GM/Y 5016-2024

# 车载 SoC 密码模块保护轮廓和测评要求研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

# 摘要

工信部文件《车联网网络安全和数据安全标准体系建设指南(2022)》指出“随着汽车电动化、网联化、智能化交融发展，车辆运行安全、数据安全和网络安全风险交织叠加，安全形势更加复杂严峻，亟需加快建立健全车联网网络安全和数据安全保障体系，为车联网产业安全健康发展提供支撑。”

智能网联汽车的安全初步可以分为车外联网安全、车内联网安全、车载组件安全等，它们都依赖于车载 SoC 芯片中的密码学能力。因此，智能网联汽车安全的基础安全锚点就是车载 SoC 密码模块（业界也称为 SoC 密码安全子系统）。

考虑到当前国内汽车联网化和智能化的紧迫性，对所使用车载 SoC 芯片的密码安全能力需求非常迫切，但作为车载安全锚点的 SoC 密码模块尚无对应的设计指南和检测规范，开展对车载 SoC 密码模块的保护轮廓和测评要求研究是非常迫切的。

本项目聚焦对车载领域 SoC 密码模块开展研究，涉及 SoC 密码模块的定义、边界和功能，以及设计及测评要求。

本项目通过调研业界 SoC 密码模块的技术和应用情况、国内外标准化现状，分析 SoC 密码模块对标现有国内密码标准 GM/T 0008 和 GB/T 37092 的适用性，总结了技术应用和标准化的趋势。参考业界 SoC 密码模块标准和优秀实践，提出车载 SoC 密码模块的定义、资产、面临的威胁，推导出可能的安全需求。

围绕上一步分析得到的资产、威胁和安全需求，从安全功能测评、安全保障要求和生命周期安全管理三个维度梳理出车载 SoC 密码模块的测评需求，并提出标准建议。

**关键词：**智能网联汽车，SoC 密码模块，设计指南，测评要求

# 目录

# 前言

本项目聚焦对车载领域 SoC 密码模块开展研究，涉及 SoC 密码模块的定义，边界和功能，以及 SoC 密码模块的相关测评要求和测评实施指导和建议。

本项目是由密码行业标准化技术委员会根据国家密码管理局批准的《2021 年密码行业标准制订计划（商用密码领域）》下达的密码行业标准编制工作任务。项目名称为《车载领域 SoC 密码模块保护轮廓与测评要求研究》，项目类型为研究类项目，项目所属工作组为测评工作组。

牵头单位为华为技术有限公司，标准参与单位包括商用密码检测认证中心、深圳市纽创信安科技开发有限公司、华中科技大学、武汉大学、清华大学、北京理工大学、浙江大学、中国科学院信息工程研究所、成都信息工程大学、成都电子科技大学、开源网安物联网技术(武汉)有限公司、重庆招商检测中心等。本标准研究报告的主要撰写人为张小虎、章庆隆、刘卓、廖楠、雷银花、刘政林、涂航、王安、张帆、杨坤、马原、张浩、贾珂婷、吴震、杜之波、王敏、肖堃、魏宁、张海春、张梦良、王恺等。

# 车载 SoC 密码模块保护轮廓与测评要求研究

## 1. 概述

### 1.1 背景

随着智能网联技术的快速发展，智能网联汽车领域正成为新一轮科技革命和产业革命的战略高地，我国智能网联汽车行业迎来了发展的黄金期，预计 2025 年中国智能网联汽车数量有望达 2000 万辆。

2018 年 12 月，工业和信息化部制定实施《车联网（智能网联汽车）产业发展行动计划》[1]，明确“强化管理、保障安全”的基本原则，围绕健全安全管理体系、提升安全防护能力、落实企业主体责任等方面，就车联网网络安全作出系统部署。

2020 年 2 月 24 日，发改委、工信部等 11 部委联合印发《智能汽车创新发展战略》[2]文件指出“要严格落实国家网络安全法律法规和等级保护，完善智能汽车网络安全管理制度，建立覆盖汽车制造企业、电子零部件供应商、网络运营商、服务提供商等产业链关键环节的安全责任体系”。

SoC 密码模块已成为解决 SoC 芯片安全性的基础解决方案，广泛应用于车载等重要领域的 SoC 芯片。车载领域的设备安全影响到整部车，进而影响到路人或交通安全。考虑到当前国内汽车联网化和智能化的紧迫性，对所使用车载芯片的密码安全能力需求非常迫切，但作为车载安全底座的 SoC 密码模块尚无测评指南，开展对车载 SoC 密码模块的保护轮廓和测评要求研究是非常迫切的。

### 1.2 研究目标

车载领域安全一般有网络安全Cyber Security、功能安全Functional Safety，前者主要面向汽车网络攻击场景下的信息保护等，后者是面向车载包含电子、电气或软件类器件的功能可靠性要求。

