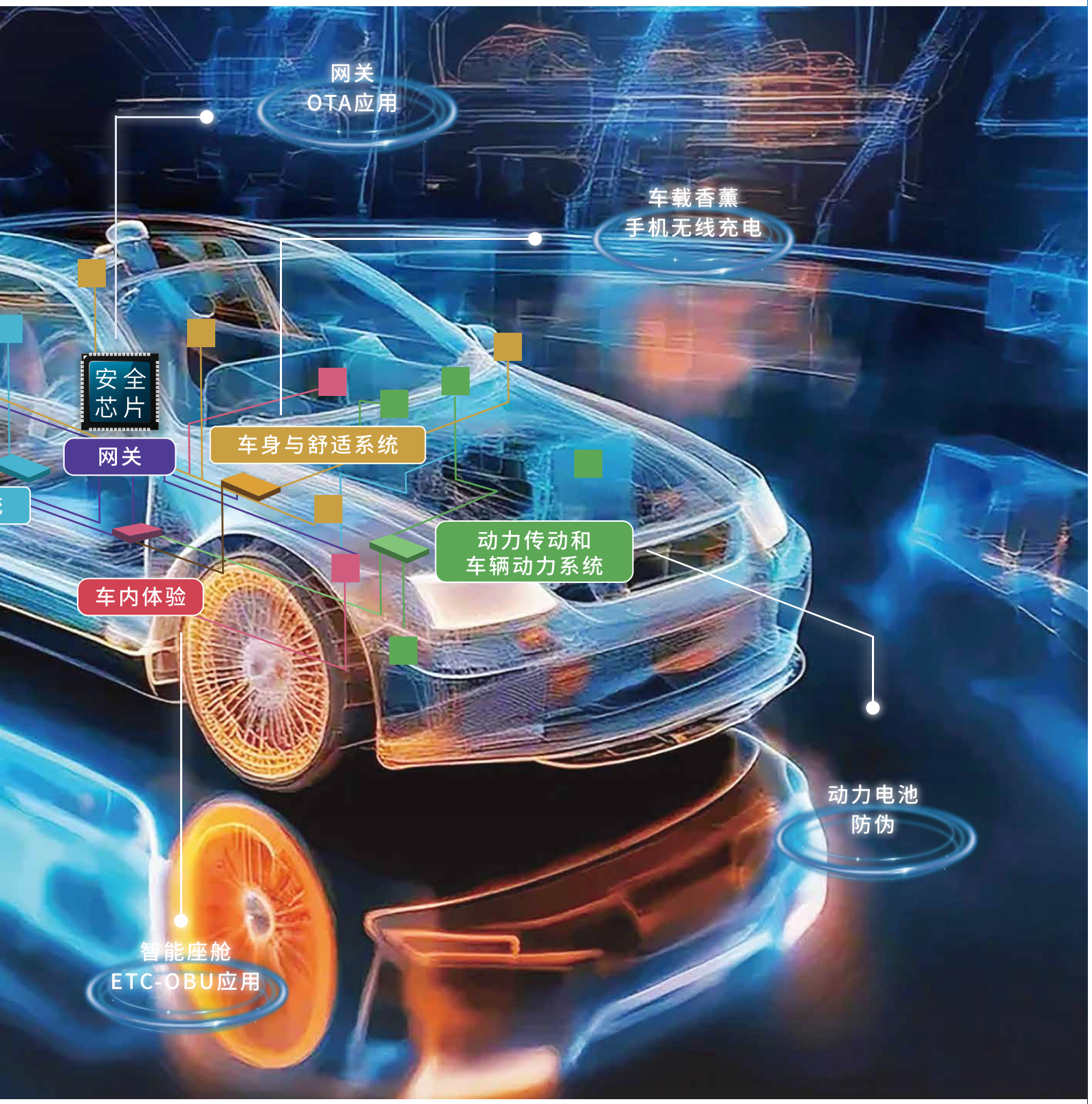
汽车安全芯片应用领域白皮书



主编单位：中国汽车芯片标准检测认证联盟

版权声明

编写组联系方式：

（1）李老师，liyujia@catarc.ac.cn;

（2）秦老师，qinwei@hdsc.com.cn;

本文件起草单位

（排序不分先后）

中汽研科技有限公司、北京中电华大电子设计有限责任公司、中国汽车技术研究中心有限公司、华大半导体有限公司、国家市场监督管理总局认证认可技术研究中心、北京华大智宝电子系统有限公司、北京华弘集成电路设计有限责任公司、上海复旦微电子集团股份有限公司、比亚迪汽车工业有限公司、宁波均联智行科技股份有限公司、天津国芯科技有限公司、吉利汽车研究院(宁波)有限公司、上海芯钛信息科技有限公司、中国第一汽车集团有限公司、紫光同芯微电子有限公司、郑州信大捷安信息技术股份有限公司、长城汽车股份有限公司、东风汽车集团有限公司研发总院、深圳联友科技有限公司、联友智连科技有限公司、重庆长安汽车股份有限公司、交通运输部公路科学研究院、交通运输部路网监测与应急处置中心、北京网路智联科技有限公司、清华大学集成电路学院

本文件主要起草人

(排序不分先后）

夏显召、崔文文、李予佳、任家鲁、吴海文、李雨冉、秦维、翟瑞卿、安文豪、王雪聪、段永刚、谭锐能、钟鹏、李杨、王鑫、李澜涛、曹凯、胡闯、孙亨博、刘嘉维、刘为华、李鑫、郭阳、雷鹏、王晓晓、李堪聪、谭成宇、李宏海、周洲、梅乐翔、秦建良、乌力吉

目录 CONTENTS

01 汽车信息安全概述

02 汽车信息安全需求分析

03 汽车安全芯片概述

04 车端安全攻防案例介绍

05 汽车安全芯片主要应用场景

06 汽车安全芯片关键技术要求

07 汽车安全芯片检测与认证

08 汽车安全芯片发展趋势和建议

01

汽车信息安全概述

1.1. 汽车信息安全形势

随着汽车行业的智能化、网联化趋势加速发展，车辆信息安全已成为全球范围内关注的焦点。智能网联汽车通过集成先进的通信、导航、传感和控制技术，为用户提供前所未有的信息化和智能化。然而，这些先进技术也带来了新的安全风险与挑战，使得车辆信息安全形势愈发复杂和严峻。这些风险不仅关乎个人隐私和财产安全，更直接威胁到人身安全、品牌信誉乃至公共安全。

1.1.1. 车辆信息安全风险

人身安全

智能网联汽车通过感知、决策和控制实现自动驾驶，一旦其信息系统遭受攻击或出现故障，可能导致车辆失控，从而引发严重的交通事故，危及驾驶员和乘客的人身安全。例如，黑客可能通过远程攻击控制车辆的制动系统、转向系统等关键部件，使车辆失去控制。

数据隐私

智能网联汽车在运行过程中会收集大量的驾驶数据、乘客信息以及车辆状态信息等敏感数据。这些数据一旦泄露或被非法利用，将严重威胁个人隐私安全。黑客可能通过攻击车辆的信息系统，窃取或篡改这些数据，用于不法目的。此外，车辆信息系统中还可能存储着车主的支付信息、位置信息等敏感数据，这些数据一旦泄露，将给车主带来极大的安全隐患。

经济损失

车辆信息安全问题还可能给车主和车企带来巨大的经济损失。一方面，车主可能因为车辆信息泄露而遭受诈骗、身份盗用等经济损失；另一方面，车企可能因为车辆信息系统遭受攻击而导致生产中断、售后服务受阻等经济损失。此外，车辆信息安全问题还可能引发法律纠纷和赔偿责任，进一步增加车企的经济负担。

品牌信誉

车辆信息安全问题对车企的品牌信誉构成严重威胁。一旦车辆信息系统出现安全漏洞或被黑客攻击，将严重损害车企的品牌形象和声誉。消费者可能对车企的技术实力和产品质量产生质疑，从而影响车企的市场竞争力和销售业绩。此外，车辆信息安全问题还可能引发公众对智能网联汽车的信任危机，阻碍整个行业的健康发展。

公共安全

智能网联汽车作为智慧城市的重要组成部分，其信息安全问题还可能对公共安全构成威胁。一旦智能网联汽车的信息系统同时遭受攻击或出现故障，可能导致交通瘫痪、事故频发等严重后果，严重影响社会

秩序和公共安全。此外，黑客还可能利用智能网联汽车的信息系统进行网络攻击或恐怖活动，对国家安全和社会稳定构成潜在威胁。

1.1.2. 车辆信息安全存在的挑战

技术没有统一标准和测评方法

➤ 缺乏统一标准：车辆信息安全领域目前尚未形成全球性或区域性的统一标准，不同国家、不同厂商之间的技术标准存在差异，导致车辆信息安全评估和防护难以统一。

➤ 测评方法不完善：由于技术标准的缺失，车辆信息安全的测评方法也缺乏统一性和科学性。这使得车辆信息安全的评估结果难以客观、准确地反映实际情况，也给黑客攻击提供了可乘之机。

技术瓶颈难以突破

➤ 安全防护技术滞后：随着智能网联汽车的快速发展，车辆信息安全的防护需求也在不断提高。然而，目前的安全防护技术仍然存在滞后性，难以应对日益复杂的攻击手段。

➤ 加密技术瓶颈：数据加密是车辆信息安全的重要手段之一，但现有的加密技术在处理大量数据、保证实时性方面仍存在瓶颈，难以满足智能网联汽车对数据安全性和实时性的双重需求。

成本居高不下

➤ 研发投入高：车辆信息安全技术的研发需要投入大量的人力、物力和财力，且研发周期长、风险高，导致成本居高不下。

➤ 维护成本高：车辆信息安全系统的维护也需要持续的资金投入，包括系统升级、漏洞修复、人员培训等方面。这对于车企而言，无疑增加了运营成本。

法律法规亟须完善

➤ 法律法规滞后：与智能网联汽车的快速发展相比，相关法律法规的制定和修订显得滞后。现有的法律法规难以全面覆盖车辆信息安全的各个方面，导致监管空白和漏洞。

➤ 法律责任不明确：在车辆信息安全事件中，法律责任往往难以明确界定。这既不利于维护用户的合法权益，也不利于车企的合规经营。

缺乏用户教育与安全意识

➤ 虽然用户对车辆信息安全的需求日益增强，但大多数用户仍缺乏足够的安全意识和防范能力。因此，加强用户教育，提高用户的安全意识，是保护车辆信息安全的重要一环。

综上所述，车辆信息安全形势面临诸多风险和挑战。为了保障智能网联汽车的安全稳定运行，需要政府、车企、供应商和用户共同努力，加强技术研发、完善法规标准、提升用户安全意识等措施，共同构建一个安全、可靠的智能网联汽车生态系统。

1.2. 国家相关政策法规

随着汽车技术的不断进步，尤其是智能网联汽车的快速发展，不仅带来了前所未有的便捷性和智能化体验，同时也带来了信息安全和数据安全的重大挑战。为了切实保障汽车行业的稳健发展，有效维护广大用户的隐私权益和数据安全，国家高度重视并积极应对，及时出台了一系列政策法规。旨在构建完善的汽车信息安全和数据安全保护体系，为汽车产业的可持续发展提供坚实的法律保障。

2016年11月，全国人民代表大会发布了《中华人民共和国网络安全法》，该法旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。

2018年，公安部发布《网络安全等级保护条例》，该条例旨在通过分等级逐步加重的保护措施，保障关键信息基础设施的安全。对于汽车领域，特别是智能网联汽车，该条例要求制造商和服务提供商按照网络安全等级保护制度的要求，履行安全保护义务，确保汽车系统和数据的安全。

2019年5月，国家互联网信息办公室发布了《数据安全管理办法》，该办法依据《中华人民共和国网络安全法》制定，旨在维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全。对于汽车领域，该办法要求汽车制造商和服务提供商建立健全数据安全管理制度，加强数据收集、存储、传输、处理等环节的安全防护。

2021年6月，全国人民代表大会通过了《中华人民共和国数据安全法》，该法旨在规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

2021年7月，工业和信息化部发布了《关于加强智能网联汽车生产企业及产品准入管理的意见》，该意见中明确提出应加强数据和网络安全管理，需强化数据安全管理能力并加强网络安全保障能力。

2021年8月20日，全国人民代表大会通过了《中华人民共和国个人信息保护法》，该法旨在保护个人信息权益，规范个人信息处理活动，汽车数据处理者在处理涉及个人信息的数据时，必须遵守该法关于个人信息收集、使用、存储等方面的规定。

2021年10月，《汽车数据安全管理若干规定（试行）》施行，该法规对汽车领域数据安全管理及数据安全保护提出明确要求。

1.3. 标准规范要求

从整车信息安全标准来看，2024年8月，国家市场监督管理总局、国家标准化管理委员会批准发布GB 44495-2024《汽车整车信息安全技术要求》，该标准规定了汽车信息安全管理体系要求，以及外部连接安全、通信安全、软件升级安全、数据安全等方面的技术要求和试验方法。对于提升我国汽车产品的信息安全防护技术水平、强化产业链风险防范和应对网络攻击的能力具有重要意义。

汽车安全芯片作为保护车辆系统安全、用户数据隐私及确保车辆功能正常运行的关键器件，在整车信息安全中扮演着关键角色。不同汽车安全芯片的功能设计和资源配置各有侧重，导致主机厂产品选型困难，产品亟需通过专业化、标准化的测试验证，解决行业选型困难的问题。因此，亟需汽车安全芯片技术要求及试验方法标准化。

在标准规范方面，信息安全通用标准（Common Criteria，以下简称“CC标准”）和GM/T 000《安全芯片密码检测准则》两项标准对芯片的信息安全能力进行了要求，但没有针对汽车芯片行业和汽车应用场景进行适配。因此，为了满足汽车芯片行业的需求，相关国家标准与行业标准也在制定当中，主要包括推荐性国家标准**《汽车芯片信息安全技术规范》（以下简称“芯片信息安全标准”）和行业标准《汽车安全芯片技术要求及试验方法》（以下简称“安全芯片标准”）**。

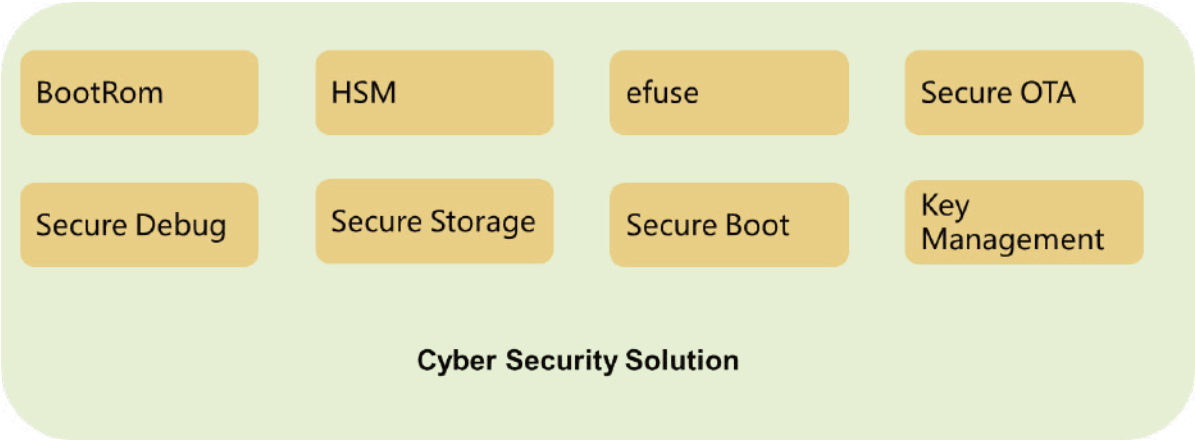
芯片信息安全标准为正在制定过程中的推荐性国家标准，由全国汽车标准化技术委员会提出并归口。芯片信息安全标准规定了汽车芯片信息安全需求分析方法、汽车芯片信息安全需求与安全功能的映射关系，以及汽车芯片信息安全功能技术要求及试验方法等，完成了对汽车芯片信息安全技术体系的补充，对于所需具备的安全功能与安全等级给出了参考。该标准给出了推荐满足的安全功能与对应的安全等级，包括密钥保护、密码算法支持、随机数生成、关键安全参数保护、固件更新支持、安全运行环境、权限控制、自测试、物理防护、安全启动机制、软件攻击保护机制、个人信息保护、漏洞管理和安全生命周期管理机制。

安全芯片标准是针对汽车安全芯片所制定的行业标准，2023年，全国汽车标准化技术委员会在工业和信息化部的指导下，启动该项标准的研究与制定工作。2024年5月24日，工业和信息化部下达了《汽车安全芯片技术要求及试验方法》标准制定计划。**安全芯片标准**规定了汽车安全芯片的技术要求及试验方法，适用于汽车安全芯片的设计开发、测试、评估和应用。结合汽车安全芯片的应用场景与特点，安全芯片标准对汽车安全芯片的功能、性能、电特性、电磁兼容、功能安全、信息安全、环境可靠性、研发与生产保障等内容进行了规范。

1.4. 汽车芯片信息安全的意义

早期由于汽车联网需求比较少、硬件设备本身设计的资源有限，信息安全考虑的也比较少，导致自身的防护能力很弱，容易导致被恶意攻击。随着智能网联汽车、车车及车路协同通信等车联网技术的发展，汽车的信息安全越来越被关注，国内外也陆续出台了一系列的政策法规和标准，对汽车整车的信息安全进行保护。虽然汽车芯片的处理能力（包括功能、性能等）在不断提升，如果芯片自身的信息安全防护能力过于薄弱，将导致芯片内的固件和应用也很容易受到攻击，比如程序篡改，敏感信息（如密钥等）泄露等。

越来越多的政府、行业组织的最佳实践也明确提出智能网联汽车的安全需要构建在安全的单元、部件和芯片基础上，比如EVITA、GSMA关于汽车安全的要求，汽车安全芯片等硬件密码模块已成为智能网联汽车的安全基础，日益成为行业普遍认可的入门级安全门槛。在参考已有国内外安全芯片标准、产品的基础上，目前汽标委TC114正在编制的汽车行业标准《汽车安全芯片技术要求及试验方法》，对国内汽车安全芯片统一标准、为顺利大量规范上车做好准备。



芯片级汽车信息安全解决方案

汽车信息安全的核心是保证使用主体的机密性、完整性和真实性。因此，安全芯片需要提供一系列的信息安全服务。

首先，安全存储是车规芯片的核心功能之一。它需要提供一个可信的环境，用于存储敏感信息，如密钥、证书等。例如SecureNVM（安全非易失性存储器）作为可信存储环境，能够确保敏感信息的安全性和可靠性。

其次，为了满足不同密码算法的性能要求，车规芯片还需提供相应的密码算法硬件加速器和密钥管理功能。这些服务包括但不限于：

- 对称密码硬件加速器：基于私密密钥的数据加解密，如SM系列算法、AES算法，能够提供高速、安全的加密解密服务；
- 非对称密码硬件加速器：用于数字签名、验签以及数据加解密等操作，确保数据的完整性和真实性；
- 摘要硬件加速器：常用于数据完整性检查和身份验证等场景，如基于摘要的HMAC算法，能够提供快速、准确的身份验证服务；
- 密钥管理功能：包括密钥导入、密钥协商、密钥派生等操作，确保密钥的安全生成、存储和使用等。

