车载智能计算平台功能安全白皮书
（2020 年）

中国软件评测中心

智能网联驾驶测试与评价工业和信息化部重点实验室

赛迪（浙江）汽车检测服务有限公司

二〇二〇年十二月

顾　　问

李克强　清华大学

尚　进　国汽智控（北京）科技有限公司

黄子河　中国电子信息产业发展研究院

编写单位（按笔画排序）

工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）

北京百度网讯科技有限公司

北京地平线机器人技术研发有限公司

北京经纬恒润科技股份有限公司

华为技术有限公司

国汽智控（北京）科技有限公司

国汽（北京）智能网联汽车研究院有限公司

英博超算（南京）科技有限公司

参研单位（按笔画排序）

中汽创智科技有限公司

中国汽车电子产业联盟

中国第一汽车集团有限公司

北京艾迪智联科技有限责任公司

泛亚汽车技术中心有限公司

浙江吉利控股集团有限公司

编写专家（按笔画排序）

王亚丽 王　伟 王舜琰 田　峰 刘法旺 李怀洲 李艳文 吴丹丹
余　响 沈伟锋 宋　娟 张妍嫣 张　斌 张露阳 高　远 褚文博

版权声明

目 录

编制概要

（一）编制方法

一是研究学习国内外相关文献，充分参考借鉴国内外最新产业动态和研究成果。

二是调研国内外智能网联汽车、功能安全相关企业，汇集整理和分析来自实践应用的相关素材。

三是邀请行业专家进行技术研讨和咨询评审。

（二）特别说明

1）研究聚焦车载智能计算平台功能安全

汽车产业是我国国民经济的重要支柱产业，是推动实现制造强国和网络强国建设的重要支撑和融合载体。在“新四化”背景下，汽车电子电气架构正在由分布式向集中式持续演进，自动驾驶成为产业竞争的焦点，汽车电子产业链和技术链面临重构。在此背景下，支撑实现自动驾驶功能的车载智能计算平台的重要性更加凸显。国内外企业都在积极布局，加快推进产品研发和应用示范。

功能安全、预期功能安全和信息安全构成了智能网联特别是自动驾驶系统的安全要素。为凝聚共识、形成合力，加强车载智能计算平台安全体系的研究，推动智能网联汽车产业高质量发展，在《车载智能计算平台白皮书（2018 年）》《车载智能计算基础平台参考架构 1.0（2019 年）》研究的基础上，本白皮书聚焦车载智能计算平台的功能安全。

2）研究内容仍有待进一步丰富完善

本白皮书的主要观点和内容仅代表编制组目前对车载智能计算平台功能安全的研判和思考，与此同时车载智能计算平台的功能安全仍在探索推进，欢迎各方专家学者和企业代表提出宝贵意见，共同推动研究的及时更新和纠偏。后续中国软件评测中心将会继续推出《汽车智能计算平台白皮书（系列）》。

一、研究背景

（一）智能网联汽车的安全体系不断完善，其中功能安全是关键要素

在汽车产业朝着智能化、网联化、电动化、共享化的“新四化”趋势不断深入发展的同时，汽车电子电气系统的复杂度与集成度不断提高，新的功能越来越多地触及到系统安全工程领域。安全是智能网联汽车持续健康发展的前提。智能网联汽车安全体系的内涵和外延也在不断发生变化，功能安全、预期功能安全和信息安全构成了智能网联特别是自动驾驶体系的安全要素。

功能安全的融入是自动驾驶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。系统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。

（二）国内外企业竞相发力车载智能计算平台，其功能安全备受重视

自动驾驶技术不断发展，车载智能计算平台是 L3 及以上自动驾驶的必要解决方案，也是汽车新型电子电气架构的核心。其包含异构处理芯片、模组、接口等硬件以及车控操作系统、应用软件等软件，处理海量多源异构数据，是用于实现全部或部分动态驾驶任务和（或）执行动态驾驶任务接管功能的软硬件一体化平台。国内外企业如英伟

达、特斯拉、华为、中兴、地平线、百度、恒润等纷纷推出高性能产品。

随着自动驾驶等级的提升，汽车的环境感知、决策权和控制权逐步实现由驾驶员为主体向自动驾驶系统为主体的过渡，智能网联汽车的安全风险急剧增加。车载智能计算平台的功能安全重要性日益凸显。车载智能计算平台及关键零部件的开发和集成验证强化了对安全相关系统开发流程的需求。整车企业和零部件供应商重视功能安全的研究和实施，重新赋能技术人员，组织架构或随之调整。

（三）车载智能计算平台功能安全缺少共识，亟需行业专家联合研究

车载智能计算平台的功能安全目前尚未形成行业共识。功能安全在 ADAS（Advanced Driver Assistance System，高级驾驶辅助系统）领域的实践已形成一定的共识，并主要由 Tier 1（汽车零部件一级供应商）巨头企业主导。当前对于整车企业、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，影响了车载智能计算平台产品功能安全开发以及上车应用。

联合行业优势资源共同研究车载智能计算平台的功能安全，可以为我国车载智能计算平台的技术创新、标准研制、试验验证、应用实践、产业生态构建等提供指导，促进行业上下游达成共识，加速汽车产业和电子产业的融合，推动车载智能计算平台的持续健康发展。

二、车载智能计算平台功能安全概述

（一）功能安全及相关标准

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。

1）ISO 26262

ISO 26262 Road vehicles Functional safety 为汽车电子电气系统提供了整个安全生命周期功能安全活动的指导。该标准定义了汽车安全生命周期，同时还提出 ASIL（Automotive Safety Integrity Level，汽车安全完整性等级）概念。ASIL 分为 A、B、C、D 四个级别，系统的功能安全风险越大，对应的安全要求越高。ASIL D 为最高安全完整性等级，对功能安全的要求最高。ISO 26262 于 2011 年发布第一版，2018 年发布第二版，目前第三版正在研制过程中。国家标准 GB/T 34590-2017《道路车辆 功能安全》修改采用了 ISO 26262-2011。

