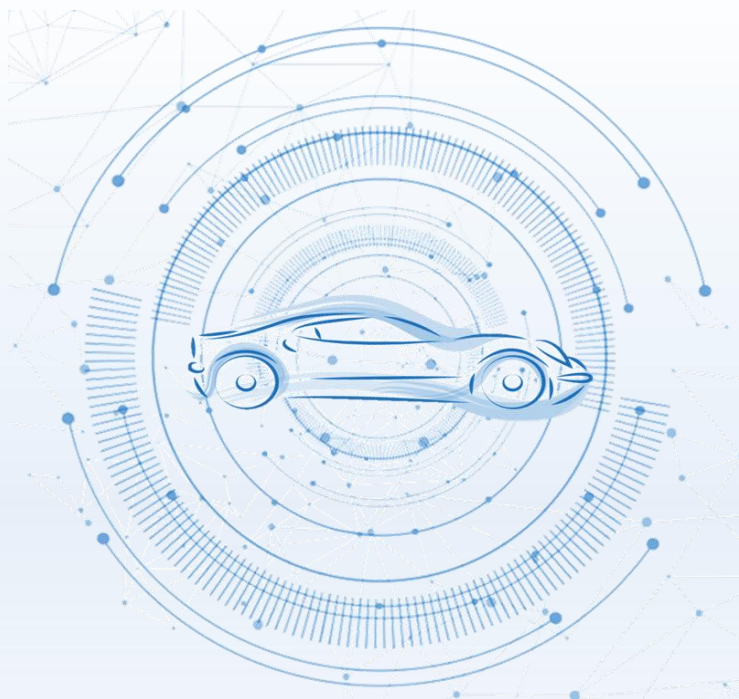


车用芯粒互联 (chiplet)

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

2025 年 12 月

前 言

随着汽车智能化、网联化的飞速发展，对电子架构也提出了更高要求。车用芯粒技术凭借其灵活集成、高效协同的优势，成为构建下一代汽车电子系统的关键技术。《车用芯粒互联（chiplet）标准化需求研究》由重庆长安汽车股份有限公司和中国汽车技术研究中心有限公司联合牵头开展，协同各相关方共同完成，内容涵盖接口与通信、环境与可靠性、电磁兼容、功能安全、信息安全、软件设计，是实现不同功能芯粒高效集成与协同工作的通用框架。

接口与通信方面是车用芯粒协同的“语言”，为满足车用软件适配的效率与兼容性，驱动创新落地，规范了接口协议、异构芯粒高密度集成及封装等方面；为满足车用的安全可靠场景需求，针对湿度预处理、功能验证、温度适应性、机械应力测试、芯粒电磁干扰与抗扰度要求及测试、芯粒架构设计、通信机制、安全防护到供应链管理全生命周期安全保障体系以及安全运行环境等给出标准化建议。

本研究项目为车用芯粒技术的规模化、可靠应用提供了坚实的技术保障，使基于芯粒技术的功能能够灵活满足智能座舱、自动驾驶等多元化场景需求，是车用芯粒技术从实验室走向量产、赋能智能汽车创新发展的坚实基础。

衷心感谢参与研究报告编写的各单位和组织：重庆长安汽车股份有限公司、中国汽车技术研究中心有限公司、中汽研科技有限公司、深圳引望智能技术有限公司、北极雄芯信息科技（西安）有限公司、上海复旦微电子集团股份有限公司、黑芝麻智能科技有限公司、英纳法智联科技（北京）有限公司、北京国家新能源汽车技术创新中心有限公司、上海彼格镁隆技术有限公司、网络空间部队信息工程大学、上海泽丰半导体科技有限公司、中茵微电子（南京）有限公司、武汉大学、中国第一汽车股份有限公司、广州汽车集团股份有限公司、比亚迪汽车工业有限公司、中汽院（江苏）汽车工程研究院有限公司。

主要编写人：吴含冰、夏显召、关鹏辉、李雨冉、唐春华、李雪梅、黄美松、张浩岩、李予佳、赵瑞、翟瑞卿、孙宇豪、王华、付春晖、宋占坤、张武科、孟飞、李鑫、王立辉、黎仁峰、吕平、张霞、陈艇、张永刚、李原、尹鸿苇、杨光、

刘雄、邱静、陶克文、李齐、张颜洲、吴倩、王洪鹏、朱红卫、刘德启、郑怀、田宜东、朱航绪、张伟锋、林积涵、辛聪、黄春梅、安炫东、周昕、朱帅帅。

目 录

一、车用芯粒的研究背景	1
1.1 车载电子电气架构演进	1
1.1.1 电子电气架构概述	1
1.1.2 国内外汽车企业电子电气架构现状概述	2
1.1.3 汽车电子电气架构技术趋势	3
1.2 车用芯粒的概述	7
1.2.1 芯粒技术	8
1.2.2 车用芯粒技术	8
1.3 车用芯粒行业现状与趋势	9
1.3.1 车用芯粒现状	9
1.3.2 车用芯粒面临的挑战及发展趋势	10
1.4 车用芯粒相关标准现状	12
1.4.1 接口与通信标准现状	13
1.4.2 环境与可靠性标准现状	13
1.4.3 电磁兼容标准现状	13
1.4.4 功能安全标准现状	14
1.4.5 信息安全标准现状	14
1.4.6 软件设计标准现状	15
二、车用芯粒关键领域的特性分析	15
2.1 车用芯粒接口与通信特性分析	15
2.1.1 车用芯粒接口与通信关键技术	15
2.1.2 车用芯粒接口与通信的关键特性	19
2.1.3 车用芯粒接口与通信的技术挑战	21
2.2 车用芯粒环境与可靠性特性分析	24
2.2.1 环境适应性关键特性	24
2.2.2 可靠性关键特性	25
2.3 车用芯粒电磁兼容特性分析	29

2.3.1 单个芯粒和模块整体电磁兼容特性	29
2.3.2 电源完整性、信号完整性的与电磁发射协同管理	29
2.3.3 车用芯粒 EMC 认证的复杂性	31
2.4 车用芯粒功能安全特性分析	31
2.4.1 功能安全需求分析	32
2.4.2 安全机制要求	33
2.4.3 评估方法	36
2.5 车用芯粒信息安全特性分析	37
2.5.1 信息安全需求分析	38
2.5.2 信息安全需求与安全功能的映射关系	39
2.5.3 信息安全功能技术要求与试验方法	49
2.6 车用芯粒软件设计特性分析	53
2.6.1 芯粒互联类型	53
2.6.2 车用芯粒软件设计特殊特性	54
三、车用芯粒关键领域标准化需求	57
3.1 车用芯粒接口与通信标准化需求	58
3.1.1 通用互联标准难以适配车规场景	58
3.1.2 车用芯粒的特殊应用场景需求	60
3.1.3 车用芯粒接口与通信的核心标准需求	62
3.2 车用芯粒环境与可靠性标准化需求	64
3.3 车用芯粒电磁兼容标准化需求	64
3.4 车用芯粒功能安全标准化需求	65
3.5 车用芯粒信息安全标准化需求	68
3.6 车用芯粒软件设计标准化需求	70
3.6.1 软硬件接口寄存器访问标准化需求	70
3.6.2 软硬件接口中断标准化需求	71
3.6.3 操作系统抽象层标准化需求	72
3.6.4 运行多操作系统需求	73
四、车用芯粒标准化路线图建议	75

4.1 车用芯粒总体标准化路线图建议	75
4.2 关键分领域标准化路线图建议	76
4.2.1 车用芯粒接口与通信标准化建议	76
4.2.2 车用芯粒环境与可靠性标准化建议	78
4.2.3 车用芯粒电磁兼容标准化建议	80
4.2.4 车用芯粒功能安全标准化建议	81
4.2.5 车用芯粒信息安全标准化建议	82
4.2.6 车用芯粒软件设计标准化建议	82
参考文献	84

一、车用芯粒的研究背景

1.1 车载电子电气架构演进

1.1.1 电子电气架构概述

随着汽车行业向智能网联方向的飞速发展，电动化、网联化、智能化、共享化的趋势愈发显著，这对汽车电子电气架构（EEA，Electronic/Electrical Architecture）的技术演进和变革提出前所未有的创新要求。在此背景下，汽车电子电气架构技术正朝着“软件定义汽车”的方向不断演绎和进化。博世将整车 EEA 划分为六个阶段：模块化、功能集成化、功能域控化、域融合化、中央集中化、中央集中及信息化，并将六个阶段对应的 EEA 分为分布式 EE 架构、域集中式 EE 架构和中央集中式 EE 架构，如图 1.1.1 所示。这一演进路径清晰地表明，未来汽车电子电气架构的算力会逐渐集中化，最终将发展到云端计算。当下，主流架构处于功能域控制器域融合化阶段，并正朝着中央集中式架构迈进。

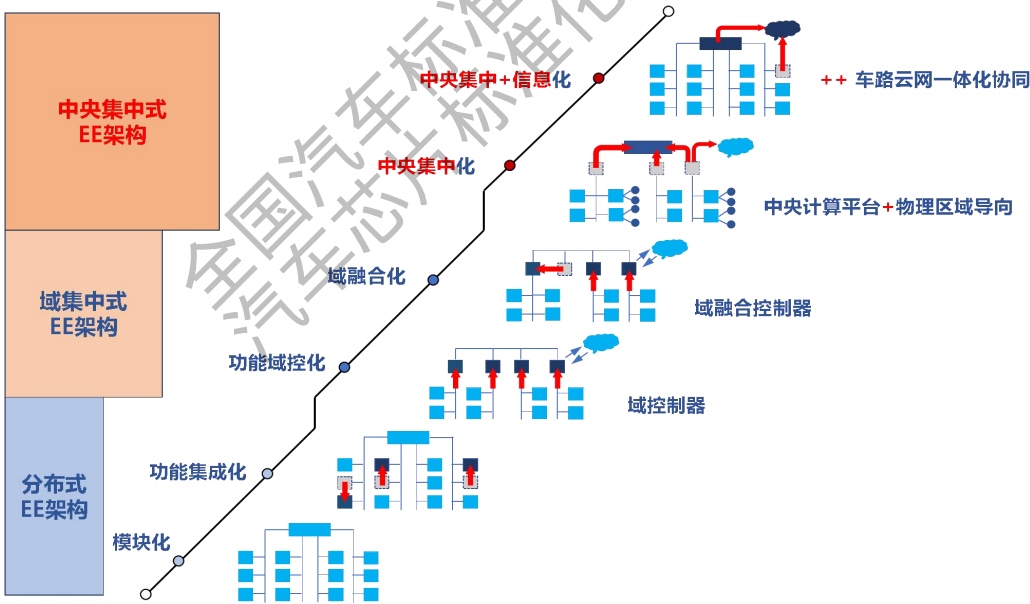


图 1.1.1 汽车 EEA 发展路线[1]

处于功能域控制器域融合化阶段的智能网联汽车新型电子电气架构，本质是为车端构建分布式面向服务的计算平台，旨在打造适配多域融合的总体系统架构，涵盖软件、硬件和通信架构三大关键部分。该新型架构以软件为核心，采用面向服务架构（SOA，Service-Oriented Architecture）。在软件架构层面，SOA 作为

车端软件系统架构风格，通过服务化封装功能逻辑，即将各功能模块转化为独立的“服务单元”，再经服务组合实现软件集成。同时，借助软件的集中化、一体化、横向化和敏捷化管理，降低软件开发成本，增强软件架构的可组合扩展性，助力智能网联汽车场景应用快速迭代更新。在硬件架构层面，新型架构依托域控制器、区域控制器和中央计算平台等高算力平台。这些平台在提升算力的同时，实现硬件平台的集成化、通用化与标准化，为软件服务的灵活部署与稳定运行提供坚实物理基础。

1.1.2 国内外汽车企业电子电气架构现状概述

在汽车产业变革的浪潮中，电子电气架构（EEA）已成为核心竞争要素，国内外相关企业纷纷布局，展现出各具特色的发展态势。

国外领先车企已全面完成从分布式向集中式电子电气架构的转型，头部企业进入“中央计算+区域控制”高阶阶段：通过域控制器实现硬件高度集成，以太网主干网支撑高带宽数据传输，并标配全域 OTA 能力，奠定软件定义汽车基础。国内车企主力处于分布式向域集中式过渡期，新势力探索域融合方案，传统车企多采用“中央网关+功能域控制器”架构（划分动力/底盘/座舱等核心域），但在软件平台复用率、车规芯片生态等基础领域与国际水平存在差距。

当前国内外汽车电子电气架构（EEA）正沿着三大技术方向快速演进：在硬件集中化方面，跨域融合趋势推动中央计算平台实现算力动态调度，配合区域控制器就近管理执行器，大幅缩减整车线束长度，降低成本；通信高效化表现为千兆以太网成为主干网络，时间敏感网络（TSN）确保实时性要求，结合 CAN FD/LIN 构成的混合通信架构满足不同场景需求；软件服务化则通过分层设计深化软硬件解耦，同时行业正在探索高/低安全等级任务的物理隔离方案，以应对架构集中化带来的潜在风险。这一系列技术演进共同推动着汽车电子电气架构向更高效、更智能的方向发展。

为突破自主可控生态瓶颈，我国汽车产业亟需构建“芯片-工具链-标准”三位一体的协同创新体系：重点突破车规级 SoC 芯片的自主研发与产业生态建设，加快推进仿真测试工具链的国产化替代进程，同时积极参与并主导车载通信协议（如 TSN、CANXL 等）的国际标准制定，通过这一系统性突破路径，为中央计

算架构下的高阶辅助驾驶技术落地和个性化服务创新提供坚实的技术支撑和产业化保障

1.1.3 汽车电子电气架构技术趋势

(1) 分布式 EEA

传统分布式电子电气架构中，数十个 ECU 各自独立运行，功能固化且软硬件耦合紧密，导致系统扩展性差、开发效率低。每个 ECU 通常仅控制单一功能单元（如发动机、刹车或车门），通过 CAN 或 LIN 总线连接交换信息。然而，随着车辆搭载的 ECU 数量增加，线束长度和重量也随之增长，不仅推高整车成本，还降低组装自动化水平。此外，由于各 ECU 来自不同供应商，嵌入式软件和底层代码各异，软件生态复杂，系统兼容性和扩展性不足，主机厂严重依赖供应商，难以实现自主维护和 OTA 升级。

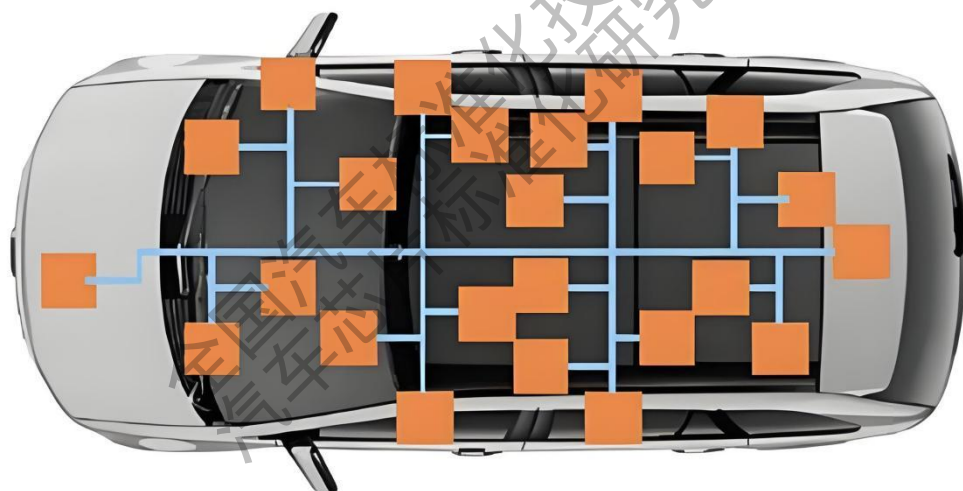


图 1.1.2 分布式架构[3]

驾驶智能化系统、智能座舱和车联网的快速发展对汽车计算能力提出更高要求。例如，L3 级别及以上的辅助驾驶需要实时融合摄像头、雷达和激光雷达等多传感器数据，并运行复杂的 AI 推理模型，这对算力和通信带宽提出严峻挑战。传统分布式架构的分散式算力布局和低速总线（如 FlexRay、LIN 和 CAN）已无法满足高带宽、低延迟的数据传输需求。同时，车辆传感器数量的增加使数据处理的实时性要求呈指数级增长，进一步暴露分布式架构的局限性。要实现 OTA

和“软件定义汽车”，必须解耦软硬件，推动电子电气架构向集中化方向演进，以适应未来汽车智能化的需求。

（2）域集中式 EEA

域集中式电子电气架构通过功能域重构解决传统分布式架构的算力分散、通信瓶颈及软硬件耦合问题。典型方案将系统划分为动力域、底盘域、车身域、座舱域及辅助驾驶域，各域控制器通过以太网骨干网与 CAN-FD 混合组网实现跨域通信。其中，座舱域与辅助驾驶域需支撑处理多模态数据融合的算力，而动力/底盘域侧重微秒级实时控制，算力需求相对较低。

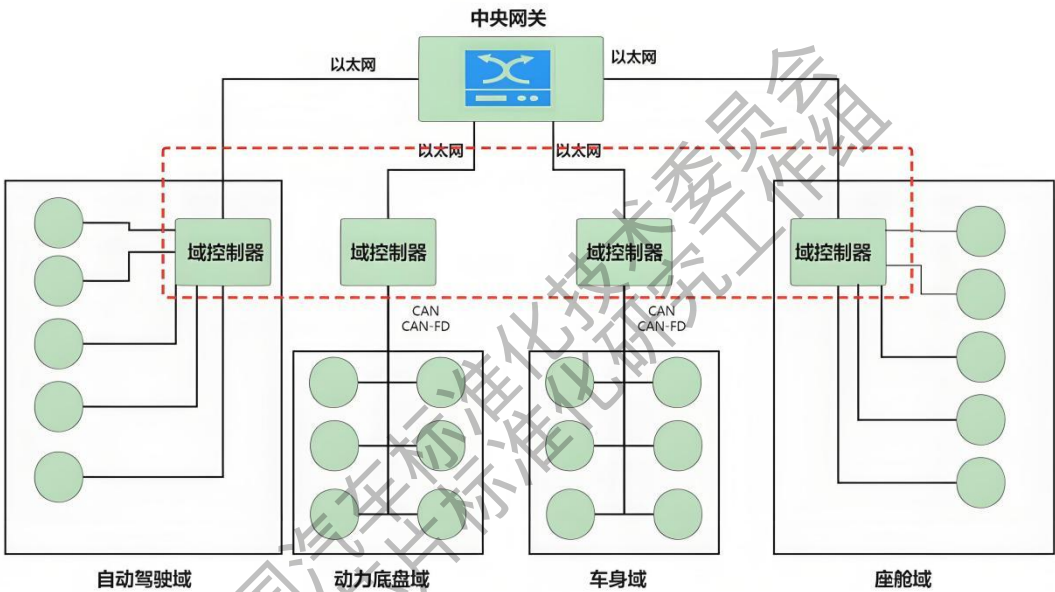


图 1.1.3 域集中式架构[2]

域控制器（DCU，Domain Control Unit）作为架构核心(应遵循 GB/T 34590《道路车辆 功能安全》系列标准进行设计开发)，采用多核异构计算架构（如 ARM Cortex-A+R 核），集成 AutoSAR CP/AP 混合中间件，实现从传统 ECU 的信号驱动到服务化架构（SOA）的转型。其优势体现在三方面：一是通过以太网替代传统 CAN 总线，通信带宽大幅提升；二是硬件抽象层（HAL，Hardware Abstraction Layer）标准化 I/O 接口，大幅缩短软件迭代周期（应符合 GB/T 36460《道路车辆 电气及电子设备的软件架构》对软件分层设计和接口标准化的要求）；三是支持整车级 OTA 并行刷写，升级效率，较分布式架构效率较为明显提升。

跨域融合阶段通过功能逻辑聚合进一步优化架构：将动力域、底盘域、车身域整合为车辆控制域（VDC，Vehicle Control Domain），基于 Adaptive AUTOSAR

实现扭矩分配与热管理协同；同时，座舱域与辅助驾驶域融合形成智能交互域（IVI-ADAS），通过算力共享与数据协同提升系统集成度（设计过程应严格遵循 GB/T 34590 系列标准中关于系统功能安全的要求）。

在域集中式电子电气架构（EEA）中，异构、高集成度的系统级芯片（SoC）扮演着至关重要的角色。这种架构通过功能域重构解决传统分布式架构中的算力分散、通信瓶颈及软硬件耦合的问题。在适用范围方面，高性能计算适用于座舱域和辅助驾驶域，这些领域需要强大的 AI 处理能力和高速的数据传输能力。对于动力域和底盘域，虽然不需要极高的算力，但需要快速响应的实时控制系统，这通常由专门设计的 MCU 或 DSP 核心完成。因此，在未来的跨域融合阶段，可能需要一种能够同时满足不同类型任务需求的异构 SoC，它不仅能提供足够的计算资源，还能确保低延迟的实时操作。从性能与成本的角度考虑，为了满足高算力需求，SoC 应具备多核异构计算架构，如结合 ARM Cortex-A 系列用于通用计算和 Cortex-R 系列用于实时控制。此外，还需集成高效的 AI 加速器，如 NPU 或 GPU，以应对机器学习任务。尽管高性能 SoC 的研发和制造成本较高，但由于其高度集成化的特点，可以减少外部组件的数量，降低整个系统的复杂性和成本。通过模块化设计和 IP 复用，可以在一定程度上控制研发成本，这对于推动汽车产业向更加智能化、网络化方向发展具有重要意义。

域集中式电子电气架构通过功能域划分和跨域融合，显著提升汽车系统的性能和可扩展性，同时简化系统的复杂性和成本。其发展趋势是从分散的 ECU 向少数强大的 DCU 过渡，并进一步向中央计算平台发展。

（3）中央集中式 EEA

中央集中式电子电气架构的发展聚焦于功能域深度整合与位置域优化布局，推动其向通用计算平台演进。功能域融合促使传统架构升级为通用计算平台，并延伸至位置域（如中域、左域、右域）。区域控制器平台（ZCU, Zonal Control Unit）作为局部核心（需符合 GB/T 34590《道路车辆 功能安全》系列标准 ASIL-D 的要求），负责特定区域内传感器、执行器及 ECU 的连接、初步数据处理与网络协议转换，优化线束配置，降低成本，减少通信接口，提升组装效率并简化系统复杂性。