车载领域的功能安全要求已有成熟的评价体系，即遵从国际ISO 26262、AEC-Q100等标准。因此，车载领域功能安全要求直接参考已有的标准。

车载领域网络安全，一般划分为车外通信安全、车内通信安全、车内组件安全三类，如下图。

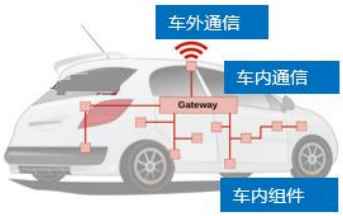


图 1-1 车载领域网络安全分层

车外通信是指汽车通过移动网络、无线信号、NFC、蓝牙等方式与外界进行通信，常见的车外通信部件有T-Box。

车内通信是指汽车内部通过CAN、以太网等通信协议处理来自车内不同组件的数据，一般会使用类似于汽车网关的部件作为中心网络节点。

车内组件是指汽车内部负责各功能域的部件，如自动驾驶、车身控制系统、传感系统。

这些汽车通信部件或组件的SoC/MCU大多采用SoC密码模块作为安全底座，构建密钥管理、安全启动、安全升级等功能。

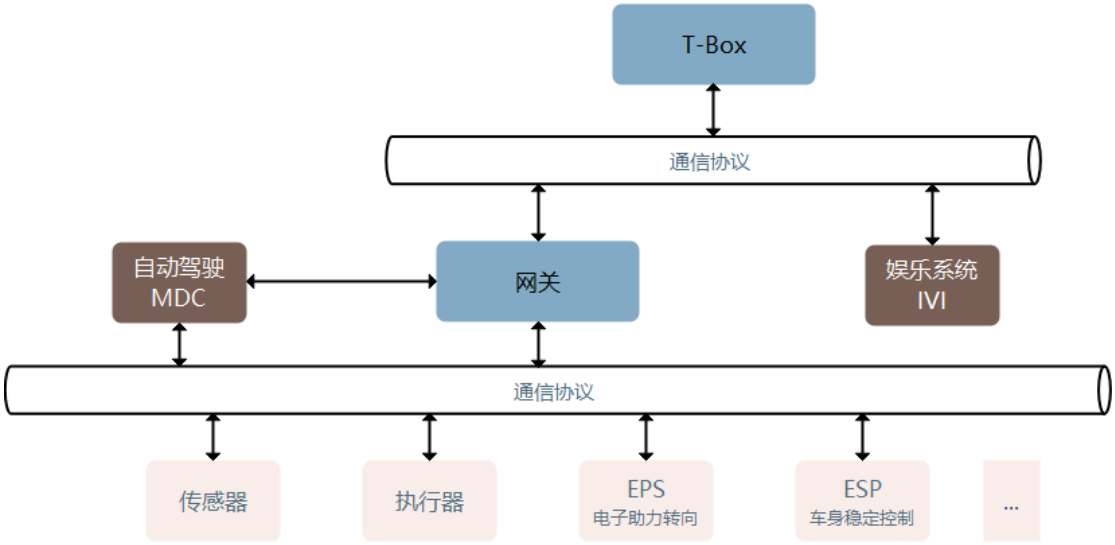


图 1-2 车载领域网络安全交互关系

### 1.2.1 研究对象

本文聚焦对车载领域SoC密码模块（业界也称为SoC密码安全子系统）开展研究，涉及其定义，边界和功能，以及设计、测评要求，并提供测评实施指导和建议。

车载领域中SoC芯片应用广泛，包括自动驾驶、智能座舱、娱乐系统、车身控制系统、传感系统等。其中用于自动驾驶等场景的SoC密码模块，对安全性要求高，可对应到密码模块标准的高等级要求，另外像娱乐系统等等场景的SoC密码模块的安全性要求较低，可对应密码模块标准的低等级要求。

### 1.2.2 研究范围

本文专注于车载领域SoC密码模块的网络安全，研究技术及标准现状、定义、边界划分、功能和需求、测评要求，如何适配当前国内密码测评体系等内容。从而探究该如何去测评车载领域SoC密码模块，保证其安全性，为后续此类产品提供设计指南和测评指导。

### 1.2.3 研究必要性

关于本文的研究必要性，主要从以下几点来分析：

1）从智能车对所使用车载芯片的密码安全能力需求角度：随着汽车信息通

讯、人工智能、互联网等行业深度融合，汽车产业已经进入技术快速演进、产业布局加速的新阶段。长期预测中国的智能网联汽车市场将不断增长，至 2025 年，市场渗透率预计超过 75%以上，高达 2000 万辆。对于庞大的智能车市场，智能车的安全影响范围极大，同时智能车上部署的车载芯片是影响智能车自身安全的关键因素，因此如何保证车载芯片的密码安全能力，如何制定测评此类安全能力的方法指导是迫在眉睫的。