此外，为了衡量和保证整个ECU系统的完整性和可用性，车规芯片还需要提供安全启动和可信启动等功能。这些功能能够确保ECU系统在启动过程中不被恶意篡改或破坏，从而保证汽车的正常运行和安全性。

02

汽车信息安全需求分析

通信技术的发展，带动了车联网的迅猛发展。车联网通过通信技术，实现车内、车云、车车、车路等全方位的互联互通，促进汽车智能化演进，提升汽车的智驾能力，构建新型交通服务业态，从而提高交通效率，改善车辆驾乘感受，为用户提供智能、安全、高效、个性化的综合服务。

2.1. 通信安全

联网包括智能网联汽车、移动智能终端、车联网服务平台、路侧终端等设施，涉及车路通信、车云通信、车内通信等场景：

- 车路通信：智能网联汽车通过移动蜂窝网络、C-V2X、WLAN、射频通信 （RFID）等技术与路侧终端进行通信。
- 车云通信：智能网联汽车通过蜂窝网络、卫星通信、WLAN等与车联网服务平台通信，传输车辆数据，接受服务平台下发的远程控制指令。
- 车内通信：智能网联汽车内部不同零部件之间通过总线等方式进行信息交互，传输控制指令和车辆工况信息。

车联网通讯安全包括如下方面：

- 加密通信：车辆与外部网络（如云端、其他车辆、基础设施）的通信应实现端到端加密，确保数据在传输过程中不被窃取或篡改。
- 身份验证：车辆应实现与通信对方的双向身份验证，确保只有经过授权的设备才能接入车辆网络。

安全协议支持：车辆应支持相关的安全协议与标准，如TLS、IPSec等，以确保与外部网络通信的安全性。

车联网是车路云协同一体化发展的的重要技术支撑，对推动汽车、交通、通信等产业业的转型升级具有重要意义。然而，庞大复杂的网络架构也暴露了大量的攻击面，进而可能造成车辆盗刷、信息泄露、行车安全等事故，亟需依托安全芯片的可信计算平台用于处理车联网中传输的交互信息，保障车联网高效、可靠、安全运行。

2.2. 安全升级

车辆安全升级在车联网时代扮演着至关重要的角色，尤其是OTA技术实现了数据包下载与刷写的无缝对接，支持智能网联汽车安全防线的构筑，为了实现车辆安全升级，需要保证升级包安全和升级链路的通信安全，为此需要实现以下安全需求：

- 硬件级安全加固

安全芯片集成：车辆应集成专用的安全芯片，负责处理敏感数据的加密、解密及身份验证操作，确保数据在传输和存储过程中的安全性。

- 软件与固件安全

安全启动机制：车辆应实现安全启动，确保在每次启动时，车载系统的完整性得到验证，防止恶意软件或未授权代码的加载。

软件更新安全：车辆应支持安全的软件更新机制，包括加密传输更新包、完整性校验及身份验证，确保软件更新过程中不被攻击者利用。

2.3. 接入安全

汽车朝着智能化方向不断演进，车辆内部存储的敏感数据也越来越多。汽车数字钥匙的出现，解决了传统射频钥匙的安全痛点，也给用户提供了显著便利。然而，数字钥匙的安全性高度依赖密钥、数字证书等与用户密切相关的敏感数据。若密钥等信息泄露，车辆可能被不法分子盗走，造成用户财产损失，并影响整车企业的口碑。

未来，车辆内部可能会存储包括用户人脸、虹膜、指纹等生物信息，用于打造个性化的产品，例如智能座舱、生物支付等场景。因此，用户的生物识别信息须存储在安全可信的存储环境。

基于安全芯片，设计方在车辆设计开发阶段，可以将与用户相关的敏感数据，包括密钥、证书，以及生物识别信息，存储在安全芯片中，为用户提供可靠、便利的用车体验。

2.4. 诊断安全

汽车与人们的出行安全息息相关，车辆发生故障时的诊断安全也显得尤为重要。

OBD系统主要由传感器、控制器和故障指示灯等组成、传感器负责采集车辆的各种运行参数，如车速、发动机转速、电池电量、电机温度等。控制器对传感器采集到的数据进行分析处理，判断车辆是否存在故障。如果检测到故障，控制器会将故障信息存储起来，并通过故障指示灯等方式提醒驾驶员。OBD诊断为车辆维修提供重要的技术支持。通过读取故障代码和实时监测车辆的运行参数，维修人员可以快速确定故障的类型和位置，从而提高维修效率和准确性。

网络诊断是通过车载通信模块，车辆的OBD系统与远程服务器进行通信，将汽车的故障信息，并把故障码上传至数据处理中心，系统在不打扰车主的情况下复检故障信息。专业技术人员可以通过网络并根据这些信息对车辆进行远程诊断和故障排除，为消费者提供更好更及时的技术支持和售后服务。

2.5. 代码安全

车辆的EEA架构内包含几十个ECU，由这些ECU构成了整车的电子控制系统，这些ECU的功能主要由运行在其上的固件代码来决定，而固件代码的安全决定了ECU的安全，从而决定了整车的安全，假定一辆车的转向系统固件被恶意篡改，在车辆转向期间无法正常转向，将对车辆及其周围的行人和设施造成严重的危害，故保护ECU代码的安全是必要的，也是必须的。

针对固件代码的保护，其核心要求如下：

- 固件代码完整性：固件代码是完整的，未经过篡改的；
- 固件代码真实性固件代码来源合法，是由ECU开发者开发并授权的；

完整性和真实性的验证，需在处理器上电启动，加载固件代码前进行验证，可使用密码算法针对完整性和真实性进行验证，具体验证方法多种多样，在此举例说明如下：

- 完整性验证：可使用对称算法，如SM4、AES等，对固件代码计算MAC，并与预存储的合法MAC进行对比，判定固件完整性；
- 真实性验证：可使用非对称算法，对固件代码和预存储的签名值进行验签计算来验证真实性，算法可使用如SM、ECC、也可使用RSA算法，但鉴于目前量子计算机的威胁，未来可能需要升级为抗量子密码算法。

从以上的分析可知，此时代码安全的核心需求是：

- 保护密钥和校验数据的存储安全：即要求芯片具备安全存储能力，防止密钥和校验数据被提取或篡改；
- 保护验证过程的计算安全：即要求芯片具备安全计算能力，防止计算过程被攻击造成密钥的露；

因此，安全芯片可用来存储校验相关的密钥和数据，能够通过安全计算能力来支撑验证过程的安全性。

2.6. 数据安全

随着汽车智能化和网联化的发展，车端安全芯片在保护密钥、隐私信息、证书、数字钥匙和信任根等方面扮演着至关重要的角色。车端安全芯片是汽车信息安全的核心硬件，其保护措施的完善性直接关系到车辆的安全性和可靠性。基于当前的安全芯片技术和行业标准，以及企业的最佳实践，本白皮书为车企提供全面的保护措施建议。

2.6.1. 哪些数据需要保护

2.6.1.1.需要保护的数据

智能汽车为了提高用户体验，需提供更多智能化功能，需要采集和处理大量用户和环境数据，以下列举一些典型需要保护的车端数据：

- 个人身份信息：包括车主和乘客的姓名、身份证、电话号码等。
- 车辆静态信息：如车牌号、车辆识别码（VIN）等。
- 车辆动态信息：包括位置信息、行驶轨迹等。
- 驾驶习惯：如驾驶员习惯、车辆使用频率等。
- 生物识别特征信息：如指纹、声纹、人脸、心率等。
- 敏感区域地理信息：军事管理区、国防科工单位等重要敏感区域的地理信息。
- 经济运行数据：车辆流量、物流等反映经济运行情况的数据。
- 汽车充电网运行数据：涉及新能源汽车的充电网络运行数据。
- 车外视频、图像数据：包含人脸信息、车牌信息等的车外视频、图像数据。

2.6.1.2.受保护原因

这些用户和环境数据需要采取适当的措施加以保护，主要基于以下原因：

- 隐私保护：防止个人身份信息和生物识别特征信息被滥用或泄露，保护个人隐私。
- 安全合规：符合相关数据安全法规和标准要求，如GB/T 44464-2024《汽车数据通用要求》。
- 防止滥用：避免车辆动态信息和敏感区域地理信息被用于非法用途，保护国家安全和公共利益。
- 维护经济安全：保护经济运行数据不被非法获取，维护国家经济安全。
- 保障消费者权益：确保车主和乘客的合法权益不受侵害，尤其是在发生交通事故时能够准确维权。

2.6.2. 基于安全芯片的保护措施

以下列举常见数据安全威胁场景及其保护方案。

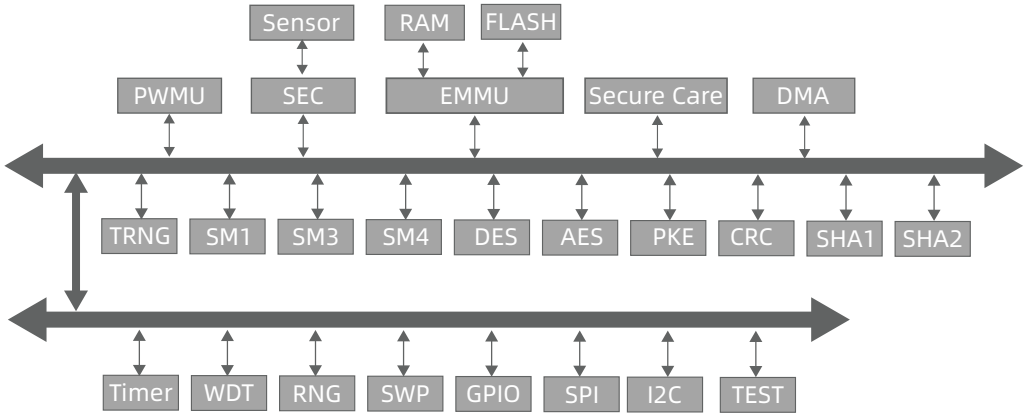
威胁场景	威胁描述	保护措施	措施描述
侧信道攻击	攻击者利用设备的接口对芯片进行电磁和功耗分析，无需破坏芯片即可获取敏感信息。	掩码	采用掩码技术、隐藏技术、混淆技术等降低侧信道信息与密钥的相关性。
故障注入攻击	通过电压、时钟等故障引起电路异常，分析芯片内部敏感信息或改变程序运行。	硬件加固	用传感器检测故障，逻辑和时钟冗余检查故障，金属外壳和特殊封装抑制攻击，逻辑深埋增加故障注入难度。
物理攻击	去除芯片封装，对内部电路进行电接触，结合其他攻击手段获取芯片内部敏感信息。	安全存储	◆ 采用被动屏蔽层和主动屏蔽层增加攻击难度，特殊封装，信号完整性和机密性保护。 ◆ 存储加密密钥、证书和其他敏感数据，防止非法访问和泄露。
身份伪造	攻击者冒充合法用户或设备，进行未授权的操作。	身份认证	加强身份认证机制，如使用数字证书和签名技术，确保通信双方的身份真实性。
重放攻击	攻击者截获并重新发送数据包，以执行未授权的操作。	安全通信	在安全通信方面，以HSM及证书体系为基础，具有完整性、加密性、假名化、匿名化等特点，实现数据隐私保护。
总线攻击	攻击者通过CAN总线等车辆内部通信网络进行攻击，可能导致车辆控制被非法接管。	安全通信	在车载设备中增加安全芯片，实现车内通信加密，身份识别，以及OBD诊断的安全接入，阻止非法报文发送。
固件劫持与篡改	攻击者篡改固件，植入恶意代码，控制车辆或窃取数据。	信任根 安全启动	◆ 信任根：建立信任链的来源，涉及安全启动和密钥管理。例如，在车端安全体系上，通过安全芯片和HSM进行硬件加固、网络加固。 ◆ 安全启动：确保ECU系统在启动过程中不被恶意篡改或破坏。 通过安全芯片SE+HSM，采用安全启动、可信区域、加密技术完成硬件安全设计，打造边界防护、车端安全、PKI认证传输、安全服务四大体系。

03

汽车
安全芯片概述

3.1. 安全芯片架构

安全芯片，Secure Element，也称为安全单元，是专为信息安全而设计的用于保护数据和应用安全的集成电路芯片。其具备硬件级别的安全保护机制，充分考虑了侵入式和非侵入式等各种攻击手段，针对性在软硬件上设计了多种防护措施，能够防止数据泄露，篡改和非法访问，能够保护信息的机密性，完整性和可用性。



安全芯片架构示意

安全芯片的硬件构成：

- CPU：Secure Core，安全内核，是安全芯片的CPU；
- 存储器：通过EMMU管理RAM和Flash；
- 电源管理：PWMU管理芯片电源系统；
- 安全IP：由安全传感器和其他安全设计构成；
- 安全算法：支持商用密码算法，国际常用算法，基于安全设计，可实现安全计算；
- 通信：可支持SWP，I2C，SPI，7816等通信接口与协议，支持GPIO；
- 随机数：支持真随机数生成，为系统提供高质量真随机数；
- 定时器：为系统提供定时器功能；

从基本功能角度看，安全芯片具备CPU，存储器，FLASH/RAM，定时器等IP，与MCU架构类似，但安全芯片在此基础上，通过实现各类安全设计，可做到防范各类攻击，这些安全设计，是安全芯片区别于非安全芯片的核心设计。

3.2. 安全芯片安全设计

3.2.1. 有源屏蔽技术

有源屏蔽防护措施采用顶层金属实现，覆盖安全芯片有效区域。当顶层金属被破坏后（如切断），安全芯片在工作过程中能够检测出来有源屏蔽连接异常，从而进入安全的状态，避免内部敏感信息泄露。

有源屏蔽技术主要是用于防止在芯片工作过程中，攻击者通过探针探测或修改安全芯片内部信号，以获得攻击者需要的敏感信息。

3.2.2. 存储器数据/地址加密加扰

安全芯片采用专用的存储加密电路来进行存储器内部数据的加密处理。通常安全芯片内部包含RAM，ROM，FLASH，EEPROM等不同类型的存储器，为了降低或避免通过物理攻击直接读取存储器数据的安全风险，安全芯片的数据或执行代码需要在写入存储器时进行加密操作，在从存储器读出时进行解密操作。

3.2.3. 总线数据保护

安全芯片中处理的敏感数据在CPU、存储器以及外设间，通过总线进行传输，因此对于总线进行探测，获取威胁信息安全的敏感数据，是物理攻击中常见的攻击方式。

保护总线传输数据的主要方法是对总线传输数据进行加密。

3.2.4. 关键信号隐藏

安全芯片的敏感信号主要包括标识芯片内部安全状态的信号和发生安全威胁后产生的报警信号，安全芯片内部的数据和地址总线，各个安全传感器的输入输出信号等。同时对于在版图上较容易识别的模块进行额外保护，防止利用物理攻击进行信号的追溯。

3.2.5. 传感器

在安全芯片中，包含了多种传感器，包括内/外部电压传感器，内/外部频率传感器，温度传感器，光传感器，电压毛刺传感器等。这些传感器的设计主要用以抵抗针对安全芯片的各类扰动攻击。

3.2.5.1.电压传感器

电压传感器的作用是检测安全芯片的工作电压，使得安全芯片始终工作在合理的工作电压范围内，确保整个系统的功能正常。

3.2.5.2.温度传感器

温度传感器的作用是实时检测安全芯片（或者环境）的温度，使得安全芯片始终工作在合理的温度范围内，确保整个系统的功能正常。

3.2.5.3.内外部频率传感器

内外部频率传感器主要功能是检测安全芯片的外部输入时钟信号和内部时钟信号的工作频率，使得安全芯片始终工作在合理的频率范围内，确保整个系统的功能正常。

3.2.5.4.电压毛刺传感器

电压毛刺传感器的作用是检测安全芯片的工作电压毛刺，使得安全芯片在工作期间能够检测到电压上存在的毛刺，确保整个系统的功能正常。

3.2.5.5.光强传感器

光强传感器的作用是检测安全芯片的工作环境光强，使得安全芯片在工作期间能够检测到异常的环境光强，确保整个系统的功能正常。

3.2.6. 数据完整性校验

安全芯片中包含寄存器和不同类型的存储器，在芯片工作过程中，安全芯片内部运行的密钥及其他敏感数据会存储在RAM、ROM、FLASH或EEPROM以及寄存器中。

无论安全芯片处在工作中或是未工作的状态，存储在ROM、FLASH或EEPROM中的数据都有被攻击导致数据被改写的风险；而RAM和寄存器中的数据在安全芯片工作过程中，有可能会被改写。安全芯片对存储数据采取各种校验方法来保证数据完整性。

3.2.7. 随机掩码

对于安全芯片中的密码侧信道分析，随机掩码在理论上是最有效的防护手段。由于侧信道分析是基于已知输入输出数据，根据采集的功耗曲线和密码运算中间值的相关性来进行密钥分析的技术，因此改变安全芯片实际运算数据和输入数据的相关性，破坏侧信道分析中密码运算中间值和功耗曲线相关性的前提条

件，就可以防止安全芯片运算过程中的密钥信息泄露，达到防止侧信道分析的效果。

3.2.8. 功耗隐藏/功耗噪声

功耗噪声的施加可以在安全芯片进行密码运算前后以及运算过程中添加，使得真实运算随机地分布在一个较为广泛的功耗噪声之中，使侧信道分析无法找到需要分析的对象，从而抵抗侧信道攻击。

3.2.9. 真随机数

在安全芯片中，无论是密码算法的密钥生成，密钥协商，还是安全功能的随机化操作，随机掩码，有源屏蔽、传感器输出保护等，都不可避免地需要用到高质量的随机数。

真随机数发生器为安全芯片提供真随机数输出，并包含标准要求的完整的真随机数自检功能。真随机数发生器需要满足AIS20[2011] PTG.2标准要求，同时如果是支持商密算法的安全芯片，其真随机数发生器还要满足商密相应级别对随机数发生器设计的要求。

随机数发生器在结构上通常包含物理噪声源，数字后处理电路和自检逻辑电路。

3.2.10. 不可逆测试模式

安全芯片在制造过程中使用的测试模式一般具有很高的权限级别。在安全芯片测试过程结束后，需要保证无法再通过任何手段进入测试模式，以保证安全芯片的配置正确和工作安全。

3.2.11.物理不可克隆功能PUF

PUF，Physical Unclonable Function,物理不可克隆功能，被称为芯片的“指纹”，因在芯片生产过程中，由于工艺在微观上的不可控，使不同芯片在微观上具有不一致性，通过特定的技术，将此微观上的差异进行提取，作为系统的信任根，为系统提供安全服务。

鉴于微观上差异，PUF具有不可预测性，不可复制，不需存储（上电产生），特征随机且唯一的特性。

3.3. 安全芯片安全服务

3.3.1. 真随机数生成

通过内置真随机数发生器，输出真随机数。可以保证对设备过去输出和内部状态的了解不能使攻击者能够预测未来的数据，对未来输出和内部状态的了解不应泄露先前的数据。

3.3.2. 数据加密与保护

提供对固件、关键数据流等提供硬件级数据加密、解密服务，有效防止数据在存储和传输过程中被窃取或篡改，增强数据安全性。

3.3.3. 密钥管理

支持密钥的生成和加密存储:所有存储的密钥都应以加密形式存在，确保即使存储设备被非法获取，密钥内容也无法被轻易解密。访问控制:对密钥存储设备的访问应严格控制，实施多因素身份认证和访问权限管理，确保只有授权人员能够访问密钥。