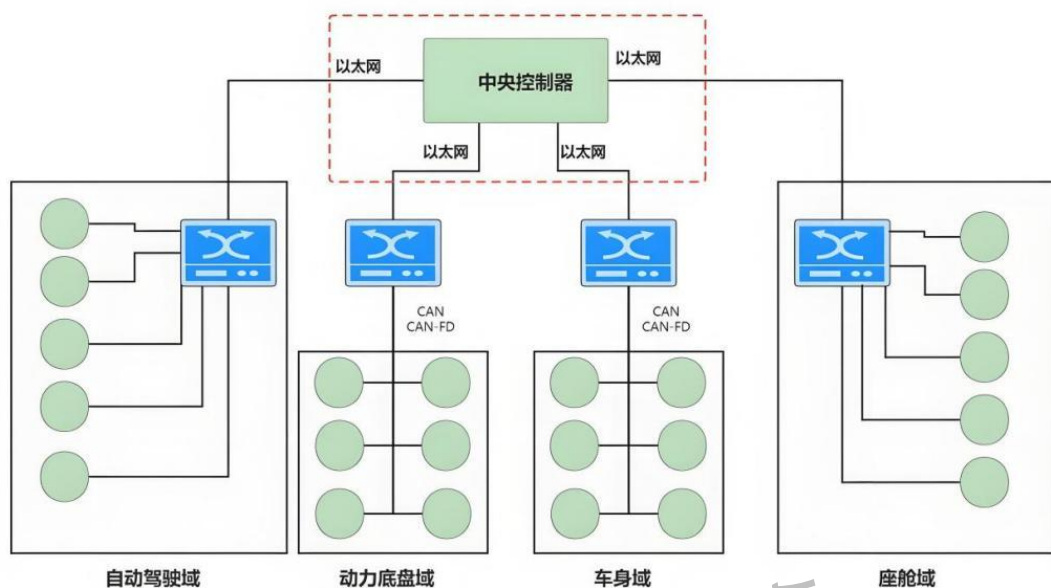


图 1.1.4 中央集中式架构[2]

各节点通过 ZCU 将原始数据传输至中央计算平台（CCP, Central Computing Platform）处理，所有数据决策在 CCP 完成，保障整车架构稳定性与功能扩展性。新增部件可经区域网关接入，硬件支持算力升级，为软件迭代提供支撑。为降低连接复杂度、提升算力利用率、降本增效并增强安全性，中央集中式架构将多个域控制器（DCU）融合为多核异构 SoC 芯片与多操作系统组合的 CCP，传感器与执行器按物理位置就近接入 ZCU，进一步简化连接（GB/T 34987《汽车电子控制单元（ECU）芯片技术要求》对 SoC 的基础性能、接口规范及环境适应性等进行规范）。

汽车云计算阶段，部分功能上云，车内架构再度简化，传感器与执行器可通过软件定义控制，零部件趋于标准化，实现“软件定义汽车”。此架构简化车内结构，提升算力利用率，降低成本并增强安全性。中央集中式 EE 架构通过功能域与位置域优化，推动通用计算平台发展，ZCU 简化硬件管理，CCP 保障稳定扩展，云计算助力架构简化，为智能汽车发展奠定坚实基础（GB/T 34986《信息安全技术 汽车电子系统网络安全指南》对数据在传输与存储过程中的机密性、完整性和可用性等规范）。

中央集中式电子电气架构（EEA）通过功能域深度整合与位置域优化布局，驱动车载计算系统向通用计算平台（CCP）演进，其核心依托于异构高集成度 SoC 技术。中央计算平台（CCP）需满足跨域融合与超异构算力需求，采用 CPU+GPU+NPU+DSP 多核架构，通过芯粒模块化设计实现算力弹性扩展；区域

控制器（ZCU）侧重低时延协议转换与多接口集成，基于 RISC-V+MCU+轻量化 NPU 架构，平衡实时数据处理与能效优化；云端协同层则通过 AI 加速器与硬件级安全模块，实现动态算力卸载与端云协同推理。关键技术匹配聚焦三大维度：算力分层（CCP 跨域整合/ZCU 边缘处理）、通信接口及安全隔离。性能与成本平衡策略涵盖硬件资源复用、动态算力调度、混合工艺节点及开源生态，形成系统性能优化闭环。

1.2 车用芯粒的概述

当前汽车电子电气架构（EEA）正经历“功能域控化-跨域融合-中央计算”三阶段演进，核心趋势包括：算力资源池化（如 NVIDIA Thor 达 2000TOPS）、通信全以太网化（10Gbps TSN 部署率超 80%）及软件分层解耦（SOA 接口标准化率超 90%）。这一演进通过域控制器整合 ECU、跨域中间件解耦功能边界、多核 SoC 芯片实现动态算力分配，使线束成本大幅降低，推动架构从硬件驱动转向软件定义。电子控制单元（ECU）内的标准计算能力无法满足未来汽车中 ADAS、通信和娱乐功能带来的巨大工作负载，高性能计算成为应对这一挑战的关键。而单片集成电路设计因尺寸和复杂性限制，难以实现超级计算。芯粒设计通过异构集成和模块化方法，在不触及单芯片物理极限的情况下扩展晶体管和组件数量，为超级计算提供了解决方案。芯粒技术通过异构集成突破、可靠性升级和开发效率革命三大维度助力 EEA 发展，实现芯片整体算力提升与功耗降低的并行优化，大幅缩短新平台开发周期，并通过国产多制程芯粒的灵活组合构建自主可控供应链。

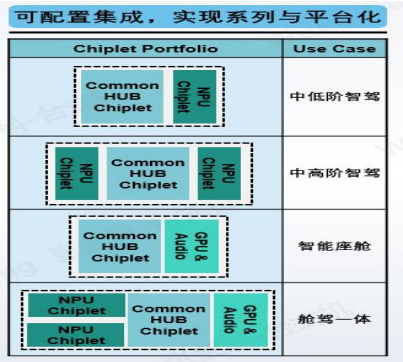


图 1.2.1 芯粒组合图

1.2.1 芯粒技术

芯粒（Chiplet，“小芯片”或“芯粒”）技术的兴起源于传统 SoC（系统级单芯片）设计的瓶颈与半导体产业对摩尔定律延续的迫切需求。随着芯片制程逼近物理极限（如 3nm 以下），单芯片设计面临性能提升趋缓、制造成本飙升及良率下降等挑战。芯粒技术通过将复杂功能分解为多个独立的裸片（Die），并采用异构集成技术，允许不同工艺节点的模块协同工作，从而突破单芯片的性能和成本限制。随着汽车行业向智能化、电动化和网联化快速迈进，对芯片的性能、功能以及可靠性等要求日益提高。芯粒技术作为一种有望突破传统芯片发展瓶颈的创新方式，在汽车领域正逐渐崭露头角，对汽车产业的变革起着至关重要的作用。

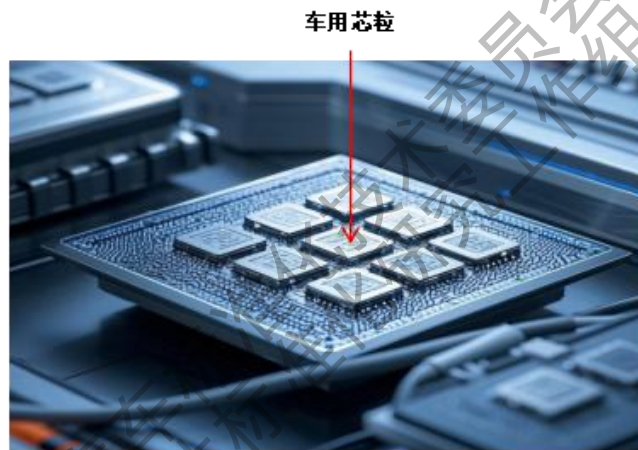


图 1.2.2 车用芯粒的示意图

1.2.2 车用芯粒技术

车用芯粒（Automobile Chiplet）属于芯粒这一概念在汽车行业的细分应用。车用芯粒是针对汽车使用场景及需求，经过特殊设计、制造与适配的芯粒。车用芯粒从最初的设计到上车应用涵盖接口与通信、环境与可靠性、电磁兼容、功能安全、信息安全、软件设计等各方面的设计、匹配与试验。车用芯粒在效率、成本和灵活性三个维度展现了显著优势。

在效率方面，通过将大芯片拆分为多个小芯粒，制造良率显著提高，传统大尺寸 SoC 因工艺缺陷导致的良率损失可能高达 50%，而采用小面积芯粒后，良率可提升至 90%以上，直接降低制造成本。

在成本控制方面，分模块的制造模式使得 CPU、GPU、存储、电源等每个

功能芯粒能采用不同的工艺进行大规模生产，例如将数字电路采用先进工艺，模拟电路采用成熟制程，显著降低单位成本。汽车厂商可以根据具体需求选择所需的功能模块，避免购买过于复杂或不必要的芯片组合，优化采购预算，减少资源浪费。

灵活性方面，芯粒构建了开放的模块化生态，企业可复用已验证的芯粒 IP（如内存控制器、PCIe 接口）。模块化设计使得汽车制造商可以快速构建定制化的芯片系统，满足从经济型家用车到高端智能汽车的多样化需求。

1.3 车用芯粒行业现状与趋势

1.3.1 车用芯粒现状

传统的芯片巨头如英特尔、AMD 等已经在芯粒技术研发上投入颇多。AMD 在第二代 EPYC 架构中将计算与 IO 部分拆分为不同的芯粒，并通过将不同数量的 CPU 计算芯粒组合出不同核数的服务器芯片，并尝试将相关成果向汽车领域拓展。Intel 将芯粒技术应用到 FPGA、CPU、GPU 等产品上。华为海思将 SoC 分解为 CPU 计算、I/O、AI 计算等芯粒，并组合出多种产品，如 AI 计算芯粒+计算/IO 芯粒组合出针对 AI 训练的芯片；计算所提出敏捷芯粒集成框架，可从芯粒库选出性能、面积、成本等指标的最优芯粒组合。随着汽车行业向智能化、电动化和网联化快速迈进，对芯片的性能、功能以及可靠性等要求日益提高。芯粒技术作为一种有望突破传统芯片发展瓶颈的创新方式，在汽车领域正逐渐崭露头角，对汽车产业的变革起着至关重要的作用。

在汽车领域，芯粒技术已开始尝试应用于多个关键系统。例如，在辅助驾驶计算平台中，通过将不同功能的芯粒集成，如处理图像识别的芯粒、负责决策运算的芯粒等，可以实现高性能计算能力的灵活组合，更好地应对复杂路况下的实时感知与决策需求。在智能座舱方面，芯粒可用于集成显示驱动、多媒体处理等功能，提升座舱交互体验的流畅性与丰富度。北极雄芯推出的启明 935A 系列芯片是全球首款基于芯粒异构集成范式的智能驾驶芯片，支持多芯粒互连（双芯粒方案带宽达 128GB/s），可灵活配置不同性能等级的 SoC。瑞萨的第五代 R-Car SoC 也采用芯粒技术，允许车企混合匹配自研 AI 加速器与第三方 IP，提升设计灵活

性。英特尔推出的开放式汽车芯粒平台支持第三方芯粒集成，目标覆盖智能座舱和智能驾驶场景。

1.3.2 车用芯粒面临的挑战及发展趋势

随着汽车智能化程度的不断加深，从 L2 级向 L3、L4 甚至 L5 级辅助驾驶的逐步演进，以及智能座舱功能的日益丰富，对高性能芯片的需求将呈指数级增长。芯粒技术凭借其在性能提升和成本控制上的显著优势，将在汽车芯片市场中占据越来越重要的份额。预计到 2030 年，全球汽车用芯粒市场规模将实现数倍乃至数十倍的增长，涵盖从豪华品牌到普通家用汽车等多个细分市场。除了目前在辅助驾驶计算平台和智能座舱的应用，汽车用芯粒还将拓展到车辆的动力系统、底盘控制系统等更多领域。在动力系统中，可用于优化电池管理、电机控制等功能，提高电动汽车的续航和动力性能；在底盘控制系统方面，能助力实现更精准的转向、制动等操作，提升车辆的操控安全性和舒适性。然而，芯粒在汽车领域的应用同样也面临着诸多挑战，同时也在孕育着新的发展趋势。

1、车用芯粒面临的挑战

可靠性与安全性挑战：汽车运行环境复杂多变，对芯片的可靠性要求极高。芯粒在长期震动、高低温等恶劣条件下的稳定性需要经过大量验证。而且汽车关乎驾乘人员生命安全，芯粒必须满足严苛的功能安全标准，当前在这方面的测试与认证体系还有待完善。例如，在极端高温环境下，芯粒的封装材料可能发生热膨胀，导致内部连接失效，影响芯片性能甚至引发安全问题。

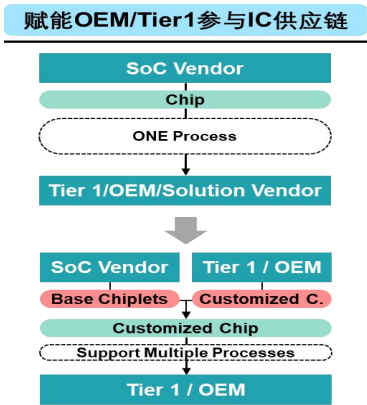


图 1.3.1 IC 供应链图

成本问题：芯粒的设计、制造以及集成封装都涉及复杂工艺，初期研发投入

大，导致成本居高不下，这在一定程度上限制了其在中低端汽车产品中的广泛应用。汽车市场对可靠性要求高且产量相对较低，同时先进节点的开发成本不断增加，导致汽车处理器供应商数量逐渐减少。为应对市场需求，这些供应商不得不采用“一刀切”的解决方案，覆盖多个细分市场。然而，当供应商数量减少到三家甚至更少时，供应链的脆弱性显然加剧。转向基于芯粒的处理器可能降低开发成本，从而吸引新的（尤其是小众）参与者进入市场，使行业更加多样化和具备弹性。但目前要实现这种混搭策略，行业需要在封装和互连技术上达成标准化，这仍需时间和努力。行业内，例如日本汽车、电气元件和半导体等 12 家公司（本田汽车公司（Honda Motor Co., Ltd.）、马自达汽车公司、日产汽车公司、斯巴鲁公司和丰田汽车公司；电气元件制造商：电装株式会社和松下汽车系统有限公司；以及半导体公司：Cadence Design Systems Japan、MIRISE Technologies Corporation、瑞萨电子公司、Socionext Inc.和新思科技日本（Synopsys Japan））于 12 月 1 日成立了“汽车先进 SoC 研究中心”（Advanced SoC Research for Automotive, ASRA），以研究和开发汽车用高性能数字半导体（芯片集成系统，SoC）。ASRA 将利用芯粒技术研发汽车 SoC，ASRA 的目标是到 2028 年建立车载芯粒技术，并从 2030 年开始在量产车中安装基于芯粒的 SoC。

行业标准缺失：虽说芯粒上车已经是一个必然的趋势，且芯粒已经悄然走入汽车市场，但目前车用芯粒缺乏统一的接口标准、通信协议等，这使得不同供应商的芯粒难以兼容，增加了汽车制造商在选择和集成芯粒时的难度，也不利于整个产业链的协同发展。

2、车用芯粒的发展趋势

技术突破推动性能升级：随着人工智能算法在汽车领域的广泛应用，对计算性能和能效的要求越来越高。存算一体芯粒将存储和计算功能集成在一起，可大幅减少数据传输延迟和功耗。存算一体芯粒将在车载实时语义分割、目标检测等任务中发挥重要作用，提升辅助驾驶系统的响应速度和准确性。在复杂路况下，能够更快速地识别行人、车辆等障碍物，为车辆决策提供更及时的信息。与此同时，为适应汽车极端运行环境，未来将引入冗余电路设计和自修复算法等容错机制，增强芯粒的抗辐射/抗电磁干扰能力。不断去探索和应用新材料和新工艺来提升芯粒的可靠性。采用新型封装材料，提高芯粒的耐高温、耐湿、耐振动性能；

采用先进的制程工艺，减小芯片尺寸，降低功耗和发热。

场景深化驱动芯粒功能融合跃迁：随着汽车智能化场景的持续细化，车用芯粒将加速向“场景定制化”与“功能一体化”演进。在辅助驾驶场景中，芯粒将集成多模态感知（视觉、雷达、激光雷达）与实时决策算法，形成“感知-融合-决策”的专用计算模组，提升变道决策的精准性。在智能座舱领域，芯粒将融合语音交互、手势识别、全息投影等功能，打造“多模态交互-个性化服务-情感化反馈”的沉浸式体验。此外，在动力与底盘控制场景中，芯粒将实现“电池管理-电机控制-线控底盘”的跨域协同，通过芯粒集成高精度传感器与 AI 算法实时优化电池充放电策略并联动底盘悬挂系统，同步调整悬挂刚度以提升操控稳定性，推动汽车从“功能集成”向“场景共生”的范式升级。

标准化与生态建设促进产业协同：为解决车用芯粒行业标准缺失的问题，芯片设计公司、代工厂、汽车制造商以及相关的行业组织等将加强合作，共同制定统一的汽车用芯粒行业标准，包括物理接口、电气规范、通信协议等方面，促进产业链上下游的顺畅对接。汽车制造商可以更便捷地采购和集成不同供应商的芯粒，而芯片企业也能更精准地根据市场需求进行研发和生产，提高整个产业的效率和竞争力。另外，借鉴开源软件的成功经验，未来车用芯粒领域也可能出现开源的芯粒设计平台和 IP 库。汽车制造商、芯片企业和科研机构可以共同参与开源生态的建设，共享芯粒设计资源和经验，降低芯粒设计的门槛和成本，推动汽车产业的智能化升级。

1.4 车用芯粒相关标准现状

标准化的车用芯粒有助于推进其在汽车上的广泛应用和更新迭代，利于汽车芯片行业的快速、高质量进步，支撑和保障汽车产业的可持续发展。依据关键的功能特性将车用芯粒的标准细分为七大类别，具体为接口与通信、环境与可靠性、电磁兼容、功能安全、信息安全、软件设计等相关标准，目前国内外的工业界、学术界、科研院所等相关机构针对芯粒的六大类标准已经开展或正在开展相应的标准制定与规划。

1.4.1 接口与通信标准现状

统一的接口标准可确保不同厂商生产的芯粒能无缝对接，避免兼容性问题，提高芯粒组合的灵活性。

目前国内外的芯粒互联接口规范协议有很多。从互联开放性角度，芯粒分为同厂芯粒和异厂芯粒。同厂芯粒通常采用企业自有协议，例如 AMD 的 Infinity Fabric，Intel 的 AIB、UPI 和 CXL 协议。异厂芯粒则需行业统一标准，国外以 UCIe 联盟为主，其成员包括英特尔、AMD、台积电、三星、日月光等，发布了 UCIe 2.0 版本规范，支持 3D 封装接口，但尚未大规模商用。同时，中国芯粒产业联盟发布《芯粒互联接口标准》ACC1.0，提供了面向车规的技术要求；中国电子科技集团公司等起草《芯粒间互联通信协议》，规定了互联通信的总体架构和技术要求。

1.4.2 环境与可靠性标准现状

车用芯粒在设计和封装上充分考虑了汽车应用场景中复杂且严酷的环境要求，从而确保其在极端条件下的稳定运行和高可靠性。

在可靠性方面，国际上 ISO16570 系列标准为专门针对道路车辆-电气电子设备环境条件及测试的标准。对芯片的可靠性进行评估和验证方面，通常遵循 AEC-Q100 等系列标准。该标准规定了芯片在严苛的汽车环境（如高温、低温、振动、湿度等）下必须满足的测试要求，以确保其长期稳定性与可靠性。AEC-Q100 覆盖环境应力测试、寿命加速测试、机械应力测试、电气特性测试等多个评估维度，并根据工作温度范围划分不同等级，其中 Grade 1（-40°C 至+125°C）是主流车规芯片的基本要求。而目前还没有出台专门针对车用芯粒的环境与可靠性标准法规。

1.4.3 电磁兼容标准现状

车用芯粒在设计、封装、材料选择和系统集成等方面均考虑了电磁兼容性要求，通过严格的标准认证，车用芯粒能够在复杂的电磁环境中确保汽车电子系统

的整体性能和安全性。

国际电工委员会（IEC）制定了一系列电磁兼容标准，如 IEC 61967 等，为车用芯片的电磁兼容性测试提供了标准依据。ISO/TC22/SC32/WG3 EMC 工作组组织制定了整车和零部件 EMC 基础试验方法，如 ISO11451 系列、ISO11452 系列等，为汽车芯片的电磁兼容测试提供了方法和依据。国内也在同步转化国际标准，如将 ISO 标准转化为 GB/T 标准，包括 GB/T33012 系列、GB/T33014 系列等。目前缺乏完善的专门针对芯粒的电磁兼容标准，对于车用芯粒的电磁兼容标准来说，可能会参考汽车行业常用的芯片电磁兼容测试方法，如采用 TEM 小室法、IC 带状线法、 $1\Omega/150\Omega$ 直接耦合法及射频功率直接注入法等进行发射及抗扰测试，实现各芯粒之间互相兼容的基本要求。

1.4.4 功能安全标准现状

功能安全是指系统在所有可能的操作条件下都能按预期正常工作，不会因硬件或软件故障而导致危险情况。对于车用芯粒来说，功能安全要求芯粒在设计、制造和运行过程中能够预测潜在的故障，并在发生故障时采取措施以进入功能安全状态，防止造成人身伤害。

ISO 26262 是国际上针对汽车电子电气系统功能安全标准，对芯片在汽车中的应用也提出了相应的功能安全要求，包括芯片的故障检测、诊断、容错等方面。对于车用芯粒来说，目前还没有出台专门针对车用芯粒的功能安全标准法规。