2）从既有标准体系、当前的测评工作角度：当前国内针对芯片类的主要测评标准有安全芯片（GM/T 0008），密码模块技术要求（GB/T 37092）。安全芯片测评主要针对独立芯片类产品，物理边界清晰，但是 SoC 密码模块是集成在 SoC 芯片中，SoC 密码模块的物理边界不可视（如图 1-3），且可能与 SoC 芯片共用外置存储器，这使得 SoC 密码模块或集成了 SoC 密码模块的芯片都难以满足高等级安全芯片认证要求。同时，目前 SoC 密码模块如何通过密码模块高等级认证的具体实施指导也是不全面的。通过高等级密码模块认证来测评 SoC 密码模块是把关其安全性的一个重要措施。当前研究 SoC 密码模块的测评要求，如何适配现有标准体系，为后续此类产品过商密检测认证提供测评实施指南是很有必要的。

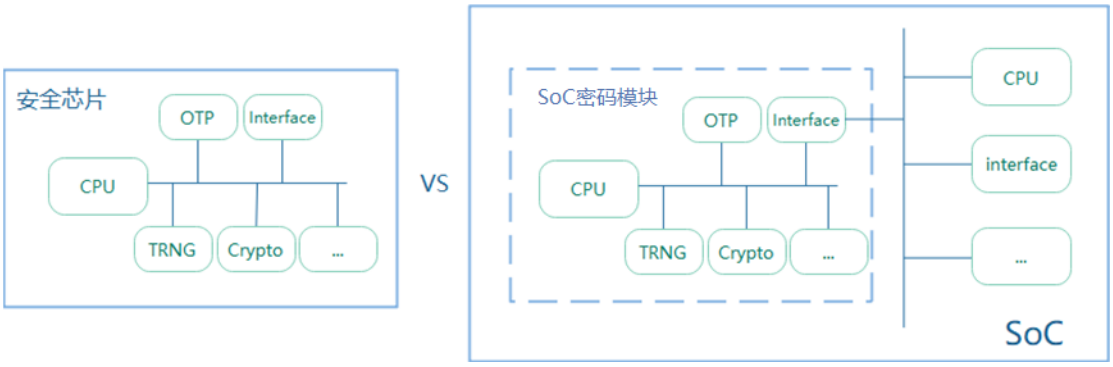


图 1-3 安全芯片与 SoC 密码模块的物理边界

### 1.2.4 研究目标

本文希望通过对车载领域SoC密码模块的密码技术现状、密码应用需求、现有标准测评现状等加以研究，梳理当前测评标准体系下SoC密码模块测评所面临的挑战，探究车载领域SoC密码模块的测评要求和实施指导，为有关部门在SoC密码模块领域开展测评提供参考。

本文拟完成以下交付物：

1）《车载 SoC 密码模块保护轮廓与测评要求研究》；

# 2. 发展现状

## 2.1 国内外 SoC 密码模块技术现状

### 2.1.1 SoC 密码模块概述及技术现状

本节介绍SoC密码模块的最新技术。

在系统安全的抽象定义中，系统设计者将一个完整的硬件密码子系统作为系统安全的可信基础。

系统设计人员假设系统中存在基于SoC密码模块的可信根，它是由受到妥善物理保护的的硬件、固件和数据组成，提供一系列密钥保护和加解密功能。

这些SoC密码模块的共同之处是，它们布局在相对隔离集中的芯片区域，有严格的访问控制策略。

根据提供的功能、硬件防篡改和保护级别以及通信接口，这些SoC密码模块可用于不同的应用领域（包括汽车、金融、电信等）。

其中几类业界常见的SoC密码模块是硬件安全模块（Hardware Security Module,HSM）、安全元件（Secure Element,SE）、可信平台/密码模块（TPM/TCM）、用户识别模块（SIM），以及业界较新定义的安全子系统（Secure Sub-system,3S）、专用安全组件（Dedicated Security Component,DSC）。

业界有代表性的厂商SoC密码模块方案包括华为inSE、苹果SEP、高通SPU、微软Pluton、英特尔CSME、AMD的PSP、以及英飞凌的HSM。

下面简要介绍典型的SoC密码模块。

#### 2.1.1.1 硬件安全模块

硬件安全模块（Hardware Security Module,HSM）通常提供加解密功能，例如若干组公钥和私钥加解密算法，以及安全密钥管理功能，例如密钥的安全生成、存储和删除。