3.3.4. 数据安全存储

安全芯片提供安全存储功能，可以用于存储汽车中的敏感信息，如车辆识别码（VIN）、用户身份信息、加密密钥等。通过采用高安全级别的加密算法和硬件防护机制，确保这些信息不被非法访问或篡改。

3.3.5. 安全计算

基于安全芯片的安全设计方法，使安全芯片具备安全计算能力，在密码算法计算过程中抵抗侧信道攻击等各类攻击。安全芯片可支持SM2、SM3、SM4商密算法，及ECC、AES、RSA、SHA2等国际算法，为业务层提供广泛的密码算法服务。

3.3.6. 身份认证

通过安全芯片内部支持的算法接口等可以支持多种身份认证方式，如数字证书、密钥对等，用于实现车辆与用户、车辆与云平台之间的身份认证。这有助于防止未经授权的访问和操作等，确保汽车系统的完整性和安全性。

3.3.7.可信度量

其他系统启动过程中，安全芯片可以对系统的关键组件和软件进行可信度量和认证，确保系统启动的完整性和安全性。防止固件等关键信息被破解篡改。

04 车端安全攻防案例介绍

针对汽车的攻击行为在近年来引起了较大的关注，但是对汽车的攻击行为却并不是近年才有的。早期的攻击行为主要是破解汽车的防盗系统，对汽车或车内财物进行盗窃。随着智能网联汽车的发展，汽车不断向智能化、网联化、电动化、自动化的发展，软件定义汽车的趋势日益显著。目前智能网联汽车关键代码规模提升了10-100倍，代码漏洞呈指数级增长，同时汽车电子控制单元（ECU）的数量和车内连通性不断增长，导致汽车受到信息安全攻击的风险大大增加，汽车也面临着更多潜在的入侵途径。

对汽车的攻击行为包括了汽车非法功能激活、汽车控制以及隐私盗窃等多种行为。智能网联汽车的环境增加了攻击者入侵的途径和可能性。恶意的攻击者可能会通过夺取汽车的控制权对车主进行勒索，也可能在行车过程中引发安全事故，甚至有可能发动大规模的恐怖袭击。

汽车信息安全事件频发使得汽车行业安全态势愈发紧张。这些汽车信息安全攻击事件，轻则给企业产品发布及产品口碑造成影响，重则导致大范围的汽车召回或股价受损，造成的经济损失和安全代价不可估量。

早在2011年，德国马格德堡大学的研究员针对车载CAN总线网络系统，采用向ECU中插入非法代码、监听内部信息、DoS（拒绝服务）等多种攻击方法，成功影响了车窗升降、防盗警告指示灯、安全气囊以及中央网关等四个子系统的控制功能，使得上述四个子系统脱离驾驶者的正常控制，由此展示了对于车辆和人员及财产的严重安全隐患。

在2015年的美国黑帽大会上，研究人员发布了攻击细节，展示了攻击者针对某美国车企的车载娱乐系统发动伪装攻击，成功入侵行驶中车辆的CAN总线网络系统，远程获取汽车的关键功能操作权限，向车辆发动机、变速箱、制动和转向等系统发送错误指令，最终使这辆车翻覆到马路边的斜坡下。这次事件直接导致该公司在全球召回140万辆汽车，这也是首起因汽车信息安全问题导致的车辆召回。

其具体攻击步骤为：

- 利用3G伪基站跟汽车通讯模组建立连接，利用通讯端口上开放的后门，获取联网模块的最高控制权限；
- 通过联网模块，将篡改过的程序刷入CAN控制芯片里，进而实现对车内CAN总线的完全控制；
- 通过CAN控制器给车内其他控制器发送控制指令，实现对车辆的非法操控。

攻击者突破了以往汽车网络安全黑客的极限，即成功实现了非物理接触条件下对车辆进行远程控制。以往的黑客只能通过物理接触，或者只能控制单个车辆，最多进行近距离攻击，而上述攻击者可以攻击并控制全国范围内几乎所有安装了该型车机的同品牌车辆。

从攻击实例的分析也可以看出，实现汽车的远程控制不是单单通过某一个漏洞，而是通过一系列的漏洞才实现了非物理接触下的入侵，而另一方面也反映出汽车中的各个子控制器存在很多潜在的漏洞。

在此之后，汽车行业积极应对信息安全挑战，但即使是搭载了先进信息通信技术的新款智能网联汽车，同样无法完全回避网络攻击的威胁。

腾讯科恩安全实验室分别在2016年、2017年两次攻击美国某著名新能源车企产品，实现对车辆的无物理接触远程攻击，利用内核、浏览器、MCU固件、UDS协议及OTA更新过程中的多个高危安全漏洞，攻入到汽车的CID、IC、网关以及自动驾驶模块，随后该实验室将其发现的安全漏洞提交给该厂商用于安全性改进。

该安全实验室成功利用多个高危安全漏洞对该车型实施了无物理接触远程攻击，实现了对驻车状态下汽车天窗、转向灯、座椅、显示器、门锁系统的远程控制，以及行驶状态下对雨刷、后备箱、刹车系统的远程控制。具体攻击手段是通过无线（Wi-Fi/蜂窝）进入，破坏许多车载系统，如 CID（Center Information Display，中控显示系统）、IC（Instrument Cluster，仪表组）、Parrot（无线及蓝牙模块）和网关等，然后将恶意的 CAN 消息注入 CAN 总线。这是全球范围内第一次通过安全漏洞成功实现无物理接触远程攻入该车型，并实现任意车身和行车控制。

具体攻击过程是：

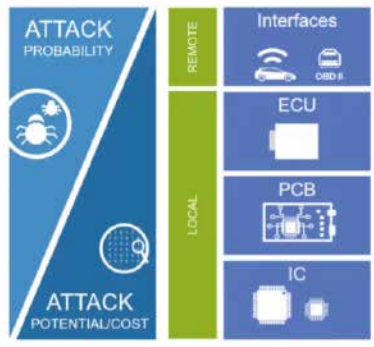
由于每辆该型产品都会提供WiFi热点，很多用户会将SSID的信息保存在车上，以便用于自动连接。如果伪造这个Wi-Fi热点，并将车载浏览器的流量重定向到攻击者的域名，即可实现远程攻击该车型。此外，当在蜂窝模式下，通过建立精心设计的域名，网络钓鱼和用户输入错误也会导致远程触发浏览器漏洞，实现在没有物理访问的情况下远程交付漏洞利用。另外，通过分析和利用该浏览器程序中的漏洞，可以获得该车型CID的shell，从而实现任意代码运行，并获得非法的控制权限。

2019年，腾讯科恩安全实验室在某欧洲厂商的多款自动驾驶汽车上，展示了利用车载信息娱乐系统和车载信息通信终端的漏洞远程无线入侵汽车，并进一步利用中央网关的安全缺陷，实现了向内部核心CAN总线注入恶意消息，获取了底层安全关键车内网络的控制权。

2020年，360集团智能网联汽车安全实验室针对另一欧洲车企产品的车载娱乐主机、车载通讯模块、车联网通信协议及后端服务等联网模块，发现了19个安全漏洞并利用漏洞形成攻击链路。

2021年，360集团智能网联汽车安全实验室发现了汽车操作系统QNX的多个安全漏洞，其中更有在通用漏洞评分系统(CVSS)中严重级别达到9.8分(满分10分)的远程代码执行漏洞，该漏洞成为影响车辆安全的重要隐患。作为汽车领域最大的操作系统供应商之一，BlackBerry发行的QNX在车用市场占有率达到75%，目前全球有超过230种车型使用QNX系统，包括大众、宝马、奥迪、保时捷、福特等众多知名汽车厂商，国内外数千万辆智能网联汽车中均搭载了基于QNX的车载娱乐系统。

综合来看，攻击者若想成功攻破汽车信息安全系统，大致可以从以下4个层次入手展开攻击：

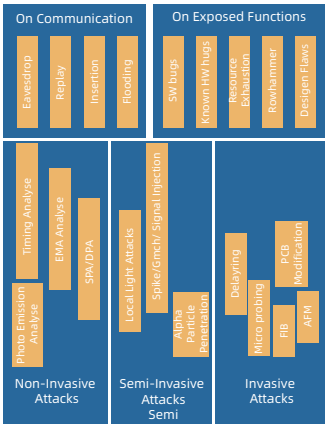


汽车信息系统攻击的侵入点种类

- 远程攻击，通过汽车的外部通道或接口进行攻击；
- 本地攻击，通过ECU的用户或受限的外部接口进行攻击；
- 本地攻击，通过PCB上互连线，测试点等进行攻击；
- 本地攻击，通过对IC芯片（MCU或者电源芯片等）进行攻击；

针对上述攻击中ECU/PCB/IC这3个层次的攻击对象，又可以细分为以下多种攻击手段：

- 通信攻击：私密通信监听，信息堵塞攻击，中间人攻击等。
- 暴露的功能模块攻击：软件漏洞，硬件漏洞，存储器溢出，栈溢出等软件攻击。
- 非侵入式攻击：时序攻击，SPA，DPA，EMA等。
- 半侵入式攻击：激光攻击，电压毛刺攻击等。
- 侵入式攻击：修改PCB/IC的连线，FIB攻击，微探针读取等。



本地攻击的攻击类型

05 汽车安全芯片主要应用场景

5.1. 乘用车T-Box应用

5.1.1. 应用场景功能介绍

T-Box，全称为Telematics Box，即车载智能通信终端，是一种安装在汽车内部的智能设备，它主要负责车辆与外部通信和数据交换。T-Box是车联网（Internet of Vehicles）和智能汽车的关键组成部分，它通过集成多种传感器和通信模块，实现车辆的远程控制、数据采集、故障诊断、信息娱乐等功能。

T-Box的应用场景非常广泛，主要包括以下几个方面：

远程控制：T-Box可以实现远程开锁、GPS追踪、动力控制管理、闪灯鸣笛寻车等功能，用户可以通过手机APP对车辆进行远程控制；

车况监测：T-Box可以实时监测车辆的各项参数，如电池电量、发动机状态、行驶里程等，帮助用户及时了解车辆状况， 预防潜在故障；

故障诊断：T-Box可以实时监测车辆的运行状态，一旦发现异常情况，会立即向车主发送警报信息，并为车主提供初步的故障解决方案，确保车辆安全；

节能环保：通过T-Box收集的车辆运行数据，用户可以合理规划出行路线，减少不必要的油耗和排放，降低出行成本，同时也有助于环保；

共享汽车：在共享汽车领域，T-Box可以实现远程开锁、定位、计费等功能，提高共享汽车的运营效率和服务质量；

充电服务：T-Box可以与充电桩进行通信，实现自动充电、智能充电等功能，提高充电的便捷性和安全性；

驾驶辅助：T-Box可以通过分析车辆运行数据和道路情况，为驾驶者提供智能化的驾驶辅助建议，提高驾驶安全性；

V2X通信：T-Box支持V2X（Vehicle-to-Everything）通信，能够提升行驶安全、提高交通效率、提供出行信息服务，辅助智能驾驶；

紧急呼叫服务：T-Box支持eCall服务，包括道路救援、自动碰撞通知等，为驾驶者提供紧急情况下的快速响应；

随着车联网概念的不断深化和应用场景的不断增加，T-Box的角色也变得尤为特殊，不仅作为通讯终端要负责对外通讯，同时备份了一些重要的车辆数据和用户身份信息，如果其遭受网络安全威胁，不管是对公司，还是对用户的损失影响都将是巨大的。

5.1.2. 应用场景的安全需求说明

T-Box（Telematics Box）作为车联网中的关键组件，面临的安全需求非常广泛，主要包括以下几个方面：

硬件安全

- 需要具备防拆保护措施，如开盖检测、拆机告警等
- 设备如开放调试接口的应在上市前进行禁用或采用安全调试模式
- 应具备足够的安全机制保证密钥的产生、分发、存储和销毁过程的安全性
- 关键加密算法实现应具备抵抗侧信道分析和故障注入分析等物理攻击的能力，防止根密钥被破解

操作系统安全

- 应支持安全启动机制，对引导程序或固件等进行有效性验证
- 升级过程应对升级文件进行签名校验和完整性校验，并确保升级失败后操作系统能有效恢复至升级前的正常工作状态
- 支持对重要事件的日志记录功能，并具有保证日志文件安全性的措施

软件安全

- 应采用签名认证机制，未经签名的应用软件须用户确认后才能执行下一步操作
- 不应非授权收集、传输用户个人信息
- 应具备代码混淆、加壳等安全措施，防止被逆向攻击
- 应采取访问控制机制，防止对系统资源和其他软件的非授权访问

数据安全

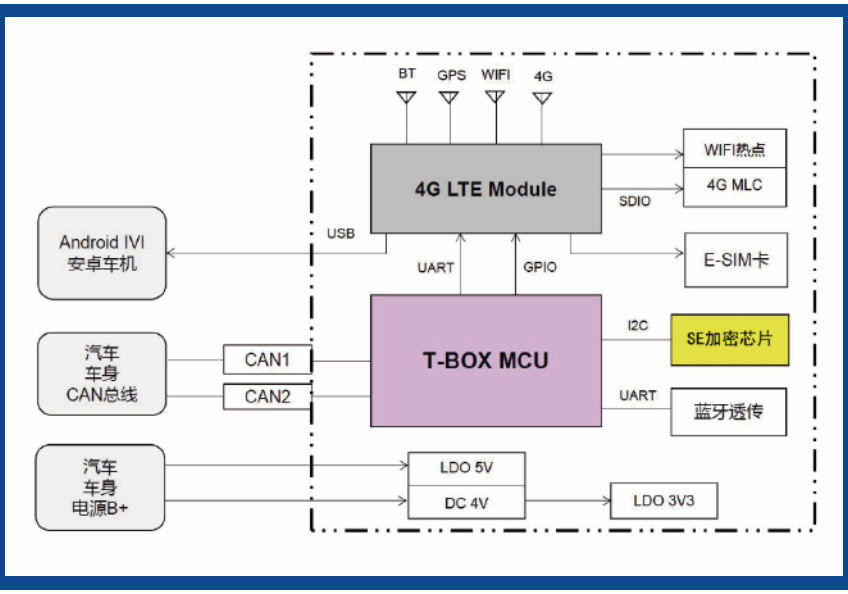
- 设备采集用户数据应对用户进行明确告知，在用户授权后可继续下一步操作
- 重要数据应加密存储，保证重要数据在存储过程中的完整性和保密性
- 数据的传输应进行完整性保护，防止数据被篡改和伪造

通信安全

- 应具备对通信数据的消息校验和认证机制，防止攻击者伪造、篡改信息
- 应采用控制策略避免大量集中地向CAN总线发送数据包，以避免造成总线拥塞和拒绝服务

这些安全需求覆盖了T-Box的硬件、软件、数据和通信等多个方面，通过采用安全芯片的解决方案可以有效保护车辆网络安全、数据安全以及用户隐私，确保车联网系统的稳定和可靠运行。

5.1.3. 如何用安全芯片去实现安全方案



安全芯片硬件逻辑图

软件架构图

业务流程

硬件安全增强	利用安全芯片（SE）的物理防攻击设计，提高T-Box的硬件安全防护能力。安全芯片内部集成了密码算法，能够抵抗物理攻击，如侧信道攻击和故障注入攻击。
安全启动	利用安全芯片实现安全启动机制，确保T-Box只运行经过认证的固件，防止恶意固件的执行和固件篡改。
数据加密与安全存储	使用安全芯片提供的数据加密功能，对T-Box中传输和存储的敏感数据进行加密处理，确保数据的机密性和完整性
安全通信	通过安全芯片实现安全的通信协议，对通讯数据进行加密、认证，防止中间人攻击、数据监听、篡改和否认。
身份认证与访问控制	利用安全芯片存储密钥和证书，实现T-Box与外部通信时的身份认证和访问控制，确保只有授权的设备和用户能够访问T-Box。

5.1.4. 应用案例

根据应用场景的安全需求，信大捷安自主研发的XSDM1505车规级轻量型安全芯片能够提供相应安全解决方案。此安全芯片具有功耗低和成本低等的特点，能够提供TLS通信协议中的身份认证、数据加密和数据完整性校验等系列算法能力，满足GB/T 32960等相关标准要求，为T-Box提供硬件级安全保障。

5.2. 商用车T-Box应用

5.2.1.应用场景功能介绍

商用车T-Box作为车联网信息交换场景的中心，可以实现深度读取并解析汽车的CAN总线数据和私有协议，实现采集、传输、分析车辆状态和车况信息等数据，并将收集的数据和分析处理结果通过移动通信网络上传到服务后台，实现降低油耗、降低碳排、减少车辆损耗、提升运营效率等目标。在商用车领域，以T-Box为核心的车联网服务中，可以帮助车企实现车辆的全生命周期管理，帮助车主实现降本增效，提升车主的用车体验等社会效益。

商用车T-Box的功能模块主要包括4G/5G模块、电话语言模块、以太网模块、GPS模块、CAN通信模块、电源模块、蓝牙模块、Airbag模块等，各个模块之间紧密联系，形成一个完整的远程通信终端。

T-Box作为商用车运行数据的收集者和实时通信的核心器件，其基于固定频率将车内各类控制器和传感器等功能器件的数据按约定的格式发送到平台，此类数据一般可以按照上报数据的业务类型、数据类型、车型、车号等多个层级进行设计和应用。例如，车辆在行驶过程中会将位置、车速、电量等信息按照固定频率上报云平台，云端应用基于这些数据，提供位置查找、超速提醒、电量提醒、地理围栏服务等信息给车主用户使用，形成良好的人车互动应用场景。

5.2.2. 应用场景的安全需求说明

《重型柴油车污染物排放限值及测量方法(中国第六阶段)》为国家污染物排放标准，并由生态环境部与国家市场监督管理总局联合发布，作为强制实施标准，为了监控重柴车排放情况，需要对新生产销售车辆进行车载T-Box前装改造，对于市场存量车辆，需由地方环保部门组织实施后装改造。

商用车T-Box利用已经安装在车辆上的车载通讯单元，实现将国家要求的车辆排放相关静态数据、动态数据和故障状态实时传输到政府平台。并要求使用安全芯片SM2算法对采集的车辆数据在上传时进行数字签名，防止数据被篡改。

针对新能源汽车的国标 GB/T 32960，其中《电动汽车远程服务与管理系统技术规范 第2部分：车载终端》针对智能汽车的联网设备T-Box做了说明，即单体式车载终端和集成式车载终端给出了明确技术指标。国标GB/T 32960.2-2016定义集成式车载终端为集成设计在车辆其他装置或系统的车载终端，而单体式车载终端则为单独设计为独立的装置或系统的车载终端，同时国标GB/T 32960.2-2016对存储在车载终端内的数据及车载终端与企业平台传输过程中的数据也做了相应的要求。“4.1.2 存储在车载终端内的数据及车载终端与企业平台传输过程中的数据是可加密的，加密数据应具有完整性、准确性和不可否认性。”在修订中的2025版本中，要求对采集的车辆状态数据进行数字签名后上送，且要求信息安全载体必需具备硬件安全机制。