1.4.5 信息安全标准现状

车用芯粒的信息安全确保车用芯粒在处理、存储和传输信息时，其数据的机密性、完整性和可用性得到保障。

全国汽车标准化技术委员会智能网联汽车分技术委员会于 2022 年组织 30 余家行业骨干单位成立标准起草组，启动《汽车芯片信息安全技术规范》标准制定工作，2024 年 5 月至 6 月组织开展了首轮验证试验，聚焦汽车安全芯片和控制芯片两类芯片。对于车用芯粒来说，目前还没有出台专门针对车用芯粒的信息安全标准法规。

1.4.6 软件设计标准现状

车用芯粒的软件为编写的驱动程序、固件以及控制算法等可以充分发挥硬件性能，同时确保与车用电子系统组件的兼容性和协调工作。

目前软件设计方面主要是基于 AUTOSAR 等软件架构标准进行车载软件的设计和开发，AUTOSAR 提供标准化的软件架构和接口，方便不同供应商的软件和硬件进行集成和交互。国内企业、研究机构等在 AUTOSAR 标准的基础上，进行本地化的优化和改进，提高软件的适应性和可靠性。对于车用芯粒来说，目前还没有出台专门针对车用芯粒的软件设计标准法规。

总而言之，目前各家芯粒接口与通信的标准并不统一；而在芯粒的环境与可靠性、电磁兼容、功能安全、信息安全、软件设计等相关标准方面还在芯片层级阶段，还未深入下探到芯粒与车用芯粒层级。车用芯粒的关键领域标准需从车载应用场景出发，遵循车用接口标准、适配车载特殊工况等要求进行制定。

二、车用芯粒关键领域的特性分析

2.1 车用芯粒接口与通信特性分析

2.1.1 车用芯粒接口与通信关键技术

芯粒技术的核心在于通过高效互联接口实现多模块芯片的集成，其主流互联接口协议可分为差分串行和并行协议两类。

串行接口以 SerDes（串行器/解串器）为代表，适用于长距离传输，具有 I/O 数量少、抗干扰强，较强的传输可靠性的优势，同时理论单线传输速率能做到更高。针对芯粒短距传输场景，XSR（极短距）和 USR（超短距）SerDes 进一步优化功耗与面积，例如 XSR SerDes 支持 100Gbps 速率，且无需复杂均衡算法，显著降低能耗。此类技术广泛应用于 PCI-E、以太网等场景，但需平衡带宽与成本。

并行接口以高带宽和低延迟为特点，利用 2.5D 封装等先进封装的工艺优势，在单线传输速率不高的情况下，通过增加传输线数达到较高的带宽，典型代表包

括：HBM（高带宽内存）提供 1024 位宽总线，带宽密度达 3TB/s 以上，广泛应用于 GPU 与 AI 芯片的存储集成；英特尔主导的开放标准 AIB（高级互连总线），支持 EMIB 等 2.5D 封装，适用于短距高密度连接，如 Stratix 10 FPGA710；由 ODSA 提出 BoW（Bunch of Wires），兼容有机基板封装，灵活性高，适合多厂商协作。

芯粒技术在协议兼容、信号增强、多场景适配等方面的核心突破支撑了其在数据中心、AI、内存 / IO 解耦等应用场景的落地，在以太网连接、内存扩展、AI 计算三大领域中得到了广泛的使用。对于车载系统，以太网 IO 芯粒侧重长距抗干扰、内存扩展芯粒聚焦宽温适配、AI 加速器芯粒强调低延迟，车载芯粒接口技术同样也需要下述高性能、高可靠性的要求：

1. 以太网 IO 芯粒：实现高可靠车载网络传输枢纽

主要承担车内跨域数据交互与芯粒间（D2D）通信，接口技术聚焦长距抗干扰与高带宽，通过自适应均衡器补偿 $\geq 35\text{dB}$ 通道损耗，配合超高标准可靠性 LDPC (Low Density Parity Check Codes, 低密度奇偶校验码) 前向纠错技术，将误码率控制在 $\leq 10^{-15}$ ，可抵御发动机点火等强电磁干扰（EMI），能效比 $\leq 5\text{pJ/bit}$ 。集成 MACsec(Media Access Control Security, 媒体访问控制安全) 加密引擎与 Root of Trust（信任根），支持封装前良率筛选的 KGD 测试与 PRBS 码型检测，满足车规级可靠性要求。

2. 内存扩展芯粒：内存解耦和高带宽存储协同核心

聚焦车载高容量内存扩展，接口技术以低延迟、宽温适配为核心，支持 LPDDR5X-8533/DDR5-6400 内存接口协议，单通道数据速率达 8533Mbps，通过嵌入式时钟（CK_t/CK_c 差分对）保障同步性，在 $-40\sim 125^{\circ}\text{C}$ 宽温环境下，依托 PVT（工艺电压温度）传感器实现 $\pm 0.1\text{V}$ 动态调压，确保信号完整性（眼图高度 $\geq 80\text{mV}@ \text{BER} < 10^{-16}$ ），还可以通过 I3C 监控总线（采样率 1kHz）实时监测链路信号衰减（精度 $\pm 0.5\text{dB}$ ），当温度 $> 105^{\circ}\text{C}$ 时自动降速至 6400Mbps，实现全生命周期可靠性的智能管控。

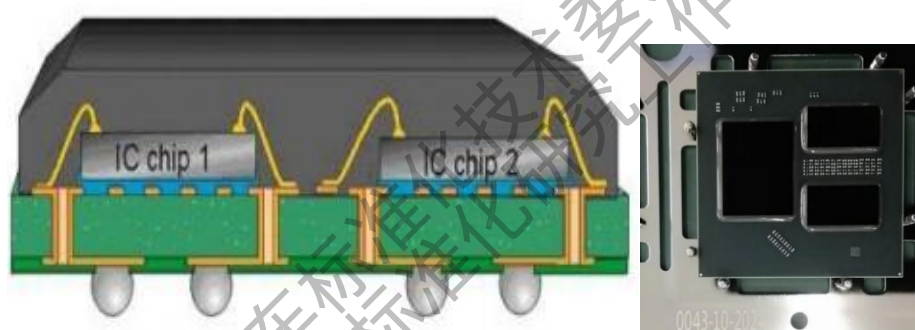
3. AI 加速器芯粒：IO 解耦和低延迟算力协同枢纽

为辅助驾驶 AI 推理提供算力支撑和辅助驾驶传感器网络的使用，接口技术以低延迟、高扩展为核心。Mesh 网络互联，环形网格采用 8x8 2D Torus 拓扑结

构，单链路速率 112Gbps NRZ（可选 224G PAM-4），通过自适应 XY 维度路由与 4 级 QoS (Quality of Service, 服务质量)保障低延迟传输，支持故障快速切换（ $\leq 200\mu\text{s}$ ），提升算力连续性。 JTAG 1149.1 和 IEEE 1687 IJTAG 的单芯粒边界扫描，多芯粒眼图测试（PRBS31 码型和误码注入）通道覆盖率 100%，确保量产可靠性。

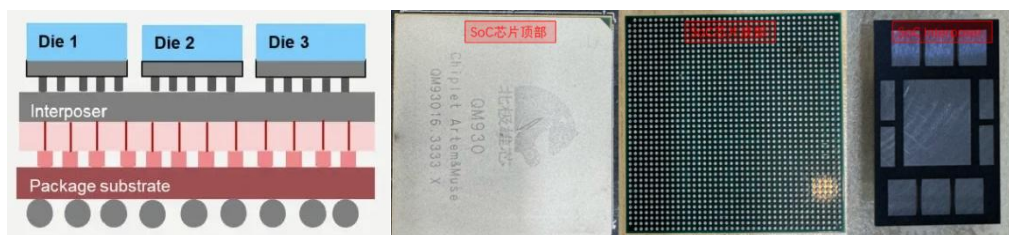
从封装层次来看芯粒技术也可分为如下关键技术路线。

MCM(Multi-Chip Module)是一种将多个未封装的裸芯片集成在共用基板上，通过高密度互连实现芯片间直接通信的先进封装技术。它突破了传统单芯片封装（SCP）的物理限制，属于混合集成组件的范畴，广泛应用于高性能计算、通信和微型化电子设备中。如下图 2.1.1 是基于 MCM 封装的 SoC 芯片，多个 die 通过基板直接封装到一起，各个 die 之间通过差分串行的 D2D 接口相连。



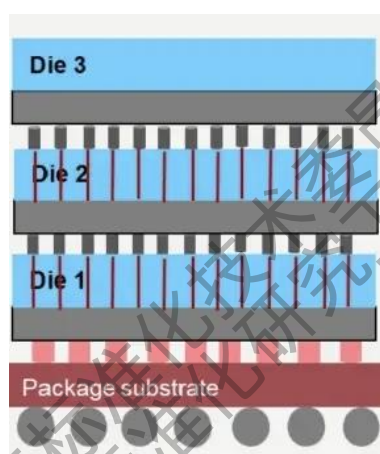
2.1.1 MCM 封装剖面示意图和基于 MCM 封装的芯粒芯片

2.5D 封装技术是一种介于传统 2D 平面封装和 3D 堆叠封装之间的先进半导体封装方案，其核心在于通过硅中介层（Silicon Interposer）实现多个裸芯片（Bare Die）的高密度互连。在 2.5D 封装中，多个裸芯片（如 CPU、GPU、HBM 存储器）并排安装在硅中介层上，而非直接堆叠。芯片与中介层通过微凸块（Micro Bump）或铜柱（Cu Pillar）连接，中介层再通过焊球与 PCB 基板相连。如下图所示 2.1.2 是基于 2.5D 封装的芯粒 SoC 芯片，多个 die 通过 interposer 层相连，最后将互联后的 interposer 封装于基板之上。个 die 之间基于 D2D 接口通过 interposer 相连。



2.1.2 2.5D 封装剖面图和基于 2.5D 封装的芯粒芯片

3D 封装（3D Packaging）通过垂直堆叠多层芯片并利用硅通孔（TSV）实现芯片间直接互连，是突破传统平面集成极限的核心技术。其核心目标是最大化性能密度、缩短互连距离，并支持超异构集成。如下图 2.1.3 是车用芯粒 3D 封装示意图。



2.1.3 3D 封装剖面示意图

表 2.1.1 是封装对比表，从整体来看，MCM 技术路线工艺成熟度，可靠性以及成本均更有优势，但是从理论性能上限来讲，2.5D 以及 3D 封装形式的优势更为明显。

表 2.1.1 封装对比表

	MCM	2.5D	3D
工艺成熟度	High	Middle	Low
成本	Low	Middle	High
可靠性	High	Middle	Low
理论带宽上限	Low	Middle	High

2.1.2 车用芯粒接口与通信的关键特性

1、功能安全

在汽车电子领域，芯粒互联技术面临的核心挑战是满足严苛的功能安全要求。需严格遵循 ISO 26262 标准，覆盖从芯片架构到接口设计的全流程。首先，需根据应用场景定义 ASIL 等级，例如辅助驾驶域控制器需满足 ASIL-D 级要求。通过硬件冗余机制（如双通道校验）、故障注入测试及安全状态机设计，确保单点故障率（SPFM）和潜在故障率（LFM）达标。其次，在互联接口中嵌入 ECC（纠错码）校验、CRC（循环冗余校验）等实时错误检测模块，并设计独立的安全监控单元（Safety Monitor），实现通信异常的快速隔离与系统降级。此外，需与车规级 MCU、传感器等模块的安全认证流程对齐，确保跨芯片的故障传播路径被有效阻断，例如通过物理隔离或加密信道实现功能安全域划分。

2、车规级可靠性

可靠性设计则聚焦于物理层（PHY）的鲁棒性提升。首先，采用差分信号（如 LVDS 或 SerDes）降低共模噪声干扰，并通过阻抗匹配优化与眼图测试确保信号完整性。针对车载振动与温度冲击（-40°C~150°C），需通过电磁兼容（EMC）仿真优化布线拓扑，抑制串扰与反射。其次，在关键数据通道部署双环冗余或交叉备份链路，结合动态信道切换技术，确保单点失效时仍能维持通信连续性。最后，针对车用芯片 10-15 年的长寿命要求，需通过加速寿命试验（如 HTOL）验证金属互连层的电迁移耐受性，并采用自适应均衡技术补偿信号衰减。

3、异构集成灵活性

车用芯粒的异构集成灵活性是突破传统单芯片限制的关键，其核心价值在于通过模块化架构实现“定制化拼装”，满足汽车电子从经济车型到豪华智能座舱的多元需求，以及不同功能需求，或者新增功能或者需要对某个功能进行迭代升级时完成快速升级和迭代，具体体现为三大维度。

1) 多工艺节点混合集成：制程自由组合，逻辑计算芯粒（如 AI 加速器）采用先进制程，而模拟/RF 芯粒则采用成熟制程，优化成本与抗干扰性。

2) 场景化模块配置：车型弹性适配，根据车型定位，例如经济车型，高端智能车等等，针对不同定位的车型采用不同的芯粒搭配，功能动态扩展。

3) IP 核复用生态：车企可复用已验证芯粒，避免重复流片，同时不同芯粒

可以采用不同代工厂制造，规避地缘政治导致的供应链中断。

4、高带宽低延时

随着智能化时代的到来，车辆智能化时代也随之到来，每一辆车都是一台超级电脑，芯片规模越来越大，拆分为各个不同的芯粒，芯粒之间的数据传输带宽也需要足够大，以满足算力日益增长，功能日益增多的车载芯片需求，单个芯粒互联接口的带宽需要不低于 256Gb/s。同时当车载芯粒用于驾控或辅助驾驶场景时，对实时性要求剧增，从而对于芯粒之间的数据传输有了低传输延时的要求，D2D 接口端到端（例如 D2D 上层协议接口时 AXI，则一端的 D2D 接口的 AXI 接口到另一端 D2D 接口的 AXI 接口的延时为端到端延时）延时需要控制在纳秒级别。

5、功耗管理与热协同

车用芯粒互联技术的功耗管理与热协同系统需构建动态闭环控制体系，通过多层级传感网络与自适应算法实现芯片级到系统级的热-电联合优化。在底层传感层，每个互联 IP 内嵌分布式电压/温度（V/T）传感器阵列，以 100 μ s 级采样周期实时捕获 Die 间互连区域的关键参数：包括互连通道的供电电压波动（ $\pm 5\%$ 精度）、结温梯度（ $\pm 1^\circ\text{C}$ 精度）以及信号完整性相关的眼图张开度等指标。采集数据通过专用低延时传感器总线传输至中央热管理单元（TMU）。

在控制策略层，系统采用分层决策机制：首先基于 DVFS（动态电压频率调整）技术，根据工作负载实时调节 D2D 接口的驱动电压和传输速率，其次通过智能通道管理算法，对非关键数据传输 lane 实施时钟门控（Clock Gating）或深度休眠（Power Gating），同时结合 3D 封装热仿真模型，对热点区域执行跨 Die 的负载均衡调度，将结温梯度控制在 $15^\circ\text{C}/\text{mm}^2$ 以内。

6、成本与供应链韧性

对于车用场景来讲，在满足安全与可靠性，以及性能的基础上，需要考虑成本与供应链韧性，例如如果采用先进封装的芯粒技术路线，对先进封装工艺依赖，而 2.5D/3D 封装（如 CoWoS）成本占芯片总成本 30% 以上，且产能集中于台积电等厂商，供应链风险高，需探索低成本有机基板方案或国产替代工艺。多芯粒协同验证复杂度高，测试成本可能不降反升，需工具链支持虚拟化验证，降低物理样片依赖。

2.1.3 车用芯粒接口与通信的技术挑战

车用芯粒接口与通信技术正通过“协议标准化 + 性能差异化”双路径，支撑辅助驾驶、智能座舱等场景的高带宽、高可靠、低延迟需求，成为汽车电子架构升级的核心驱动力。同样，车用芯粒接口与通信技术也面临着技术挑战。

1、功能安全与可靠性挑战

车用芯粒互联在功能安全与可靠性保障方面面临多重挑战，核心在于如何满足汽车电子严苛的 ISO 26262 功能安全标准要求，同时应对复杂车载环境的长期稳定性需求。

功能安全挑战方面，芯粒异构集成架构的分布式特性显著增加了系统失效风险。多芯片间的高速互连需构建端到端的数据完整性保护机制，例如 ECC 纠错、CRC 校验等，以防范单粒子翻转或信号串扰引发的数据错误。此外，功能安全目标的分解需贯穿芯片间协同设计，例如关键控制模块需在多个芯粒中实现冗余校验，但冗余模块间的同步误差可能导致逻辑冲突。互连协议的安全状态切换机制设计尤为关键。

可靠性挑战则集中体现在物理环境适应性上。车载芯片需耐受 -40°C 至 150°C 的极端温度循环，互联接口的 TSV 硅通孔、微凸点等 3D 封装结构在热应力下易出现疲劳断裂。振动环境下微米级互连结构的机械稳定性直接影响信号完整性，需通过有限元仿真优化封装材料与结构。电磁兼容性方面，高速 SerDes 通道的串扰抑制需从芯片布局、屏蔽层设计到 PCB 阻抗匹配的全链路优化。长期可靠性还需考虑电迁移、应力迁移等失效机制，车载 15 年寿命要求对互联结构的耐久性提出更高标准。

系统级验证复杂度呈指数级增长。多供应商芯粒的兼容性测试需覆盖物理层、协议层、电源完整性的跨域协同，故障模式影响分析（FMEA）需建立跨芯片的故障传播模型。功能安全认证需要重构传统单芯片的验证方法论，开发针对互连失效的专用测试向量。此外，先进工艺节点的老化效应与芯粒异构封装的热耦合效应叠加，使得寿命预测模型的建立面临数据匮乏的困境。

解决这些挑战需要构建涵盖架构设计、材料工艺、测试验证的全链条技术体系，同时推动行业建立针对芯粒互联的车规级标准与认证流程。

2、复杂环境下的信号完整性挑战

车用芯粒互联在复杂环境下的信号完整性挑战，主要源于车载工况的高动态物理干扰与多物理场耦合效应，这对高速互连通道的设计与稳定性提出了严苛要求。

极端温度扰动直接影响信号传输质量。芯粒间采用 TSV 硅通孔、微凸点（ μ Bump）等高密度互连结构，不同材料（如铜凸点与有机基板）的热膨胀系数差异在 -40°C 至 150°C 的循环温变中易引发微米级形变，导致阻抗失配和信号反射。此外，温度梯度引发的时钟抖动可能破坏多芯粒间的时序同步。

机械振动与冲击对物理互连结构的稳定性构成威胁。车载环境下 10-2000Hz 的宽频振动可能引起微凸点焊盘微裂纹扩展，导致接触电阻增大甚至断路。3D 封装中堆叠芯粒的机械共振效应会加剧信号衰减，需通过有限元仿真优化封装结构与阻尼材料。

电磁兼容性问题在车用场景尤为突出。动力系统的高压逆变器、无线充电模块等产生的宽带电磁噪声（如数十 MHz 至 GHz 频段）可能通过辐射或传导耦合至芯粒互连线。

多物理场耦合效应进一步放大挑战。例如，电热耦合可能导致电源完整性（PI）恶化：大电流传输时的焦耳热引发互连电阻变化，通过 IR Drop 影响信号电平稳定性。同时，热-机械应力与电迁移（EM）的协同作用会加速互连金属的晶界空洞形成，造成渐进性信号劣化。

系统级设计复杂度剧增。多芯粒间的信号完整性需跨层级协同优化——从芯片端的均衡器（EQ）设计、封装端的传输线阻抗控制，到板级的去耦电容布局，均需建立多尺度仿真模型。例如，在辅助驾驶域控制器中，AI 芯粒与传感器接口芯粒的互连需同时满足低延迟与抗扰度要求，这对通道衰减（Insertion Loss）和回波损耗（Return Loss）提出矛盾性指标。

解决这些问题需构建覆盖材料、封装、电路、算法的全链路技术体系，同时推动车载芯粒互连的信号完整性标准与测试方法的制定，以应对汽车电子在复杂工况下的可靠性需求。

3、跨厂商生态协作与标准化进程挑战

随着汽车电子架构向域控制与中央计算模式演进，传统 SoC 方案面临算力密度、散热效率与迭代周期的多重挑战。芯粒技术通过模块化异构集成，为车载

芯片提供了突破物理极限的创新路径。但该技术在汽车领域的商业化落地，正经历着跨厂商生态协作与标准化进程的关键转折。

在产业协作层面，汽车行业正打破传统封闭供应链，构建新型合作范式。

标准化进程则聚焦三大核心维度：**1) 物理接口标准**，涵盖信号完整性、电磁兼容等车规级特殊要求，AEC（Automotive Electronics Council）汽车电子委员会正着手制定芯粒专项测试规范；**2) 互连协议标准**，包括支持确定性通信的 NoC 架构和低延迟缓存一致性协议；**3) 安全认证体系**，建立跨工艺节点的可信执行环境，ISO/SAE 21434 标准新增芯粒级网络安全认证流程。

当前发展仍面临车载环境适应性（-40°C~150°C 温域）、全生命周期可靠性（15 年质保）、多厂商责任界定等挑战。但行业共识正在形成：只有通过开放协作构建统一技术底座，才能实现车载算力的持续升级与成本优化。预计到 2026 年，基于标准化芯粒架构的域控制器将占高端车型 60% 以上市场份额，推动汽车电子研发周期缩短 40%，硬件升级成本降低 35%。这场由技术革新驱动的产业生态重构，正在重塑全球汽车半导体竞争格局。

4、其他车用芯粒互联接口与通信关键技术要求挑战

中国企业在车规级芯粒领域已实现突破，为国产芯片绕过先进制程限制提供路径。国际巨头如英特尔、AMD 加速布局开放式芯粒平台，而中国凭借新能源汽车市场优势，有望通过生态协同抢占技术高地而对于车用芯粒互联接口与通信有如下关键技术要求挑战。

高带宽：满足高速互联吞吐量需求。对于高性能计算场景，单个芯粒互联接口要求 256 Gbps 以上传输速率；

低时延：确保实时性和响应速度。端到端延时需要做到纳秒级别，如 UCIe 定义的从发送端的 FDI 接口到 PHY Main Band 接口，再从接收端的 PHY Main Band 接口到 FDI 接口的总延迟（TX+RX）小于等于 2ns，但不包括接口信号在有机衬底或 Interposer 上的布线延迟；