HSM提供的关键能力是，这些操作发生在受硬件加固和防篡改的环境中，真随机数和实时时钟通常也包括在内。

传统HSM主要用于服务器后端系统，以管理密钥或支付系统，例如在银行系统中。传统HSM通常是整机形态。

随着行业发展，后续也出现用作协处理器形态的HSM，连接到主机系统。它的体系结构通常包括微处理器/微控制器、一组加密协处理器、安全易失性和非易失性存储器、真随机数、实时时钟和I/O，这些操作通常发生在防篡改外壳内。协处理器HSM通常是包含多个组件的一块单板形态。

最近，在一些前沿应用领域，如汽车和通信领域，HSM功能不再作为独立模块提供，而是现在作为安全协处理器集成在较大的片上系统（SoC）中。事实上，摩尔定律的发展已经允许一个SoC有更高的集成性，作为系统安全可信根的SoC密码模块集成到SoC中是行业的重要发展方向。

HSM功能到底涵盖了什么取决于应用域。因此，安全级别的合规性也由专门的独立评估实验室根据特定的保护轮廓文件（Protection Profile）进行评估。

#### 2.1.1.2 SE 安全元件

与HSM类似，SE安全元件提供了若干组密码算法,包括公钥、私钥、HMAC等，以及安全密钥的存储、生成和删除。

SE与HSM的主要区别是成本、尺寸和外形规格，以及应用场景。

它们通常作为一个单个集成电路实现，并且具有从大约50平方毫米到小于1平方厘米的外形规格。

与安全元件强相关的一个名词是智能卡，智能卡和安全元件之间的主要区别在于外形规格和它们所面向的市场，安全元件是一个更通用的术语，而智能卡具有银行卡的非常特定的外形。

安全元件产量非常巨大，需要非常便宜。

它们的应用场景包括手机SIM卡、银行卡、付费电视卡、国民身份证和护照等，最近还用于物联网设备、车辆系统等。

防篡改和物理保护是安全元件的基本要素。

它们是计算机体系结构域中被称为“域特定处理器”的一种明确实例，根据应用领域，存在特定的保护轮廓文件：金融、汽车、付费电视等。

典型的嵌入式安全元件是一个没有外部器件的集成电路。

它由一个带有加密协处理器、安全易失性和非易失性存储、真随机数等的小型微控制器组成。

I/O通常是受限的，通过一组特定的管脚或NFC无线对外连接。

构建安全元件对硬件设计者来说是一个挑战，因为人们需要将嵌入式电路的安全性和非安全性需求结合起来：小外形尺寸（无外部存储器）、低功耗和/或低能耗，以及防篡改和抗物理攻击，例如侧信道和故障注入攻击。

近年来，随着行业的发展和摩尔定律的演进，在手机、机顶盒等特定领域SE安全元件也逐步向SoC集成方向发展，作为一个安全子系统集成到大型SoC中，以提供更加灵活配置的领域安全应用能力。

他们安全级别的合规性通常按照经典SE的保护轮廓文件（Protection Profile）进行评估，近年也有专用SoC集成形态的安全子系统保护轮廓提出（Secure Sub-System in SoC Protection Profile）。

#### 2.1.1.3 TPM 可信平台模块

TPM模块由行业协会TCG（Trusted Computing Group）定义，为个人计算机（PC）平台提供特定的安全功能。更具体地说，TPM是嵌入在PC平台上的信任根，因此PC+TPM平台可以识别自己及其当前配置和运行软件。

TPM提供了三个特定的可信根：度量可信根（RTM）、存储可信根（RTS）、报告可信根(RTR)。除了这三个基本功能之外，TPM的其他功能还包括：加解密功能、安全密钥存储、安全登录支持等。

它还在部署方式中提供了更灵活的形态，确定了四种类型的TPM：专用集成电路“分立元件”TPM提供最高的安全级别；保护级别低一步是“集成TPM”作为更大SoC中的IP模块；固件和vTPM提供最低级别的保护。

TPM作为一个专用集成电路的形态实现时，很像一个安全元件，但具有到PC平台的特定总线接口，例如， SPI、LPC或I2C总线接口。它的体系结构至少包括一个嵌入式微控制器、若干加密协处理器、用于根密钥的安全易失性和非易失性存储以及一个高质量的真随机数生成器，一般支持哈希函数（SHA1、SHA256和SM3）、公钥（RSA、ECC和SM2）、对称密钥(AES、SM4)和HMAC计算的硬件引擎。TPM是一个单独的模块，物理保护和防篡改对于安全性至关重要。

集成TPM虽然是TCG已定义的四种安全形态之一，但是当前还没有针对集成TPM的保护轮廓定义。

最初，主要的重点是支持安全引导和相关的软件堆栈，以便对安装的软件进行完整的度量。问题是，这个完整的软件基础的复杂性增长得太快，使得很难完全度量有效配置中的所有变化。因此，TPM很少用于保护完整的软件堆栈，直到更高层的软件。