2）SAE J2980

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。

3）UL 4600

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。

4）ISO TR4804

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）。

5）A-SPICE

A-SPICE（Automotive Software Process Improvement and Capacity dEtermination，汽车软件过程改进及能力评定）是汽车行业用于评价软件开发团队的研发能力水平的模型框架。最初由欧洲 20 多家整车企业在 SPICE（ISO 15504）的基础上共同制定，是专门针对汽车软件开发的行业标准。多年以来，A-SPICE 在欧洲汽车行业内被广泛用于研发流程改善及供应商的研发能力评价。A-SPICE 根据度量框架将企业的软件研发能力划分为 6 个级别，0 级为最低，5 级为最高。

（二）安全生命周期

功能安全明确定义了安全生命周期，要求将安全生命周期要求融入到自身的流程体系中，建立安全文化，对企业的功能安全做全面管理，满足 ISO 26262 中对流程活动的要求。功能安全生命周期包括概念阶段、产品研发、生产、运行、服务和报废等阶段。概念阶段包括相关项定义、危害分析和风险评估、功能安全概念的确定。系统层面的产品开发基于 V 模型，包含技术安全要求、系统架构、系统设计和实施、集成、验证和安全确认。硬件层面的开发过程也是基于 V 模型，包括硬件需求规范、硬件设计和实现、硬件集成和验证。软件层面的开发过程同样是基于 V 模型，包括软件需求规范、软件架构设计、软件单元设计和实现、软件单元测试、集成和验证。生产、运行、服务和报废阶段的计划以及相关要求规范是在系统层面的产品开发阶段开始的，并且与系统层面的产品开发、硬件层面的开发、软件层面的开发同步进行。此阶段确保相关项或要素的生产、运行、服务和

报废的功能安全。

车载智能计算平台开发一般为 SEooC（Safety Element out of Context，独立于环境的安全要素）方式。这种开发方式不会受限于某个具体的项目，需要基于前期市场调研或以往项目积累，对车载智能计算平台承接的安全目标、功能安全要求以及汽车电子电气架构做基础假设。企业可根据自身的产品和业务特性对 ISO 26262 中不必要的章节进行裁剪，将裁剪后的安全生命周期应用到实际的项目中。图 1 为车载智能计算平台功能安全生命周期参考示意图。

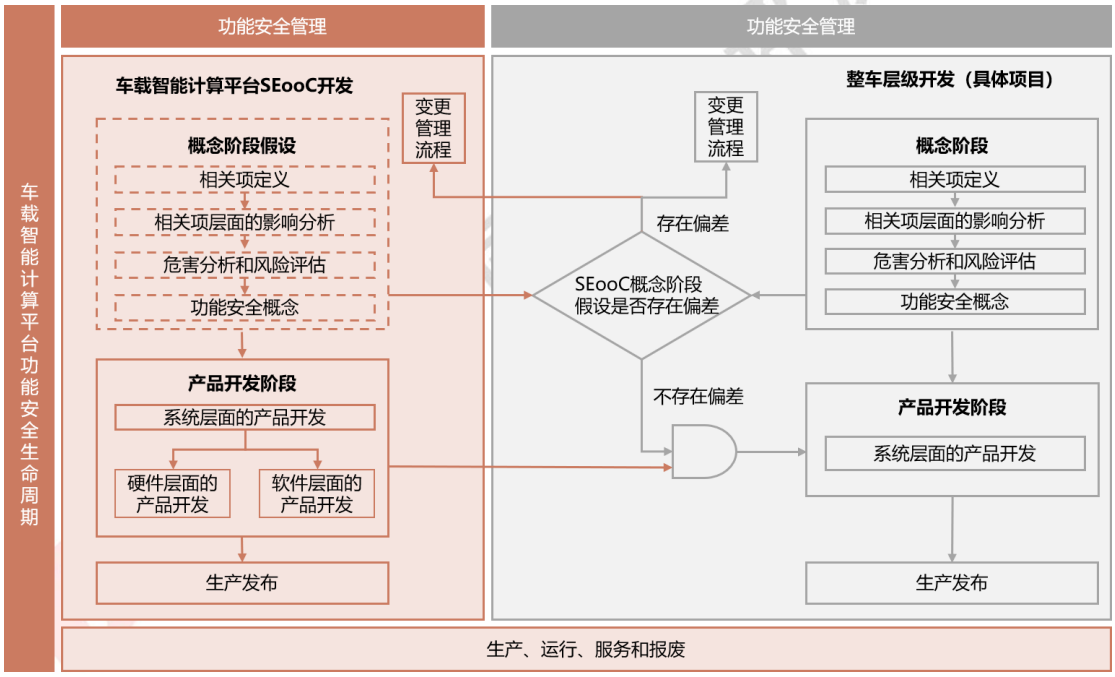

图 1 车载智能计算平台功能安全生命周期参考示意图

（三）功能安全管理

车载智能计算平台功能安全管理贯穿于整个安全生命周期，并与安全生命周期的每个阶段并行，大体可以分为整体安全管理、产品开发阶段安全管理以及产品发布后的安全管理。整体安全管理侧重于企

业或部门层面，聚焦功能安全文化建设、功能安全能力建设等。开发阶段安全管理侧重于产品开发过程中的组织架构、人员配置、开发活动计划以及文档交付计划等。产品发布后的安全管理主要是关注生产和售后层面，包括生产、运行、服务、报废。

在整体安全管理中，质量管理是功能安全管理的基础，相关企业或部门须具备质量体系，具有独立的质量部门实施产品质量审核。功能安全部门和质量管理部门可以合二为一，但是功能安全需要满足独立性要求。功能安全的管理要求应该融入到基础质量管理活动中，根据产品不同的功能安全等级要求选择不同的安全活动以及安全措施。在企业或部门内部要建立一种正向的功能安全文化，鼓励能够提升产品安全性的活动。对于功能安全相关人员必须建立完整的能力培养及评定体系，培养识别优秀的功能安全经理及功能安全工程师。同时应当建立起必要的沟通机制以及异常管理机制。