误码率：对于低速传输，误码率一般低于 1e-15；如表 2.1.2 不同功能安全对应不同级别的误码率要求。

表 2.1.2 误码率表

安全等级	BER 目标
ASIL_D	$\leq 10^{-18}$
ASIL_B/C	$\leq 10^{-16}$
ASIL_A	$\leq 10^{-15}$

纠错机制：提供错误检测机制和纠错机制（如 CRC、重传机制），并支持链路故障恢复和冗余设计；

可扩展性：允许动态调整带宽和链路配置；

功耗管理：提供低功耗设计方案以节省能耗；包括动态链路带宽调整、低功耗模式设计等；

协议兼容性：芯粒接口规范通常包括物理层、数据链路层和协议适配层，所支持的上层协议与所传输的业务类型有关。为保证扩展性和兼容性，通常接口规范会定义透传模式，支持用户自定义协议的传输；

安全性：支持数据加密和完整性验证，防止数据被篡改或窃取；支持身份验证和权限管理，防止未经授权的访问和攻击。芯粒互联通信的安全性可以通过上层协议设计来保证。

2.2 车用芯粒环境与可靠性特性分析

环境与可靠性是指产品在规定的条件下、在规定的时间内完成规定的功能的能力，在车用芯粒芯片制造、工程使用中具有重要的意义。

2.2.1 环境适应性关键特性

芯粒的环境与可靠性测试通过多维度验证体系，为产品质量、性能优化及市场竞争力提供了系统性保障。在质量保障方面，通过高温、高湿等极端条件模拟，快速筛选出早期失效产品并剔除缺陷，结合严格测试流程与制造控制标准，确保仅符合质量要求的芯片进入市场，显著降低故障率。寿命评估方面，采用温度循环测试、高温工作寿命测试（HTOL）等方法量化芯粒长期稳定性，结合功能测

试与动态测试验证其在真实场景下的信号处理能力，为寿命预测提供数据支撑。设计与工艺优化通过测试数据反哺改进，暴露材料、封装或电路设计的薄弱环节，同时借助 ESD 测试、机械冲击测试等完善制造流程，加速技术迭代。合规性方面，测试项目严格参照 IEC、军规等国际标准，确保产品通过汽车电子、医疗设备等领域的高门槛认证。成本控制上，早期缺陷筛查降低售后返修率，优化材料与设计延长芯片使用寿命，减少用户更换频率。环境适应性验证通过温度冲击、振动、湿度及噪声测试，确保芯片在航空航天、汽车等复杂场景下的稳定运行能力。最终，这些测试体系不仅强化了产品可靠性，更通过建立用户信任、构建差异化竞争优势，助力企业在半导体行业竞争中占据技术高地。

环境指系统、设备或产品在运行、储存或运输过程中所接触的外部条件总和。这些条件可能包括自然因素（如温度、湿度、气压、辐射、振动、腐蚀性气体等）和人为因素（如电磁干扰、机械冲击、电源波动、操作方式等），关键要素如下。

气候条件：高低温、湿度、气压、风雨、冰霜等；

机械条件：振动、冲击、摇摆、恒加速度、噪声等；

生物条件：霉菌、有害动物、海洋生物、昆虫等；

辐射条件：太阳辐射、电磁辐射、核辐射等；

化学活性物质：硫化氢、二氧化硫、盐雾等；

机械活性物质：沙尘、尘埃等。

2.2.2 可靠性关键特性

可靠性指系统、设备或产品在规定条件和规定时间内无故障完成规定功能的能力。它是衡量系统稳定性和耐久性的核心指标，常用以下参数量化。

（1）MTTF（平均故障间隔时间 Mean Time to Failure），主要用于不可修复的系统或组件。它表示设备或组件从开始运行到发生第一次故障所经历的平均时间。MTTF 用于评估产品的寿命，即在其无法修复的情况下，平均可以使用多长时间。常见应用包括灯泡、电子元件、设备上的零部件等。

$$MTTF = \sum T1/N$$

其中，T1 是每个系统或组件的连续运行时间，N 为样本数量（如系统或组件的数量）。

(2) 失效率 $\lambda(t)$: 产品在 t 时刻后的单位时间内, 失效的产品数相对于 t 时刻还在工作的产品数的百分比值, 称为产品的瞬时失效率 (instantaneous failure rate), 简称失效率。

$$\lambda(t) = \frac{\text{在时间 } (t, t + \Delta t) \text{ 内每单位时间失效的产品数}}{\text{在时刻 } t \text{ 仍正常工作的产品数}} = \frac{\Delta n(t)}{(N - n(t))\Delta t}$$

其中, $\Delta n(t)$ 为 t 时刻后 Δt 时间内的故障的产品故障数; Δt 为所取的时间间隔; $Ns(t)$ 为在 t 时刻没有发生故障的产品数。

(3) 可靠度 $R(t)$: 如表 2.2.1 为可靠度模型图, 产品在规定条件下使用时间 t 后, 还能完成规定功能的概率, 被定义为产品的“可靠度”(也称残存概率)。

$$R(t) = P(T > t); R(t) = [N - n(t)]/N$$

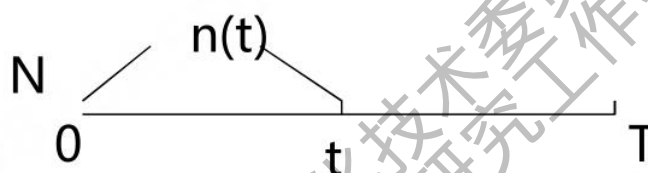


图 2.2.1 可靠度模型图

其中, N 为测试样品总数; $n(t)$ 为测试时间 t 后样品故障数。

(4) 寿命分布: 威布尔分布。

$$f(t) = m/t_0(t - \gamma)^{m-1} \exp[-(t - \gamma)^m/t_0]$$

其中, m 为形状参数, 表示函数的走势, $m > 1$, 表示失效率随时间增加, $m < 1$, 表示失效率随时间减小; t_0 为参数或特征寿命, 表示函数的缩放。 γ 为位置参数, 且 $\gamma > 0$; 表示设备在 $[0, \gamma]$ 之间不会发生故障。

威布尔分布之所以好用, 是因为通过调整不同参数, 可以表征整个产品生命周期, 即可靠性常提到的浴盆曲线, 分为早期失效、随机失效和老化失效三个阶段。如图 2.2.2 为失效率分布图。

形状参数 < 1 , 故障概率从无穷大呈指数递减, 等于浴盆曲线的早期失效期。

形状参数等于 1, 失效率随着时间的推移保持一致, 等于浴盆曲线的随机失效期。

形状参数在 1~2 之间, Weibull 分布迅速攀升到峰值, 然后随着时间的推移下降。失效率总体上是增加的, 最初增加得最快。此形状表示早期磨损失效。

形状参数等于 2，表示在产品的使用寿命内，磨损失效风险随着时间的推移不断增加。

形状参数在 3~4 之间，Weibull 分布就会变为对称的钟形，就像正态曲线一样。这种形式的 Weibull 分布对产品寿命的最后阶段（大多数失效发生在这一阶段）中的快速磨损失效进行建模。

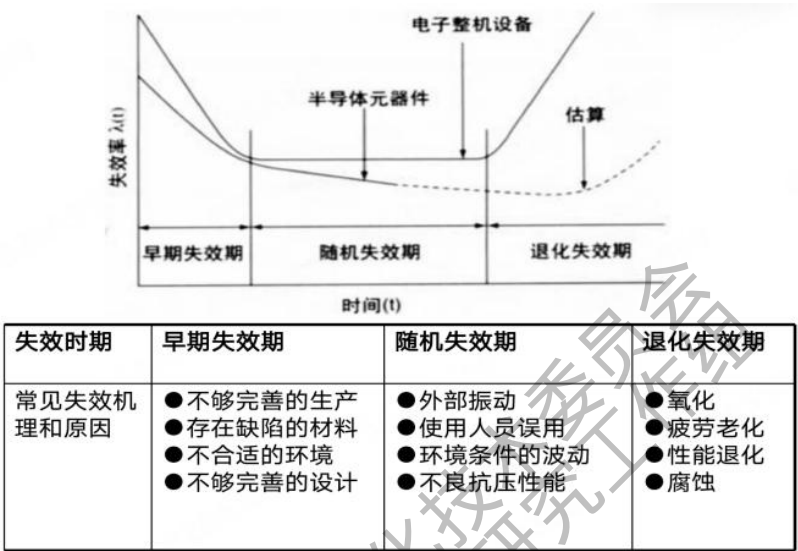


图 2.2.2 失效率分布图

（4）二项式分布模型

假设进行 n 次独立试验，每次试验成功概率为 R ，失败概率为 $1-R$ 。根据二项分布，获得 k 次成功的概率为：

$$P(k; n, R) = \binom{n}{k} R^k (1 - R)^{n-k}$$

置信度和样本量根据二项式分布计算公式，若要求以置信度 C 保证可靠度不低于 RL ，所需最小样本量 n 为：

$$n = \frac{\ln(1 - C)}{\ln RL}$$

（5）高温加速寿命试验（Arrhenius 阿伦尼斯模型）

Arrhenius 反映的是化学反应速率，因此最好应用于寿命变化与化学反应相关的产品中。同时，它在工程中通常运用于温度应力下的加速寿命试验模型中。如表 2.2.1 为不同故障机制的常用激活能量值图。

$$F = \frac{\partial P}{\partial t} = A e^{-\frac{E_a}{kT}}$$

$$AF = e^{-\frac{E_a}{k}(\frac{1}{T_0} - \frac{1}{T_1})}$$

其中，F 为反应速率，取倒数可作产品寿命的度量；P 为产品状态；t 为时间；A 为常数变量，大于 0；k 为玻尔兹曼常数，其值为 8.617385×10^{-5} ；T 为绝对温度，摄氏度+273；AF 为加速因子；T0 为产品所处的普通温度，通常为 25+273；T1 为测试条件下加速状态下的温度值，单位 K（开尔文）；Ea 为激活能，不同失效模式的激活能不同，芯粒建议使用 0.6~0.9eV。

表 2.2.1 不同故障机制的常用激活能量值

Failure Mechanism	Activation Energy, EA (eV)
Gate oxide defect	0.3-0.5
Bulk silicon defects	0.3-0.5
Silicon junction defect	0.6-0.8
Metallization defect	0.5
Au-Al intermetallic growth	1.05
Electromigration	0.6-0.9
Metal corrosion	0.45-0.7
Assembly defects	0.5-0.7
Bond related	1.0
Wafer fabrication (chemical contamination)	0.8-1.1
Wafer fabrication (silicon/crystal defects)	0.5-0.6
Dielectric breakdown, field > 0.04 micron thick	0.3
Dielectric breakdown, field <= 0.04 micron thick	0.7
Adhesive tack: bonding-debonding	0.65-1.0

（6）Hallberg-Peck 模型(高温高湿)

Hallberg Peck 模型综合考虑了温度、湿度影响，它相比于模型二更能准确的描述在温湿度条件下进行的老化测试，其表达式为：

$$AF = (RH_t/RH_u)^3 \cdot \exp\{(E_a/k) \cdot [(1/T_u) - (1/T_t)]\}$$

其中，AF 为加速因子；Ea 为激活能。一般来说，激活能的值在 0.3eV~1.2eV 之间；K 为玻尔兹曼常数，其值为 8.617385×10^{-5} ；Tu 为使用条件下(非加速条

件下)的温度值。此处的温度值是绝对温度值，以 K(开尔文)作单位；Tt 为测试条件下(加速条件下)的温度值。此处的温度值是绝对温度值，以 K(开尔文)作单位；RHu 为使用条件下(非加速状态下)的相对湿度值；RHt 为测试条件下(加速状态下)的相对湿度值。

车用芯粒可靠性测试和传统芯片车规 AECQ100 测试的主要区别点有：

车用芯粒可靠性测试更具聚焦芯片间互连可靠性（如中介层、硅桥）、热应力分布、信号完整性等。目标是解决先进封装带来的新失效模式（如热膨胀系数不匹配导致的翘曲）。和 AECQ100 相比，还包括 AECQ104 的 BLR,MCM-Drop 测试，关注互连可靠性：硅通孔（TSV）、微凸点（Microbump）的疲劳断裂测试。

热阻测试关注 3D 堆叠中的局部热点分析（需红外热成像工具）。温度条件芯粒温度范围可从-55°C~125°C（侧重温度冲击），短期数百次循环，更关注温度快速变化对互连的影响。偏压要求，AECQ100 是施加额定电压/电流负载，芯粒则是多芯片协同工作负载模拟。为确保芯粒封装技术的可靠性，每个 Die 要进行预先的 Burn-in Test。

2.3 车用芯粒电磁兼容特性分析

2.3.1 单个芯粒和模块整体电磁兼容特性

芯粒技术通过将芯片系统分解为多个独立的小芯粒（Die），每个芯粒具备不同的电磁特性。例如，对高敏感或高干扰的模块（如射频或模拟电路）可能单独进行了屏蔽设计。这种模块化布局降低了整体电磁辐射的耦合风险，并通过独立接地和滤波设计减少传导干扰。由于单个芯粒和模块整体的电磁兼容性能不同，在不同的车载应用下，可能表现出不一样的电磁特性。

2.3.2 电源完整性、信号完整性与电磁发射协同管理

电源完整性（PI）、信号完整性（SI）和电磁发射（EMI）是高速电子系统设计中紧密耦合、相互影响的三大核心问题如图 2.3.1 为 PI、SI、EMI 之间相互影响图。PI 不良是导致 SI 恶化和 EMI 超标的根源性原因之一。SI 问题（如回流

路径差、不平衡）也会直接贡献 EMI。

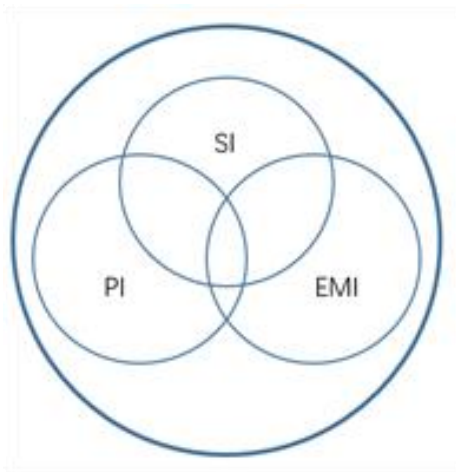


图 2.3.1 PI、SI、EMI 相互影响

芯粒技术的电源完整性(Power Integrity, PI)面临着比传统单芯片(Monolithic Die)设计更严峻的挑战,具有路径更长更复杂,阻抗显著增加,IR 压降和 Ldi/dt 噪声问题严重;多域异构电源需求导致强烈的噪声耦合,SSN 是主要威胁;局部电流密度极高,电热协同设计至关重要;电压容差极其严格,达到毫伏级裕量;封装基板成为性能瓶颈,寄生参数高。高频去耦部署困难且受限等特点。

如图 2.3.2 芯粒高速互连信号完整性示意图,芯粒间采用高速互连技术,容易带来信号传输中的串扰和反射问题,这都会引起 EMI 发射增大。通过优化互连布线密度(如硅基中介层)和采用低功耗传输协议(如并行接口),减少电磁辐射和功耗。此外,2.5D/3D 封装中的中介层(Interposer)可提供更短的互连路径,降低信号延迟和干扰。

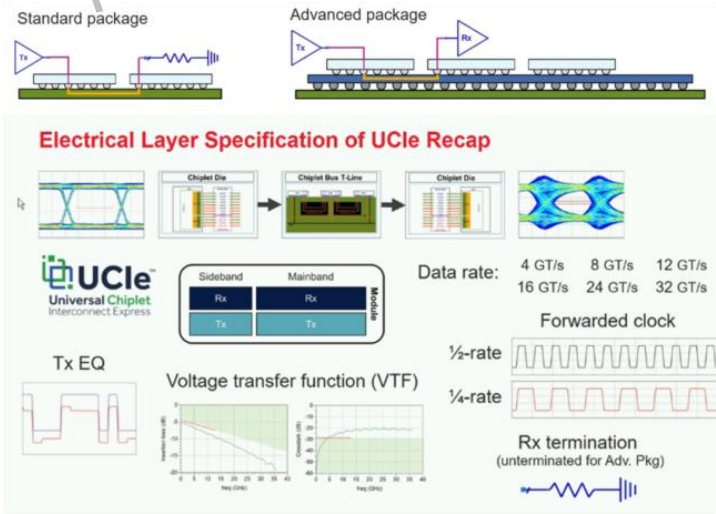


图 2.3.2 芯粒高速互连信号完整性示意图

2.3.3 车用芯粒 EMC 认证的复杂性

芯粒系统对汽车电子中的电磁兼容性（EMC）带来了显著挑战。由于多芯粒集成，每个芯粒的制造工艺和封装工艺可能不同，这导致在极端温度和振动条件下，各芯粒的老化速度和性能变化可能不一致。这种差异可能引发芯粒之间的电磁特性变化，进而影响整体系统的信号完整性和辐射特性。传统单芯片设计中，EMC 特性相对单一和可控，但在芯粒集成中，复杂的信号传输路径和多芯粒之间的耦合效应大大增加了设计的难度。

在车用芯粒系统中，极端温度（ $-40^{\circ}\text{C}\sim 125^{\circ}\text{C}/150^{\circ}\text{C}$ ）和振动等环境因素会加速芯粒的老化过程。不同工艺和封装方式的芯粒在老化过程中可能表现出不同的电阻、电感和介质层特性变化，这会直接影响系统的阻抗匹配和信号传输质量。此外，芯粒之间的屏蔽和滤波效果也可能因老化而发生变化，导致高频信号泄漏或滤波性能下降。这些因素使得芯粒系统的 EMC 设计比传统单芯片设计更加复杂，需要从信号完整性、辐射抑制和抗干扰能力等多方面进行综合考虑。

2.4 车用芯粒功能安全特性分析

在汽车电子领域，功能安全关乎车辆的整体性能和安全性。芯片的功能安全通常通过集成安全机制（如监控、自检、冗余设计等）来实现。在芯粒架构中，功能安全可以通过将安全机制分散到不同的芯粒中实现，每个芯粒可以独立地执行安全功能，并通过高速互连技术进行组合。

此外芯片的功能安全测试与验证通常需要在整个系统层面进行，这可能导致测试周期延长和测试成本增加。芯粒架构则允许对每个芯粒进行独立的功能安全测试和验证，降低了测试难度和成本。同时，由于芯粒可以重复使用，因此可以基于已知的测试结果来评估新系统的安全性。

不同于单颗芯片系统，多芯粒系统可以采用芯粒层级的冗余设计来提高系统的容错能力。例如，可以设计多个相同的芯粒作为备份，在主芯粒出现故障时自动切换到备份芯粒。此外，还可以采用故障检测和恢复机制来及时发现并修复系统中的故障。

芯片安全机制在芯粒设计层面的特殊性主要体现在其分布式架构、异构集成、

物理互连等维度，这些特性既带来了新的安全挑战，也催生了独特的防护方法。例如分布式安全策略协调需要考虑到动态权限管理和安全启动链扩展；异构信任边界管理需要考虑混合安全等级芯粒共存和安全协议同步延迟的情况；物理互连层的安全需要考虑跨芯粒侧信道攻击面和物理攻击面的扩展。

2.4.1 功能安全需求分析

首先实现安全目标与 ASIL 等级的分配。根据 GB/T 34590《道路车辆 功能安全》标准，将系统级安全目标（如避免意外加速）分解到芯粒层级。再根据每个芯粒在系统中的功能为其分配适当的 ASIL 等级，例如：计算芯粒（执行安全关键算法）可能需满足 ASIL D，通信芯粒（负责安全数据交互）需满足 ASIL B，非安全芯粒（如协处理器）可能无需 ASIL 认证，但需通过隔离确保不影响安全功能。然后通过单点故障度量（SPFM）、潜伏故障度量（LFM）和随机硬件失效概率（PMHF）进行量化评估。典型车用场景对功能安全等级要求如表 2.4.1 中所示。

表 2.4.1 典型车用场景对应芯片功能安全等级要求

功能安全等级	典型车用场景
ASIL D	传动系统、行驶系统、转向系统、制动系统等
ASIL C	发动机系统、新能源电驱系统、能源系统等
ASIL B	环境感知系统、智能决策系统、车身控制系统、车身内饰系统、车身外饰系统、车身安全系统、开闭件系统、热管理系统、仪表系统、流媒体后视镜等
ASIL A	电子不停车收费系统、汽车事件数据记录系统等

还要实现安全功能分区。将多芯粒系统的不同安全功能分配到不同芯粒（如刹车控制、电池管理分属不同芯粒），同一芯粒内通过硬件隔离实现安全分区。

芯粒和芯粒系统层面的安全分析,可采用失效模式、影响及诊断分析（FMEDA）、故障树分析（FTA）、相关失效分析（DFA）或适合硬件安全分析的其他类似方法。芯粒和芯粒系统层面的安全分析总结，应至少包括：

- a) 芯粒系统架构层级要素；

- b) 芯粒层级要素；
- c) 要素的功能描述；
- d) 要素的潜在安全相关失效模式；
- e) 失效影响；
- f) 失效原因；
- g) 安全措施；
- h) 安全机制的说明。

2.4.2 安全机制要求

在芯粒设计阶段就应考虑功能安全机制的实现，确保每个芯粒都具备必要的安全功能，并能够与其他芯粒协同工作以实现整体系统的安全目标，确保多芯粒系统符合 GB/T 34590《道路车辆 功能安全》标准中对芯片的功能安全认证标准。