大多数新PC现在都有TPM，但它们用于保护加密密钥、避免固件回滚并协助一般引导过程。

在应用上，除了主要的完整性保护范围外，TCG逐渐扩大了其使用范围，设立了如云、嵌入式系统、物联网、移动、网络设备等工作组。

#### 2.1.1.4 3S in SoC 安全子系统

3S安全子系统是由行业组织Eurosmart定义的一种安全子系统（3S），作为片上系统（SoC）的功能块实现。

3S安全子系统由处理单元、安全组件、I/O端口和存储器组成，可提供面向不同场景的一系列安全功能。

3S安全子系统基于物理和/或逻辑隔离机制，提供与其余SoC组件隔离的安全功能和安全服务，可能依赖于外部存储器来存储内容（数据、代码或两者）。

3S安全子系统与整个SoC设计基本解耦，只需保留3S和SoC之间的接口，就可以保障3S可以从初始SoC重用到其他SoC。

3S安全子系统可用于需要高安全性的多个应用领域，包括且不限于：

- 用户认证和密码存储
- 内容保护
- 金融支付
- 用户识别模块(SIM)
- 数字身份的存储和管理
- 安全的密钥存储
- 可信根(RoT)
- 存储敏感用户数据（例如，医疗保健记录）。

Eurosmart定义的3S保护轮廓文件[3]定义了3S应提供的一组基本安全服务和安全功能。安全服务和安全功能可以扩展以支持特定配置的额外需求。

3S安全子系统可支持多种存储模式：

- 3S集成式存储，如嵌入式flash存储模式；
- 3S与SoC共用外部存储，如与SoC共享外置式flash存储模式；
- 3S专用外部存储，即3S专用外置式flash存储模式。

不同的存储模式会对3S的形态有一定影响，但是整体的安全性需要做到是一致的。

### 2.1.2 车载领域 SoC 密码模块技术现状

车载领域SoC密码模块可以算作通用SoC密码模块的一个子集，通常是用作提供车载系统的可信根功能和密码学能力，除符合通用安全子系统的定义之外，还需要符合车规的可靠可用和功能安全要求，以及面向车载系统的不同场景提供更加轻便的子系统能力。

#### 2.1.2.1 HIS-SHE

作为行业的第一个硬件密码子系统标准，安全硬件扩展(Secure Hardware Extension,SHE)是由德国的汽车行业组织Hersteller Initiative Software(HIS)于2009年定义的。它早于EVITA项目，描述了一种向ECU处理器添加安全区域的方法。

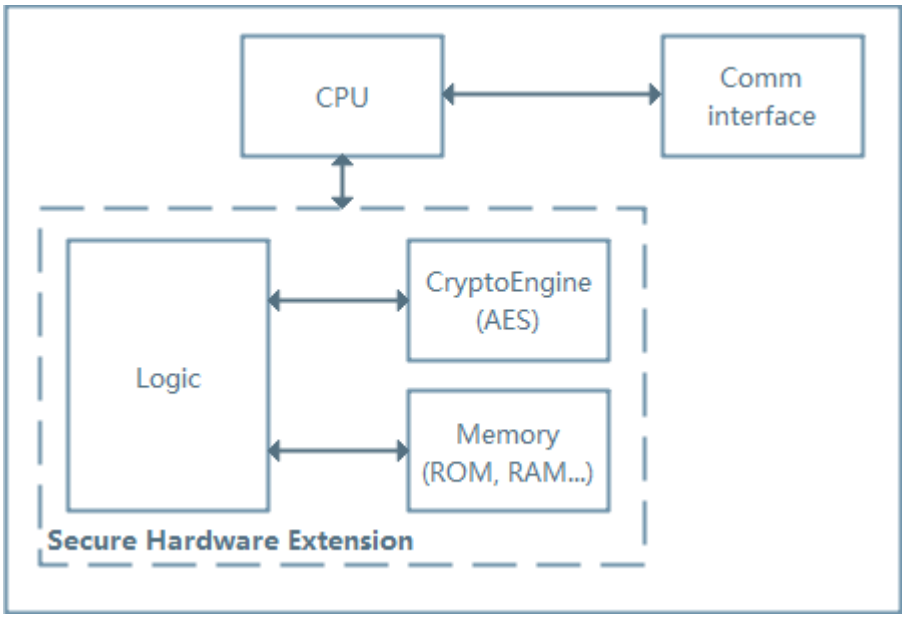


图 2-1 HIS SHE 框架[4]