在产品开发过程中，需要配备独立的安全经理跟踪安全相关的活动，解决安全相关的问题。对每个开发阶段，需要制定详细的开发计划、验证计划以及认可评审计划。如果涉及到供应商，需要通过签署DIA（Development Interface Agreement，开发接口协议）明确双方责任和义务。在开发计划中，必须定义各个阶段的交付产物以及责任人、交付时间点等。在交付产物中相关内容要建立关联关系，做到需求和设计、设计和开发、开发和测试双向可追溯。安全经理需要跟踪这些活动以及要求的落地，对因为安全导致的成本问题、交付时间问题需要及时沟通，合理有效地协调资源以更好地平衡功能安全和成本、开

发时间之间关系。认可评审产品不同的 ASIL 等级需要满足不同的独立性要求，必要时可以引入第三方机构进行独立功能安全评估。

在生产、运行、服务和报废阶段，功能安全管理需要定义明确的生产操作规范、维修流程、报废回收流程保证最终产品在全生命周期不会影响环境及人身安全。

三、车载智能计算平台概念阶段功能安全

（一）相关项定义及要素划分

相关项是实现车辆层面或部分功能的系统或者系统组。相关项定义并描述系统或系统组，以及其与环境、其他相关项之间的依赖关系和交互影响，为充分理解相关项提供支持，以便执行后续阶段的活动。车辆层面的相关项定义如图 2 所示，主要包括相关项的功能、系统边界与接口、环境条件和法律要求等。车载智能计算平台的相关要素主要包括传感器接入及管理、AI（Artificial Intelligence，人工智能）计算、通用计算、车控、内部通信、V2X（Vehicle to Everything，车用无线通信技术）、高精度地图数据存储等。

图 2 相关项定义

（二）相关项层面的影响分析

车载智能计算平台的开发项目分为新开发、修改或复用，若为修改和复用，则需要进行相关项层面的影响分析。影响分析应识别和指出因相关项的修改、相关项使用条件的修改所带来的影响，可能的修改包括运行场景和运行模式、与环境的接口、安装特性、环境条件等。

高级别自动驾驶相对于辅助驾驶在运行环境感知范围和驾驶任务上会发生变化，例如:

1）设计运行范围对感知要求的变化

相对于辅助驾驶系统面临的运行环境条件，高级别自动驾驶系统相对减少对驾驶员的依赖，需要感知的车内外环境范围更广，以确保自车行驶过程中的道路安全。在某些场景和系统设计中，需要对自车周围影响道路安全及自车定位的动态和静态物体感知。

2）动态驾驶任务和人为因素的变化

L3 及以上的自动驾驶系统相对于辅助驾驶系统容许一定程度的驾驶员不在环。在系统发现预期无法处理或者无法保证动态驾驶任务安全执行等紧急情况时，为使车辆控制权被快速接管并避免危害，驾驶员状态也需要被感知（如监测驾驶员专注度、心率等生理状态）。

（三）危害分析和风险评估

通过危害分析和风险评估确定 ASIL 等级和安全目标，以避免不合理的风险。为此，根据相关项中潜在的危害事件，对相关项进行评估。安全目标以及分配给它们的 ASIL 等级是通过对危害事件进行系

统性的评估所确定的。ASIL 等级是通过对影响因子严重度、暴露率和可控性的预估所确定的，影响因子的确定基于相关项的功能行为，因而不一定需要知道相关项的设计细节。关键步骤具体包括场景分析及危害识别、危害分级、ASIL 等级的确定、安全目标的确定。由于在动态驾驶任务中，L3 及以上自动驾驶相对于辅助驾驶，容许一定程度的驾驶员不在环，将会导致对危害的可控性降低，在进行危害分析与风险评估时，可控性或将变为 C3，可能会引起功能安全等级需求的提升。

（四）功能安全概念

功能安全概念是从安全目标中导出功能安全要求，并将其分配给相关项的初步架构要素或外部措施。功能安全概念包括安全目标、初步安全架构设计、安全分析、安全要求。

安全架构设计方面，L3 自动驾驶系统已经允许驾驶员的手长时间脱离方向盘，无需时刻观察道路状况，从系统出现失效到驾驶员反应并接管控制存在一定时间间隔。在这段时间间隔内，系统要确保车辆的安全性，需要做到某一个单元失效的情况下，车辆能够维持横纵向控制直到驾驶员接管或安全停车，因此需要冗余的架构设计。一般来说，对于整个自动驾驶系统的冗余设计又可以细分为电源冗余、执行机构冗余、传感器冗余、计算平台冗余、用户交互链路冗余等。

从安全目标可以导出安全要求，安全要求继承安全目标的 ASIL 等级。一个安全要求可以分解为两个或多个子安全要求，分配到独立冗余的安全架构设计中。独立性是 ASIL 分解的重要要求，即冗余单元之间应避免共因失效和级联失效。