芯粒和芯粒接口的功能安全是确保多芯粒系统中芯粒之间通信可靠性和安全性的关键。芯粒和芯粒接口的功能安全主要关注以下几个方面：

数据传输的可靠性：确保数据在芯粒之间传输时不会因噪声、干扰或硬件故障而损坏。

错误检测与纠正：能够检测并纠正传输过程中发生的错误。

故障隔离：防止单个芯粒的故障扩散到整个系统。

实时监控与诊断：实时监控接口状态，记录错误信息，便于系统诊断和修复。

为了实现上述目标，芯粒和多芯粒系统应针对表 2.4.2 中的要素和失效模式具备表中规定的安全机制。

表 2.4.2 芯粒和多芯粒系统典型失效模式的安全机制

类别	失效模式	典型安全机制
电源	过压	过压监控
	欠压	欠压监控 上电复位
	电源尖峰	电压钳位
	过流	过流监控 限流器

时钟	频率错误	时钟频率监控
	周期抖动	时钟频率监控
非易失性存储器	寻址错误	奇偶校验位
	软错误模型	奇偶校验位 改进的校验和 使用错误探测纠错码（ECC）监控存储器 存储器签名 存储块复制 运行数据完整性检查
	读取错误	存储块复制 存储器内置自检测（MBIST）
	写入错误	存储器内置自检测（MBIST）
	擦除错误	存储器内置自检测（MBIST）
易失性存储器	寻址错误	奇偶校验位 随机访问存储器（RAM）跨步测试
	软错误模型	奇偶校验位 随机访问存储器（RAM）跨步测试 使用错误探测纠错码（ECC）监控存储器 存储块复制 运行校验和/CRC 运行数据完整性检查
	读取错误	随机访问存储器（RAM）模式测试 存储块复制 存储器内置自检测（MBIST）
	写入错误	随机访问存储器（RAM）模式测试 存储器内置自检测（MBIST）
	擦除错误	随机访问存储器（RAM）模式测试 存储器内置自检测（MBIST）
模拟和数字输	直流故障模型	通过在线监控进行失效探测

入/输出		测试模式 编码保护 多通道并行输出 受监控的输出 输入对比/表决 模数转换器（ADC）衰减探测 模数转换器（ADC）通道卡滞探测
	漂移	多通道并行输出 受监控的输出 输入对比/表决
	振荡	多通道并行输出 受监控的输出 输入对比/表决
处理单元	控制逻辑错误	通过软件进行自检 两个独立单元间的软件交叉自检 硬件支持的自检（单通道） 软件多样化冗余（单硬件通道） 通过软件进行相互比较 堆栈上溢出/下溢出探测 具有独立时间基准，无时间窗口的看门狗 具有独立时间基准和时间窗口的看门狗 程序序列的逻辑监控 对程序序列的时间和逻辑监控的组合 基于时间的程序序列的时间和逻辑联合监控 程序流监控
	软错误模型	软件多样化冗余（单硬件通道） 通过软件进行相互比较 硬件冗余（例如：双核锁步、非对称冗余、编码处理）
	直流故障模型	硬件冗余（例如：双核锁步、非对称冗余、编码处理）

		配置寄存器测试 集成硬件一致性监控
通信	通讯节点丢失	CRC
	报文损坏	CRC
	不可接受的报文延迟	CRC
	报文丢失	CRC
	非预期的报文重复	CRC
	错误的报文排序	CRC
	报文插入	CRC
	报文伪装或路由错误	CRC
多芯粒系统接口	信道故障	冗余信道 CRC
	互相干扰	硬件隔离
	芯粒故障	冗余设计

2.4.3 评估方法

芯粒供应商应具备功能安全相关总结性文档，并保证与产品实际开发的一致性、可追溯性。具体包括：

- a) 多芯粒系统层面的安全分析总结；
- b) 芯粒硬件层面的安全分析总结；
- c) 安全机制总结；

芯粒供应商应具有下列相关开发文档，并保证文档的一致性、可追溯性。

- a) 详细芯粒硬件层面的安全分析；
- b) 若有，其他支撑性材料或数据。

对于硬件安全分析的评估，应涵盖表 2.4.3 的检查项。

表 2.4.3 安全分析评估检查清单

编号	检查清单
1	是否在流程上定义了安全分析？
2	是否定义了安全分析的相关模板？
3	是否在项目中按照所定义的流程及模板实施了安全分析？
4	是否对芯片的所有设计进行了安全分析，比如数字、模拟、IO 等。
5	安全分析中识别出风险比较高的失效，是否增加安全机制？

本身实现安全功能的安全关键芯粒应在封装前进行独立的测试和验证，确保其满足功能安全要求。同时对整个系统进行综合测试和验证，以确保各个芯粒之间的协同工作正常且安全可靠。

在系统运行过程中持续监控芯粒的性能和安全性，及时发现并处理潜在的安全隐患。此外，随着技术的不断进步和新的安全威胁的出现，需要定期对芯粒进行更新和升级以确保其安全性和可靠性。

芯粒功能安全与芯片功能安全在集成度、复杂度、实现方式以及测试与验证等方面存在显著差异。其中芯粒和芯粒接口的功能安全是实现多芯粒系统可靠运行的关键。通过错误检测与纠正、冗余设计、协议级保护和实时监控等技术，可以有效提升芯粒接口的安全性，确保每个芯粒都具备必要的安全功能并能够与其他芯粒协同工作以实现整体系统的安全目标。随着芯粒技术的普及，功能安全将成为设计和实现中的重要考量因素。

2.5 车用芯粒信息安全特性分析

芯粒技术虽然为半导体行业带来了模块化、灵活性和成本效益等优势，但在涉及芯片和芯粒的车用等很多应用场景中，在信息安全方面也面临多个关键风险点，例如供应链安全与硬件木马风险、芯粒间通信安全、逆向工程与知识产权窃取以及系统级安全挑战等。

芯片通常将多个功能单元集成在单一芯片上，这种高度集成可能导致安全漏洞的集中化，一旦某个功能单元被攻破，整个芯片的安全性都可能受到威胁。多芯粒系统则是通过先进的封装技术将不同的功能单元拆分成独立的小芯片进行

集成。这种分散化的集成方式可以降低单个芯粒被攻破的风险，因为即使某个芯粒出现问题，其他芯粒仍然可以保持独立运行，从而提高了整体系统的信息安全

性。

信息安全的实现也存在差异。在芯片中，安全机制通常需要在整个芯片层面进行设计和实现，这可能涉及复杂的硬件和软件协同工作，以及大量的安全验证和测试。相比之下，芯粒架构允许将安全机制分散到不同的芯粒中实现。每个芯粒可以独立地执行安全功能，如加密、解密、身份认证等，并通过高速互连技术进行组合。这种分散化的安全机制实现方式可以提高系统的灵活性和可重用性，同时降低安全机制的设计和实现难度。

芯片中的安全机制一旦设计和实现完成，通常难以进行更新和维护。随着技术的不断进步和新的安全威胁的出现，芯片的安全机制可能逐渐过时或无法应对新的威胁。芯粒架构则支持在需要时更新或替换特定的芯粒。这意味着当新的安全威胁出现时，可以通过更新或替换受影响的芯粒来增强系统的安全性。此外，芯粒的模块化设计也使得系统的维护和升级变得更加容易和高效。

在芯粒设计阶段就考虑信息安全机制的实现，确保每个芯粒都具备必要的安全功能，并能够与其他芯粒协同工作以实现整体系统的安全目标。

2.5.1 信息安全需求分析

依照 GB 44495-2024《汽车整车信息安全技术要求》等标准，先将整车信息安全目标分解到零部件，通过对零部件的信息安全需求进行细化分解，导出可通过汽车芯粒实现的信息安全需求。汽车芯粒的信息安全需求通过多种汽车芯粒的信息安全功能实现。

在进行汽车芯粒信息安全需求分析过程中，将汽车芯粒作为独立于环境的安全产品，通过假定安全需求和安全设计，确定汽车芯粒信息安全需求。

假设信息安全需求和信息安全设计。对于针对不同使用方和不同应用开发的汽车芯粒，为满足零部件信息安全要求，先做出关于汽车芯粒的信息安全需求以及安全设计的假定。汽车芯粒与所假定的外部设计和更高层次设计所组成的系统可以满足零部件所有的信息安全需求。

验证假设有效性。在基于假设开发独立于环境的安全产品过程中，假设一个

既定的信息安全功能以及包含外部接口的使用环境。在零部件的环境中集成独立于环境的安全产品时，证实这些假设的有效性。

2.5.2 信息安全需求与安全功能的映射关系

在芯粒设计阶段就应考虑信息安全机制的实现，确保每个芯粒都具备必要的信息功能，并能够与其他芯粒协同工作以实现整体系统的安全目标，确保多芯粒系统符合《汽车芯片信息安全技术规范》标准中对芯片的信息安全认证标准。

芯粒及芯粒接口的信息安全是确保多芯粒系统中数据传输和通信过程中数据机密性、完整性和可用性的关键。芯粒及芯粒接口的信息安全需要从硬件、协议和系统层面进行综合防护。

芯粒及芯粒接口的信息安全主要关注以下几个方面。

数据机密性：防止数据在传输过程中被窃取或泄露。

数据完整性：确保数据在传输过程中未被篡改。

可用性：确保芯粒接口在受到攻击时仍能正常运行。

身份认证：确保通信双方的身份合法，防止伪装攻击。

抗攻击能力：抵御物理攻击、软件攻击等威胁。

车用芯粒的信息安全需求通过多种车用芯粒的信息安全功能实现，它们之间的映射关系如表 2.5.1 所示：

表 2.5.1 芯粒信息安全需求与安全功能的映射关系

信息安全需求	安全功能
安全启动	密钥保护； 密码算法支持； 关键安全参数保护； 安全运行环境支持； 安全启动机制；
安全更新	密钥保护； 密码算法支持； 关键安全参数保护； 固件更新支持； 权限控制； 安全运行环境支持
安全通信	密码算法支持； 安全运行环境支持；

	随机数生成； 关键安全参数保护。
安全访问	密码算法支持； 关键安全参数保护； 权限控制； 安全运行环境支持。
安全存储	密钥保护； 密码算法支持； 关键安全参数保护； 安全运行环境支持。
生命周期管理	密钥保护； 关键安全参数保护； 固件更新支持； 权限控制； 安全运行环境支持； 自测试； 安全生命周期管理机制。
攻击防护	物理防护； 软件攻击保护机制； 漏洞管理。
个人信息安全	个人信息保护功能

在汽车典型应用场景中，车用芯粒信息安全可满足的信息安全需求和对应具备的信息安全功能可参考表 2.5.2。

表 2.5.2 汽车不同应用场景的安全需求及车用芯粒应提供的安全功能示例

芯粒类型	产品类型	功能	应用场景	安全需求	安全功能
安全芯粒	独立安全硬件	密钥保护、 密码算法、 敏感数据存储	数字钥匙、 车载支付、 紧急呼叫系统、 污染排放平台数据 上传、V2X 功能等场景	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■

					物理防护■ 安全启动机制■ 软件攻击保护机制□ 个人信息保护□ 漏洞管理■ 安全生命周期管理机制■
通信芯粒	直连芯粒 蜂窝芯粒 卫星通信芯粒	远距通信	V2X 功能、紧急呼叫系统、电动汽车远程服务与管理系统、数据采集、OTA 升级、远程控制、远程诊断等	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护■ 漏洞管理■ 安全生命周期管理机制■
	蓝牙/ Wifi/ UWB/	近场通信	投屏、音乐播放、拨打电话数字/电子钥匙等	安全启动■ 安全更新■ 安全通信■	密钥保护■ 密码算法支持■ 随机数生成■

	星闪/ NFC/			安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护□ 漏洞管理■ 安全生命周期管理机制■
	百兆/千兆 /10G 以太网芯片 SerDes 芯片	车内通信	数据传输	安全启动□ 安全更新□ 安全通信■ 安全访问□ 安全存储□ 生命周期管理□ 攻击防护□ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成□ 关键安全参数保护■ 固件更新支持□ 权限控制□ 安全运行环境支持■ 自测试□ 物理防护□ 安全启动机制□ 软件攻击保护机制□

					个人信息保护□ 漏洞管理□ 安全生命周期管理 机制□
	网关芯粒	车内通信	数据传输	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保 护■ 固件更新支持■ 权限控制■ 安全运行环境支 持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机 制■ 个人信息保护□ 漏洞管理■ 安全生命周期管 理机制■
控制芯粒	控制器	控制器	BMS、EPS、ESC、EMB等底盘控制器、发动机控制器、车身控制器等	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保 护■ 固件更新支持■ 权限控制■

				个人信息保护□	安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制□ 个人信息保护□ 漏洞管理■ 安全生命周期管理机制■
			智驾控制器、智能座舱控制器、中央车载计算平台、T-BOX	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护■ 漏洞管理■ 安全生命周期管理机制■

	执行器	执行器	胎压监测等	安全启动□ 安全更新■ 安全通信□ 安全访问□ 安全存储□ 生命周期管理□ 攻击防护□ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成□ 关键安全参数保护□ 固件更新支持■ 权限控制□ 安全运行环境支持■ 自测试□ 物理防护□ 安全启动机制□ 软件攻击保护机制□ 个人信息保护□ 漏洞管理□ 安全生命周期管理机制□
计算芯粒	智能驾驶芯粒	自动化功能计算任务、数据采集、处理和分析	数据采集、处理与分析	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□

					安全启动机制■ 软件攻击保护机制■ 个人信息保护■ 漏洞管理■ 安全生命周期管理机制■
	智能座舱芯粒	语音处理、图像处理、视频处理	娱乐模块、语音识别	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护■ 漏洞管理■ 安全生命周期管理机制■
传感芯粒	毫米波雷达芯粒	环境感知	毫米波雷达	安全启动■ 安全更新■ 安全通信■ 安全访问■	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保

				安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护□ 漏洞管理■ 安全生命周期管理机制■
	激光雷达芯粒	环境感知	激光雷达	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护□

					漏洞管理■ 安全生命周期管理机制■
	图像传感器芯粒	图像传感	图像传感器	安全启动■ 安全更新■ 安全通信■ 安全访问■ 安全存储■ 生命周期管理■ 攻击防护■ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成■ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支持■ 自测试■ 物理防护□ 安全启动机制■ 软件攻击保护机制■ 个人信息保护□ 漏洞管理■ 安全生命周期管理机制■
存储芯粒	Secure FLASH	加密存储	智驾平台	安全启动■ 安全更新■ 安全通信□ 安全访问■ 安全存储■ 生命周期管理□ 攻击防护□ 个人信息保护□	密钥保护■ 密码算法支持■ 随机数生成□ 关键安全参数保护■ 固件更新支持■ 权限控制■ 安全运行环境支

					持■ 自测试□ 物理防护□ 安全启动机制■ 软件攻击保护机制□ 个人信息保护□ 漏洞管理□ 安全生命周期管理机制□
--	--	--	--	--	--

2.5.3 信息安全功能技术要求与试验方法

根据车用芯粒信息安全攻击危害性和攻击易实施性两个方面对车用芯粒信息安全要求分级进行评估确定。评估攻击危害性的方法见表 2.5.3，评估攻击易实施性的方法见表 2.5.4。

表 2.5.3 攻击危害性评估表

危害性	信息泄露影响	功能操作影响
高	国家地理信息、测绘数据等涉及国家安全、社会公共利益	可能导致非预期操作或无法操作
中	个人信息主体可被识别，可能导致个人财产安全受到严重危害	可能导致部分功能失效
低	个人信息主体可被识别，可能会给个人信息主体合法权益带来负面影响	功能性能降级造成使用不便
无	相关数据在任何场景下均无法关联或识别到个人信息主体；或个人信息主体可主动公开或经授权公开的数据	无影响或影响不可感知
注：危害性评估中，符合信息泄露影响或功能操作影响二者较高等级之一即为对应危害等级		

表 2.5.4 攻击易实施性评估表

攻击易实施性	攻击途径	说明	示例
容易	车外网络攻击	通过远程网络或本地网络实现的攻击	借助wifi、蓝牙、NFC进行的无接触攻击等
中等	车内网络攻击	在外部攻击渗透后开展的车内网络攻击	内部 CAN 总线、ECU 之间的攻击等
困难	物理攻击	需要接触到物理实体开展的攻击	故障注入攻击、侧信道分析与反向工程等

车用芯粒信息安全分级方法见表 2.5.5，分为一级、二级和三级，其中三级为最高信息安全等级要求，一级为基础信息安全等级要求。

表 2.5.5 分级方法

危害性 攻击易实施性	高	中	低	无
容易	三级	二级	二级	/
中等	三级	二级	一级	/
困难	三级	一级	/	/

车用芯粒具备的安全功能技术要求与信息安全等级对应关系见表 2.5.6 所示。一级表示对车用芯粒信息安全基础能力的要求、二级表示对车用芯粒信息安全管理与维护能力的要求、三级表示对车用芯粒抵抗恶意攻击能力的要求。

表 2.5.6 安全功能分级参考

安全功能	一级	二级	三级
密钥保护	密钥生成 密钥存储 密钥使用 密钥销毁	密钥生成 密钥存储 密钥使用 密钥销毁	密钥生成 密钥存储 密钥使用 密钥销毁
密码算法支持	密码算法支持	密码算法支持	密码算法支持
随机数生成	支持安全随机数生成能力	支持安全随机数生成能力	支持安全随机数生成能力

	符合 GB/T 32915 规定的随机性检测要求	符合 GB/T 32915 规定的随机性检测要求	符合 GB/T 32915 规定的随机性检测要求 具有随机数检测功能
关键安全参数保护	关键安全参数保护	关键安全参数保护	关键安全参数保护
固件更新支持	不做要求	固件更新支持	固件更新支持
权限控制	存储访问控制 接口授权访问	存储访问控制 接口授权访问	存储访问控制 接口授权访问
安全运行环境支持	安全运行环境的固件 可信应用	安全运行环境的固件 可信应用	安全运行环境的固件 可信应用
自测试	自测试记录 自测试执行	自测试记录 自测试执行	自测试记录 自测试执行
物理防护	不做要求	不做要求	侧信道攻击防护 故障注入攻击防护 反向工程防护
安全启动机制	安全启动机制	安全启动机制	安全启动机制
软件攻击保护机制	软件攻击保护机制	软件攻击保护机制	软件攻击保护机制
个人信息保护	个人信息保护	个人信息保护	个人信息保护
漏洞管理	漏洞管理	漏洞管理	漏洞管理
安全生命周期管理机制	安全生命周期管理机制	安全生命周期管理机制	安全生命周期管理机制

汽车典型应用场景下不同芯粒类型的信息安全等级见表 2.5.7。

表 2.5.7 车用芯粒信息安全分级示例

应用场景	芯粒类型	信息安全等级
T-Box	控制芯粒	二级
	存储芯粒	一级
	蜂窝通信芯粒	二级/ 三级
	直连通信芯粒	二级
	安全芯粒	三级

网关	有线通信芯粒	二级
	存储芯粒	一级
	控制芯粒	二级
智能驾驶	计算芯粒	二级
数字钥匙	近场通信芯粒	二级/ 三级
	安全芯粒	三级
智能座舱	计算芯粒	二级
	控制芯粒	二级
	通信芯粒	二级
	安全存储芯粒	一级
车身控制器	有线通信芯粒	一级
	控制芯粒	二级
VCU	有线通信芯粒	一级
	控制芯粒	二级
门窗、门锁、天窗、雨刮	控制芯粒	一级

车用芯粒信息安全功能试验方法包括车用芯粒信息安全文档检查和产品测试。应先基于以上的分析方法确定试验范围；再依据试验范围对车用芯粒信息安全功能相关的说明文档进行检查，确认被测产品符合相关要求；最后依据试验范围开展测试，确认被测产品符合相关要求。

本身实现安全功能的安全关键芯粒应在封装前进行独立的测试和验证，确保其满足信息安全要求。同时应对整个系统进行综合测试和验证，以确保各个芯粒之间的协同工作正常且安全可靠。

在系统运行过程中持续监控芯粒的性能和安全性，及时发现并处理潜在的安全隐患。此外，随着技术的不断进步和新的安全威胁的出现，需要定期对芯粒进行更新和升级以确保其安全性和可靠性。

芯粒信息安全与芯片信息安全在集成方式、安全机制实现、更新与维护等方面存在显著差异。其中芯粒及芯粒接口的信息安全是实现多芯粒系统安全运行的关键，通过数据加密、完整性保护、身份认证、抗攻击设计和安全协议等技术，

可以有效提升芯粒接口的安全性。确保每个安全芯粒都具备必要的安全功能并能够与其他芯粒协同工作以实现整体系统的安全目标。随着芯粒技术的普及，信息安全将成为设计和实现中的重要考量因素。

2.6 车用芯粒软件设计特性分析

2.6.1 芯粒互联类型

对于硬件自洽接口而言，无需软件干预，芯粒间互联对软件完全透明。此时，芯粒的软件设计，包括驱动设计与软件适配，与传统 SOC 没有差异。

对于软件管理接口而言，在支持需要软件管理物理层和协议层的芯粒架构中，芯粒之间的互联不再仅依赖于硬件自动完成，而是要求系统软件参与管理。这种架构通常采用标准或自定义的高速互连协议（如 Die-to-Die 协议、CXL、UCIe 等）。因此软件需承担以下新增职责。

- 1) 物理层驱动（PHY Driver）：负责初始化和配置芯粒间的物理互连接口（如 SerDes、High-Speed Link），保证链路的建立、同步与健康状态监测。
- 2) 协议层驱动（Protocol Driver）：实现芯粒之间通信协议的解析、封装、重传管理、流控等机制，确保数据能够可靠、高效地在芯粒间传递。

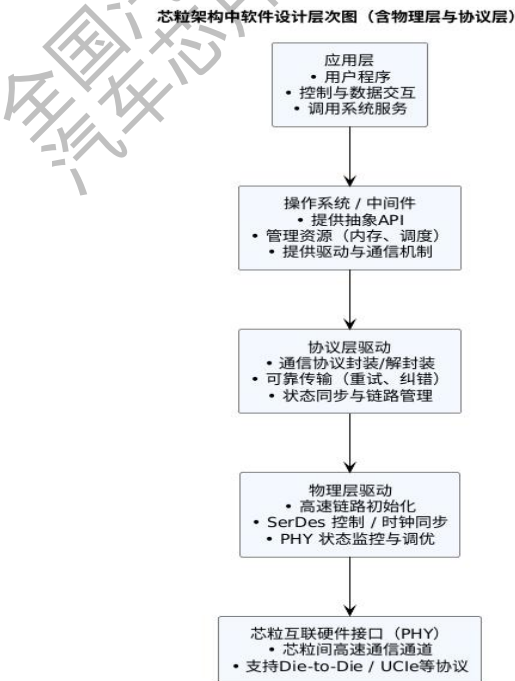


图 2.6.1 芯粒架构中软件设计层次图

上述引入将带来更多软件架构层面的变动，包括中断处理路径、DMA 传输管理、链路状态监控、调试接口等模块的新增或修改，如图 2.8.1 芯粒架构中软件设计层次图。这要求操作系统、固件或中间件进行相应的适配，以保障系统的可用性与性能。