上图描述了一个简化的示意图。安全区域提供安全存储（RAM、ROM、Flash）、加密功能和控制逻辑。SHE安全硬件扩展支持加密/解密的AES引擎、CMAC和哈希函数。SHE被认为与2.1.2.2节提到的EVITA HSM Light级别具有同等的安全性。相当多的芯片制造商在其设备中实施了SHE硬件（恩智浦、英飞凌、富士通、瑞萨、博世等）。SHE设计是一个非常具体的解决方案，可以重用于其他行业的实现中。基于SHE的车载安全解决方案及API接口近年也被行业组织AUTOSAR（汽车开放系统架构联盟）进行了进一步的详细定义。

#### 2.1.2.2 EVITA HSM

要提高嵌入式设备在非安全环境中的安全性，需要硬件安全功能。欧盟E-safefy vehicle intrusion protected applications（EVITA）项目通过指定硬件功能来认识到这一点，这些功能被定义在保护ECU的HSM中。EVITA HSM定义了三个级别：Light、Medium和Full。

HSM Light至少应实现对称加解密操作的硬件支持：

- AES-128硬件密码引擎
- AES-PRNG硬件随机数生成器
- 安全实时时钟
- 定义良好的硬件接口

HSM Medium在Light的基础上还提供：

- 安全的单调计数器
- 安全CPU
- 安全的RAM
- 安全的NVRAM

HSM Full在Medium的基础上提供：

- ECC非对称密码引擎
- 安全哈希引擎

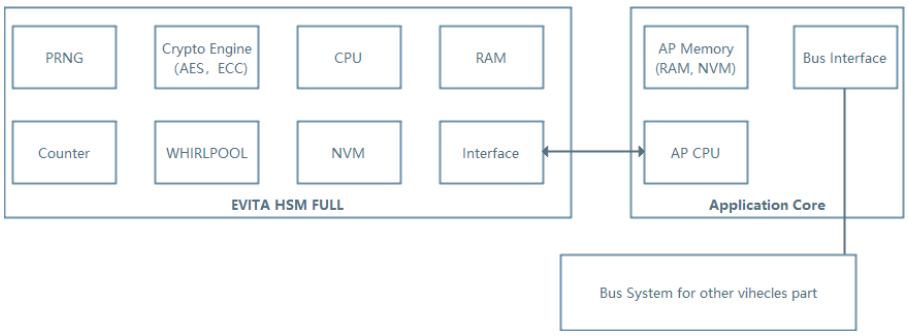


图 2-2 EVITA HSM Full 级别逻辑框架[5]

该规范还定义了HSM和安全功能的软件接口。上述定义已成为许多处理器和ECU制造商定义它们提供的安全能力的参考，汽车行业通常参考而不是直接使用这些规格。

### 2.1.3 车载领域 SoC 密码模块的优势

SoC密码模块主要有集成式（集成于SoC内部）和非集成式（独立芯片）。在构建安全解决方案时，集成在SoC内部的SoC密码模块比非集成式的有安全性上的提升，主要表现在以下两方面：第一，与SoC其他模块的交互（如物理连线）都在SoC芯片内部，所以交互通道上天然地增加了物理保护；第二，SoC密码模块对整个SoC的启动态和运行态增强了管控，可更方便地度量SoC启动镜像度量值，运行态度量值，从而提升整体解决方案的安全性。

因此，本标准研究报告提及的SoC密码模块是指集成于SoC内的形态，这种形态已被业界接受，并逐渐成为芯片构筑整体安全性的一个重要发展方向。

## 2.2 业界现有 SoC 密码模块标准化现状

从上一节技术现状看出，SoC 密码模块承担所在系统或产品的关键操作和重要数据的存储，为系统的启动和运行安全提供保障。同时，汽车领域，SoC 密码模块应用场景非常广泛，如智能驾驶、智能座舱相关的 SoC 等。

因此，SoC 密码模块本身的安全性对所在系统非常重要，有必要调研当前国内外 SoC 密码模块测评相关的标准化现状，梳理 SoC 密码模块的定义、结构组成、资产、潜在的威胁、安全目标、测评方法。

本节会从四个部分展开描述。

**国外标准化现状**。本节重点描述国际上涉及 SoC 密码模块定义、测评的标准化情况。

**国内标准化现状**。本节阐述 SoC 密码模块在国内标准组织的现状，尤其是密码相关的测评标准。

**SoC 密码模块与现行密码标准体系的关系**。本节重点说明 SoC 密码模块的特殊性，在对标现行密码测评标准时遇到的困扰和疑问。

**车载领域 SoC 密码模块的标准化现状**。本节梳理针对车载领域的 SoC 密码模块在国内外标准组织的现状和动作。

### 2.2.1 国外 SoC 密码模块标准化情况

- **基于 CC 体系的 SoC 密码模块标准化**

Common Criteria（以下简称国际CC）是国际认可的信息安全产品测评体系之一，遵循ISO/IEC 15408《Information technology — Security techniques — Evaluation criteria for IT security》系列标准。