5.2.3. 如何用安全芯片去实现安全方案

安全芯片是商用车T-Box中保证数据安全和防止车辆被恶意攻击的关键器件，其可以实现对数据进行加密和解密，以及实现访问控制和身份认证的安全功能。商用车T-Box中的安全芯片具有高安全的加解密算法，能够保护T-Box中的数据免受非法获取和篡改，保障商用车辆的信息安全。

基于商用车T-Box的安全芯片使用场景中，传输信道中的数据可以采用SM4分组加密算法，以保证数据传输的机密性，同时可以使用散列算法SM3保证数据的完整性，以防止数据在传输的过程中被篡改，还可以使用非对称算法SM2的私钥签名来保证数据的不可抵赖性，确保数据归属于特定的车辆。

5.2.4. 应用案例

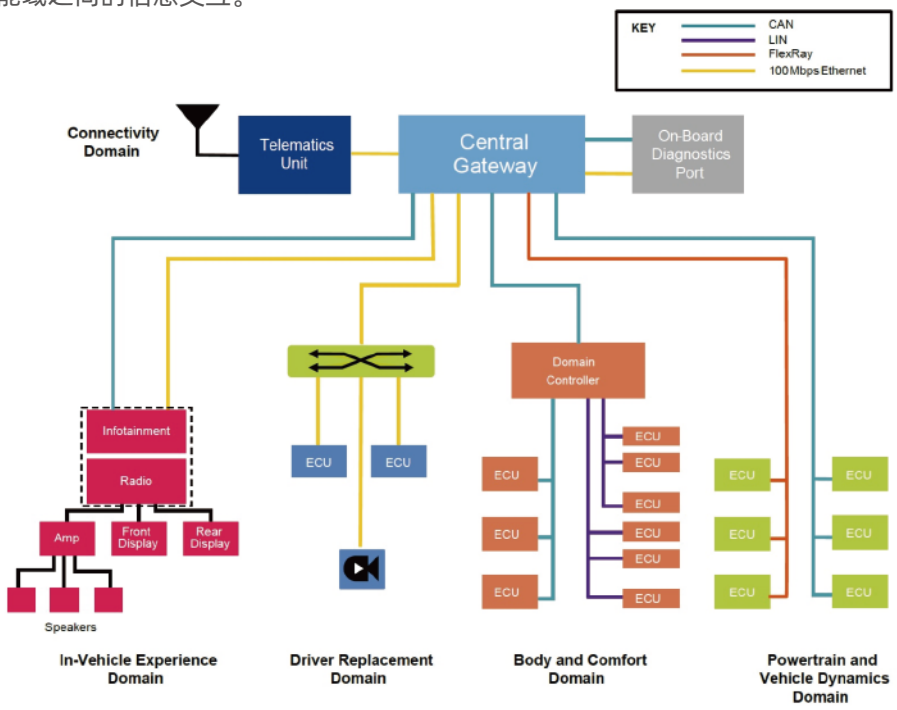
根据应用场景的安全需求，紫光同芯T97系列产品是基于安全芯片开发的一套适用于T-Box场景的安全解决方案，可为用户提供安全存储、身份认证、安全算法、IoT设备到云服务间的安全通信等功能，可保证芯到云，端到端的安全性。T97系列产品可应用于不同的主机平台和主机操作系统T-Box，来保证主机中各种不同应用的安全性。紫光同芯T9系列产品已助力多个厂家的T-Box在中国重卡市场占有率排名进入前三。

华大电子CIU98_B系列车规级安全芯片,满足商用车远程排放监控技术要求，满足非道路车辆污染物排放控制技术要求，通过了商密二级认证，已广泛部署于国内商用车与非道路车辆，为远程排放监控数据提供了安全保障。

5.3. 网关应用

5.3.1. 应用场景功能介绍

汽车网关（Vehicle Gateway）是一个电子控制单元，通常被称为中央网关，旨在安全可靠地在车辆内的多个网络间进行数据转发和传输。它通过不同网络间的隔离和不同通信协议间的转换，实现各个共享通信数据的功能域之间的信息交互。



汽车网关业务流程图

汽车网关的主要功能如下：

数据通信：汽车网关作为连接桥梁，能够实现不同总线类型（如CAN、LIN、FlexRay、以太网等）之间的数据交换，确保各个电子控制单元（ECU）能够高效协同工作。

协议转换：网关负责将一种通信协议的数据转换为另一种协议，使得不同类型的设备能够相互理解和交流。例如，它可以将来自发动机控制单元的数据转发到仪表盘显示。

安全管理：作为防火墙，汽车网关控制从外部接口（如互联网）到车辆内部网络的访问，并确保只有授权的节点能够相互通信。这种功能对于保护车辆免受网络攻击至关重要。

信息隔离：网关提供功能域隔离，例如在不受信任的信息娱乐系统和受信任的安全关键系统之间，确保信息流动的安全性和完整性。

故障诊断与维护：汽车网关能监控车辆内部网络的状态，支持故障诊断，并可通过空中软件更新（OTA）进行远程维护和升级，以保持系统的最新状态和安全性。

5.3.2. 应用场景安全需求

安全芯片在汽车网关上的应用涉及多种安全需求，以确保车辆信息系统的完整性、保密性和可用性。

主要的安全需求如下：

1. 数据加密与解密：安全芯片需要提供强大的数据加密和解密功能，以保护车辆内部和外部通信中的敏感信息。这包括对传输数据进行加密，确保信息在传输过程中的机密性和完整性，防止数据被截获或篡改。

2. 身份认证：安全芯片负责对设备和用户进行身份认证，确保只有经过授权的设备或用户才能访问车辆网络。这一功能对于防止未授权访问和潜在的网络攻击至关重要。

3. 访问控制：通过访问控制列表（ACL）等技术，安全芯片能够限制对车辆内部网络的访问权限，确保只有符合特定条件的用户或设备可以进行数据交互，从而增强车辆网络的安全性。

4. 敏感数据存储：安全芯片提供安全的存储解决方案，用于存放加密密钥、身份凭证及其他敏感数据。这种物理隔离措施能够有效防止物理攻击和侧信道攻击。

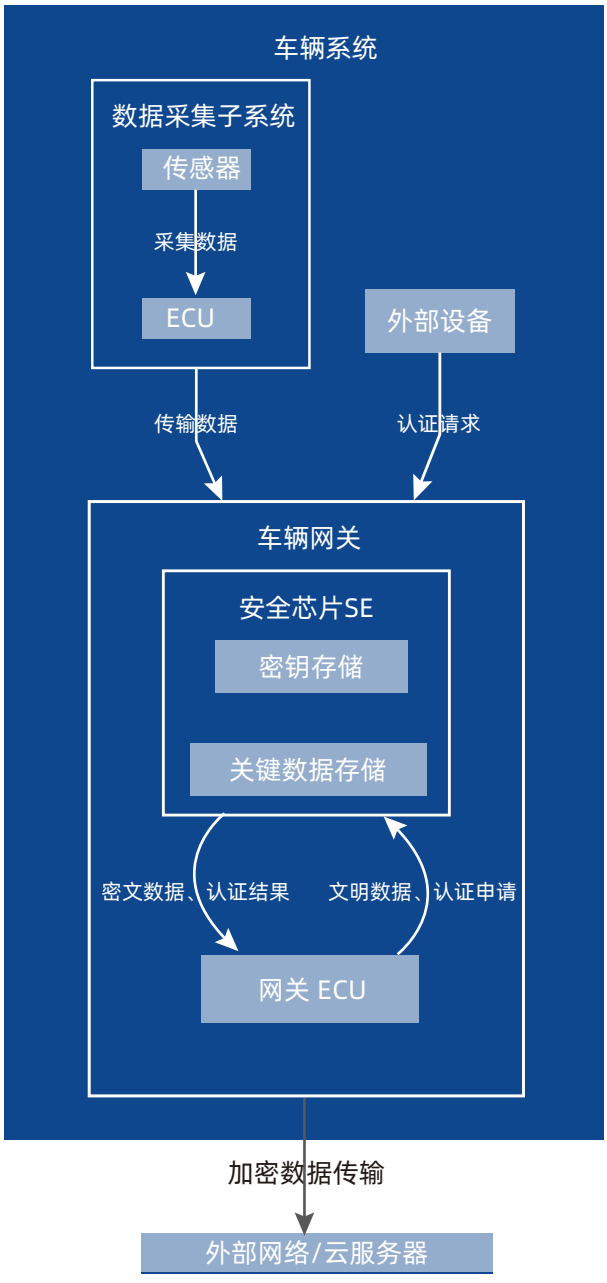
5. 软件更新安全：随着车辆软件的不断更新，安全芯片支持空中软件更新（FOTA）的安全性，确保更新过程不被恶意干扰或篡改。安全芯片能够验证更新内容的完整性和来源，保障系统始终处于安全状态。

6. 物理安全：安全芯片设计时考虑了物理攻击防护，如抗拆卸、抗故障攻击等。这些硬件级别的保护措施确保了芯片及其存储的数据不易被非法访问或破坏。

5.3.3. 安全方案实现

安全芯片 SE 是车辆系统的核心安全模块，负责关键数据存储、认证管理、数据加密和访问控制等功能，确保系统内部与外部设备之间通信的安全性。

概念框图如下：



汽车网关安全方案的实现

（1）认证管理与访问控制

√认证请求：当外部设备请求访问车辆网关时，SE 执行身份认证，确认请求者的合法性。认证通过后，SE 决定是否授权访问。

√访问控制：通过 SE 的访问控制功能，只有获得授权的设备和请求才能访问系统的敏感数据，防止未经授权的访问。

（2）密钥存储与关键数据保护

SE 提供密钥存储模块和关键数据存储模块，用于安全存储系统密钥和敏感数据。这些区域通过硬件保护，防止未经授权的访问，确保密钥和数据安全。

（3）数据加密与传输保护

车辆系统与外部网络/云服务器之间的通信由 SE 加密保护。加密技术确保传输过程中的数据安全，防止数据被截获或篡改。常用加密算法包括：

√对称加密：如 AES、SM4，适合快速加密大量数据的场景。

√非对称加密：如 RSA、ECC、SM2，适合认证和密钥交换等对安全性要求较高的场景。

（4）数字签名与数据完整性

在通信过程中，SE 通过数字签名（如 SM2 或 RSA）验证数据来源，确保消息未被篡改。同时，哈希算法（如 SM3）用于检测数据完整性，保证接收到的数据与发送时一致。

5.3.4. 应用案例

信大捷安自主研发的XSDM3275车规级安全芯片，具有较高的SM4等对称算法运算性能，能够面对HPC为代表的智能网关提供高性能的数据加解密能力，满足包括车载以太网等高速车内网通信的安全需求，并已经在国际知名Tier1项目中实现了量产应用。

5.4. 智能座舱应用

智能座舱作为集成多种先进的电子技术和智能化的系统，是实现人、车、生活深度融合的核心平台。随着汽车电动化、网联化、智能化的发展，智能座舱已从传统的信息显示和娱乐系统，升级成为集信息交互、智能控制、娱乐服务、车联网等多功能于一体的综合系统。

随着智能座舱的功能越来越丰富，它与座舱域以外的车内控制器或者是对车外的其它网联实体的交互也日益增多，这就使得智能座舱的信息安全面临着多样化的挑战。一方面，智能座舱涉及大量用户的个人隐私信息，如位置、行程、通话记录等，如果这些信息被泄露或被不法分子利用，将给用户带来极大的安全风险及经济损失。另一方面，智能座舱中的各种控制系统，如车控指令、车载支付等，如果受到网络攻击，可能导致车辆功能失效、财产损失甚至危及生命安全。为了保障智能座舱的信息安全，就需要从硬件、软件、网络等多个层面采取措施。而汽车安全芯片，作为智能座舱信息安全防护的基石，提供了加解密、来源认证、安全协议、安全存储等多方面的基础信息安全服务。汽车安全芯片在智能座舱的应用场景可分为以下几个层面：

5.4.1. 数据安全需求

用户个人信息保护

智能座舱系统存储了大量用户个人信息，包括联系人、行程记录、支付信息等。这些数据必须进行加密存储，并建立严格的访问控制机制。系统需要实现数据分级管理，对不同敏感级别的数据采用不同强度的加密算法和存储策略。汽车安全芯片可以提供芯片级别的加密和安全存储。

位置信息安全

导航系统产生的位置信息涉及用户隐私，汽车安全芯片可以提供完整的位置信息保护机制。

车辆状态数据保护

车辆运行状态、故障信息等数据对车辆安全至关重要，汽车安全芯片可以提供芯片级的防护措施，比如SecOC等技术用于进行实时数据的完整性保护、来源验证以及数据的加密等。

5.4.2. 支付安全

汽车安全芯片在车载支付中充当了“安全守卫”的角色，确保支付过程的各个环节都具备强大的安全保护机制。通过数据加密、身份验证、防止恶意软件、隔离存储以及远程更新等多重功能，安全芯片能够为用户提供安全便捷的支付体验。

支付数据加密和保护

安全芯片的核心功能之一是加密支付数据，以防止支付信息被窃取或篡改。它可以对支付过程中传输的敏感信息（如支付账号、银行卡信息等）进行加密，确保数据在传输过程中不被恶意攻击者截获或利用。这种保护机制可以有效防止支付信息泄露，保障用户的资金安全。

身份验证与认证

安全芯片可以在支付前对用户进行身份验证，如生物识别（指纹、人脸识别）。这种身份验证确保只有车主或授权的驾驶员能够使用车载支付功能，从而降低支付风险。认证过程通常在芯片内完成，避免将数据暴露在网络环境中，进一步提高安全性。

防止恶意软件攻击

汽车安全芯片可以在硬件层面提供安全的执行环境，隔离支付应用程序的运行空间，防止恶意软件或病毒对支付应用的干扰。这种隔离和保护使得支付应用即使在遭遇攻击时，仍能保证支付过程的安全性。

安全存储

支付系统通常需要存储用户的支付信息，如银行卡信息或虚拟卡片信息。汽车安全芯片可以提供安全的存储区域，以保护这些敏感信息。安全芯片中的存储模块经过特殊加固，即使汽车或系统被拆解，攻击者也难以直接获取到存储的信息。

5.4.3. 通信安全需求

数据加密

安全芯片的主要功能之一是为汽车内外部通信提供数据加密，确保数据在传输过程中不被截获或篡改，保证敏感数据（如位置、速度、导航信息）在无线传输时的安全性。通过对数据进行加密，安全芯片确保只有合法的接收方能够解密并读取信息，防止信息泄露。

身份认证和授权管理

安全芯片可以提供身份认证功能，确保通信的合法性。例如，安全芯片可以在车辆与云端或其他车辆通信前，通过公钥基础设施（PKI）对通信双方的身份进行验证，确认信息发送方和接收方的真实性和合

法性。通过这种双向认证机制，安全芯片可以防止未经授权的设备与车辆建立连接，从而保护通信的安全性。

数据完整性校验

安全芯片通过散列函数对通信数据进行完整性校验。这意味着在数据传输过程中，任何试图篡改数据的行为都会被检测到。通过校验信息的完整性，安全芯片可以帮助检测并防止数据篡改，确保接收到的数据是完整且可信的。

安全协议支持

汽车安全芯片可以支持多种安全协议，如TLS（传输层安全协议）、IPSec（互联网协议安全）、SecOC等，用于保障数据在传输层和网络层的安全。这些安全协议的应用可以确保车辆对内对外的通信安全，防止通信过程中信息被窃取或篡改以及验证信息的来源。例如，车与云（特别是私有云）之间的通信可以通过TLS协议来保护，而车内局域网通信则可以使用IPSec等协议来加密数据，用IPSec和SecOC等协议做来源验证。

5.4.4. 防物理攻击

安全芯片通常具有防篡改设计，能够抵抗物理攻击，包括防止芯片被拆卸、逆向工程、侧信道攻击、其他硬件攻击等手段。这一特性尤为重要，因为汽车可能会面临物理攻击风险，通过防物理攻击的设计，安全芯片能保护车载支付系统的核心安全。

5.4.5. 数字版权保护

内容加密与解密

安全芯片可以对受版权保护的多媒体内容（如音乐、电影、导航数据等）进行加密保护。加密的内容只有在特定授权的情况下才能解密播放，防止内容在未经许可的情况下被复制或分发。安全芯片可以直接在硬件级别进行加密和解密操作，有效地防止了内容在传输或存储过程中被非法访问。安全芯片通常内置支持多种数字版权管理协议（如Widevine、PlayReady、FairPlay等），以确保兼容不同的内容服务平台和数字内容提供商。通过支持标准化的DRM协议，汽车制造商和内容提供商能够更方便地实施版权保护措施，保证用户在车载系统中安全访问受保护内容。

密钥管理

汽车安全芯片可以提供密钥管理服务，用于生成、存储和保护解密所需的密钥。安全芯片的防篡改设计可以确保密钥的安全存储，防止未经授权的访问或篡改，从而保障受版权保护内容的完整性。通过安全芯片管理的密钥，仅有合法授权的用户和设备才能获取和使用密钥，进一步确保了内容的版权保护。

授权管理

安全芯片可以通过授权管理功能，限制内容的播放权限。例如，可以对内容的播放设备、播放次数、播放时间等进行控制，从而防止未授权的使用。授权管理的方式包括设备绑定（如限制内容只能在特定车辆或设备上播放）和时间限制（如内容在租赁期后无法访问），从而保障了版权方的利益。

5.4.6. 系统升级安全

验证升级包的完整性

安全芯片可以对升级包进行完整性验证，确保升级包在传输过程中未被篡改。通常情况下，升级包在发布时会附带数字签名，安全芯片通过验证签名的方式，确保升级包未被修改。

身份认证与授权管理

在进行系统升级时，安全芯片可以执行身份验证，确保只有授权的用户或设备能执行升级操作。通过公钥基础设施（PKI），安全芯片可以对升级请求进行认证，以确认升级操作是由合法用户或授权的服务器发起的。这样的身份认证机制可以防止未经授权的用户或攻击者利用升级功能进行恶意操作，进一步保障系统安全。

加密升级包传输

在远程升级过程中，升级包通常需要通过无线网络传输。安全芯片可以对升级包进行加密，以保护数据在传输过程中的安全。加密传输不仅能防止黑客截取和分析升级包内容，还可以避免攻击者在传输过程中篡改升级包，从而确保升级包的安全交付。

防止回滚攻击

安全芯片可以防止系统被恶意回滚到早期版本，防止已修复的漏洞再次被利用。每次升级后，安全芯片会记录当前的固件或软件版本信息，以确保系统不会回到旧版本，从而保护系统免受旧版本的安全漏洞攻击。

这些安全机制共同构建了一个完整的智能座舱安全防护体系，实现了从用户隐私、安全支付、数字版权到安全通信等多方面的安全架构。

5.4.7. 应用案例

信大捷安XDSM3275车规安全芯片，为新能源汽车智能座舱提供安全解决方案，提供包括T-Box通信安全、用户个人隐私安全、车企API开放授权认证和系统升级安全等典型场景安全保障，为智能座舱生态快速健康发展保驾护航。