四、基于功能安全的车载智能计算平台开发

（一）系统层面

1）应用环境

车载智能计算平台，作为自动驾驶的主要部件，其应用环境参考如图 3 所示：

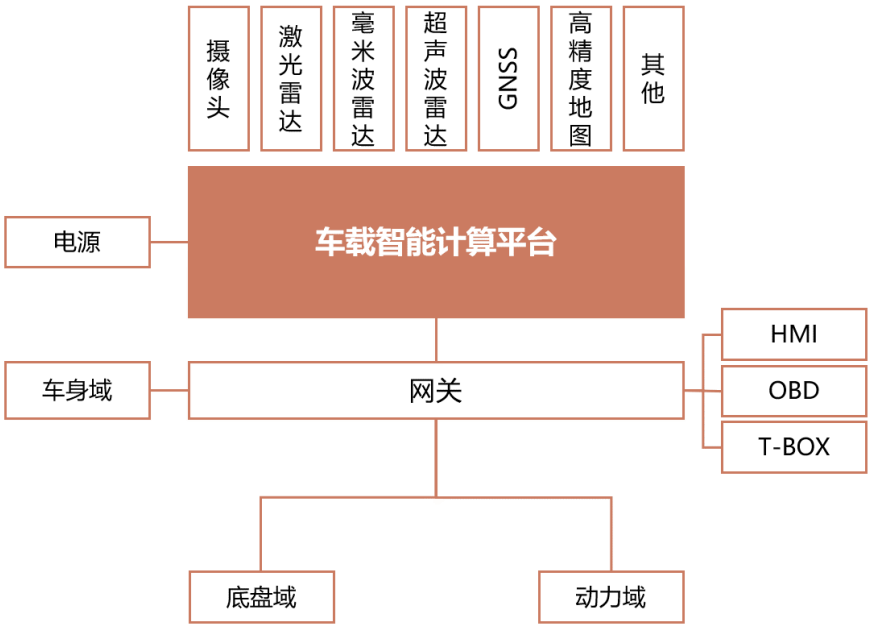

图 3 车载智能计算平台应用环境参考示意图

车载智能计算平台的应用环境主要包含用于环境感知（如摄像头、激光雷达、毫米波雷达、超声波雷达等）和位置定位（如 GNSS、高精度地图等）的传感器，整车底盘域、动力域以及车身域的执行器，人机交互的 HMI（Human Machine Interface，人机界面），以及外部互联与通信的 T-Box（Telematics Box，远程车载信息交互系统）和 OBD（On Board Diagnostics，车载自动诊断系统）等。随着自动驾驶等级的不断提高，车载智能计算平台对应用环境中的传感器、执行器、人

机接口和外部互联通信有更高的功能要求及功能安全要求。

2）功能划分

车载智能计算平台按照功能可以分为传感器接入及管理、AI 计算、通用计算、通信、存储和车控等。不同的功能依赖不同的系统模块实现。传感器接入与管理单元提供丰富的软硬件接口，使能传感器接入及管理。AI 计算提供深度神经网络算法加速计算能力。通用计算主要是指面向常规算法的计算能力。车载智能计算平台内部通信提供车载智能计算平台内部各个要素之间通信能力。V2X 通信提供车载智能计算平台连接车辆外部设备能力。存储功能提供诸如高精度地图存储及服务能力。车控提供车控下发能力，对接车辆执行器。车载智能计算平台功能单元参考 ASIL 等级如表 1 所示。

表 1 车载智能计算平台功能单元参考 ASIL 等级[1]

功能单元	ASIL 等级
传感器接入与管理	B
AI 计算	B
通用计算	D
计算平台内部通信	D
V2X	D
存储	B
车控	D

[1] 鉴于各企业的解决方案并不相同，表 1 提供的部分功能单元 ASIL 等级并非通用性参考。

3）安全策略

自动驾驶功能目前的系统安全策略大体分为两种，即 Fail-Safe（失效-安全）以及 Fail-Operational（失效-可操作）。Fail-Safe 要求系统监控关键的部件以达到失效后系统关断的目的。但是对于 L3 及以上的功能，驾驶员处于脱眼、脱手的状态，系统的关闭并不能保证可靠地完成驾驶权的转移。例如，高速公路场景中，车辆紧急停止在本车道是一种潜在的风险状态，很容易发生高速追尾。Fail-Operational 安全策略解决了这一问题，即使在主功能系统失效的情况下，仍然有备份系统可以保证车辆进行降级操作，让车辆转移到安全区域。

4）系统设计

车载智能计算平台的安全策略可以是独立的监控模块或冗余的系统设计。独立的监控模块实时监控功能实现模块的软硬件故障，一旦检测到有安全相关故障，车辆即进入安全状态，如需要可先进入紧急运行模式（Emergency Operation）。例如，功能降级、当前车道停车、安全地点停车等。

冗余的系统设计是指两个或多个功能模块互为备份。例如，车载智能计算平台可以采用“主处理单元+辅处理单元”双处理架构，以确保 L3 及以上自动驾驶车辆的安全。在该架构下，主处理单元对车辆的运动轨迹进行规划和控制，辅处理单元的作用是监控主处理单元。同时两个单元不断地进行交叉检查，当两个通道在规划轨迹和控制策略存在较大偏差时，系统就会进入降级模式。主处理单元和辅处理单元可以按照 ASIL B 设计开发，仲裁模块可以按照 ASIL D 设计开发。

在系统阶段进行设计时，需要考虑不同系统单元的故障以及对应的处理策略，具体包括传感器接入能力失效，比如丢帧、乱序等；通用计算能力或 AI 计算能力失效，比如代码跑飞、执行超时等；内部或 V2X 通信能力失效，比如超时等；存储失效，比如高精度地图数据损坏等；车控失效，比如非预期发送车控等；电源失效；时钟失效。

5）技术安全概念

技术安全概念是车载智能计算平台系统设计中安全策略与安全设计的集合。技术安全概念的内容主要包含基于系统架构的功能安全分析，基于上级功能安全要求与功能安全分析导出的技术安全要求，最终集成安全设计的系统架构，以及后续生产过程中需要采取的安全措施。技术安全要求需要定义具体的安全机制并分配到相应的架构要素中，以确保在下一级的开发过程中，安全机制可以被进一步细化与实施。在车载智能计算平台的开发过程中，技术安全概念可能针对于某一系统或子系统，因而技术安全要求涉及的架构层级可以不止一层。在车载智能计算平台的技术安全要求中，若采取多层次的技术安全要求，其基本原则不变，即技术安全要求要与架构层级相映射并最终被分配到软件与硬件中，以保证软件与硬件的功能安全开发有明确和完整的输入。

6）测试验证

车载智能计算平台在功能安全概念阶段开发或假设了上层的安全目标和功能安全要求，安全要求在之后各个阶段被逐渐细化和实现。最终完成硬件层面及软件层面开发和集成的车载智能计算平台能否

正确实现安全要求，以及是否存在非预期的功能，需要通过系统层面的集成测试进行验证。系统层面的测试验证，一方面需要确保安全要求能够被正确地使能，另一方面还需要确保车载智能计算平台不会因为安全要求非预期使能而导致系统可用性降低。

制定有序的系统层面测试计划，并进行持续的过程跟踪管理，是保障车载智能计算平台测试验证工作有序可靠进行的必要途径。开发测试团队应重点考虑项目整体时间计划、测试验证的人员安排与责任分工、测试方法、测试环境、测试工具等方面的内容，综合评估和确认之后形成测试计划。

