表所示：

表 7 车载计算平台连接互通标准化建议

标准化对象	必要性	可行性	启动建议
多摄像头之间时间同步精确同步机制	多摄像头之间时间同步精确同步机制，当前摄像头图像时间戳是从 ISP 送入，SoC 中加入，存在一定延迟，当高帧率情况下建议摄像头数据中自带时间戳，涉及硬件、协议等细节标准化需求	与车载计算平台具体架构有关，由于架构未统一，暂不具备标准化基础	推迟启动
板级标准化接口	不同传感器（摄像头、Lidar/Radar 等）采用不同类接口（MIPI、以太网、CAN 等），对接口数量的要求、硬件配置仍在变化中	接口数量和配置未统一，暂不具备标准化基础	推迟启动

6.5 车载计算平台性能要求标准化建议

车载计算平台与PC计算架构有一定相似性，特征在于：1）异构；2）硬件模块化，可扩展；3）计算能力可配置。因此计算平台内根据使用场景和功能、安全、成本和装配等约束下，针对不同类别的计算功能模块、应用性能分别建立相应评测标准，来客观衡量该领域行业参与者的产品性能，横向对比，为Tier1、OEM提供可执行的性能测试方法，减少评测成本，加速量产落地。

表 8 车载计算平台性能要求标准化建议

标准化对象	必要性	可行性	启动建议
车载计算平台性能技术要求以及测试方法（如测试工具、设备等）	确定计算平台性能测试关键指标项（如算力芯片实际性能、时延、信号传输性能、数字信号准确率等），及相应测试工具、设备	需要在计算平台架构标准化基础上开展	推迟启动
计算平台AI算力实际性能评测方法	AI计算性能评估可采用独立于算法的算力评测方法，在芯片功耗可测前提下，也可以得出 MAPS/W 指标	需要在计算单元AI算力评测标准上开展	推迟启动
控制、通信性能评测方法	评估控制模块、各类通信接口模块实时性能	需要在计算平台架构标准化基础上开展	推迟启动
时延与同步性能评估方法	评估端到端时延与多传感器输入间同步性能的方法	需要在计算平台架构标准化基础上开展	推迟启动

6.6 车载计算平台标准化建议总结

综合本报告以上的标准化研究和标准化建议，优先启动车载计算平台的术语和定义、车载计算平台的信息安全标准化工作；推迟启动车载计算平台功能安全、性能要求、连接互通标准化工作。

综上所述，推荐启动《车载计算平台信息安全技术要求》标准立项，内容包含车载计算平台的术语和定义、硬件安全技术要求及测试方法、通信协议与接口安全技术要求及测试方法、AI 安全技术要求及测试方法、应用软件及数据安全技术要求及测试方法等。由于车载计算平台是智能网联汽车的关键部件，该标准也将构成智能网联汽车信息安全标准体系中的重要部分。