华大电子CIU98_H高性能车规级安全芯片，为座舱应用场景下的大数据量数据加解密，OTA数据包验证及解密，提供高性能安全计算能力，提升业务场景效率，提升用户体验性。

5.5. C-V2X应用

5.5.1. 应用场景功能介绍

随着智能交通系统技术的快速发展，基于蜂窝的C-V2X（Cellular Vehicle-to-Everything，简称C-V2X）逐渐成为车联网技术的基础组件，正逐步成为推动智能网联汽车和交通行业转型升级的关键力量。C-V2X技术通过车辆与车辆、车辆与路侧基础设施、车辆与云平台、车辆与行人等之间的实时通信，极大地提升了道路安全性、交通效率和驾驶体验。C-V2X又可以细分为车与车通信（V2V）、车与路通信（V2R）、车与云平台通信（V2N）、车与设备互联（移动互联网终端等），具体通信数据包括：基本安全消息、路侧交通消息、路侧安全消息、信号灯相位与配时消息、平台交互信息、设备交互信息等。

5.5.2. 应用场景的安全需求

C-V2X通信实体身份和数据来源需保证真实性、完整性、机密性、不可否认性。安全需求说明如下：

C-V2X通信实体身份和数据来源的真实性保护需求

C-V2X通信中，车载通信单元、路侧单元、云平台以及其他通信设备需实现身份真实性保护，以应对通信实体面临的身份仿冒风险，避免非法用户以假冒的身份进行C-V2X通信。

对于C-V2X通信中发送的数据需要进行来源真实性保护，避免数据被伪造。

C-V2X通信数据的机密性保护需求

C-V2X通信中需实现数据的机密性保护，以应对通信过程中的数据和隐私泄露风险。智能网联汽车侧的行车数据，涉及车辆状况、行车轨迹等个人信息。C-V2X通信实体发出的信息在传输过程中，如果缺乏机密性保护，则可能被非授权的第三方获取、恶意利用从而对个人、行业造成损害。

C-V2X通信数据的完整性保护需求

C-V2X通信中需实现数据的完整性保护，以应对通信过程中的数据篡改风险。如果缺乏完整性保护，攻击者会通过篡改通信过程中的各类数据，达到恶意攻击车辆、交通的目的，引发不同程度的交通问题或事故。

C-V2X通信行为的不可否认性需求

C-V2X通信中需实现对通信行为的不可否认性（抗抵赖），以应对C-V2X通信实体可能出于自身利益对信息的发送进行否认（抵赖）。

5.5.3. 如何用安全芯片去实现安全方案

真实性保护

通过安全SDK调用安全芯片的能力：安全芯片基于公钥密码算法（如SM2）进行私钥和公钥的生成和安全保存，并通过利用安全芯片的签名和验签能力，基于数字证书技术进行V2X通信实体身份信息生成和鉴别；

通过安全SDK调用安全芯片的能力：安全芯片基于公钥密码算法（如SM2）采用数字签名技术对C-V2X通信的数据进行签名，对数据来源真实性进行保护。

机密性保护

C-V2X通信时如发送需要加密保护的数据（如不能明文泄露的数据），通过安全SDK调用安全芯片的能力：安全芯片采用对称密码算法（如SM4）或公钥密码算法（如SM2）等对V2X通信数据进行加密保护。

完整性保护

通过安全SDK调用安全芯片的能力，基于对称密码算法或密码杂凑算法的消息鉴别码机制或基于公钥密码算法的数字签名机制可实现消息完整性保护。

不可否认性保护

通过安全SDK调用安全芯片的能力：安全芯片采用基于公钥密码算法（如SM2）的数字签名技术对发送的C-V2X通信数据进行签名，来实现数据发送行为的不可否认性。

5.5.4. 应用案例

信大捷安自研设计的XDSM3276　V2X车规级高性能安全芯片，具备高速的非对称算法签名验证性能，能够满足汽车紧急制动、前向碰撞等典型的PC5低时延通信要求，并结合V2X　CA系统为网联终端签发用于身份认证的数字证书，从而能够达到信息防篡改，保障车-车、车-路、车-人和车-云等通信安全的效果。目前该芯片已经在国内自主和合资主流主机厂、路侧RSU厂商中得到了广泛的量产应用。

华大电子CIU98_B系列车规级安全芯片，可为C-V2X直连通信提供数据报文签名功能，防止报文被篡

改，保障通讯安全。华大电子CIU98_H系列车规级高性能安全芯片，基于其高性能安全计算能力，可为C-V2X直连通信实现高速报文签名与验签功能，为C-V2X提供高性能安全方案。

5.6. OTA应用

5.6.1. 应用场景

在汽车领域，OTA（Over-the-Air，OTA）技术得到了广泛应用，对汽车的智能化、便捷性和安全性产生了深远影响。目前，众多汽车制造商已广泛采用OTA技术，包括软件升级（SOTA）和固件升级（FOTA），以实现对自动驾驶、动力电池管理、电机控制等关键控制器的远程更新。随着汽车行业的数字化和智能化发展，OTA技术在汽车领域的应用将越来越广泛。未来，OTA技术可能会进一步拓展到车辆安全系统的实时更新、智能驾驶功能的持续优化等方面。

5.6.2. 安全需求

OTA过程虽然带来了诸多便利，但也存在着一些不容忽视的风险：

安全性风险：

OTA升级过程中，数据传输可能会被黑客截获、篡改，从而引入新的安全漏洞。这些漏　洞可能被利用来攻击车辆系统，对用户个人隐私和车辆安全构成威胁。

隐私泄露风险：

OTA升级可能需要收集大量个人信息，如车辆位置、驾驶习惯等。这可能会引发用户对隐私泄露的担忧；

云端安全风险：

云服务器端存储着车辆系统升级相关数据，如车辆升级日志、车辆升级包等。黑客攻击可能导致数据篡改、删除，影响车辆的正常远程升级和使用安全；

网络传输安全风险：

OTA技术通过通信网络将软件升级包传送给车载终端，传输过程中可能受到黑客攻击，如重放、拒绝服务攻击(DoS)等，影响车辆的升级过程。

使用汽车安全芯片可以合理规避以上针对OTA整套流程中存在的安全风险。

5.6.3. 安全方案的实现

固件加密、解密

对需要升级的固件进行SM4/AES等算法对称加密，使用安全芯片接口进行解密，可以避免传输过程中固件泄露风险。

固件完整性、真实性验证

通过对固件原文进行摘要计算，然后对摘要值签名，在升级前使用安全芯片内置公钥进行验签，检查固件包是否在传输过程中被篡改。

保护通信链路安全

安全芯片能够对通信链路进行加密、解密，提供底层硬件算法接口，供 TLS 等加密协议调用，在车端与服务器端之间构建安全的传输通道。这样，传输的升级包、配置文件等数据就不会被外部攻击者轻易窃取或监听，防止敏感信息泄露，保障整个 OTA 过程中数据交互的保密性和完整性，像车辆的软件版本号、即将更新的关键功能参数等信息都能得到妥善保护。

密钥管理

OTA 过程涉及到众多加密和解密操作，需要用到多组密钥，安全芯片提供了一个安全可靠的密钥存储环境。它可以将对称密钥、非对称密钥等进行妥善保存，防止密钥被非法提取。并且，在需要使用密钥进行加解密、签名验证等操作时，在芯片内部的安全区域完成相应运算，避免密钥在芯片外部暴露，最大程度减少因密钥泄露而导致整个 OTA 系统安全防线崩溃的风险，确保 OTA 各项安全机制能够依靠稳定且保密的密钥正常运行。

防止回滚攻击

一些攻击者可能会试图将汽车电子系统的软件回滚到旧版本，以利用旧版本中存在的已知漏洞。安全芯片可以通过记录软件版本更新的相关信息，并在每次启动及 OTA 过程中进行校验，当检测到异常的回滚操作时，拒绝执行，确保汽车电子系统始终运行在合法、安全且经过官方认证的软件版本之上，维持车辆的安全状态。

保护车辆敏感数据

汽车内部存在大量和驾驶习惯、车主隐私等相关的敏感数据，在 OTA 过程中也需要保证这些数据的安全。安全芯片可以提供安全存储功能，并可以对涉及这些敏感数据的操作进行管控，比如只有经过授权

的 OTA 相关进程才能访问、修改部分数据，而且对这些数据的存储区域进行加密保护。即使在极端情况下，如车机系统遭受入侵，攻击者也难以获取到有价值的敏感信息，进一步提升了车辆整体的数据安全性。

安全芯片在汽车电子 OTA 领域的应用是多方位的，从保障升级流程安全到保护数据和防范各类攻击等方面，为汽车能够安全、可靠地实现远程软件更新发挥着不可或缺的作用。

5.6.4. 应用案例

信大捷安自主研发的XDSM3275车规安全芯片能够提供相应安全解决方案。此安全芯片已经成功应用于国内头部新能源车企，除了基于硬件保障通信身份安全、数据安全和数据完整性，还通过其内在高性能SM4等对称算法的加持，为OTA固件升级包提供了快速加解密的能力，有效提升了软件定义汽车概念下用户的使用体验。

5.7. ETC-OBU应用

5.7.1. 应用场景功能介绍

ETC-OBU（On Board Unit）是电子不停车收费系统（Electronic Toll Collection System）中的一个重要的组成部分，即车载ETC单元，ETC-OBU通过无线通信与路侧RSU(Road Side Unit)进行通信，实现车辆在不停车的情况下完成道路缴费。

ETC系统组成

ETC-OBU的主要功能包括识别车辆、记录通行信息、发送和接收数据、处理交易等。当车辆进入ETC车道时，OBU会向RSU发送识别信号，同时从RSU获取通行凭证。然后，ETC中心管理系统根据通行凭证和收费标准计算出应支付的费用，并生成扣款指令。OBU通过预设的支付渠道（如银行账户、预付费账户等）发起扣款操作，并将扣款结果反馈给RSU。最后，车辆在出口处只需确认费用并通过OBU发送付款确认指令即可完成整个收费过程。

5.7.2. 应用场景的安全需求说明

由于ETC-OBU具有收费交易处理的核心功能，为确保交易过程中的支付安全，通常ETC-OBU包含了如MCU、多种射频通信芯片、RFID芯片、安全芯片等关键芯片和组件。安全芯片为ETC-OBU提供了加密存储、密码算法、访问权限控制、安全认证、数据完整性保护等功能，从而确保了在不停车收费系统中车辆与路侧收费单元的发送和接收数据、处理交易等过程中的安全认证、数据安全与支付安全。

5.7.3. 安全芯片实现方案

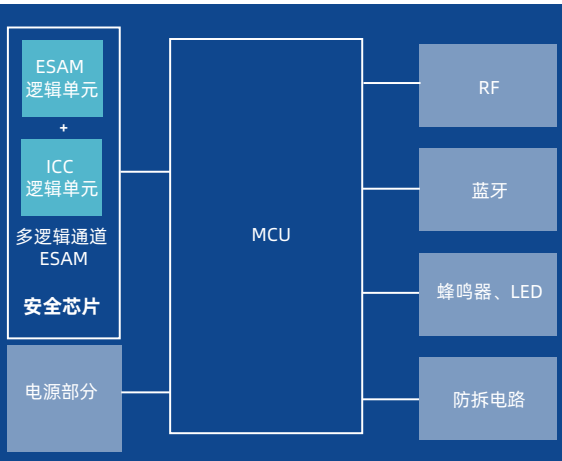
安全芯片在ETC-OBU的应用场景中，通常封装成ESAM安全模块（OBE-SAM）。

OBU按用户卡的类型来分类，可以分为双片式OBU和多逻辑通道OBU。双片式OBU的用户卡与ESAM是分开的，会有一张单独的用户卡插入到OBU设备中；多逻辑通道OBU是采用多逻辑通道合成技术把用户卡和ESAM合成到了一个ESAM中。

按安装的阶段来分，可以分为前装OBU与后装OBU。前装OBU即在汽车出厂前OBU已经安装好，OBU整机需要通过车规级的认证；后装OBU则是汽车出厂后安装的，没有车规级认证的限制。

虽然OBU分类看起来很复杂，但是总体的架构并没有太大的差别。OBU的架构大致如下图（以多逻辑通道OBU为例）所示：

如图，OBE-SAM作为ETC加密存储和数据安全保障的核心器件，通过ISO　7816标准协议与主控单元进行高效通信，在车辆与路侧收费单元的发送和接收数据、处理交易等过程中为ETC设备提供安全认证与数据安全的核心安全保障。



ETC-OBU 系统组成

5.7.4. 应用案例

2022年9月，交通运输部关于发布《收费公路联网收费技术标准》的公告，公告中相关技术要求，对ETC发行系统进行国密接入改造，全面发行支持国产密码算法ETC车载装置升级改造，国密安全芯片在ETC应用进一步深入。

根据《2024-2029年中国ETC行业市场供需及重点企业投资评估研究分析报告》，截至2023年底，中国ETC用户数量已达到2.7亿，占全国汽车保有量(约3.19亿辆)的86%左右。随着ETC应用场景的进一步拓展和用户体验的不断提升，预计ETC用户规模将进一步提高。

目前，众多车型在出厂时就已经配备了ETC设备，例如沃尔沃的S90、XC60、XC90，比亚迪唐DM-i荣耀版、汉EV荣耀版等。

伴随智能交通、大数据、人工智能等技术的不断发展，ETC密码系统改造的深入，ETC系统将作为智能交通体系中重要的组成部分，为用户提供便捷的通行体验，节约时间成本，减少排队等待，通过自动扣费和无感支付的特性，减少人工收费带来的交通拥堵问题。未来在智能交通的建设中，通过ETC实现与交通管理、信号灯、车联网等系统的互联互通，可进一步实现交通信息的共享与优化，极大的提升交通路网通行效率。

华大电子CIU98_B系列车规级安全芯片，通过了ITSC检测认证，支持国际/商密双算法，满足双片式ESAM和单片式ESAM应用需求，保障车辆信息的安全存储，保护通行费用安全支付。

5.8. 数字钥匙应用

5.8.1. 应用场景功能介绍

数字钥匙本质是“手机与车辆之间的通信”。手机通过通信信号向车端传递身份信息并验证，车端通过定位技术判断手机是否趋近、远离、进入车辆，从而执行开锁、落锁、启动操作。

一个完整的数字钥匙系统不仅包括实现手机端与车端通信硬件模块，还包括云端的软件管理平台，涉及多方生态。

数字钥匙的技术路线主要包含三种：

▶ 数字钥匙基于NFC近场通讯技术，实现了车辆进入与启动功能，但基本没有位置感知的能力。同时，NFC的通信距离只有厘米级，车主需要将数字钥匙贴近车身才能开启车门。此代数字钥匙的使用体验较差，同时功能拓展潜力不高。

▶ 数字钥匙是采用BLE蓝牙技术，是目前市占比最大的数字钥匙种类。蓝牙数字钥匙通信距离比第一代更远。第二代数字钥匙可以通过蓝牙信号的强弱粗略感知车与钥匙的位置关系，但其感知精度与准确性都有所欠缺。

▶ 数字钥匙是UWB、BLE、NFC三种无线通信技术相结合的产品。UWB技术使得第三代数字钥匙位置感知精度得到了质的飞跃。值得一提的是，UWB测距序列可以支持8000个安全位，钥匙和车端需要滚码才能解锁，极大地提升了数字钥匙的安全性。

5.8.2. 应用场景的安全需求说明

数字钥匙 CCC(Car Connectivity Consortium)标准是数字钥匙目前使用广泛，且在海外的唯一的标准。该标准由国际CCC组织开始制定，由特斯拉Model3开始使用，大家纷纷跟进。国内联盟组织ICCE（Intelligent Car Connectivity Industry Ecosystem Alliance）/ICCOA（Intelligent Car Connectivity Open Alliance）纷纷针对自己的产业链推出相关标准。国际CCC组织2023年底也推出了CCC安全认证，对安全提出了要求。

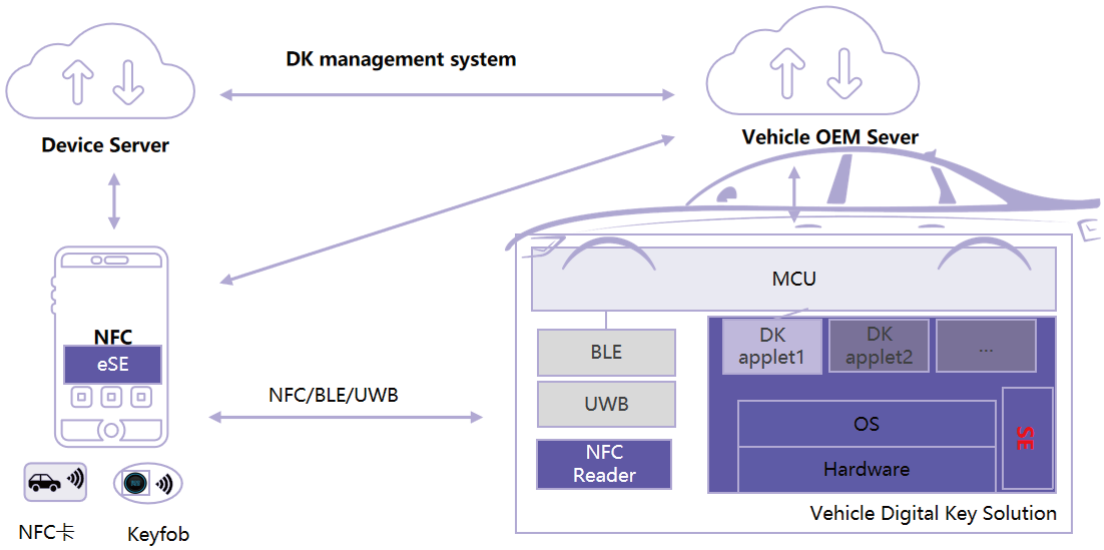
2023年起苹果手机实现CCC钥匙的标准化，提升客户体验，推出了MFI认证。对车辆的整体性能提出了要求，国内目前只有比亚迪正式通过了认证，认证时间大概一年。MFI认证对车端交易的性能要求：快速交易300ms，标准交易600ms，朋友首次交易700ms。客户要求SE执行时间越短越好，目前越来越多的国产车规级安全芯片可以满足车厂MFI性能需求。

基于安全芯片可信架构，用一颗安全芯片统一管理多个场景，从生态链底层环境保证车联网安全，可以为数字钥匙提供端到端的全路径安全支撑。

5.8.3. 安全芯片实现方案

基于安全芯片搭建信息安全、身份认证安全、连接安全、电子支付安全四位一体的可信应用环境，可以形成满足车-云-端安全性的数字钥匙整体解决方案。

数字钥匙的安全芯片实现方案一般如下：



数字钥匙全芯片实现方案

智能汽车面临诸如非法接入车载网络，威胁后台系统安全等安全威胁时，可以基于安全芯片构建可信环境。汽车数字钥匙安全芯片解决方案，保障安全存储、身份认证、安全算法、IoT设备到云服务间的安全通信等功能，保证端到端的安全性。