基于 SEooC 模式开发的车载智能计算平台实际应用到目标车型时，系统集成测试和整车集成测试是发现系统性故障不可或缺的安全活动。在系统集成测试和整车集成测试活动中，需重点验证目标车型的功能安全要求是否得到正确实现，集成真实的传感器和执行器等其他其它要素之后的系统响应是否满足安全机制的要求，车载智能计算平台与目标车型其他要素之间的接口与交互过程是否正确，以及安全要求在外界严苛的环境条件和运行工况下能否正常实现。

（二）硬件层面

作为车载智能计算平台功能软件与系统软件的载体，硬件的失效可能直接导致功能软件输出不可信任的结果，从而违背安全目标。由于硬件故障在硬件生命周期中发生时间的随机性，在通过改善流程降低系统性失效的同时，ISO 26262 功能安全标准在硬件层面重点关注识别安全相关的硬件故障以及采取安全机制诊断相应硬件故障，并对

发现的硬件故障进行处理（例如进入安全状态），从而将硬件随机失效对安全目标的影响降低到可接受的程度。

1）随机失效概率量化指标

根据硬件故障对安全目标产生影响的不同，硬件故障可分为安全相关故障与非安全相关故障，其中安全相关故障又进一步分为单点故障、残余故障、多点可探测故障、多点可感知故障、多点潜伏故障与安全故障。其中，单点故障和残余故障可以直接导致安全目标的违背。多点潜伏故障虽然不会单独导致安全目标的违背，但可能会在与其它故障同时发生时导致安全目标的违背。因此用于表示单点故障与残余故障诊断覆盖率的 SPFM（Single-Point Fault Metric，单点故障度量），多点潜伏故障诊断覆盖率的 LFM（Latent Fault Metric，潜伏故障度量）与 PMHF（Probabilistic Metric for random Hardware Failures，随机硬件失效概率度量）[2]是功能安全用于衡量随机硬件失效率是否达到可接受程度的重要衡量指标。针对于不同的功能安全等级，ISO 26262 针对上述指标给出了表 2 中的参考性量化目标。下列数值是广泛应用于业界评估安全系统是否满足相应功能安全等级的重要指标。

[2] 对违背安全目标的每个原因进行评估（EEC）是另一种可选度量，参考 ISO 26262-5。

表 2 硬件随机失效度量参考量化目标

硬件度量指标	ASIL B	ASIL C	ASIL D
SPFM	≥90 %	≥97 %	≥99 %
LFM	≥60 %	≥80 %	≥90 %
PMHF	$<10^{-7}\,h^{-1}$	$<10^{-7}h^{-1}$	$<10^{-8}\,h^{-1}$

2）关键器件的选型与集成

车载智能计算平台的硬件主要由 AI 单元、计算单元与控制单元组成。根据不同的架构需求，上述单元可由一个或多个芯片组成，芯片的种类可能包含 GPU（Graphics Processing Unit，图形处理器）/FPGA（Field Programmable Gate Array，现场可编程逻辑门阵列）/ASIC（Application Specific Integrated Circuit，专用集成电路）、SoC（System on Chip，系统级芯片）、MCU（Micro Control Unit，微控制单元）等。

芯片多采取 SEooC 开发模式。安全相关芯片供应商在提供产品的同时会提供给车载智能计算平台的系统集成者相应的安全使用手册。安全使用手册一般包含芯片供应商对系统功能安全要求的假设，可支持的最高功能安全等级，集成的安全机制以及实现承诺功能安全等级需要满足的假设条件。

车载智能计算平台选用的安全相关器件需要满足分配到该器件的技术安全要求。芯片通常会对内部处理单元、存储单元、通信总线、接口等元件提供相应的安全机制以满足安全相关故障的诊断覆盖率要求。除此之外，由于芯片的正常性能表现受限于一定的条件约束，保证时钟、温度、供电等在可操作范围内的安全机制也对功能安全的

实现极为重要。车载智能计算平台需要按照各芯片厂商提供的安全手册搭建安全芯片外围电路和配置内部参数，确保芯片的安全内外部安全机制正常运行，从而在出现故障时能够及时进入安全状态。确保每个芯片正确集成的同时，还需确保集成后的硬件架构满足所有安全目标的随机失效概率量化指标要求。

3）硬件架构设计

由于现有关键器件的功能安全能力的局限性与 ASIL D 系统对单点失效度量的严格要求，硬件冗余是实现高功能安全等级安全目标的常见方式。冗余式硬件架构的主体是通过对冗余计算单元输出结果的相互校验达到提高计算单元硬件故障诊断覆盖率的目的。由于对相互冗余系统的独立性要求，相互冗余的系统需尽可能的避免由同源输入、共用资源、环境影响等因素引起的共因失效。

功能安全在硬件层面，关注硬件器件中的安全相关故障可以通过自检或外部监控的方式被检测到，并在故障容忍时间内实现安全状态。硬件器件实现安全状态的方式多为重启、断电、报错、禁言等，因此单硬件通路的硬件架构可以满足 Fail-Safe 概念的需求。根据车载智能计算硬件平台所承载功能与功能安全要求分配的不同，AI 单元、计算单元与控制单元所选用的芯片可通过单器件或冗余的方式实现相应的功能安全等级，如图 4 所示。