2.6.2 车用芯粒软件设计特殊特性

芯粒系统的软件架构需要针对硬件特性进行深度优化：一种是**硬件抽象层重构**；再者是**驱动模型变革**；此外，还有**实时性保障差异**。

从硬件抽象层重构来看，芯粒架构相对于传统 SoC 架构方案主要有如下的**特殊性**。

传统方案：传统单芯片系统中的 BSP（Board Support Package）和 HAL（Hardware Abstraction Layer）设计是为一颗 SoC 精细裁剪；资源访问路径固定，寄存器、中断、电源等管理集中统一；驱动程序只需访问单一地址空间，无需考虑跨芯粒地址映射或控制域。

对于芯粒架构面临的挑战包括：芯粒功能分布在多个独立 Die 上，各自具有独立寄存器空间；中断和电源信号需要跨芯粒域传输，导致中断路由复杂化；芯粒间电源/时钟管理可能存在异构性（不同电压等级、时序差异）。

因此对于芯粒 HAL 的设计而言，设计需求包括：

在芯粒架构中，寄存器地址空间不再集中管理，不同芯粒的控制寄存器可能分布在独立的地址域。为了保证上层驱动程序和应用逻辑对底层硬件访问的一致性，HAL（硬件抽象层）需要支持**分布式寄存器映射机制**。这通常通过动态地址解析、配置表驱动映射或统一访问接口实现，使系统在运行时能够根据芯粒标识或功能类型，自动定位对应寄存器区域并进行访问，避免硬编码错误和访问冲突。

随着芯粒间资源解耦，**中断管理机制也需随之演进**。传统的集中式中断控制器不再适用，跨芯粒产生的中断信号需通过 HAL 进行**重路由与归并**，将多个物理来源的中断虚拟成逻辑统一的事件流。实现方式上可通过中断仲裁模块、消息中断（MSI）机制或链路传输通道（如通过 UCIe/CXL）将中断传输至主控芯粒进行统一处理，从而确保操作系统能够正确识别并调度来自异构芯粒的中断事件。

芯粒的异构特性还带来了电源与时钟管理的复杂性，不同工艺节点的芯粒可

能具有不同的电压、时钟要求，且这些要求可能具有先后启停或同步的依赖关系。因此，HAL 需要具备**协同电源管理策略**，在系统上电、休眠唤醒等阶段，按照依赖图或优先级顺序对芯粒的电源和时钟进行协调控制。这类策略一般结合 PMIC 驱动、电源状态机以及跨芯粒通信机制实现，确保整个系统在多芯粒状态变化下仍能稳定运行。

从驱动模型变革来看，驱动方式由单一驱动到跨芯粒协同驱动转变。

传统方案：一个硬件功能模块由一个驱动管理；操作系统将其视作本地外设，驱动直接读写本地寄存器；功能边界与物理封装一致，无需跨芯片通信。

由 SoC 架构转变到芯粒架构，芯粒架构所要面临的挑战包括：功能被拆分至多个芯粒（如 AI 核与控制器分布在不同芯粒）；芯粒间通信依赖 UCIe、BoW、CXL 等互联协议；驱动程序需支持远程访问、资源协调与链路管理。

因此，芯粒驱动模型需要进行分层设计，主要包含如下设计内容。

在芯粒架构中，各芯粒之间通过高速互联协议（如 UCIe、CXL 等）实现通信与资源共享。为支撑这些物理连接的初始化与运行维护，软件架构需引入**基础驱动层（Physical Link Layer）**。该层负责完成芯粒间链路的初始化配置，包括链路训练、拓扑识别、通道映射等基础操作；同时保障数据传输的可靠性与一致性，支持流控、错误检测与恢复机制。此外，基础驱动还须具备链路状态监测、动态带宽调整与链路健康评估等能力，为上层功能模块的稳定通信提供强有力支撑。在基础链路建立的基础上，为了实现具体功能的软硬件交互，芯粒驱动架构需进一步抽象出**功能驱动层（Functional Driver Layer）**。该层按照功能模块（如 AI 加速、GPU 渲染、图像处理等）进行封装，对上层操作系统或中间件提供统一的 API 接口；对下层通过基础链路驱动访问远程芯粒资源。此设计实现了驱动功能与物理拓扑的解耦，具备良好的可移植性与可扩展性，能够适配不同厂商、不同形态的芯粒组合，有效支持模块化、可重构的系统设计需求。如图 2.6.2 为相应的结构 UML 图。

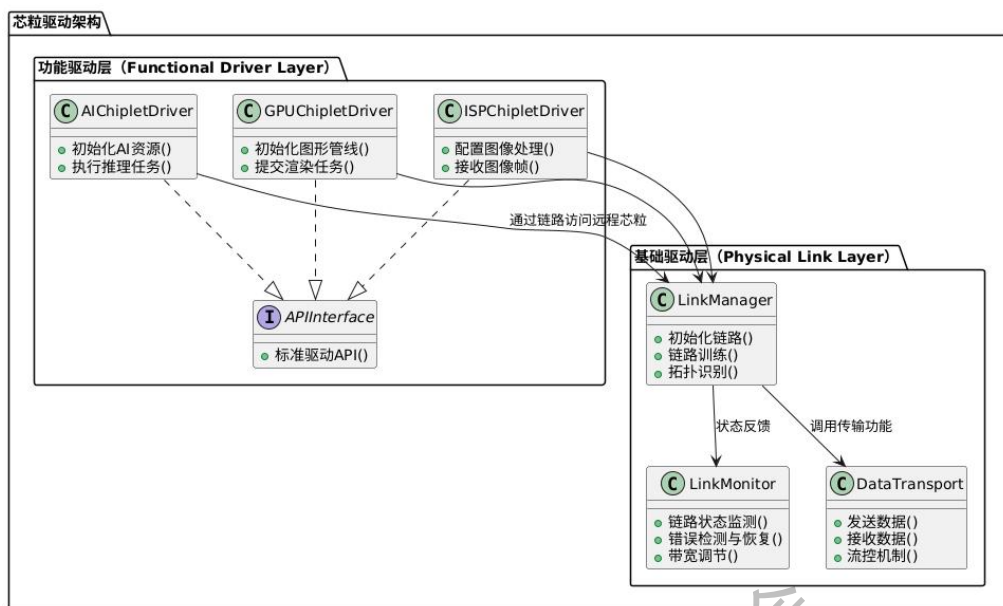


图 2.6.2 芯粒驱动架构 UML 图

对于实时性保障差异来说，时钟方面需要从全局时钟到跨芯粒时钟的对齐。

传统方案：单芯片 SoC 使用统一的全局时钟源；多核任务调度、DMA 传输、计时器等基于统一时间基准；操作系统中断调度精度与同步性高。

由传统方案到芯粒方案其架构面临的挑战包括：各芯粒可能具有独立的时钟源（异构时钟域）；缺乏全局统一时钟，容易导致跨芯粒调度/通信延迟不一致；时间同步变得依赖链路协议和软件逻辑。因此对于芯粒架构而言，其时钟对齐机制有着相关需求如图 2.6.3 所示。

在芯粒系统中，由于各芯粒可能源于不同的制造工艺或设计厂商，往往会采用独立的本地时钟源，这就引入了多时钟域并存的问题。为了保证跨芯粒协同操作的时序一致性，需要建立一种软硬件协同的时钟对齐机制。常见做法是在系统启动阶段，通过精准同步协议（如 PTP，Precision Time Protocol）在各芯粒之间建立统一的参考时间；在系统运行期间，则周期性地执行校准与漂移补偿，确保各芯粒间的时间基准保持在可接受的偏差范围内，从而保障系统运行的同步性和实时性。

此外，在芯粒间的数据交互过程中，链路协议层也需要原生支持时间戳信息的传递。例如，通过 UCle 等芯粒互联协议，在数据包中携带发送时间戳，使接收端能够据此判断数据的时间顺序与偏移情况。这种机制对于保障跨芯粒操作的逻辑时序一致性极为关键，特别是在需要进行带时间关联的任务处理（如多通

道音视频处理、跨芯粒传感器融合)时,时间戳机制能有效提升系统准确性与同步效率。

同时,为了进一步提升系统层级的协同效率,操作系统或调度器还须具备对**多时钟域的感知与调度能力**。具体而言,系统需采用逻辑时钟映射机制,将不同时钟域下的事件统一转换为一个可比较的逻辑时间轴,从而支持跨芯粒的统一任务调度与资源分配。这类调度策略通常融合硬件时钟读取、中间层抽象转换和调度策略融合,实现对芯粒系统的精准控制和高效管理。

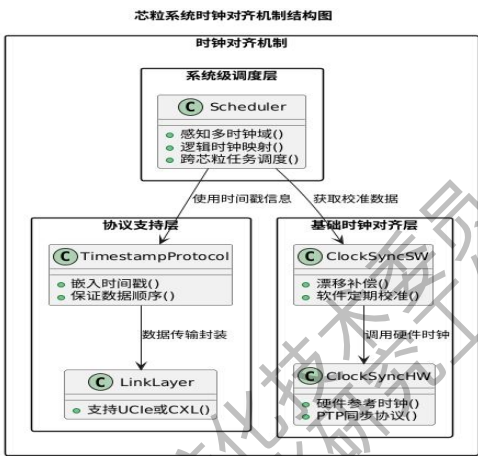


图 2.6.3 芯粒系统时钟对齐机制结构图

三、车用芯粒关键领域标准化需求

智能汽车对算力的需求呈指数级增长,但车载电源系统受限于 12V/48V 电压平台,能效优化成为核心挑战。芯粒技术通过异构集成实现算力与功耗的灵活配比:将高算力模块(如 AI 加速器)采用先进制程以降低功耗,而低功耗模块(如传感器接口)保留成熟制程以控制成本。

传统汽车供应链遵循“Tier1-Tier2”垂直分工模式,但芯粒技术需重构为“芯粒供应商-封装集成商-车企”的网状生态。这一转变面临三重阻力:

(1) 供应链响应速度不匹配:车规芯片验证周期长达 2-3 年,而芯粒的模块化迭代要求开发周期压缩至 6-12 个月;

(2) 责任界定模糊:多厂商芯粒集成后出现故障时,封装缺陷、接口协议错误或单一芯粒失效的责任划分尚无标准依据;

(3) 生态壁垒:车企倾向于自研关键芯粒以掌控核心技术,但封闭生态与

芯粒的开放互操作性目标冲突。解决这些矛盾需建立跨行业的“芯粒认证池”和标准化的责任追溯机制，同时通过联盟化合作降低生态门槛。

3.1 车用芯粒接口与通信标准化需求

汽车电子需满足全球最严苛的可靠性标准。以 AEC-Q100（芯片级车规认证）为例，其要求芯片在-40℃至 150℃温度范围内稳定工作，并通过机械振动、湿热循环等多项极端环境测试。然而，芯粒技术引入多芯片异构集成后，不同工艺节点的芯粒（如 7nm 计算单元与 40nm 电源模块）因热膨胀系数差异，易在封装界面产生应力裂纹，导致长期可靠性风险。此外，ISO 26262 功能安全标准要求芯粒间通信具备 ASIL-D 级冗余机制，但现有 Die-to-Die 接口（如 UCIe）缺乏标准化故障隔离设计，导致车企需额外开发监控电路，增加系统复杂度与成本。

3.1.1 通用互联标准难以适配车规场景

（1）通用标准与车规标准的差异

如表 3.1.1 所示，通用芯粒互联标准与车规芯粒互联标准在数字部分（例如链路层和协议层）主要存在功能安全架构上的差异，例如数据传输格式、错误检测和纠正机制、流量控制等方面与车规标准存在差异。通用标准可能更侧重于数据传输的效率，而车规标准则更注重数据传输的可靠性和安全性。而在模拟部分（例如物理层），通用标准可能更注重成本和通用性，而车规标准则对电气特性、引脚定义、信号传输方式等有着严格的要求，以确保在复杂车载环境下的可靠性。通用标准的引脚定义可能较为灵活，以适应多种应用场景，但在车载环境中，这种灵活性可能导致接口的稳定性不足。车规标准对引脚的机械强度、抗腐蚀能力等有更高的要求，以保证在车辆长期使用过程中接口的物理连接可靠。

表 3.1.1 通用和车用芯粒互联对比表

维度	通用芯粒互联标准	车用芯粒互联标准
功能安全	无功能安全要求（QM）	ASIL_B/C/D
工作温度范围	0℃ ~ 85℃	-40℃ ~ 125/150℃
自检	无	要求启动自检

抗振动与抗冲击	通常仅满足消费电子级振动要求	需要抗振抗冲击设计与防护，以确保急刹、颠簸等场景下的通信稳定；
抗电磁干扰	聚焦基础信号完整性	需要抗电磁干扰设计，且需要做相关测试

（2）不同厂商接口标准差异

当前，汽车智能化发展迅速，不同汽车制造商和芯片供应商为满足自身产品需求，纷纷推出各自的接口标准。这些标准在物理层、链路层和协议层等方面存在显著差异，导致系统集成难度大幅增加。以物理层为例，不同厂商的接口在电气特性、引脚定义和信号传输方式上各不相同。某些芯片供应商的接口采用差分信号传输，以提高抗干扰能力，但引脚定义与其他厂商不兼容，使得在系统集成时，无法直接将不同厂商的芯片进行连接，需要额外设计转接电路，这不仅增加了硬件成本，还可能引入新的信号干扰和传输延迟问题。在链路层，数据的传输格式、错误检测和纠正机制以及流量控制等方面也存在差异。部分接口采用简单的循环冗余校验（CRC）进行错误检测，而另一些则采用更为复杂的海明码纠错，这使得不同接口之间的数据交互变得复杂，增加了软件编程的难度和工作量。在协议层，通信的握手协议、数据解析方式和命令集也各不相同，导致不同厂商的芯片之间难以实现互联互通。一家汽车制造商若要同时采用 A、B 两家芯片供应商的产品，由于接口标准的差异，需要投入大量的人力和物力进行接口适配和系统调试，这无疑增加了汽车电子系统的开发成本和时间成本。

（3）开发与维护成本增加

由于接口标准的不统一，汽车电子系统开发过程中需要针对不同标准进行适配，这极大地增加了开发和维护成本。在开发阶段，汽车制造商需要组建专业的技术团队，对不同厂商的接口标准进行深入研究和分析，以实现芯片之间的互联互通。这不仅要求技术人员具备深厚的专业知识，还需要投入大量的时间进行接口适配和调试工作。开发一款智能座舱系统，若涉及多个不同标准的芯片，开发周期可能会延长 3 - 6 个月，开发成本可能会增加 20% - 50%。在维护阶段，当系统出现故障时，由于接口标准的复杂性，定位和解决问题变得更加困难。不同厂商的芯片在出现故障时，错误信息的反馈和诊断方式也各不相同，技术人员需

要熟悉多种标准的故障诊断方法，才能准确找出问题所在并进行修复。这不仅增加了维护的难度，还可能导致车辆停机时间延长，给用户带来不便，同时也增加了汽车制造商的售后维护成本。若某款车型的辅助驾驶系统出现故障，由于接口标准不统一，排查故障的时间可能会延长数小时甚至数天，这不仅影响了用户的使用体验，还可能导致汽车制造商面临用户的投诉和索赔。

3.1.2 车用芯粒的特殊应用场景需求

（1）高温、高湿、强电磁干扰环境

车载环境中的高温、高湿以及强电磁干扰对互联技术的信号传输稳定性和设备可靠性产生了严重影响。在高温环境下，芯片和互联线路的物理性能会发生变化。芯片内部的晶体管阈值电压会漂移，导致性能下降与不稳定，可靠性降低，从而导致出现信号失真的情况，更甚者造成永久性物理损坏。高温还会加速芯片和互联线路的老化，降低其可靠性和使用寿命。在一些极端高温的地区，如沙漠地带，汽车长时间行驶后，芯片和互联线路的故障率明显升高。

高湿环境同样对互联技术造成威胁。水分可能会侵入芯片和互联线路，导致短路、腐蚀等问题。在沿海地区或雨季，汽车内部的湿度可能会达到 80% 以上，这种高湿环境下，芯片引脚和互联线路的金属部分容易被腐蚀，从而增加电阻，影响信号传输的质量。严重时，可能会导致线路短路，使设备无法正常工作。

强电磁干扰是车载环境中又一严峻挑战。汽车发动机在运行过程中会产生强大的电磁干扰，其频率范围广泛，可能会覆盖互联技术所使用的频段。车载通信设备，如收音机、蓝牙等，也会产生电磁干扰。这些干扰会导致信号传输过程中出现噪声、误码等问题。在强电磁干扰环境下，高速串行接口的误码率可能会增加 10 倍以上，严重影响数据传输的准确性和可靠性。

（2）车辆振动与冲击

车辆行驶过程中的震动和冲击对接口物理连接和信号传输有着显著影响，而现有互联技术在应对这些问题时存在明显不足。汽车在行驶过程中，会受到来自路面的各种震动和冲击，这种震动和冲击可能会导致接口的物理连接松动，如连接器引脚可能会出现接触不良的情况。在一些越野车型中，由于行驶路况更为复杂，接口物理连接松动的问题更为常见。

接口物理连接的松动会直接影响信号传输的稳定性。当引脚接触不良时，信号传输可能会出现中断或时断时续的情况。在智能驾驶系统中，传感器与计算芯片之间的信号传输中断可能会导致车辆对周围环境的感知出现偏差，从而影响驾驶决策的准确性。震动和冲击还可能会导致互联线路的疲劳损坏，缩短其使用寿命。在长期的震动和冲击作用下，互联线路可能会出现断裂的情况，这将导致设备无法正常工作。现有互联技术在设计时，往往对震动和冲击的考虑不足，缺乏有效的加固和防护措施，难以满足车载环境的要求。

(3) 对实时性和可靠性的极致要求

智能驾驶等场景对数据传输实时性和可靠性有着极高的要求，而现有互联技术在延迟和错误处理方面存在局限性。在智能驾驶系统中，车辆需要实时处理来自多个传感器的大量数据，以做出准确的驾驶决策。现有互联技术在高速数据传输时，往往会出现延迟增加的问题。如网口等高速串行接口在传输大量数据时，由于信号衰减、干扰等因素，延迟可能会达到几十毫秒，这对于智能驾驶系统来说是不可接受的，可能会导致车辆对突发情况的响应延迟，增加交通事故的风险。在错误处理方面，现有互联技术的能力也有待提高。智能驾驶系统对数据传输的准确性要求极高，任何数据错误都可能导致严重后果。现有互联技术的错误检测和纠正机制可能无法完全满足这种要求。在一些复杂的电磁干扰环境下，数据传输过程中可能会出现大量错误，现有互联技术可能无法及时检测和纠正这些错误，从而影响智能驾驶系统的正常运行。对于一些关键数据，如车辆的制动信号、转向信号等，一旦出现错误且未被及时纠正，可能会导致车辆失控，危及乘客的生命安全。

在高速数据传输过程中，电互连接口存在着显著的信号衰减与延迟问题，这对数据传输速率和距离产生了严重的限制。

信号衰减是由于传输线路的物理特性所导致的。传输线路中的电阻会使信号在传输过程中产生能量损耗，随着传输距离的增加，信号的幅度逐渐减小。电容和电感的存在也会对信号产生影响，它们会导致信号的相位发生变化，进一步降低信号的质量。当信号衰减到一定程度时，接收端可能无法准确地识别信号，从而导致数据传输错误。据相关研究表明，在高频信号传输时，信号衰减的速度会更快。

信号延迟同样是一个关键问题。如果信号延迟过高，可能会导致车辆对周围环境的感知和响应出现延迟，从而影响行车安全。

(4) 物理线路布局限制

传统物理载体中线路布局对信号串扰产生了显著影响，为减少串扰而增加的设计复杂度和成本也不容忽视。在高密度的芯片封装和电路板布线中，线路之间的距离往往非常接近，这使得信号串扰的问题更加突出。当多个信号在相邻的传输线路中同时传输时，由于电磁感应的作用，一个信号的电磁场会影响到相邻传输线路中的信号，导致信号失真和误码率增加。串扰的严重程度与传输线路的布局、信号的频率以及传输线路之间的距离等因素密切相关。密集的传输线路布局和高频信号更容易产生串扰。在智能座舱芯片中，由于需要传输大量的多媒体数据，信号频率较高，且芯片内部的线路布局较为密集，这使得信号串扰的问题尤为严重。为了减少信号串扰，工程师们需要采取一系列复杂的设计措施，这无疑增加了设计的复杂度和成本。在电路板设计中，需要合理规划线路的布局，避免相邻线路之间的平行布线，增加线路之间的距离，以减少电磁感应的影响。还可以采用屏蔽技术，如在传输线路周围添加屏蔽层，将信号与外界的电磁干扰隔离开来。这些措施不仅需要耗费大量的时间和精力进行设计和优化，还会增加电路板的面积和成本。采用屏蔽技术可能会使电路板的面积增加，同时增加了材料成本和制造工艺的难度。在芯片封装中，也需要采用特殊的封装结构和材料，以减少信号串扰。这些措施都使得传统物理载体在实现高速、高密度互连时面临着巨大的挑战。

3.1.3 车用芯粒接口与通信的核心标准需求

车用芯粒的设计和开发面临着严峻的挑战。车用芯粒需要在功能安全、可靠性、电磁兼容性等方面达到极高的标准，以应对汽车长久的使用寿命和复杂的行驶环境。因此，开发定制化协议和支持未来升级的接口变得尤为重要。此外，接口还需要具备良好的抗震动和冲击能力，高抗电磁干扰能力，以及严苛的耐久性测试。错误检测和纠正机制的完善也至关重要，以避免数据传输错误导致的安全风险。同时，多芯粒集成带来的热密度问题需要通过创新热管理技术来解决，如微流道冷却。

(1) 功能安全与可靠性需求

车规级芯片在功能安全、可靠性、电磁兼容性等方面遵循着极为严格的标准，其中 ISO 26262 标准在功能安全领域具有权威性。该标准为汽车电子电气系统的功能安全提供了全面的指导，从概念阶段到生产、售后等全生命周期都制定了严格的要求。汽车的设计寿命通常在 15 年左右，行驶里程可达 20 万公里，这就要求车规级接口在长期使用过程中能够保持稳定可靠的性能。现有互连标准（如 UCIe）主要面向消费电子，缺乏针对功能安全（ISO 26262 ASIL-D）和长寿命周期的适配，需开发定制化协议并支持未来升级。