5.8.4. 应用案例

数字钥匙行业起源于国际市场，所以特斯拉和合资主机厂一般使用国际芯片，包括供应商也集中在国际大型厂商。从2021年以来，国内新型的方案商或者一级供应商，逐步进入该市场，形成了强大的国内体系，给国内车型提供了很大的选择空间。

华大电子CIU98_B系列安全芯片，面向智能网联车信息安全领域，可为智能网联车车载终端提供核心基础的硬件安全，主要应用于车载网络设备联网SE、数字车钥匙安全SE、高速公路ETCOBE-SAM以及C-V2X基础安全SE。

紫光同芯T97系列高性能安全芯片，可同时安装CCC、ICCE、ICCOA、私有协议等Applet，满足苹果MFI认证性能要求，保证数字钥匙从车到云、云到端的安全性，提供SE+COS+SDK一站式解决方案和Applet灌装及个人化服务，并且已经成功装车数百万颗

国芯科技自主研发的CCM33系列车规级信息安全芯片，内置高等级安全特性的硬件算法协处理器，支持国际和商密安全算法，相关芯片获得EAL5+安全认证证书，为汽车PEPS、ETC、T-BOX、OBD、ECU及V2X等领域提供了坚实的信息安全保障。

复旦微电子FM1280安全芯片，已在重型车T-BOX上出货超百万颗，涵盖全部主流车型；已用于乘用车T-BOX、ETC ESAM、域控制器、数字钥匙等。复旦微的国内首款车规级NFC读写器芯片FM17660A，也在数字钥匙中批量应用。

NXP推出全新的汽车数字钥匙解决方案，使得智能手机、遥控钥匙和其他移动设备能够安全地存储、验证数字钥匙、与车辆安全通信并共享数字钥匙。

此外，随着汽车电子电气架构向集成化、融合化方向发展，整车厂从降本增效的角度考虑，对安全芯片也提出了新的要求。车内外数据交互越来越多地集成到座舱域，将V2X、TBOX、数字钥匙等功能集成到了智能座舱，且提出了一颗安全芯片可以实现多个场景的信息安全需求。对汽车安全芯片的需求，也从一个设备一个安全芯片，逐渐转向多个设备共用一个安全芯片，多接口安全芯片的需求越来越多。

5.9. eSIM应用

5.9.1. eSIM简介

eSIM（Embedded SIM）是一种嵌入在设备内部的可编程SIM卡，与传统的物理SIM卡不同，eSIM是一个集成电路芯片，用户无需插入或更换实体SIM卡即可通过软件切换运营商或更改通信服务。

eSIM是由GSMA规范定义的。目前有SGP02（M2M），SGP22（consumer RSP），SGP32（IoT）等规范标准。由于汽车逐渐成为个人的消费品，所以目前SGP22规范逐渐被汽车行业接受。

eSIM的优势：使用灵活、统一物料、最终用户体验好、降低部署成本。

5.9.2. eSIM应用场景

eSIM提升连接便捷性与灵活性

相比传统SIM卡，eSIM无需实体插拔，可通过远程配置快速激活并连接网络，车辆生产和部署时能更高效地实现联网功能。能在不同网络运营商之间灵活切换，车辆可根据所处位置和网络信号质量，自动选

选择最优网络，确保网络连接稳定。

增强可靠性与稳定性

直接集成在车辆硬件中，减少了因SIM卡松动、接触不良等硬件问题导致的网络故障，提高了车联网系统的稳定性。支持多网络连接备份，主网络出现故障时，可迅速切换到备用网络，确保车辆关键功能如紧急救援、自动驾驶辅助等不受影响。

实现成本节约

硬件成本降低：无需安装实体SIM卡插槽等硬件，降低了车辆生产中的硬件成本和空间占用，为车辆设计和布局提供更多灵活性。远程管理功能使运营商能远程进行配置和管理，减少了现场维护和管理的人力成本。同时，多网络切换功能可帮助用户选择性价比高的网络套餐，降低通信费用。

助力安全与隐私保护

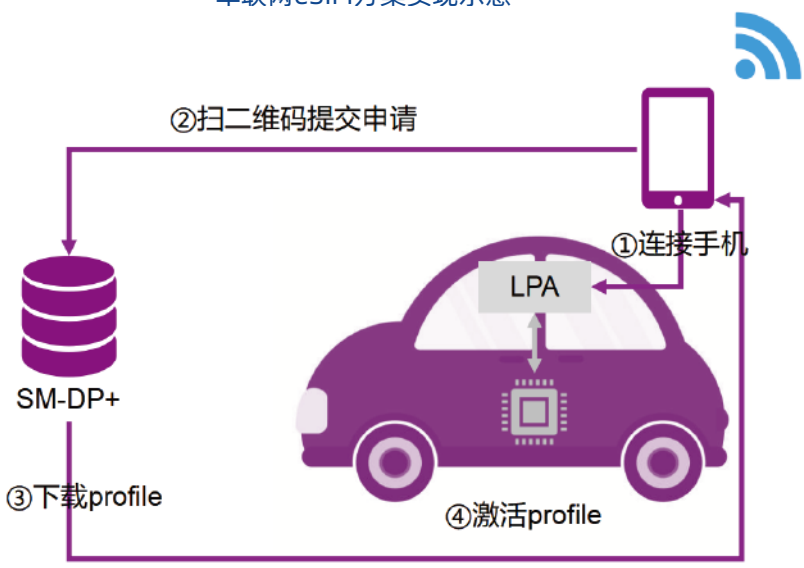
eSIM采用先进的加密技术和安全认证机制,需要基于CC EAL5+认证的安全芯片,软件需要过GSMA的安全认证。为车辆与网络之间的数据传输提供更高级别的安全保障，防止数据泄露和恶意攻击。可实现车辆身份的匿名化管理，在数据传输过程中对车辆和用户的身份信息进行加密处理，保护用户隐私。

拓展业务创新空间

车企能借助eSIM快速推出新的车联网服务和应用，如基于大数据分析的个性化驾驶建议、车辆共享服务等，为用户提供更多增值服务。为车联网与其他行业的融合提供了更便捷的连接方式，促进车联网与智慧城市、智能交通等领域的深度融合。

5.9.3. 实现方案

车联网eSIM方案实现示意



硬件集成

车辆制造商需选择适配的通信模块，模块要支持eSIM功能，能够与车辆的电子控制单元（ECU）及其他系统进行通信，并具备4G、5G等不同网络通信能力。eSIM芯片集成到车辆的通信模块或主板上，确保其与其他硬件电路良好连接。

网络连接配置

车企或车联网服务提供商与eSIM运营商签订合作协议，根据业务需求选择合适的网络套餐和服务，获取相应的网络资源和权限。运营商通过远程配置平台（DP+），通过标准化的协议和接口，运营商网络配置信息、认证密钥等数据（Profile）写入车辆的eSIM芯片，过程可以通过借助手机终端APP扫码方式完成。

软件与应用开发

为满足eSIM通信模块与车辆的操作系统及其他软件系统兼容，需开发相应的插件程序，用户端安装LPA助手或者车载终端实现对应满足eSIM产品通信协议要求插件。

5.10. 北斗导航智能系统应用

5.10.1. 应用场景功能介绍

汽车车载北斗导航智能系统在车辆导航和驾驶辅助方面发挥着重要的作用。其高精度定位、多模式导航、实时交通信息等特点，以及在实现精准导航、提高驾驶安全性和促进智能交通发展等方面的作用，使得导航智能系统成为现代汽车不可或缺的重要组成部分。

尤其在重载货运车辆，通过安装北斗导航智能系统，能够有效加强道路运输动态监管，提升道路运输安全管理水平。国家交通运输部部署建设了全国道路货运车辆公共监管与服务平台，发布了《关于充分发挥全国道路货运车辆公共监管与服务平台作用支撑行业高质量发展的意见》，提出要推进车载终端装备升级、加快单北斗终端研发推广，深入开展新一代单北斗定位终端的技术研发，推动基于北斗三号的单北斗终端应用，稳步推进全国货运车辆单北斗终端的换代工作，推动建成基于北斗的重载货车数字化动态监管体系，推进道路运输成为北斗导航智能系统的民用重点领域。

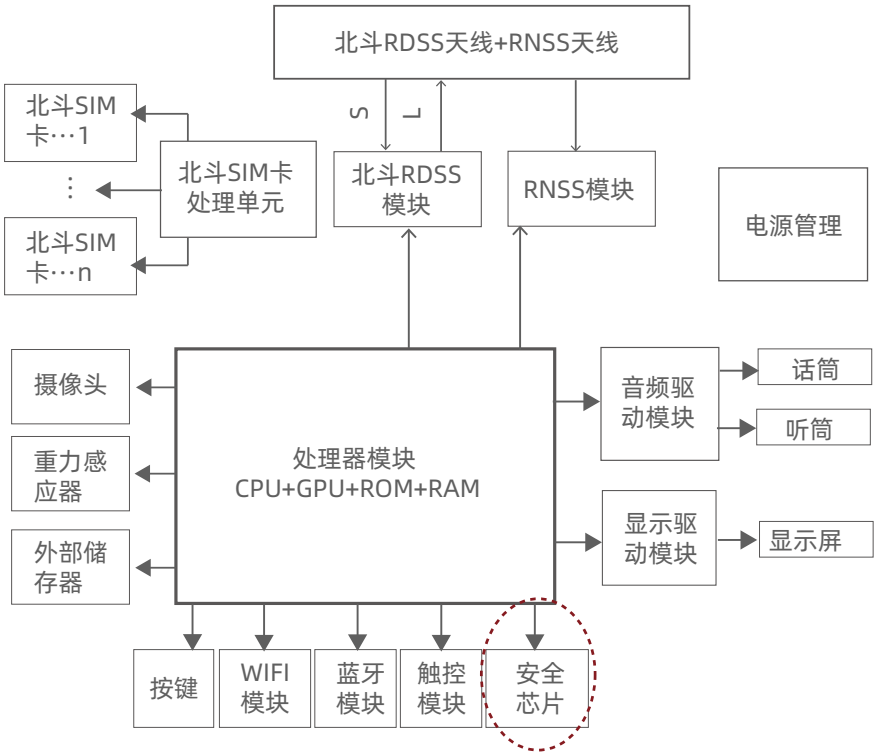
5.10.2. 应用场景的安全需求说明

信息安全作为车载北斗导航智能系统的重要组成部分，通过增加商密算法的安全芯片，实现车载北斗导航智能终端与实时监测平台之间的身份认证和数据安全，确保车载端数据采集真实性，防止平台端用户数据泄漏，保障定位导航数据在采集、传输和存储全生命周期的安全。

安全芯片在北斗导航智能系统中能够有效保障车载导航终端设备的数据安全、防止黑客攻击、保障驾驶安全等，是车载北斗导航智能系统不可或缺的一部分，对涉及关键行车数据、控制和通讯的防攻击篡改至关重要。

5.10.3. 安全芯片实现方案

安全芯片在车载北斗导航终端提供安全认证和数据安全核心能力，确保定位数据源真实不可篡改，保障定位导航数据的个人隐私、防止数据泄漏。一般情况下，车载北斗导航智能终端系统组成如下：



车载北斗导航终端系统构成

如上图所示，安全芯片通过提供的数据加密和安全存储功能，为北斗车载导航终端系统在运行过程中的定位数据、行驶轨迹、车主身份等敏感数据提供全面的安全防护。

5.11.动力电池防伪应用

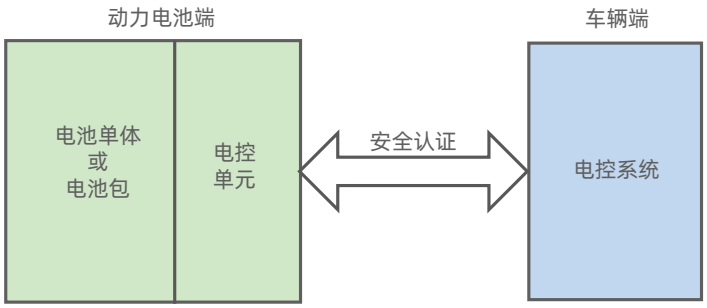
5.11.1. 应用场景功能介绍

随着全球电动化和绿色能源转型的加速，电动汽车开始兴起，越来越多的消费者选择电动汽车作为代步工具。动力电池作为电动汽车的核心部件，直接关系到车辆的性能、续航能力、使用寿命以及乘客的安全，其中乘客的人身安全是最为重要的。然而，市场上也出现了不少伪劣的动力电池产品，消费者可能无法区分判别动力电池产品的真伪，这将给消费者带来巨大的安全隐患和经济损失。因此，保证车辆所使用的电池是经过相关标准安全认证的，这一点非常重要。

5.11.2. 应用场景的安全需求说明

对电池真伪的识别不应依赖消费者主观意识，而是必须通过车辆与电池之间自动化的物与物识别方式，避免错判、误判，甚至故意的使用伪劣动力电池。

动力电池包括电池单体或电池包、电路和电控单元（如电池控制单元、电流接触器）等部分，电动汽车通过电控系统与动力电池进行连接和管理。为了保证车辆所使用的是符合国家标准的动力电池，需要对动力电池端的电池控制单元和车辆端的电控系统提出防伪识别要求，要求在动力电池端增加防伪安全芯片，作为动力电池的有效身份安全标识，也要求在车辆端增加防伪安全芯片，实现对动力电池安全标识的安全认证，只有车辆端完成对动力电池的身份认证，才允许车辆系统正常工作。

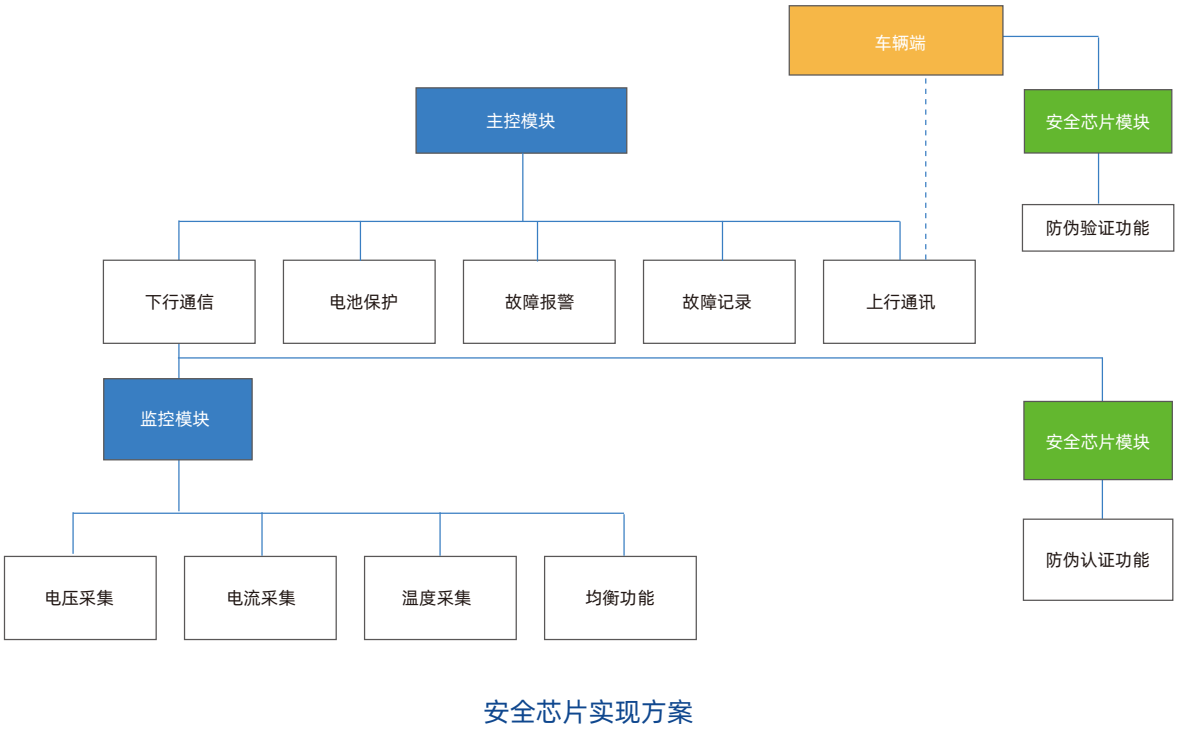


动力电池与电动汽车防伪认证示意图

5.11.3. 安全芯片实现方案

安全芯片应用于动力电池端的电控单元，并通过主控模块的上/下行通信功能与车辆端进行防伪认证数据的加密和提交，主控模块为数据转发作用。车辆端的电控系统内同样加载安全芯片，用于对电池端传递过来的防伪认证数据进行计算验证。

防伪认证过程采用PKI密钥体系，例如国际算法ECC或者商密算法SM2，并引入随机数据参与认证运算，增加认证数据的随机性，防止交互数据被监视后的仿冒。同时电池端的每颗安全芯片均存储有唯一的密钥值，保证动力电池个体之间的独有性，避免被攻击后的批量复制。



安全芯片实现方案

5.12. 车载手机无线充电应用

5.12.1. 应用场景功能介绍

车载手机无线充电作为现代汽车的便捷功能，为驾驶者提供了极大的便利。它采用非接触式充电方式，只要将手机等电子设备放在充电区域即可快速充电，无需频繁插拔充电线，这不仅提高了驾驶的便利性，还增加了行车安全。由于各品牌手机通常都会定义私有协议，碎片化严重，无线充电联盟（Wireless Power Consortium，WPC）通过统一的标准，减少了市场上无线充电设备的碎片化，避免了用户需要购买特定品牌充电器的情况，大大提高了设备间的兼容性。经过多个版的迭代，WPC的Qi1.3.3版本已经成为车载无线充电的主要标准。

佐思汽研发布《2024年中国乘用车手机无线充电研究报告》，2024年6月乘用车手机无线充电标配率已达44%。2024年通过Qi认证的产品中，主要为Qi2认证。

5.12.2. 应用场景的安全需求说明

WPC Qi1.3标准增加身份认证功能，在5W以上的无线充电发射设备中加装安全芯片（鉴权芯片），要求基于硬件层面的身份鉴权，只有通过身份验证，才可以大功率输出。硬件安全芯片需要满足特定安全等级，如CC EAL4+，确保存储证书和私钥的安全性。

Qi 2.0标准定义了统一的手机无线充电协议，尤其是引入了基于苹果MagSafe磁吸充电技术的MPP（Magnetic Power Profile）技术，通过优化磁场分布和软件校正，MPP可以提高充电效率，使得设备在无线充电时更加稳定、可靠。