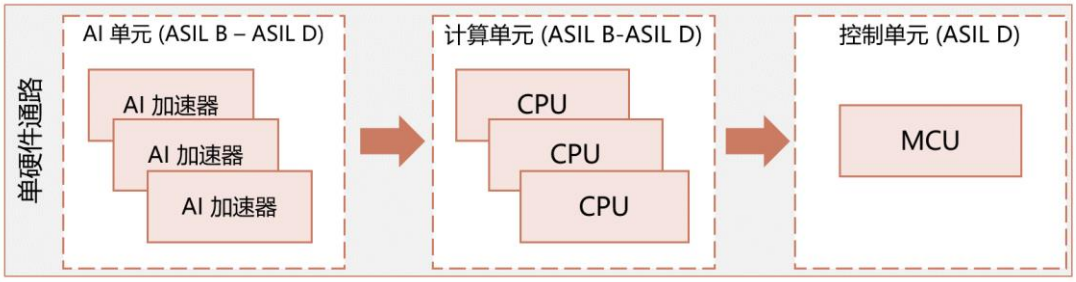

图 4 单硬件通路 Fail-Safe 抽象硬件架构示例

随着自动驾驶的发展，Fail-Safe 的安全策略难以满足高级别自动驾驶的安全要求。基于 L3 以上自动驾驶功能对系统 Fail-Operational 的需求，越来越多的车载智能计算平台在主通路实现 ASIL C-ASIL D 的基础上增加与主通路相互监控的 Fail-Operational 通路，实现主通路失效情况下硬件层面的失效可操作性，以提高系统的安全性和可用性，如图 5 所示。需要注意的是，根据自动驾驶功能等级对 Fail-Operational 系统在主通路失效情况下需要完成的紧急运行模式的不同，Fail-Operational 通路所包含的硬件单元可能会有所差异。

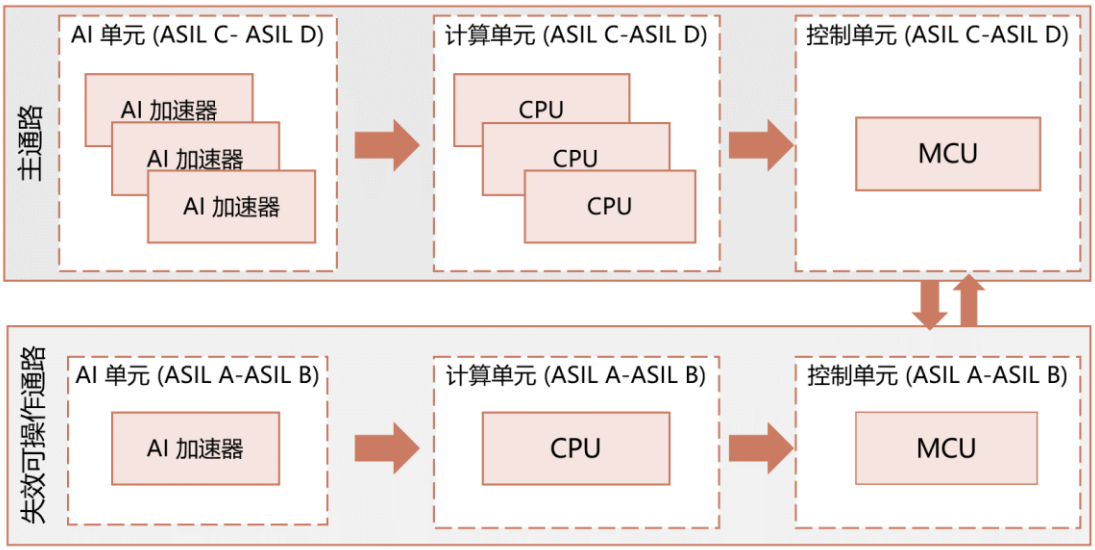

图 5 多硬件通路 Fail-Operational 抽象硬件架构示例

4）供电系统设计

电源是整车电子电气架构中最基础的共用资源。如若电源系统发生失效，则可能导致车载智能计算平台的所有功能失效，对于 L3 及以上自动驾驶系统是不可接受的风险。车载智能计算平台的供电系统需要满足 Fail-Operational 的要求，通常会采用双电源供电的方式。需要考虑双路电源供电有足够的隔离措施，确保一路供电出现故障（电压过高、过低甚至出现短路）时，另外一路供电不受影响。

为满足车载智能计算平台系统 ASIL D 的要求，参考 ISO 26262-5 附录 E 中关于电源系统失效模式与应对措施的要求，车载智能计算平台的供电系统需要能够监控电源输入和输出是否存在异常，尤其是电源系统输出的监测和控制。若电源系统出现输出电压过高或过低故障时，车载智能计算平台内部的主芯片有可能会因为供电电压不稳而导致运算结果异常，最终导致违反安全目标。因此，电源系统需在输出电压异常时，及时关断对应的主芯片供电，确保车载智能计算平台输出为确定状态。

5）通信系统设计

车载智能计算平台作为 L3 及以上自动驾驶的运算核心，通常通过专用的通信通道传输外界环境信息，而车载智能计算平台实现融合决策和车辆控制之后，将车辆运动控制指令通过通信总线发送至车辆的纵向和横向控制执行器。总线通信通道可能因为线束破损、外界电磁干扰和其他节点损坏等因素导致通信失效，包括报文丢失、报文延迟和报文篡改等多种类型的失效模式。参考 ISO 26262-5 附录 D 的要

求，采用多种安全监测工具的组合可以满足高诊断覆盖率的要求，但此种方法只能满足 Fail-Safe 的要求，即发现通信故障，但无法维持系统正常工作。为了实现 L3 自动驾驶功能 Fail-Operation 的要求，可采用硬件冗余的方式，一方面提高了诊断覆盖率，另一方面可满足 Fail-Operation 的要求。通信通道的冗余设计需要考虑二者的独立性，例如采用不同类型的通信协议（如 CAN-FD 和 FlexRay），避免发生共因失效。

6）硬件测试

车载智能计算平台的硬件集成完成后，需要对硬件的安全性做全面的测试。硬件测试用例的导出方法包含硬件安全要求分析、内部及外部接口分析、等价类生成和分析、边界值分析等。硬件测试需要涵盖功能测试、故障注入测试、电气测试等测试方法来验证硬件安全要求的正确性和完整性，另外还需要涵盖最恶劣情况测试、超限测试、EMC（Electromagnetic Compatibility，电磁兼容）测试和 ESD（Electro-Static Discharge，静电放电）测试等测试方法来验证车载智能计算平台硬件的鲁棒性和耐久性。测试完成后需要输出全面的测试报告作为硬件安全的佐证。