(2) 车用芯粒接口须具备抗振动和冲击能力需求

为应对汽车行驶过程中的各种颠簸和震动。汽车在行驶过程中会受到来自路面的各种震动和冲击，这些外力可能会导致接口的物理连接松动或损坏，从而影响数据传输的稳定性。为了提高接口的抗振动和冲击能力，在设计时可以采用特殊的封装和固定方式，如使用加固的连接器和抗震支架，确保接口在恶劣的机械环境下仍能正常工作。

(3) 车用芯粒接口须具备高抗电磁干扰能力需求

汽车内部是一个复杂的电磁环境，存在来自发动机系统、无线电频段和其他电子设备的干扰。这些电磁干扰可能会对接口传输的信号产生干扰，导致信号失真、误码率增加，从而影响系统的正常运行。为了提高接口的抗电磁干扰能力，可以采用屏蔽和滤波等技术。在接口电路中添加屏蔽层，将接口与外界的电磁干扰隔离开来；使用滤波器对信号进行处理，去除信号中的干扰成分，保证信号的纯净度。

(4) 车用芯粒接口需通过严苛的耐久性测试需求

芯粒封装引入的复杂互连结构可能增加失效风险，先进封装中硅通孔（TSV）的热膨胀系数差异因热应力可能导致长期使用后连接失效，需通过材料创新（如铜混合键合）和冗余设计提升可靠性和耐久性，进行如温度循环、振动、EMC 等的失效控制。

(5) 车用芯粒接口需严格的错误检测和纠正机制需求

在辅助驾驶系统中，传感器与计算芯片之间的接口一旦出现数据传输错误或中断，可能导致车辆对周围环境的感知出现偏差，进而引发严重的交通事故。因

此，车规级接口需要具备完善的错误检测和纠正机制，能够实时监测数据传输的准确性，一旦发现错误，立即采取纠正措施，如重传数据或切换到备用通道，以保证系统的安全运行。

（6）车用芯粒接口需高要求的功耗和热管理需求

多芯粒集成会加剧热密度分布不均问题，尤其在车载环境下，高温工况可能导致性能降级或寿命缩短。传统封装散热方案（如散热片）难以满足晶圆级集成系统的需求，需开发新型热管理技术（如微流道冷却）。

3.2 车用芯粒环境与可靠性标准化需求

车载芯片需适应振动、高低温、电磁干扰等严苛环境，标准化测试成为保障安全性的关键。汽车芯片环境与可靠性标准如国内参考标准：GB/T 4937、IEC 60749、IEC 62880 等半导体器件环境可靠性试验方法系列；国际参考标准：ISO16750 系列：道路车辆电气及电子设备的环境条件和试验、机械负载等，AEC 国际汽车电子协会车用到导体测试系列标准，SAE 汽车电气部件环境试验相关标准；JEDEC 微电子环境、封装等可靠性标准等，国内国际的标准还没有芯粒芯片多 die 堆叠特点的环境与可靠性标准规范。

芯粒在封装尺寸、功耗和单芯片有比较大的差异，在湿度等级、预处理、功能验证、环境温度、机械应力测试标准上和传统标准有一些差异，传统的加速模型是否适用需要进一步论证分析，既要保证测试充分，又要保证不过度测试而损坏芯片；die 级别的测试在合封之前，测试需求明确测试芯粒本身，还是芯粒系统；芯粒在 CP 阶段需要可靠性测试，尤其芯片的良率不高的情况下，CP 阶段可靠性风险非常高。

综上所述，需要深入研讨和制定基于汽车应用场景的芯粒环境与可靠性要求及相应测试方法标准。

3.3 车用芯粒电磁兼容标准化需求

汽车用芯粒要求具有电磁兼容性（Electro-Magnetic Compatibility, EMC），即要求芯粒芯片在整车系统的电磁环境中能够正常工作的同时不会对环境其他组件造成无法承受的电磁干扰，保证在有限空间、时间和频谱资源等条件下，

芯片与其他用电设备及广义上的生物体可以共存并不致引起设备工作异常。从两个方面规范芯粒芯片的电磁兼容性：一方面是芯片在正常运行过程中对所在环境产生的电磁干扰不能超过一定的限值，即电磁干扰性（ElectroMagnetic Interference, EMI）；另一方面是芯片对所在环境中的电磁干扰具有一定程度的抗扰能力，即抗扰度（ElectroMagnetic Susceptibility, EMS）。

因此，应对汽车芯粒电磁干扰性和电磁抗扰度进行规范，制定相应标准，包括汽车用芯粒电磁干扰要求及测试方法、汽车用芯粒电磁抗扰度要求及测试方法。其中，汽车用芯粒电磁干扰要求及测试方法涉及 TEM 小室法、GTEM 小室法、带状线法、1 Ω /150 Ω 直接耦合法；汽车用芯粒电磁抗扰度要求及测试方法涉及 TEM 小室法、GTEM 小室法、DIP 法、带状线法、脉冲抗扰度、系统级 ESD。

目前，已发布汽车用芯粒电磁兼容相关标准包括 GB/T 44937-2024《集成电路电磁发射测量》系列标准、GB/T 42968-2024《集成电路电磁抗扰度测量》系列标准、GB/T 43034-2024《集成电路 脉冲抗扰度测量》、IEC 61967 “Integrated circuits. Measurement of electromagnetic emissions”、IEC 62132 “Integrated circuits - Measurement of electromagnetic immunity”、IEC 62215 “Integrated circuits - Measurement of impulse immunity”等。尚无针对汽车用芯粒的电磁兼容标准。

综上所述，需要在现有集成电路电磁兼容标准基础上，制定基于汽车应用场景的芯粒电磁兼容要求及相应测试方法标准。

3.4 车用芯粒功能安全标准化需求

为确保车用芯粒在复杂且严苛的汽车环境中能够安全、可靠地运行，有必要对车用芯粒功能安全标准化。GB/T 34590《道路车辆 功能安全》标准第 11 部分《半导体应用指南》虽然标准未直接提及芯粒，但其对半导体模块化设计的要求可延伸至芯粒场景，例如：芯粒间通信需满足功能安全标准（如 GB/T 34590），确保数据完整性、时序确定性；不同工艺/供应商的芯粒需独立认证，并在系统级验证组合安全性；通过硬件隔离防止故障传播等。

除了确保多芯粒系统符合 GB/T 34590《道路车辆 功能安全》标准之外，还应明确地对芯粒和芯粒接口功能安全进行标准化。

目前芯粒和芯粒接口功能安全面临如下的挑战。

- 1) 复杂性：多芯粒系统的接口设计复杂，需平衡性能、功耗和安全性。
- 2) 信号完整性：高频信号传输易受噪声和干扰影响，需优化物理层设计。
- 3) 标准化：目前各种芯粒接口标准仍在发展中，功能安全的具体实现可能因厂商而异。
- 4) 成本：冗余设计和错误检测机制会增加硬件和软件成本。
- 5) FMEDA 量化：芯粒的模块化、异构集成和跨工艺特性对芯粒的 FMEDA 量化带来额外挑战，需要重点考虑芯粒间互连失效的量化分析。

将功能安全分解到芯粒设计中是一个复杂但关键的过程。芯粒的模块化特性既带来了灵活性，也引入了新的安全挑战（如跨芯粒通信、异构验证等）。以下表 3.4.1 是车用芯粒功能安全标准化应重点关注以下实现方法。

表 3.4.1 车用芯粒功能安全标准化关注重点

类别	解决方案	典型实现方法
芯粒架构的安全分解	系统级安全目标分解	根据 GB/T 34590，将系统级安全目标（如避免意外加速）分解到芯粒层级。
	ASIL 等级映射	每个芯粒根据其功能分配适当的 ASIL 等级（如 ASIL A-D）。
	安全功能分区	将不同安全功能分配到不同芯粒。
芯粒间安全通信	安全互连协议	错误检测与纠正：在芯粒间互连（如 UCIe、BoW）中集成 ECC、CRC、重传机制。 时序安全：确保时间确定性以满足实时性要求。 身份认证：防止恶意芯粒接入。
	冗余与多样性	冗余通信路径：双通道通信（如主备路径）或投票机制。 异构设计：不同芯粒采用不同实现（如双核锁步 vs. 多样化软件）。
芯粒级安全机制	硬件安全特性	故障检测：内置自检（BIST）、看门狗定时器、电压/频率监控。 容错设计：锁步核（Lockstep）、冗余执行单元。 隔离机制：物理隔离（如 NoC 防火墙）、逻辑隔离（内存保护单元 MPU）。

	安全监控	运行时监控：芯粒内嵌入安全监控模块。 跨芯粒协调：中央安全管理器协调多个芯粒的故障响应。
测试分析与认证	独立分析与验证	FMEDA（失效模式、影响及诊断分析）：针对每个芯粒分析单点故障（SPF）和潜在故障（LF）。 故障注入测试：模拟芯粒间通信错误或硬件故障。
	组合认证	芯粒级认证：单个芯粒通过 GB/T 34590。 系统级认证：验证芯粒组合后的整体安全性（尤其关注互连和依赖关系）。
供应链与生命周期管理	可信供应链	确保芯粒来源可靠（如硬件信任锚、PUF 身份标识）。
	可追溯性	记录每个芯粒的安全属性（如 ASIL 等级、认证状态）。
	在线更新	支持安全固件更新（如安全启动、OTA 签名验证）。
工具与标准支持	工具链兼容性	EDA 工具需支持多芯粒安全分析。
	标准协同	结合 GB/T 34590。

如果在芯粒设计中实施功能安全机制的仿真验证，需要 EDA 工具链在多物理域、跨层级、异构集成等维度进行协同分析，面临的核心挑战有：

- 1) 跨 Die 交互安全：信号完整性/电源噪声引发的安全状态机跳变。
- 2) 异构验证兼容：数字/模拟/光电混合仿真的时序对齐。
- 3) 故障传播分析：单个芯粒失效在 2.5D/3D 系统中的级联影响。
- 4) 国产化：核心技术自主可控，防止被禁用。

仿真层面的关键技术实现主要有：

- 1) 安全关键信号建模；
- 2) 分层故障注入仿真；
- 3) 动态安全监控机制。

通过上述方法，可在 EDA 工具链中构建完整的芯粒功能安全仿真验证体系，满足 GB/T 34590 等标准要求。

综上所述，车用芯粒功能安全标准化需求涉及多个方面，为实现这些需求，不仅需要实现芯粒架构的安全分解、芯粒间安全通信和芯粒级安全机制，还要强化测试分析与认证、加强供应链与生命周期管理、推动工具与标准支持等方面的工作。通过这些措施的实施，可以确保车用芯粒在复杂且严苛的汽车环境中能够

安全、可靠地运行，为汽车行业的可持续发展提供有力保障。

3.5 车用芯粒信息安全标准化需求

为确保车用芯粒能够抵御外部攻击，保护汽车系统的数据安全性和功能完整性，有必要对车用芯粒信息安全标准化。除了确保多芯粒系统符合《汽车芯片信息安全技术规范》中对芯片的信息安全认证标准之外，还应额外对芯粒和芯粒接口信息安全进行标准化。

目前芯粒和芯粒接口信息安全面临如下的挑战。

1) 性能开销：加密和认证机制会增加延迟和功耗，需在安全性和性能之间权衡。

2) 标准化：目前芯粒接口标准仍在发展中，信息安全的具体实现可能因厂商而异。

3) 复杂性：多芯粒系统的接口设计复杂，需综合考虑功能安全 and 信息安全。

4) 攻击面扩大：芯粒接口的增加可能引入新的攻击面，需全面评估安全风险。

5) 芯粒安全分级：根据芯粒种类和零部件信息安全需求对其进行安全分级。

其中，针对芯粒接口的信息安全攻防技术主要有以下几大类如表 3.5.1 所示。

表 3.5.1 车用芯粒 Die-to-Die 攻防技术

威胁类别	攻击手段	防护技术
总线窃听	通过探针拦截或修改芯粒之间通信数据。	加密与认证：采用 AES 等算法加密芯粒间数据流，采用 SHA3 等算法确保数据完整性。
物理侵入	通过聚焦离子束（FIB）直接修改互连线路或插入探测点，或利用激光故障注入诱发通信错误。	加密与认证：采用 AES 等算法加密芯粒间数据流，采用 SHA3 等算法确保数据完整性。
硬件木马	在硅中介层中植入木马电路，窃取或篡改跨芯粒通信数据	木马检测：使用环形振荡器来检测木马触发时的异常。

将信息安全需求分解到芯粒设计中是一个复杂但关键的过程。首先参考《汽车芯片信息安全技术规范》，将零部件信息安全需求细化分解到芯粒层级，并通

过多种车用芯粒的信息安全功能实现。再根据车用芯粒信息安全攻击危害性和攻击易实施性两个方面对车用芯粒的信息安全要求进行分级。根据分级结果，制定每个车用芯粒的信息安全功能技术要求和试验方法。

以下表 3.5.2 是车用芯粒信息安全标准化应重点关注的信息安全功能技术要求和试验方法。

表 3.5.2 车用芯粒信息安全标准化关注重点

信息安全功能	技术要求
密钥保护	密钥生成的一般要求；密钥存储的一般要求，包括长期密钥保护、临时密钥保护、对称密钥的安全存储、非对称密钥的安全存储； 密钥使用的一般要求，包括密钥访问控制、密钥建立、密钥派生、密钥导入与更新、密钥导出；密钥销毁的一般要求；
密码算法支持	密码算法的一般要求；
随机数生成	随机数生成的一般要求，包括真随机数和伪随机数；
关键安全参数保护	关键安全参数保护的一般要求；
固件更新支持	固件更新的一般要求；
权限控制	权限控制的一般要求，包括存储访问控制、接口授权访问；
安全运行环境支持	安全运行环境的一般要求，包括安全运行环境的固件、可信应用；
自测试	自测试的一般要求，包括自测试记录、自测试执行；
物理防护	物理防护的一般要求，包括侧信道攻击防护、故障注入攻击防护、反向工程防护；
安全启动机制	安全启动机制的一般要求；
软件攻击保护机制	软件攻击保护机制的一般要求；
个人信息保护	个人信息保护的一般要求；
漏洞管理	漏洞管理的一般要求；
安全生命周期管理机制	安全生命周期管理机制的一般要求。

综上所述，车用芯粒信息安全标准化需求涉及多个方面，包括车用芯粒信息安全需求分析方法、车用芯粒信息安全需求与安全功能的映射关系、车用芯粒信息安全功能技术要求以及试验方法等。为实现这些需求，需要制定和完善信息安全标准体系、加强技术研发和创新、推动认证和评估工作、加强国际合作与交流

以及持续更新和优化标准等方面的工作。通过这些措施的实施，可以确保车用芯粒在信息安全方面达到高水平，为汽车行业的可持续发展提供有力保障。

3.6 车用芯粒软件设计标准化需求

3.6.1 软硬件接口寄存器访问标准化需求

传统芯片中，寄存器访问通常依赖固定的物理地址映射和静态头文件定义方式，开发人员基于手工编写的寄存器地址宏或结构体访问硬件寄存器。然而在芯粒系统中，由于多个芯粒分别封装、异地部署，寄存器分布呈现出分布式、动态化的特点，传统方式会出现下面 3 个需要解决的挑战。

1.动态地址解析。在芯粒系统中，寄存器的地址往往在运行时才确定，而不是像传统单芯片那样固定在编译器。每个芯粒上的寄存器可能通过固件或互连桥动态分配具体地址，所以程序需要在运行时查询或解析这些地址才能正确访问。这就造成了动态地址解析的困难，传统依赖静态头文件和宏定义的方法无法适用。

2.跨芯粒访问。当程序需要访问不在本芯粒上的寄存器时，数据必须通过互连总线、桥或网络传输到目标芯粒。不同互连路径可能有访问限制、延迟或对齐要求，如果直接按本地访问方式操作远端寄存器，就容易出错或者导致数据损坏，这就是跨芯粒访问的困难所在。

3.一致性管理的需求。多芯粒系统中，每个芯粒可能有自己的缓存或局部状态，如果各自独立更新寄存器，可能导致不同芯粒看到的寄存器值不一致。传统方法没有提供跨芯粒数据同步机制，如果不加管理，就会出现逻辑错误或不可预测的行为，这就是一致性管理面临的挑战。

为了应对动态地址解析的困难，芯粒系统需要建立统一的寄存器描述标准，例如基于现有 IP-XACT（IEEE 1685）格式进行扩展，形成一种标准化、机器可读的寄存器组描述语言。

通过这种标准，各芯粒供应商可以提供结构化的寄存器映射文件，系统集成阶段可以通过工具链自动生成访问代码。在程序运行时，这些工具生成的代码能够根据元数据动态解析寄存器的实际物理地址，从而消除了手工维护静态头文件的需求，保证了软件在不同芯粒组合或部署情况下都能正确访问寄存器，大大降

低了运行期错误的风险。

对于跨芯粒访问问题，统一的寄存器描述标准可以提供一致的接口抽象。寄存器描述不仅包含地址信息，还可以标注访问属性、互连路径和约束条件，工具链生成的访问接口会自动处理跨芯粒访问的细节，如桥路由、对齐、事务大小等。开发者无需关心底层互连复杂性，就能以统一方式访问远端芯粒寄存器，这显著降低了跨芯粒访问的出错概率，并简化了驱动和固件的开发逻辑。

在一致性管理方面，标准化的寄存器描述有助于实现跨芯粒的数据同步和状态一致性。通过在描述文件中定义寄存器的访问类型、缓存策略和原子性要求，工具生成的访问代码可以在访问前自动插入必要的同步或屏障操作，确保多芯粒之间读取到的寄存器值保持一致。这不仅提高了系统的可靠性，也便于后续的调试和维护，因为一致性策略是自动化管理的，而不依赖开发者手动处理。

综上所述，制定统一的寄存器描述标准，不仅解决了动态地址解析、跨芯粒访问和一致性管理的核心问题，还提升了软件的可维护性和系统的可扩展性。标准化描述和自动化生成的代码，使得芯粒系统的集成更高效、更可靠，同时降低了维护成本和潜在风险，为大规模、异地开发和部署的芯粒系统奠定了坚实的基础。

3.6.2 软硬件接口中断标准化需求

在多芯粒系统架构中，中断优先级与路由机制的设计直接影响系统的响应性能与容错能力。为支持芯粒间高效协作，软件需基于 AUTOSAR OS 标准建立统一的中断管理模型，定义跨芯粒中断的优先级规则与路由路径。每个芯粒应具备本地中断控制器，并通过一个集中式或分布式的中断互联机制（如 Inter-Chip Interrupt Router）实现中断源到目标处理单元的映射与调度。中断的配置应遵循 AUTOSAR 中 Category 1/2 中断划分、嵌套使能、服务优先级等原则，确保软件具备结构化且可扩展的中断管理能力。

为满足 ASIL-D 等级的安全应用场景（如制动控制、电机保护或冗余通信系统），中断嵌套处理机制必须支持高速切入，确保高优先级中断能够在极短延迟内响应系统状态变化。为此，系统需实现硬件辅助的中断优先级判断与抢占机制，配合操作系统中的快速上下文切换路径，保障嵌套中断延迟控制在 $\leq 200\text{ns}$ 范

围内。这一要求推动软件与中断控制器（如 GIC 或自定义多核中断模块）深度耦合，在驱动层实现最小化的中断服务入口及快速中断分发路径。

此外，在芯粒间存在主从控制、冗余备份或负载迁移机制的系统中，还必须支持动态中断重映射能力。一旦某个芯粒因故障脱离系统或进行角色切换，原本由其接收和处理的中断需要在不中断业务运行的前提下，动态迁移至其他芯粒的中断控制器并维持优先级一致性。这种机制对于提升系统鲁棒性、实现故障恢复和维持实时控制路径至关重要。设计中断映射策略时，应结合 AUTOSAR OS 提供的中断管理接口和系统状态感知机制，在系统运行时完成对中断路由表的更新与同步，构建出具备自适应能力的芯粒间中断子系统。

3.6.3 操作系统抽象层标准化需求

为适配车载领域多芯粒系统的异构性与复杂性，系统软件亟需构建统一的硬件抽象层（HAL, Hardware Abstraction Layer），以屏蔽底层芯粒差异性并提升软件的可移植性和复用性。通过定义标准化的访问接口，软件可以以统一方式访问芯粒资源，如寄存器、中断控制器、时钟控制和 I/O 接口等，无需针对每颗芯粒重复适配底层驱动逻辑。这样不仅可以兼容多种车载操作系统（如 AUTOSAR OS、Linux RT、QNX 等），还能够加速新平台集成，减少平台差异带来的开发负担，提升整体软件架构的模块化程度。

多芯粒架构通常具有计算资源和通信资源的动态可扩展能力，因此需要明确动态资源管理规范，以实现运行时对芯粒间资源（包括算力、内存、带宽）的智能分配与回收。这一机制尤其关键在于支持混合关键性任务调度场景，如将安全相关任务优先分配至高可靠核心，而将非关键性应用动态迁移到负载较低的芯粒。合理的资源管理策略不仅提升了芯粒间协同效率，还能防止资源竞争引发的实时性退化，是构建高性能、高可靠车载平台的基础。

此外，为满足功能安全和系统运维要求，每颗芯粒都应提供标准化的安全诊断接口。这些接口需支持对芯粒运行状态的持续监测，例如温度、电压、误码率等硬件健康指标，同时记录关键安全事件的触发信息，如双核锁步机制下的错误次数、ECC 校验失败统计、看门狗超时等。这些数据可被系统诊断模块采集，用于故障预测、异常隔离与系统自恢复策略执行，满足 GB/T 34590 等标准下对

安全监控的可证性要求。统一的诊断接口设计也是实现整车级健康管理（Vehicle Health Management, VHM）的核心支撑之一。

在多芯粒车载系统中一个统一的硬件抽象层（HAL）标准总结如下。该标准的核心目标是屏蔽不同芯粒的差异性，使上层软件能够以统一接口访问底层硬件资源，从而提升可移植性和复用性。