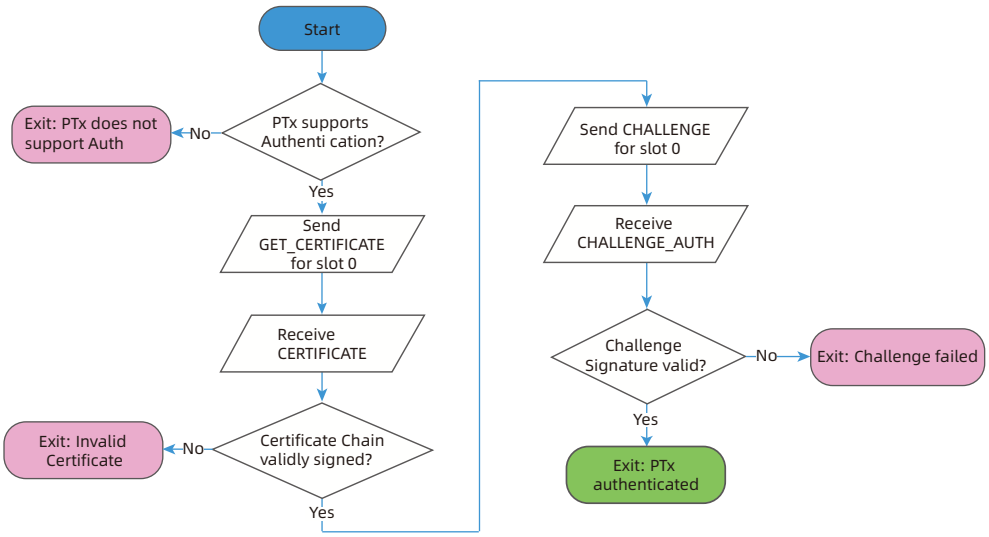
Qi 2.0标准规定每个Qi2认证充电器必须包括EPP（Extended Power Profile）或MPP (或两者)，都必须加一颗满足一定安全等级的安全芯片，以确保Qi标准下的产品具有更高的稳定性、安全性、高效性，让用户放心使用每一个带有Qi认证的无线充电器。

车载无线充除了有安全芯片，还加入了NFC读写功能，来识别充电位置是否有各种NFC卡片（身份证、银行卡等）或RFID标签，避免在大功率无线充电开启时，烧坏这些卡片或标签。

5.12.3. 如何用安全芯片去实现安全方案

Qi 充电认证流程在首次配对时候需要进行证书交换，接收器（手机）获取充电器的数字证书和摘要，验证证书的签名是否有效；然后再发起挑战-认证流程，由充电器通过私钥进行数字签名，接收器验证签名通过后，即可开启Qi 1.3/2.0标准的充电。两台设备后续再配对，若接收器存储过充电器的证书摘要和公钥，则直接进行挑战-认证流程，减少验证时间。

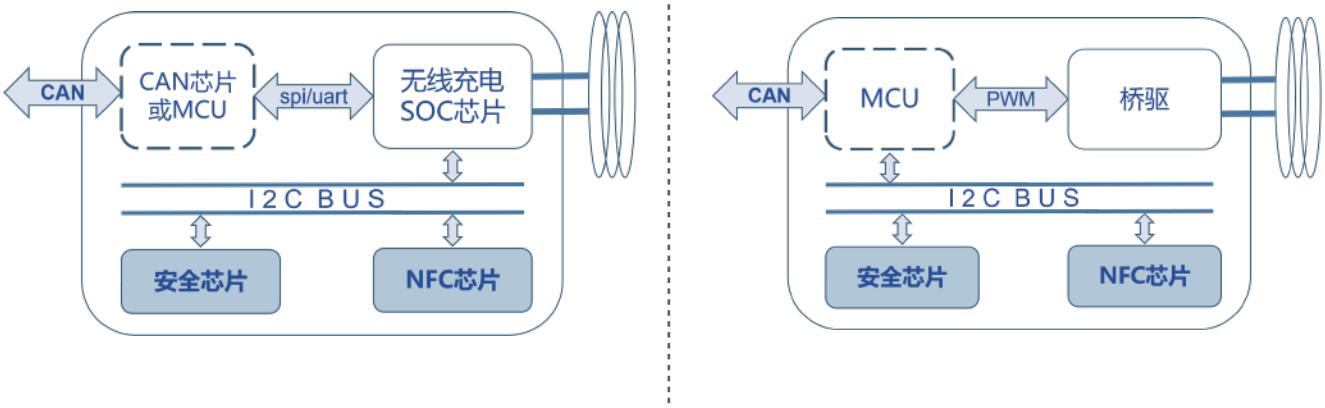
Figure 2. Simple Power Receiver



充电认证硬件逻辑图，软件架构图，业务流程

厂商的无线充产品如果想取得WPC的Qi认证，需要制造商在WPC中注册Qi无线充的型号，从WPC中获取制造商代码PTMC与所注册无线充型号的Qi ID 码，然后将Qi ID 码发给数字证书服务商（MCSP），然后进行WPC签发产品单元证书，制造出合格的Qi无线充电器。数字证书服务商帮助无线充厂商去跟WPC签发产品单元证书，完成安全芯片样品的烧录，提供给无线充厂商，无线充厂商将产品送到实验室进行符合性测试。

无线充主流架构如下：



安全芯片在Qi无线充电系统中，发挥了重要角色，主要功能如下：

身份认证

√ 设备验证：安全芯片可以验证放置在无线充电板上的设备是否符合Qi标准。只有通过验证的设备才能开始充电过程，开始大功率充电，这有助于防止非标准设备的误用。

√ 双向认证：安全芯片支持双向身份认证，确保充电设备和接收设备之间的通信是安全的。这种双向认证可以防止中间人攻击和非法设备的接入。

数据加密

√ 通信安全：安全芯片对充电过程中传输的数据进行加密，确保数据的安全性和隐私性。

√ 防止篡改：通过数据加密，可以防止数据在传输过程中被篡改或截取，确保认证过程的完整性和可靠性。

√ 数据保护：安全芯片可以很好地保护好WPC证书的安全性，安全芯片的高安全性可以避免被破解与复制。

防伪和防克隆

√ 唯一标识：每个安全芯片都有唯一的标识符，用于区分不同的设备。这有助于防止假冒设备的使用，保护制造商和消费者的权益。

√ 防克隆：安全芯片采用复杂的加密算法和安全机制，防止芯片被克隆或仿冒，确保每台设备都是正品。

标准化和兼容性

√ 标准遵循：安全芯片严格遵循Qi标准，确保不同品牌和型号的无线充电设备之间的可以相互信任。

√ 兼容性测试：通过安全芯片的标准化设计，可以确保设备通过兼容性测试，符合WPC的标准要求。

5.12.4. 应用案例

复旦微FM1230安全芯片是国产首款通过WPC Qi2标准认证的鉴权芯片，适用于车载无线充电、T-Box、FOTA等场景，累计出货量数千万颗。在丰田、本田、塔塔、尼桑等车载无线充已批量应用。

此外，国内已有华大电子，紫光同芯，天津国芯获取WPC认证的MCSP资质，可为Qi无线充电产品提供认证SE安全芯片。

5.13. 车载香薰应用

5.13.1. 应用场景功能介绍

车载香薰是一种专为汽车设计的香薰产品，旨在改善车内的空气质量，提供舒适的驾驶和乘车体验。一些车型配备有内置的香薰系统，在香水瓶带有NFC 标签，可以通过车载系统调节香型和强度，为用户提供更个性化的体验。

5.13.2. 应用场景的安全需求说明

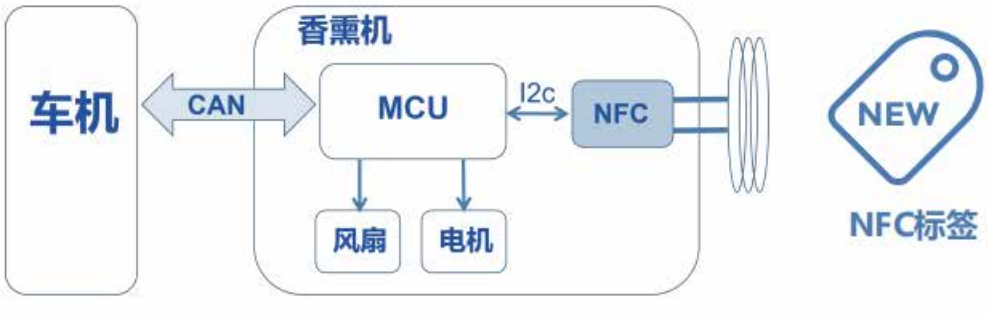
NFC 标签芯片可以存储汽车香薰的详细信息，如品牌、型号、香型、成分、使用说明、有效期等。消费者只需使用支持 NFC 功能的设备（如智能手机）靠近汽车香薰上的 NFC 标签，就能快速获取这些信息，方便购买决策和使用。

- 个性化香薰选择：通过与汽车的智能系统连接，通过识别NFC标签芯片可以根据不同用户的喜好和需求，实现个性化的香氛设置。例如，用户可以在汽车的控制面板上选择自己喜欢的香薰味道，系统通过读取 NFC标签芯片中的信息，自动调整香薰的释放强度和频率，为用户营造出舒适的驾乘环境。

- 防伪与溯源：在汽车香薰的生产和销售过程中，NFC 标签芯片可作为防伪和溯源的有效手段。每个香薰产品都有唯一的 NFC 标签，其中存储了产品从原材料采购、生产批次、生产日期到销售渠道等信息。消费者和商家可以通过读取标签来验证产品真伪，并追溯产品的来源。

5.13.3. 如何用安全芯片去实现安全方案

每个香薰瓶底部都装有一个NFC标签，当瓶子放入汽车内部的专用插槽时，内置的NFC读写器会读取UID，自动识别香薰类型，并与存储数据比较，鉴别真伪。然后，根据预存的用户偏好调整车内环境。



香薰硬件逻辑图，软件架构图，业务流程

NFC标签芯片需具有安全特性如下：

唯一标识	每颗芯片拥有独立7 byte UID（唯一序列号），UID不可改写 。
防篡改	受控的加密区域有OTP（一次性写入）功能，具有抗撕裂能力，防止恶意解锁。确保NFC标签的信息不能被轻易修改，避免非授权人员更改设置或植入恶意代码。
访问控制	只有授权的设备或人员才能读取或写入NFC标签的数据，保证系统的安全性。
耐用性和稳定性	考虑到汽车环境的特殊性，RFID标签需要具有良好的抗干扰能力和物理耐久性，以适应各种恶劣的工作条件。

5.13.4. 应用案例

根据应用场景的安全需求，蔚来汽车部分车型配备了定制的个性化香薰系统，使用了复旦微FM17622A车规级NFC读写器芯片，允许车主通过选择不同种类的香薰来定制车内的氛围。

5.14. 充电认证应用

5.14.1. 应用场景功能介绍

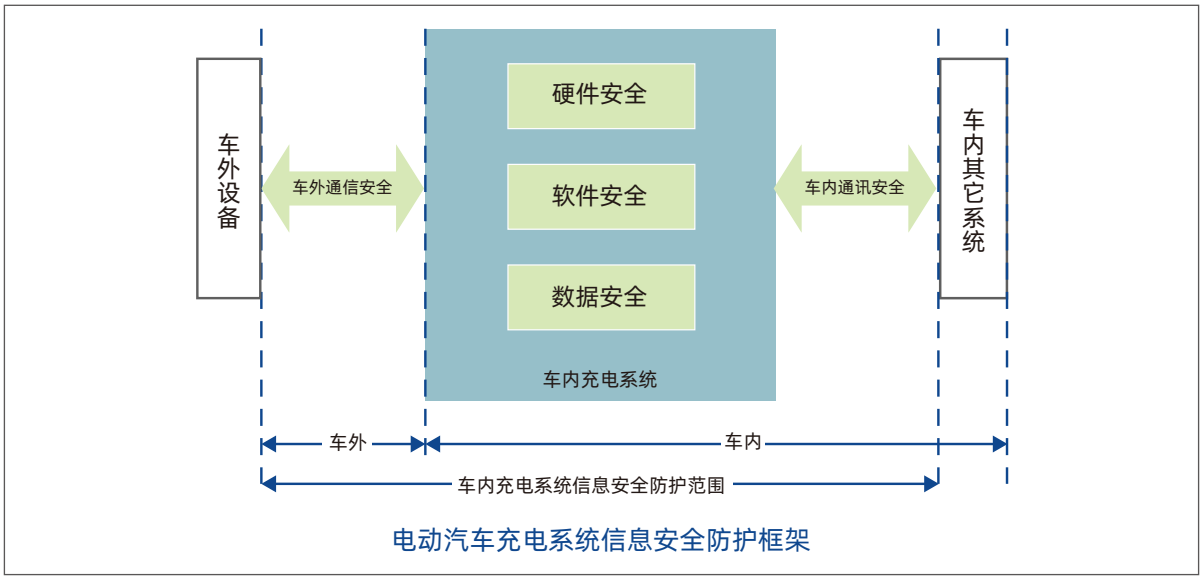
车辆充电是新能源汽车发展的关键环节之一，为确保安全和稳定的充电过程，通常需要采用适当的认证方法和装置来验证车辆、充电桩和充电流程的有效性和合规性。

伴随新能源汽车充电基础设施（充电桩）的日益普及，其网络安全的重要性越来越大。充电设备网络有可能面临多重网络攻击的风险，如果大量设备不受控的充电、非法通讯或断开连接，可能会对本地配电网络产生潜在影响。

即使电动汽车实施了软件相关的安全协议和安全算法以及安全措施，充电桩本身是分离且非常碎片化的，当车辆将插入充电桩充电或使用其相关应用程序时，并不能完全保证充电过程中的安全性，因为电动汽车充电桩生态系统中可能存在安全漏洞，这可能会危及个人隐私、车辆安全，甚至整个电网基础设施安全。

5.14.2. 应用场景的安全需求说明

根据《电动汽车充电系统信息安全技术要求》标准规范要求，新能源电动汽车充电系统信息安全由硬件安全、软件安全、数据安全和通信安全四部分组成，并对硬件、软件、数据和通信等方面的安全技术提出要求，要求在硬件安全、软件安全、数据安全和通信安全方面防护车内充电系统面临的充电数据被窃取、个人隐私泄漏和车内数据被窃取等风险，并要求车内充电系统使用加密芯片、通信芯片等关键芯片来提升车辆充电系统的信息安全。

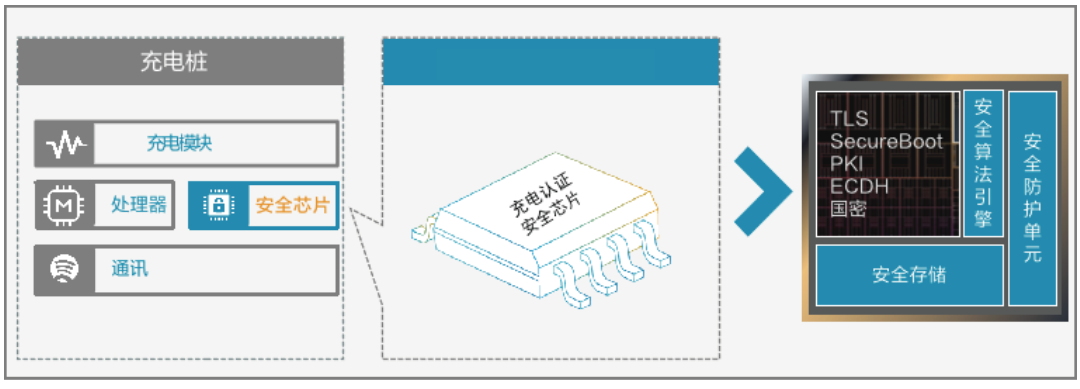


电动汽车充电系统信息安全防护框架

安全芯片作为电动汽车充电过程中确保车辆与充电桩安全认证、通信安全、数据安全的关键元器件，将在新能源电动汽车充电认证中被广泛应用。

5.14.3. 安全芯片实现方案

安全芯片在新能源电动汽车充电系统中通常会在车内、充电桩基础设施中被部署，从而保证汽车在充电过程中的安全认证和数据安全防护。



充电桩安全芯片实现方案

在充电桩的安全芯片实现方案一般如下：

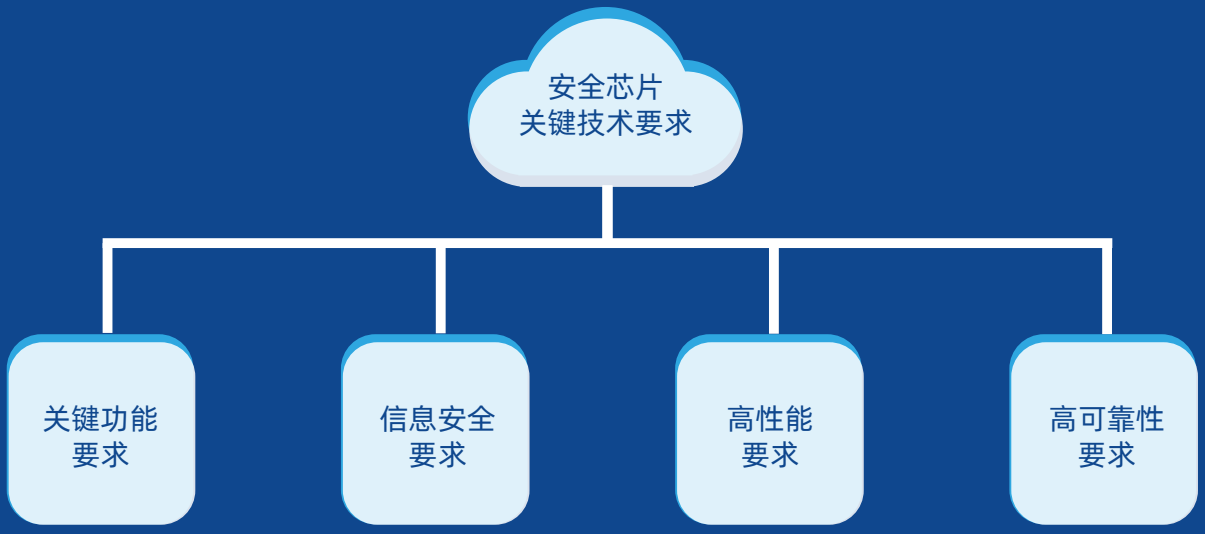
车辆在与充电桩连接并进行通信认证中，充电桩通过安全芯片验证车辆的合法和有效性，实现车辆连接充电桩的安全合规性，同时在充电认证过程中提供对个人隐私保护、充电数据加密等数据安全能力，从而保障了电动汽车充电系统的安全性。

5.14.4. 应用案例

汽车智能网联已成为趋势，充电桩作为电动汽车的首要接口，更间接变成了交通信息的收集者、传递者与承载者。充电桩一旦信息泄露，后果严重。新能源汽车充电安全性和可靠性正成为众多用户以及场站运营商重点关注的部分。严格保护用户隐私数据，平衡数据流通与泄露风险，才能使智能网联汽车产业健康快速发展。

吉利旗下的极氪能源ZEEKR　Power电动汽车交流充电桩，是首个通过中国网络安全审查技术与认证中心安全评估，获得“IT产品信息安全认证证书”的充电桩产品。除了常见的短路、漏电、过压、联机等多重保护设计外，最重要的是，运用安全芯片技术，具备完善的信息安全技术保障，能够及时发现、报告并处理网络攻击或异常行为。

此外，华为近年来也在电动汽车充电系统产品方面取得显著进展，构建了“云管边端”的架构体系和产品解决方案，从安全芯片、操作系统、数据库、端到端可信安全技术，有效实现能源智能化和数据信息安全防护。