如下图所示，参与到国际CC认证的角色包含认可机构Accredited Body（AB）、发证机构Certified Body（CB）、评估机构Evaluated Body（EB）、申请认证的厂商Manufacturer。厂商可以遵照现有的保护轮廓（PP）定义其产品的安全目标，也可自行定义安全目标作为产品的认证范围声明，并向发证机构提交认证申请。在发证机构受理认证申请后，厂商与评估机构确定产品的评测范围，由评估机构完成评测后向发证机构提交评测报告。发证机构在审核评测报告后，作出是否向厂商发证的决定。

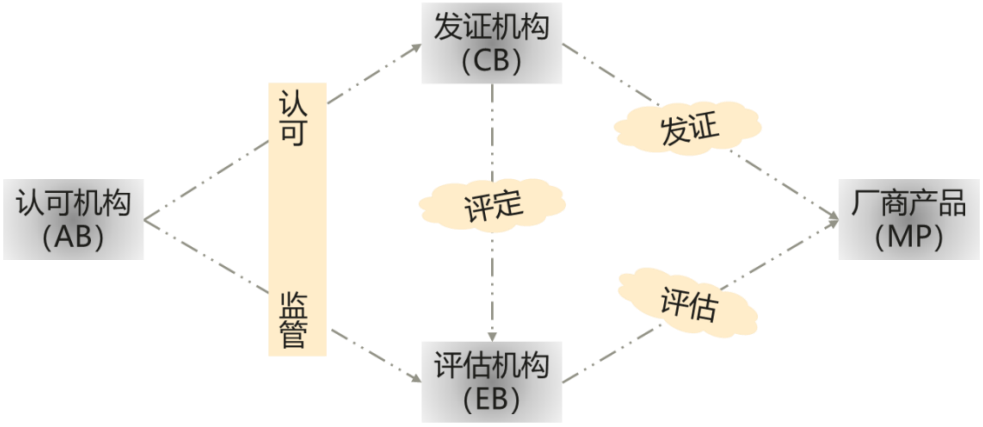


图 2-3 CC 认证角色及流程

Common Criteria官网发布了多个SoC密码模块相关的PP。

- 《Collaborative Protection Profile for Dedicated Security Component》[7]（以下简称 DSC cPP）
- 《Protection Profile V2X Hardware Security Module by CAR 2 CAR Communication Consortium Version 1.0》[8]（以下简称 V2X HSM PP）
- 《Secure Subsystem in System-on-Chip (3S in SoC) Protection Profile, version 1.5》[3]（以下简称 3S in SoC PP）。

DSC cPP是由多家制造商、检测机构和CC发证机构主导编写，如苹果、Atsec和美国National Information Assurance Partnership等，2020年首次发布。DSC cPP针对SoC集成多个子系统的场景，将子系统作为一个单独测评对象提取出来，命名为DSC，并按照保护轮廓的标准框架定义了子系统的逻辑框架、资产、威胁风险、安全目标、安全功能要求和安全保障要求等。这样，评测通过的子系统可以帮助搭载了它的多个SoC或设备复用其安全能力证明和认证结果。DSC可用于支撑密钥库、用户/平台认证、移动商务等场景。

V2X HSM PP是由CAR 2 CAR Communication Consortium联盟主导撰写的，经德国BSI认可后在CC官网发布。V2X HSM面向汽车智能传输系统（VCS）提供密码学运算、密钥管理、数字签名生成、加解密和随机数生成等服务，可依据不同的汽车系统，以独立芯片或SoC密码模块集成的形式搭载。考虑到汽车领域的应用，V2X HSM在使用过程中支持固件/软件升级，固件/软件应该在升级前遵从本PP获得CC认证。V2X HSM PP描述了此类产品的资产、威胁、安全目标、

安全功能要求和安全保障要求。下表呈现了V2X HSM的资产、面临的威胁和要实现的安全目标之间对应关系。

表 2-1 V2X HSM PP 定义的资产、威胁和安全目标

| 资产 | 威胁 | 安全目标 |
|---|---|---|
| 密钥 | 密钥替换 | 私钥访问控制<br>密钥管理<br>自我保护能力 |
| | 密钥泄漏 | |
| HSM 固件/软件 | 固件/软件篡改 | 自我保护能力 |
| | 固件/软件替换 | |
| 安全服务 | 安全服务失效 | |
| VCS 数据 | VCS 数据篡改 | 自我保护能力<br>VCS 数据保护 |
| | VCS 数据泄漏 | |