（三）软件层面

车载智能计算平台作为智能汽车的安全关键系统，软件层面的安全性至关重要。由于车载智能计算平台功能丰富，应用场景复杂，对软件的实时性、安全性、可靠性要求极高，应通过技术和流程两个方面保障软件的功能安全。技术上确保软件层级的每个功能安全相关软

件节点都有相应的故障监测和处理机制，流程上按照软件安全生命周期模型规范软件开发过程。

1）软件安全要求

车载智能计算平台软件安全要求是对软件安全相关的功能和性能的具体要求，主要是通过技术安全要求在软件层面的分配得到，并通过继承或分配得到相应的 ASIL 等级。另外，在软件架构阶段执行的软件安全分析也可能会识别出额外的软件安全要求。采用专业的需求管理工具来实现需求的编写、评审、管理以及双向追溯性检查可大幅降低软件层面的系统性安全风险。

2）软件架构设计

软件架构设计是对软件需求的设计与实现，用来描述软件的框架要素和软件各分层结构之间的相互作用，其范围层面应到能够识别所有软件单元的程度。软件架构设计不仅需满足相应 ASIL 等级的软件安全要求，还应满足软件其他非安全要求。在软件架构层面，软件安全要求会分层次地分配给软件组件直到软件单元，每个软件组件应按照分配给它的安全要求中最高的 ASIL 等级来开发。车载智能计算平台应在软件架构设计阶段进行软件安全分析和相关失效分析，完善错误探测和错误处理的安全机制，以便识别或确认软件安全相关部分，证明软件的安全相关的功能和性能满足相应的 ASIL 要求，支持安全措施的定义及其有效性。车载智能计算平台软件架构设计完成后，应对其开展验证活动，输出软件验证报告，证明软件架构设计严格遵守设计规则，兼容目标环境，满足相应 ASIL 等级的需求，并且相关评

审证据充足。

3）软件单元设计与实现

在软件单元设计与实现阶段，基于软件架构设计对车载智能计算平台的软件单元进行详细设计。软件单元设计应满足其所分配的ASIL 等级要求，与软件架构设计和软硬件接口设计相关内容保持一致。为了避免系统性失效，应确保软件单元设计的一致性、可理解性、可维护性和可验证性，应采用自然语言与半形式化方法相结合的方式进行描述。说明书应描述实施细节层面的功能行为和内部设计，包括数据存储和寄存器的使用限制。在源代码层面的设计与实施应使得软件单元设计简单易懂，软件修改适宜，具有可验证性和鲁棒性，确保软件单元中子程序或函数执行的正确次序，软件单元之间接口的一致性，软件单元内部及软件单元之间数据流和控制流的正确性。车载智能计算平台软件包含数百个软件单元，软件单元的标准化、单元间解耦是高效实现软件功能安全的基础。车载智能计算平台中不同安全等级的软件可以采用硬件虚拟化、容器、内存隔离等技术进行隔离，防止软件单元之间的级联失效。软件代码设计过程中应遵守成熟的代码设计规范，例如 MISRA C（汽车产业软件可靠性协会嵌入式 C 编码标准）。企业可以基于 MISRA C 建立一套满足车载智能计算平台安全编码要求的内部编码规范，并严格执行。

4）软件单元验证

软件单元验证是通过评审、分析和测试的方法对功能安全相关的软件单元设计与实现进行验证，证明软件相关安全措施已经在设计与

实现中全部落实。软件单元设计满足相应的 ASIL 等级的软件需求和软硬件接口规范要求，软件源代码的实现与单元设计一致，不存在非期望的功能和性能，且支持功能和性能实现的相关资源充足。

车载智能计算平台的软件单元验证可通过需求分析、等价类的生成与分析、边界值分析和错误推测相结合的方法合理设计测试用例，确保对软件单元进行充分验证。为了评估软件单元验证的完整性，为单元测试的充分性提供证据，应确定在软件单元层面的需求覆盖率，同时对结构覆盖率进行测定。车载智能计算平台软件单元测试的结构覆盖率目标为 100%，如果已实现结构覆盖率不能达到目标，可以定义额外的测试用例并提供接受理由。车载智能计算平台软件单元的结构覆盖率测试应采用满足相关安全要求的测试工具，确保在测试过程中测试工具和检测代码不会对测试结果产生影响。

车载智能计算平台软件单元测试应根据测试范围，选用适当的测试环境。测试环境应适合完成测试目标，尽可能接近目标环境，如果不是在目标环境执行，应分析源代码与目标代码的差异、测试环境和目标环境之间的差异，以便在后续测试阶段的目标环境中，定义额外的测试。

5）软件集成验证

软件集成验证需要根据软件验证计划、接口规范、软件架构设计规范、软件验证规范等对软件架构中所描述的集成层次、接口、功能等进行持续测试，以验证其与设计的符合性。由于车载智能计算平台软件的复杂性，实时性、可靠性、安全性既是设计目标也是基础性能，

集成测试设计阶段应对其功能、逻辑、性能、边界、接口进行详细分析。车载智能计算平台的软件集成验证，不仅需涵盖所有应用软件、功能软件、系统软件以及与硬件之间的接口，并且应涵盖软件单元之间的接口。测试用例在测试工作中至关重要，其输出需要考虑功能需求、性能需求、边界值、接口、逻辑关系等。

6）嵌入式软件测试

车载智能计算平台嵌入式软件测试主要是基于软件安全要求的测试，并针对软件安全要求进行充分的故障注入测试，最终确保软件安全要求的正确实现。为了验证车载智能计算平台软件在目标环境下是否满足软件安全要求，应进行硬件在环测试、车辆电控系统和网络通信环境下的测试以及实车测试。硬件在环测试是将车载智能计算平台软件烧写到目标芯片中，在目标芯片的硬件异构平台环境下验证软件的安全要求。然后，将车载智能计算平台与部分或全部的车辆电子电气设备进行网络通信，在车辆电控系统和网络环境下验证软件的安全要求。最后，将车载智能计算平台安装到实际车辆中，进行软件安全要求的验证与确认。