具体来说，HAL 标准应包含以下几个方面：

1.统一的资源访问接口：规定寄存器、中断控制器、时钟控制、I/O 接口等基础资源的标准化访问方式，避免每颗芯粒重复适配驱动逻辑，并兼容多种车载操作系统（如 AUTOSAR OS、Linux RT、QNX）。

2.动态资源管理规范：支持运行时对算力、内存、带宽等资源的智能分配和回收，确保在混合关键性任务场景下能够合理调度，例如优先保障安全相关任务在高可靠核心上运行。

3.标准化的安全诊断接口：要求芯粒提供统一的监测和诊断机制，包括温度、电压、误码率等健康指标，以及 ECC 错误、看门狗超时等关键安全事件。这样可满足 ISO 26262、SOTIF 等功能安全标准，并为整车级健康管理（VHM）提供数据支持。

通过这样的 HAL 标准，芯粒系统能够在异构环境中实现统一访问、动态扩展和安全可证，既降低了平台集成与维护成本，又为高性能、高可靠的车载平台奠定了统一的体系基础。

3.6.4 运行多操作系统需求

为满足车载及智能计算场景的复杂需求，芯粒系统需要在设计之初就考虑对多操作系统的兼容性。不同车载平台可能选用 AUTOSAR OS、Linux RT、QNX 等操作系统，同时还逐渐引入专用的 AI 操作系统或运行环境。如果缺乏统一的标准，软件就必须针对每一种操作系统重复适配底层逻辑，导致开发成本高昂、平台迁移困难。通过在芯粒系统中定义标准化的接口与描述规范，可以让上层应用和中间件以一致的方式访问底层资源，从而在多个操作系统之间实现平滑移植。这不仅显著降低了多平台开发的重复工作，还能加速新系统的集成与验证，提升整个软件架构的可扩展性。

在 AI 应用快速发展的背景下，芯粒系统还需特别关注对 AI 操作系统和推理框架的支持。通过建立统一的算力调度和数据流接口，芯粒能够为不同的 AI Runtime（如 TensorRT、ONNX Runtime、AscendCL 等）提供一致的服务，避免因硬件差异和操作系统差异而反复修改应用逻辑。这样一来，AI 模型和任务就可以灵活迁移到不同的芯粒资源上执行，既提升了开发效率，也增强了系统对未来新平台和新算法的适应能力。

全国汽车标准化技术委员会
汽车芯片标准化研究工作组

四、车用芯粒标准化路线图建议

4.1 车用芯粒总体标准化路线图建议

芯粒技术正成为重塑半导体竞争格局的关键力量。随着通用芯粒互连联盟的成立，行业开始向统一互连协议迈进，解决接口碎片化问题并推动跨平台兼容。然而，其大规模应用仍需克服标准化、测试等关键挑战。在汽车领域，芯粒技术通过硬件模块化升级实现芯片产品的换代升级，并通过不同车用芯粒的组合适应不同车型定位。芯粒技术还可通过灵活组合算力单元满足定制化需求。然而，芯粒技术在汽车电子领域的推广面临标准化缺失的瓶颈。尽管模块化设计解决了算力扩展与成本优化的矛盾，但接口碎片化、互操作性不足及车规适配难题成为制约其大规模落地的关键障碍。

当前车用芯粒互联协议尚未形成统一标准，不同厂商采用专有接口或不同版本的协议，导致芯粒间通信存在兼容性壁垒。而现有芯粒技术多源自数据中心领域，缺乏车规级验证及测试。此外，芯粒间冗余校验、故障隔离机制的标准化缺失，导致功能安全认证成本陡增。因而，建议车用芯粒从接口与通信、环境与可靠性标准、电磁兼容标准、功能安全标准和信息安全标准、以及软件设计进行标准化。如图 4.1.1 所示为拟定的车用芯粒标准体系图。

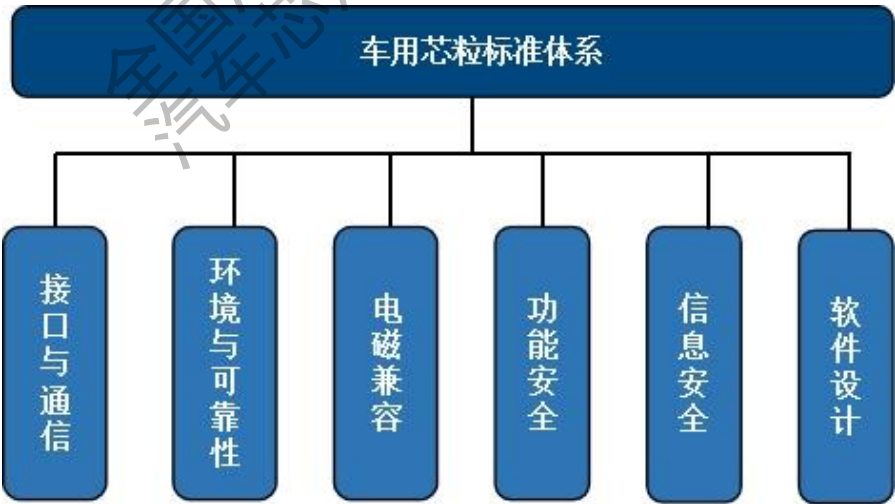


图 4.1.1 车用芯粒标准体系图

车用芯粒生态涉及 EDA 工具、封装厂商、IP 供应商及车企的多方协作，通过跨行业协作及车规专用标准的制定，方能突破产业化瓶颈，推动智能汽车向模

块化、可进化的下一代架构演进。标准化车用芯粒重构汽车芯片产业链的分工模式，产业链可解耦为“芯粒设计-封装集成-系统验证”三层分工，使芯片设计厂商能够复用芯粒 IP，降低研发投入，推动测试方法统一，降低测试成本。

4.2 关键分领域标准化路线图建议

4.2.1 车用芯粒接口与通信标准化建议

车用芯粒接口与通信标准化面临多重技术瓶颈。高速通信与信号完整性矛盾突出：辅助驾驶场景要求芯粒间通信带宽但传统并行接口（如 HBM）在车规级 EMC 限制下易受电磁干扰，导致误码率激增。其次，热管理与可靠性冲突：3D 堆叠封装虽提升集成度，但芯粒间热耦合效应（如台积电 CoWoS 封装热阻达 0.8℃/W）加剧局部高温风险，难以满足 AEC-Q100 规定的-40℃~150℃工作范围。此外，功能安全验证复杂度高：ISO 26262 要求芯粒间通信协议需支持端到端 CRC 校验及冗余链路切换，但现有标准仅定义基础错误检测机制，车企需定制开发安全层协议。基于车用芯粒接口与通信的特性以及场景下的特殊要求，给出关键领域标准化的建议。

（1）对车用芯粒接口与通信电学参数要求如表 4.2.1。

表 4.2.1 车用芯粒接口与通信要求

参数	建议要求
数据率	8GT/s, 16GT/, 32GT/s, 64GT/s, 128GT/s
物理层传输延时	≤6ns
可传输距离	≤50mm
静电防护（充电设备模型）	≥100V

（2）车用芯粒接口协议要求

为满足车-车、车-路、车-人、车-云等通信场景下车载网络面临的庞杂、动态、实时、多模态通信挑战，芯粒接口在统一硬件架构下，须具备可重构能力，接口可软件定义为多种协议（如 PCIe、CXL、以太网等），适应不同车载场景（如行车时优先低延迟，停车时优先带宽），既能兼容已有的车用接口协议，又可满足后续的芯粒接口统一标准的发展需求。

（3）异构芯粒高密度集成要求

芯粒通过标准化接口可实现异构芯片（CPU、GPU、AI 加速器、传感器接口等）的灵活组合，可有效降低开发周期，为了突破传统工程技术路线的瓶颈，需以晶圆基板为物理载体，借助晶圆级集成实现车载系统的超高密度、超短距离互连，集成多种类型的芯粒，减少车载系统体积和信号延迟，提升车载计算等模块的性能（如算力密度）和能效。

（4）车用接口芯粒功能安全设计要求

根据车用场景下的芯粒接口与通信功能安全要求，对于接口与通信标准的功能安全相关设计建议如下。

存储保护：在标准的逻辑电路中，存在基于 sram 的存储，在存储上须加入 ECC 校验保护，确保存储的数据保护，实现 1bit 纠错，2bit 以上检测出错误，检测出无法纠正的错误时上报预警，从而以 ECC 为安全机制实现存储从单点失效，转换为双点失效，同时对 ECC 安全机制进行逻辑 BIST，已检测到 ECC 逻辑的失效。

端到端总线保护：通过一端 CRC 计算对数据生成冗余位，当数据传输到对端后将数据进行 CRC 校验，从而避免数据传输中的单点失效，囊括数据在传输过程中的失效问题。同时对 CRC 计算与校验逻辑进行 BIST 检测，对 CRC 计算与校验逻辑进行失效检测。

预警上报：对于影响 D2D 传输数据正确和稳定性的事件发生均需要进行预警上报，包括但不限于数据 ECC，CRC 校验出错，FIFO 中空满标志，PLL 失锁，电气物理层 PLL 失锁，信号探测模块 signal_detect 在传输过程中检测不到信号能量波动，CDR 失锁等。以保证在传输数据过程中发生不稳定事件后进行预警，以便上一层做出最后的决策。

存储器自检：对嵌入式存储器需要采用内建自测试结构，目标是在车辆使用空闲时，能够启动存储器测试；且使用尽可能少的测试管脚，存储器自测试结构需要内置激励产生单元，来完成激励输入，检测输出。

逻辑自测试：车辆使用空闲时刻的逻辑自测试。对于片上逻辑需要加入自测试结构；启动逻辑自测试后，伪随机图形产生器产生测试图形，经过内置有线性反馈移位寄存器的解压缩逻辑解压后灌入扫描链中，通过一系列移位，捕获，再

移位操作，抓取电路反馈值并且与期望值相比，判断电路是否存在故障。

信道冗余以及重映射设计：为了提高可靠性，以及满足车规需求，在信道组之外，需要添加冗余信道。当某一信道发生故障时，用冗余信道去替换故障信道，这一冗余设计将提升良率和可靠性。

可测性设计：车用 D2D 接口需要考虑多 die 互联以后的可测性，例如通过 die 之间互发特殊序列（PRBS31）来判断多 die 互连后的数据通路是否正常，以此进行封装后的 FT 测试，或者车辆空闲时的自检测试；

关键逻辑的双核锁步设计：对关键逻辑，例如状态机控制，进行双核锁步设计，以确保诊断这部分关键逻辑的错误；

关键信号的监控：对车用芯粒接口的关键信号进行监控，例如监控时钟复位的正确性，发生异常后及时上报错误预警。

（5）车用接口芯粒封装的要求

根据工艺成熟度、可靠性、成本、以及供应链韧性等方面考虑，建议采用 2D MCM 封装的芯粒路线。在该封装路线下需匹配 bump pitch 等于 153um 的 Flip-Chip(FC)封装形式。

基于如上的封装策略，封装信号走线参照规范建议如表 4.2.2。

表 4.2.2 车用芯粒接口封装信号走线建议表

封装特性	最大值
走线长度最大值	50mm
走线阻抗最大值	110 Ω
插入损耗最大值	3dB（32GT/s）
回波损耗最大值	-10dB（32GT/s）
差模隔离度最大值	-30dB（32GT/s）
共模隔离度最大值	-15dB（32GT/s）

4.2.2 车用芯粒环境与可靠性标准化建议

根据 3.2 节针对车用芯粒环境与可靠性标准需求的分析，在国内国际环境与可靠性测试标准的基础上，研究制定基于汽车应用场景的芯粒环境与可靠性标准。

标准建议主要包括以下几个方面：

（1） 环境可靠性基本要求

根据汽车用芯粒的应用场景，标准需要对工作环境温度等级，潮湿敏感等级提出要求。

（2） 加速环境应力试验要求

根据汽车用芯粒的应用场景，标准需要对预处理的时间、流程等，加速模型包括温度、电压、测试时长、升降温速率等提出要求。

（3） 加速寿命模拟试验要求

根据汽车用芯粒的应用场景，标准需采用合适的寿命分布模型，对温度、测试时长、电压以及测试过程中阶段性功能检查等提出要求。

（4） 封装完整性试验要求

根据汽车用芯粒的应用场景，标准需根据不同 die 和基板的特点，对锡球可焊性、锡球剪切力、内部不同 die 的剪切力、物理尺寸测量等提出要求。

（5） 晶圆工艺可靠性试验要求

根据汽车用芯粒的应用场景，标准需根据不同 die 之间的互联的特点，对微电子的失效机理如：电迁移、电介质击穿、热载流子注入、负偏压温度不稳定、应力迁移等试验提出要求。

（6） 电性能验证试验要求

根据汽车用芯粒的应用场景，标准需明确车用芯粒的整体电气输出、ESD、闩锁、电性参数分布、软失效等提出要求。

（7） 缺陷筛选试验要求

根据汽车用芯粒的应用场景，标准需采用合适的分布模型，对样本数量、测试周期等提出要求。

（8） 板级温度循环试验要求

根据汽车用芯粒的应用场景，标准需采用合适的板级设计，对温度、测试循环次数等提出要求。

（9） 可靠性加速模型的优化

环境适应性的测试需确保芯粒在极端环境（如高温、低温、湿度、振动）下保持性能，明确测试环境条件和时间。测试方法标准化需涵盖内建自测试（BIST）的设计指南、测试压缩技术的算法规范以及自动测试向量生成（ATPG）的流程

标准。

4.2.3 车用芯粒电磁兼容标准化建议

根据 3.3 节针对车用芯粒电磁兼容标准需求的分析，已发布相关电磁兼容标准均为集成电路电磁兼容通用试验方法类标准，建议在此基础上制定汽车应用场景的芯粒电磁兼容要求及相应测试方法标准。该标准建议主要包括以下几个方面：

（1）单个芯粒和模块整体的电磁兼容性能要求

针对 ESD 试验，由于车用芯粒每个 IP 的工艺不同，ESD 性能会存在差异，建议在 IP 选型阶段和模块整体均提出要求。限于目前的试验条件和试验成本，建议除 ESD 外，仅对模块整体的电磁兼容性能提出要求，包括发射 EMI 和抗扰度 EMS 的要求。

（2）电磁兼容试验方法

根据现有成熟的通用集成电路电磁兼容试验方法 GB/T 44937、GB/T 42968、GB/T 43034、IEC 61967、IEC 62132、IEC 62215 等，及车辆集成电路电磁兼容试验通用规范，其中的辐射发射、传导发射、辐射抗扰、传导抗扰、EFT、ESD 的六项试验方法适用于汽车用芯粒。

其中辐射类试验考察模块整体的性能，传导发射、DPI、EFT、ESD 需要根据车载应用场景，选择典型的受试引脚。

电气特性测试需确保芯粒在电气环境中的稳定性和抗干扰能力，包括 ESD 测试、闩锁效应分析和电磁兼容性测试，明确测试设备、方法和合格标准。

（3）电磁兼容与可靠性结合的要求和试验方法

根据前面的分析，由于多芯粒集成，每个芯粒的制造、封装工艺不同，由于温度等引起的老化速度可能不一样，会造成芯粒的整体电磁特性造成变化，这是与传统的单芯片的 EMC 特性的重要差异，建议进行几款典型芯粒老化前后的电磁兼容试验验证的数据收集，如果经验证电磁性能差异不大，可不在标准中规定老化后再进行电磁兼容试验。如果差异较大，建议标准对老化后的电磁兼容性能也提出要求，并在可靠性老化试验后，进行部分指标变化较大的电磁兼容试验。

电磁兼容作为汽车用芯粒的重要性能，且目前尚无标准规范基于汽车应用场景的电磁兼容要求及特定试验方法，故建议制定汽车用芯粒电磁兼容标准，重点

对单个芯粒和模块整体的电磁兼容性能要求、电磁兼容试验方法、可靠性老化试验后电磁兼容要求及试验方法进行规范。汽车用芯粒电磁兼容性作为其基础通用性能，建议在制定汽车芯粒产品标准前先制定电磁兼容行业标准，以便适用于各类汽车芯粒使用。

4.2.4 车用芯粒功能安全标准化建议

功能安全标准规范汽车芯粒企业流程管理措施、芯粒产品内部多功能模块的流程管理及技术措施等要求，其主要目的是避免系统性失效和硬件随机失效导致的不合理风险。

随着汽车电动化、智能化和网联化的快速发展，汽车芯片（包括芯粒）的功能安全成为行业关注的重点。芯粒技术通过模块化设计提升了芯片的灵活性和性能，但也带来了新的安全挑战，如供应链安全、通信安全和系统级安全等。制定统一的功能安全标准路线图，有助于推动芯粒技术在汽车领域的应用，提升产业链的协同效率和安全性。

GB/T 34590 是汽车功能安全的国家标准，涵盖了从设计到生产的全生命周期要求，同样适用于芯粒技术的功能安全开发。中国发布了《国家汽车芯片标准体系建设指南》，计划到 2025 年制定 30 项以上汽车芯片重点标准，明确功能安全、信息安全等基础性要求，逐步完善芯粒技术的标准化框架。基于 GB/T 34590 标准，将制定芯粒的单点故障度量（SPFM）、潜伏故障度量（LFM）和随机硬件失效概率度量（PMHF）等关键指标。并通过建立基于风险的功能安全评估体系，制定故障注入和仿真测试流程，验证芯粒在故障情况下的安全响应，并完成 FMEDA 流程的安全等级认证。

该标准将规定车用芯粒功能安全分级检测的术语与定义，根据车辆不同应用场景的推荐任务剖面，开展车用芯粒功能安全等级划分，明确不同等级功能安全检测要求，并给出不同车用芯粒的推荐功能安全等级，适用于车用芯粒企业面向不同应用场景的产品研发、整车企业及零部件企业对芯粒的选型评价。

技术路线如下：

（1）分析现有的 GB/T 34590《道路车辆 功能安全》国家标准中关于功能安全的分级要求。

- (2) 调研不同应用场景的车用芯粒应用特点，制定分级策略。
- (3) 提出不同车用芯粒功能安全分级技术。
- (4) 设计车用芯粒功能安全分级检测认证流程及规则。

4.2.5 车用芯粒信息安全标准化建议

信息安全标准规范汽车芯粒应满足的信息安全要求和应具备的信息安全功能。通过芯粒的信息安全设计、流程管理等措施，避免因攻击导致芯粒数据、外部接口及软硬件安全等受到威胁。

随着汽车电动化、智能化和网联化的快速发展，车用芯粒技术成为提升芯片性能、降低成本和加速迭代的重要途径。然而，芯粒技术的模块化和异构集成特性也带来了新的信息安全挑战，如数据泄露、恶意攻击和供应链风险。目前国内汽车芯片信息安全标准体系仍在完善中，包括《汽车芯片信息安全技术规范》、《汽车安全芯片技术要求及试验方法》，并依托《国家汽车芯片标准体系建设指南》推进后续标准制定。因此，制定汽车芯粒信息安全标准路线图，对于保障汽车电子系统的安全性、推动芯粒技术的广泛应用具有重要意义。

该标准将规定车用芯粒信息安全分级检测的术语与定义，根据车辆不同应用场景的推荐任务剖面，开展车用芯粒信息安全等级划分，明确不同等级信息安全检测要求，并给出不同车用芯粒的推荐信息安全等级，适用于车用芯粒企业面向不同应用场景的产品研发、整车企业及零部件企业对芯粒的选型评价。

技术路线如下：

- (1) 分析正在制定的相关国家标准中关于信息安全的分级要求。
- (2) 调研不同应用场景的车用芯粒应用特点，制定分级策略。
- (3) 提出不同车用芯粒信息安全分级技术。
- (4) 设计车用芯粒信息安全分级检测认证流程及规则。

4.2.6 车用芯粒软件设计标准化建议

- (1) 软件接口及工具链基础框架要求

接口规范要求：完成芯粒硬件抽象层（HAL）与通信中间件接口标准草案，

联合主流 OS 厂商（QNX、Linux 基金会）试点验证。

工具链基础框架要求：发布芯粒驱动开发工具链（SDK）的最小功能集要求，支持主流 EDA 工具集成。

（2）软件信息安全及虚拟化技术要求

安全认证体系落地：建立芯粒软件安全评估中心，发布符合 ISO 21434 的信息安全测试认证流程。

虚拟化技术标准化要求：完成车规级 Hypervisor 对多芯粒资源池化管理的性能指标与测试方法标准。

（3）软件生态及 AI 芯粒协同要求

全栈软件生态整合要求：推动芯粒软件接口与 AUTOSAR AP/CP、ROS 2 等框架的深度融合，形成跨车型平台的可移植性标准。

AI 芯粒协同规范要求：制定面向辅助驾驶的芯粒间 AI 模型分布式计算标准（如模型分片、梯度同步机制）。

参考文献

- [1] 郭王虎. 智能网联汽车技术路线图 2.0 发布[J]. 智能网联汽车, 2020(6): 4.
- [2] 国家车联网产业标准体系建设指南(总体要求)[J]. 机械工业标准化与质量, 2018.https://www.gov.cn/zhengce/zhengceku/2018-12/31/content_5440205.htm.
- [3] 中银证券. 汽车智能化系列报告之智能驾驶域控制器篇 [R]. 2023-12-04.https://data.eastmoney.com/report/zw_strategy.jshtml?encodeUrl=u2OJ4bj1eELgSO1IcShSme+0j7agL4Vp4HdYv/j24JI=.
- [4] 集成芯片与芯粒技术白皮书 [Z]. 2024. https://www.sgpjbg.com.cn/baogao/142807.html?bd_vid=11712574726667196621
- [5] 车规级芯粒系统芯片综合研究报告 [Z]. 2024.<https://nevc.com.cn/portal/index/articleides/id/239.html>.
- [6] ISO 26262:2018, 道路车辆功能安全[S].<https://www.iso.org/standard/68383.html>.
- [7] ISO/IEC 27001 , 信息技术 安全技术 信息安全管理体系 [S].<https://baike.baidu.com/item/ISO27001/2326653>.
- [8] ISO/IEC 29147 , 信息技术 安全技术 漏洞披露指南 [S].<https://www.iso.org/standard/72311.html>.
- [9] 国家汽车芯片标准体系建设指南[S]. www.gov.cn/zhengce/zhengceku/202401.