汽车安全芯片作为汽车电子系统中至关重要的一环，其关键技术要求涵盖了多个方面，以确保芯片能够在汽车这一特殊应用场景中发挥出卓越的安全性和稳定性。

06 汽车安全芯片关键技术要求

6.1. 关键功能要求

安全芯片关键功能要求如下：

- 芯片标识：安全芯片应具备唯一的芯片标识且具备逻辑或物理的安全机制保证标识不被修改且不被擦除；

- 真随机数生成：安全芯片应支持真随机数生成和实时自检功能。真随机数发生器（TRNG）是安全芯片的重要组成部分，其随机源的数量直接影响随机数生成的质量和安全性；

- 密码算法支持：安全芯片应支持符合国际、国家或行业标准要求的密码算法，包括但不限于对称加密算法（如SM4、AES等）、非对称加密算法（如SM2、ECC、RSA等）以及杂凑算法，以满足不同安全需求，并保证在标称的工作环境中其功能正确性与算法安全性；

- 密钥管理：安全芯片应支持对密钥的生成、存储、使用、更新、导入和销毁功能进行管理；

- 敏感数据管理：安全芯片应支持对内部敏感数据进行管理，包括数据的存储、访问、运算、清除和传输；

- 安全生命周期管理：安全芯片应对自身的安全生命周期进行管理。

6.2. 信息安全要求

安全要求如下：

- 随机数要求：安全芯片应具有硬件机制保障随机数生成的安全性，支持应至少2个（宜4个）相互独立的物理随机源。

- 密码算法要求：安全芯片应具有硬件机制保障密码算法运算环节的安全性，对称算法密钥长度应不少于128位，非对称ECC算法密钥长度应不少于256位，非对称RSA算法密钥长度应支持3072位及以上，杂凑算法结果长度应不少于256位。

- 密钥安全要求：安全芯片应具有硬件机制保障密钥生成、存储、使用、更新、导入和销毁的功能，且应具备相应的密钥管理策略。

- 敏感数据安全要求：安全芯片应具有敏感数据的权限管理、保护与校验机制，保障敏感数据的信息安全。

- **接口安全要求：**安全芯片物理接口与逻辑接口应全部声明且不会泄露内部敏感数据，各个接口的输出应一致，且具备调试接口的认证机制或被禁用。

- **固件安全要求：**安全芯片应具有固件安全机制，保障固件在运行与更新的过程中的正确性，且在固件异常的状态下能够正确识别并响应。

- **固件安全升级要求：**具备固件安全升级机制，支持启动升级前的权限验证，且支持固件升级不破坏用户数据，升级失败不影响固件正常运行。

- **抗脆弱性攻击要求：**安全芯片应具有版图保护措施、主动屏蔽层、异常环境检测机制、抗侧信道分析能力和对故障注入的抵抗能力。

6.3. 高性能要求

安全芯片高性能要求如下：

- **高性能：**安全芯片应具备强大的处理能力，以满足实时性要求。

- **低功耗：**安全芯片应在保证高性能的同时，尽可能降低功耗，对汽车能源系统的使用降到最低。

6.4. 高可靠性要求

高可靠性要求如下：

- **车规级：**安全芯片应根据部署的环境要求，如对车规级要求应至少符合相关车规级温度要求，以保证芯片功能正常使用。

- **极端环境下的稳定性：**汽车运行环境复杂多变，安全芯片需要在高温、低温、高湿度、振动等极端环境下保持稳定的性能。

- **长期使用寿命：**汽车的使用寿命通常在十年以上，安全芯片需要具备同样长的使用寿命，并经过严格的可靠性测试。

- **全生命周期可靠性测试：**安全芯片应在不同周期进行相应测试以保证可靠性，如加速环境应力试验、加速寿命模拟试验、封装组装完整性试验、晶圆可靠度试验、电性能验证试验、缺陷筛选试验等。

01

汽车安全芯片检测与认证

7.1. 安全能力评估相关

7.1.1. Common Criteria for Information Technology security Evaluation（CC标准）

CC标准是一个用于表示IT产品或系统安全评估深度与严谨程度的分级标准，用评估保障级EAL划分不同的安全级别。这个评级体系由低到高分为七个等级（EAL1至EAL7），每个等级都代表了不同的安全保障程度。

EAL检测认证主要基于标准ISO/IEC 15408《Information security, cybersecurity and privacy protection - Evaluation criteria for IT security》，在国内也有对应的标准GB/T 18336《信息技术 安全技术 信息技术安全评估准则》，同时考虑到不同领域之间的差异性，CC标准的应用也会有不同的细化要求。在芯片领域，GB/T 22186《信息安全技术具有中央处理器的IC卡芯片安全技术要求》针对具有中央处理器的集成电路（IC）卡芯片达到EAL4+、EAL5+、EAL6+所要求的安全功能要求及安全保障要求进行了规定，适用于IC卡芯片产品的检测。

在检测内容方面，CC标准对密码支持、用户数据保护、标识和鉴别、安全管理、安全功能保护和资源利用六个安全功能进行了要求。

7.1.2.《安全芯片密码检测准则》

GM/T 0008《安全芯片密码检测准则》是一个针对安全芯片信息安全能力的通用分级标准，将安全芯片的安全能力划分为三个安全能力依次递增的安全等级，同时对各个安全等级的安全芯片的检测方法提出了要求。标准规定安全等级1的安全芯片可应用于外部运行环境能够保障安全芯片自身物理安全和输入输出信息安全的应用场合；安全等级2的安全芯片可应用于外部运行环境不能保障安全芯片自身物理安全和输入输出信息安全的应用场合,在该环境下安全芯片对各种安全风险具有基本的防护能力。达到安全等级3的安全芯片可应用于外部运行环境不能保障安全芯片自身物理安全和输入输出信息安全的应用场合,在该环境下安全芯片对各种安全风险具有全面的防护能力。

在测试内容上，安全芯片密码检测准则对安全芯片的密码算法、安全芯片接口、密钥管理、敏感信息保护、固件安全、自检、审计、攻击的削弱和防护、生命周期保证共9个方面进行了规范，不仅覆盖了芯片自身所具有的安全能力，还对厂商的管理资质提出了要求。

7.1.3. 功能安全系列标准

功能安全认证方面，当前行业主要依据ISO 26262系列标准（对应转化国家标准GB/T 34590）。SO26262是基于IEC 61508功能安全标准在汽车领域的细化。在ISO 26262系列标准2018年发布的版本中明确了半导体功能安全的内容，例如要对复杂芯片进行模块化分析，定义了供应商和集成商的角色定位，以及如何把整个芯片作为一个SEooC来开发（即独立安全单元，不考虑具体应用环境），同时规定了需要具备的文档，相关方的接口和责任等内容。功能安全系列标准将安全等级ASIL划分为了A、B、C、D四个等级，其中ASIL A 是最低的安全等级，ASIL D 是最高的安全等级，并从严重性、暴露性和可控性三个维度进行具体评估：

- 严重性，用SX表示，4个等级，S0无伤害；S1轻伤；S2重伤；S3致命伤害；
- 暴露性，用EX表示，5个等级，E0是几乎不可能暴露于危险中，E4是可能性极高。
- 可控性，用CX表示，4个等级，最低C0可控，最高C3几乎不可控。

除了这四个等级QM 表示与安全无关。评估结果范例表格如下表所示。

严重度	暴露率	可控性		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

7.2. 环境可靠性及电磁兼容

7.2.1. AEC-Q系列标准

AEC-Q系列标准是由汽车电子委员会制定的汽车零部件认证和质量体系标准，以汽车实际应用要求

为核心，从汽车芯片可能承受的环境条件及使用耐久性要求等角度出发，通过相关基础研究、实际数据测量，结合芯片生产、制造环节不同阶段需要把控的指标参数，从晶圆制造、封装、外观检测、缺陷筛选、功能测试等环节对汽车芯片提出了测试要求。

AEC-Q系列标准主要包括AEC-Q100、AEC-Q101、AEC-Q102、AEC-Q103、AEC-Q104和AEC-Q200等，其中AEC-Q100主要针对车载应用的集成电路产品提出了一套应力测试标准。

安全芯片主要适用于针对集成电路产品的可靠性进行评价的AEC-Q100标准。在测试条件划分方面，

名称	测试目标	测试内容
AEC-Q100	芯片应力测试	AEC-Q100 基于失效机制对集成电路芯片及封装的应力测试 AEC-Q100-001 邦线切应力测试 AEC-Q100-002 人体模式静电放电测试 AEC-Q100-004 集成电路闩锁效应测试 AEC-Q100-005 可写可擦除的永久性记忆的耐久性数据保持及工作寿命的测试 AEC-Q100-007 故障仿真和测试等级 AEC-Q100-008 早期寿命失效率（ELFR） AEC-Q100-009 电分配的评估 AEC-Q100-010 锡球剪切测试 AEC-Q100-011 带电器件模式的静电放电测试 AEC-Q100-012 12V系统灵敏功率设备的短路可靠性描述

AEC-Q100标准主要内容

温度等级	最低环境工作温度℃	最高环境工作温度℃
0	-40	150
1	-40	125
2	-40	105
3	-40	85

环境工作温度范围

AEC-Q100根据产品测试的温度范围分为四个温度等级，其中第3级标准的工作温度范围在-40℃至85℃之间；最严格的第0级标准工作温度范围可达到-40℃至150℃。安全芯片主要适用的温度等级为1级或2级。

7.2.2.《车辆集成电路电磁兼容试验通用规范》

《车辆集成电路电磁兼容试验通用规范》对车辆集成电路（IC）电磁兼容性（EMC）的通用试验要求和方法进行了规定，确保车辆集成电路在复杂的电磁环境中能够稳定、可靠地工作，不受外界电磁干扰影响，同时也不对其他电子系统产生不可接受的电磁干扰。在技术要求方面，该标准对IC的RF发射、RF抗扰度、脉冲抗扰度、系统级ESD进行了规定，并对发射和抗扰度的试验方法进行了规范。

7.3. 汽车安全芯片产品标准

7.3.1.《汽车安全芯片技术要求及试验方法》

汽车安全芯片行业标准《汽车安全芯片技术要求及试验方法》（下称“汽车安全芯片标准”）是由汽标委组织起草的针对汽车行业安全芯片应用场景的实际需要所制定的，包含技术要求和和试验方法的产品标准。

在技术要求方面，汽车安全芯片标准对功能、性能、电特性、电磁兼容、功能安全、信息安全、环境可靠性、研发与生产保障八个部分提出了要求，不仅覆盖了安全芯片的功能测试与信息安全相关能力，也对功能安全、电磁兼容、环境可靠性等部分进行了要求，是一个面向汽车安全芯片的行业标准。

在试验方法上，汽车安全芯片标准规范了功能、性能、电特性和信息安全这四个部分的试验方法，在功能要求上对芯片标识、安全生命周期、随机数、密码算法、密钥管理和敏感数据管理这六项主要的功能进行要求，并给出了明确的检测方法；电特性试验主要包括电压容限测试、电压跌落测试和电流最大值测试，针对不同电源环境下芯片的功能和性能进行检测；性能测试主要针对不同工作环境与工作模式等条件下芯片的密码算法性能，以及启动和唤醒的响应时间进行检测；信息安全则对芯片信息安全保护机制的实现方法和外部攻击防护机制有效性进行检查与测试。

08

汽车安全芯片发展趋势和建议

8.1. 安全芯片发展趋势

趋势一：汽车信息安全加快进入强监管时代。中国多项有关汽车网络安全与数据安全政策与指南的发布，以及《汽车整车信息安全技术要求》等标准的制定发布和即将实施。汽车信息安全强监管的时代将加速到来，这也必将推动整个行业汽车信息安全管理体系能力的快速提升。在信息安全强监管时代，整车信息安全将触及汽车制造商新车型市场准入的资格，届时信息安全将会成为汽车安全的核心指标之一，安全芯片需求将会更为强烈。

趋势二：国产芯片替代进程加速发展。硬件安全模块是抵御攻击和保障智能网联汽车安全可控的重要技术手段。在日益复杂的国际环境及国家安全战略的背景下，支持SM系列商密算法的安全芯片的国产化替代将成为主流趋势。国内芯片企业和基础软件供应商纷纷发力，研发自主可控的国产化方案，支撑我国汽车网络信息安全可靠与稳定发展。

趋势三：以合规为基础，以成本为导向，促进密码产品形态创新。在“降本增效”大环境下，以更低成本高效提升汽车信息安全能力成为关键策略之一。面对持续叠加的安全修复成本与代价，如何以更低成本高效解决信息安全问题，并提升原生安全能力，成为当前智能网联产业链共同的关注点。未来，具备商密算法安全资质的独立式安全芯片和具备HSM的MCU和SoC等安全模块，将成为支撑车辆信息安全的核心。

趋势四：后量子密码世代的到来。来自中国科大、国盾量子、国科量子、济南量子技术研究院与上海交大等单位组成的科研联合团队完成了全球首次量子密钥分发（QKD）和后量子密码（PQC）融合可用性的现网验证，我们有理由相信这是后量子密码商用的“星星之火”。国产安全芯片行业在不久的将来将会出现支持后量子密码的安全芯片类产品。

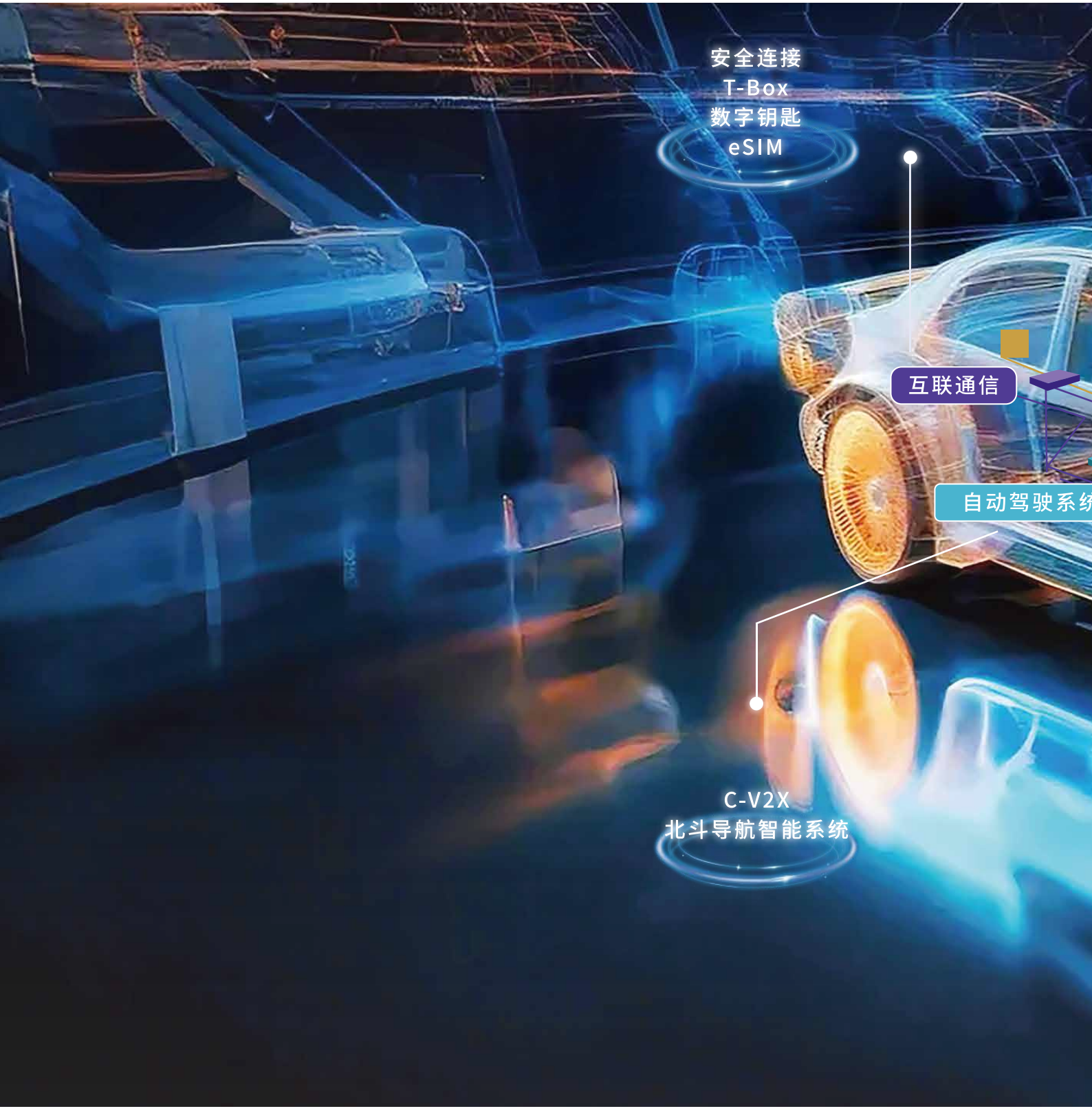
8.2. 安全芯片应用的政策建议

01 加快标准制定及安全规范制定出台：在当前《国家汽车芯片标准体系建设指南》的科学规划和系统部署指导下，我国汽车芯片标准化工作正在高效推进。其中，行业标准《汽车安全芯片技术要求及试验方法》现已开展标准制定工作，旨在为汽车安全芯片的设计开发、测试、评估和应用提供技术规范和试验方法。同时，除特定应用场景外，当前基于汽车全生命周期密码使用角度下的相关技术安全规范仍属空白，建议加快出台汽车全生命周期密码使用角度的技术安全规范标准，以确保安全芯片在整个使用周期中的安全性。

02 出台汽车信息安全应用场景匹配的强制性安全芯片政策：鉴于我国新能源汽车行业的快速发展，汽车信息数据、汽车芯片数据传输以及车路云协同等关键领域的安全问题日益凸显。当前，此类领域木马软件和篡改软件攻击的威胁，对用户的电池安全、行驶安全以及隐私安全造成严重影响。为了有效应对未来可能出现的突发和极端安全挑战，建议相关部委、管理机构，考虑出台、实施包含T-Box、C-V2X以及北斗系统在内相关方向强制使用带商密算法的独立安全芯片政策，增强车辆的网络安全防护能力，以应对未来突发的、极端形势下的安全挑战。

03 推进抗量子密码算法标准与监管规范制定工作：我国目前尚未出台抗量子密码算法相关的商密标准和监管规范，需根据今后密码算法趋势及抗量子算法的技术进步与应用实施，推进包括法律法规的制定、行业标准的研制以及商用密码应用安全性评估的指导性文件等相关修订工作，不断完善标准和规范，以适应技术的不断发展和应用需求，为行业提供更为标准化、商业化应用指引。

04 加强市场业务生态安全性评估与合规性指导：市场业务生态方面，目前国内已有多种专用于C-V2X业务的高算力、高可靠性的商密安全芯片产品。同时，目前已颁布的C-V2X安全标准中已明确了必须使用商密SM2/SM3/SM4算法，但并未明确密码算法运算单元的资质合规性要求，因此，在实际业务应用中，有部分密码应用方案仅有部分功能使用安全芯片，签名验证、证书链验证采用均外部认证，存在安全风险。应尽快明确密码算法运算单元的资质合规性要求，尽快制定实际业务生态中具体方案的实施合规性、安全性评估指导措施等。


安全连接
T-Box
数字钥匙
eSIM
互联通信
自动驾驶系统
C-V2X
北斗导航智能系统