7）人工智能

通过实施完善的开发流程可降低车载智能计算平台人工智能的系统性安全风险。车载智能计算平台人工智能的开发包含需求分析、算法设计、数据采集和标注、模型训练、测试验证以及运行等流程。人工智能的需求分析应包含算法的基本功能需求和功能安全要求（如算法精度目标、算法 Fail-Operational 等）。算法设计阶段应考虑采用

多算法、多模型、多帧数据、多传感器等多种冗余机制的组合以提升安全性。数据采集和标注阶段应确保数据标注精度、数据场景分布，并避免数据错标和漏标，从而确保模型训练不受影响。模型训练阶段采用业界成熟、文档全面的人工智能框架。测试验证阶段对所有需求进行闭环的测试，同时全面考虑各种潜在应用场景及环境影响因素，进行长距离的实车试验。根据测试结果不断重复进行数据的采集、标注、模型训练和测试验证的阶段，通过迭代的方式逐步提高人工智能的安全性。在运行阶段，应持续地对实际运行数据和人工智能的安全性进行监控，通过分析实际运行数据对人工智能算法和模型不断优化。

五、车载智能计算平台生产、运行、服务和报废

（一）软件升级

在智能网联汽车中应用 OTA（Over-the-Air，空中升级）已经成为当前市场上一种主流的趋势。使用 OTA 进行软件升级能够快速更新迭代整车功能，或者修复软件缺陷。车载智能计算平台搭载的深度学习和视觉模块和地图数据等部件甚至基础固件均可以通过 OTA 及时更新，甚至完全扩展出新的功能，更新内部软件程序后的车载高性能运算平台仍需要保证原有的安全性，杜绝因为 OTA 过程中存在系统性失效而引发人身伤害。此外，OTA 过程通常发生在车辆 SOP（Standard Operation Procedure，标准作业程序）之后的运行维护过程中，整车企业和软件开发工程师难以直观地控制所有车辆的 OTA 过程，因此保证 OTA 完整流程的安全性是车载智能计算平台必须考虑的因素。作为整车企业与 Tier 1，应当从安装包的安全验证、安装包完整性保护与监测、传输过程的通信保护与监测和本地升级条件监测保证 OTA 过程的安全性。

（二）安全事件应急响应机制

安全事件应急响应机制在信息安全领域非常普遍，建立功能安全的安全事件应急响应机制同样价值显著。应急响应机制可作为验证不充分的补充，在发现安全隐患时及时上报、处理。车载智能计算平台功能安全事件应急响应机制应参考整车企业已有的现场问题响应机制。

六、发展建议

（一）明确需求统一认识

发展车载智能计算平台，关键共性技术攻关难度大，涉及产业链上下游范围广。因此，必须要进一步梳理明确产业对车载智能计算平台功能安全的实际应用需求，建立和完善车载智能计算平台的功能安全流程开发体系，明确统一术语，凝聚形成行业共识，推动汽车产业与电子产业的加速融合。依托重点实验室、标委会、产业联盟等平台，定期召开技术研讨会、标准发布会、先进技术成果应用示范等活动，积极宣传推广优秀的研究和实践成果。

（二）推进配套工具研发

结合企业对车载智能计算平台功能安全技术服务的迫切需求，推动可以支撑符合功能安全开发全流程的工具链的完善，以及功能安全综合公共服务平台的建设。鼓励支持需求管理工具、安全分析工具、代码生成工具、编译器、测试工具的研发和认证，逐步打造自主化的功能安全工具链。

（三）完善检测认证体系

高度关注产品质量和安全保障工作，在车载智能计算平台关键核心技术的研发和应用过程中，同步关注安全体系的研究和测评规范研制。支持相关检测机构加快检测平台建设和检测能力的提升，建设和完善测试用例库，构建测评和认证体系，强化技术保障能力，以测促研，加快推动产品研发和应用示范。

（四）加强专业人才培养

目前深耕智能网联汽车功能安全的专业人才相对紧缺，亟需整合业内专家资源，尽快构建智能网联汽车功能安全领域的专业人才队伍。现有的功能安全人才培养模式仍主要由企业牵头，速度较慢、规模较小。因此，需要联动高校、研究机构等资源，构建符合自动驾驶知识和能力需求的专业学科体系，努力提高汽车功能安全人才的系统性专业知识和实践能力。

附件：缩略语

缩略语	英文名称	中文名称
ADAS	Advanced Driver Assistance System	高级驾驶辅助系统
AI	Artificial Intelligence	人工智能
ASIC	Application Specific Integrated Circuit	专用集成电路
ASIL	Automotive Safety Integration Level	汽车安全完整性等级
A-SPICE	Automotive Software Process Improvement and Capacity dEtermination	汽车软件过程改进及能力评定
EMC	Electromagnetic Compatibility	电磁兼容
ESD	Electro-Static Discharge	静电放电
FPGA	Field Programmable Gate Array	现场可编程逻辑门阵列
GNSS	Global Navigation Satellite System	全球导航卫星系统
GPU	Graphics Processing Unit	图形处理器
HMI	Human Machine Interface	人机界面
IMU	Inertial Measurement Unit	惯性测量单元
LFM	Latent Fault Metric	潜在故障度量
MCU	Micro Control Unit	微控制单元
OBD	On Board Diagnostics	车载自动诊断系统
OTA	Over the Air	空中升级
PMHF	Probabilistic Metric for random Hardware Failures	随机硬件失效概率度量
SEooC	Safety Element out of Context	独立于环境的安全要素
SoC	System on Chip	系统级芯片

SOP	Standard Operation Procedure	标准作业程序
SPFM	Single-Point Fault Metric	单点故障度量
Tier 1		汽车零部件一级供应商
UL	Underwriters Laboratories	美国保险商实验室
V2X	Vehicle to Everything	车用无线通信技术

- **单位地址： 北京市海淀区紫竹院路 66 号**
- **邮政编码： 100048**
- **通信地址： 北京市海淀区紫竹院路 66 号赛迪大厦 12 层**
- **电话/传真： 010-88559296/88559333**
- **电子信箱： wangwei@cstc.org.cn**
- **投诉电话： 010-88559315**