2022年3月经德国BSI认可发布的3S in SoC PP是由欧洲EUROSMART组织主导撰写，重点参考智能卡领域广泛引用的PP0084《Security IC Platform Protection Profile with Augmentation Packages》。3S in SoC应用领域包含可信根、密钥安全存储、用户鉴权、支付等场景。相比PP0084，3S in SoC PP在评测对象、功能和生命周期管理有较大刷新，如下表所示。

表 2-2 3S in SoC PP 的重要刷新

| | PP0084 | 3S in SoC PP |
|---|---|---|
| 评测对象 | 独立的安全芯片，边界内包含CPU、NVRAM在内的组件 | SoC 内部安全子系统，SoC 其它部分不在评测范围<br>基于存储器的位置，划分三种框架：<br>• 存储器位于安全子系统内<br>• 存储器在 SoC 外且为安全子系统独享<br>• 存储器在 SoC 外且与整个 SoC 共享 |
| 功能 | 数据安全保护<br>密码学运算<br>随机数生成 | 增加硬件可信根相关特性：<br>安全启动、构建信任链、安全升级 |
| 生命周期管理 | 分成 7 个阶段，从硬件设计、制造、封装、集成、使用进行阐述 | 分成 7 个阶段，在阶段 2 特别提出的保护要求：<br>• 安全子系统交付给 SoC 期间的传输保护<br>• 对 SoC 集成环境的保护 |

- **基于美国 FIPS 体系的 SoC 密码模块测评标准化**

美国NIST SP800-140系列标准描述了密码模块安全和检测等方面的要求，也是FIPS 140-2/-3 CMVP（Cryptographic Module Validation Program，密码模块认证体系）的主要测评依据。基于2001年发布的标准版本形成了FIPS 140-2密码模块测评体系，并自2006年陆续升级为ISO/IEC 19790:2006《信息技术 安全技术 密码模块安全要求》和ISO/IEC 24759:2008《信息技术 安全技术 密码模块检测要求》两个标准。当前最新的SP800-140系列标准等同采标于ISO/IEC 19790:2012/Cor.1:2015。

FIPS 140-2/-3 CMVP认证流程和CC认证基本类似，也有发证机构、检测实验室、密码模块厂商等角色，特别之处在于发证机构只与检测实验室联系，保障与厂商的独立关系，如图2-4。

SoC密码模块的厂商依据确定产品的安全策略，也可自行定义安全目标作为产品的认证范围声明，并向发证机构提交认证申请。在发证机构受理认证申请后，厂商与评估机构确定产品的评测范围，由评估机构完成评测后向发证机构提交评测报告。发证机构在审核评测报告后，作出是否向厂商发证的决定。

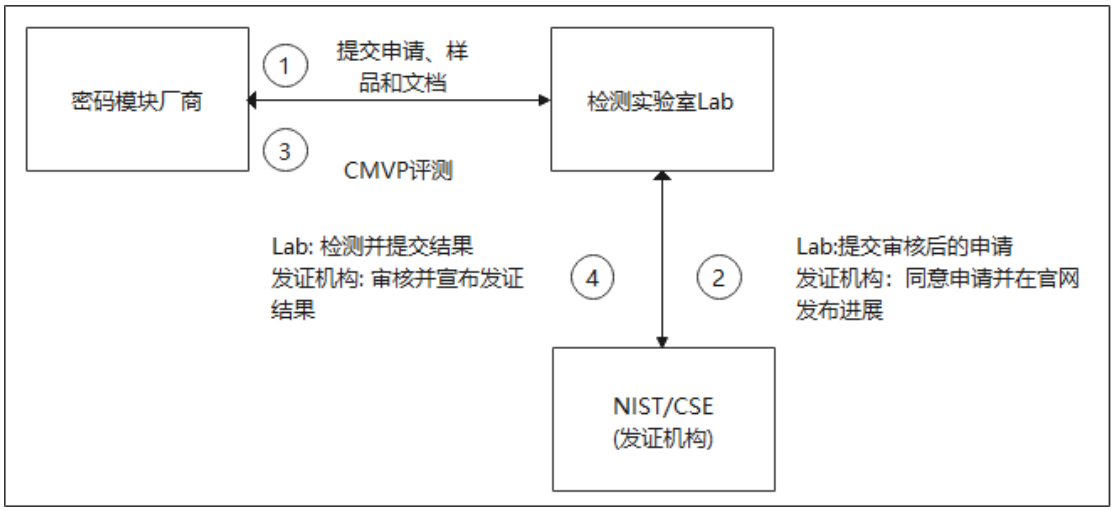


图 2-4 FIPS CMVP 认证流程

FIPS CMVP 更详细的测评内容和针对 SoC 密码模块的测评方法在 4.1 节进行介绍。

### 2.2.2 国内 SoC 密码模块标准化情况

国内信息安全的测评体系有两大类，一个是基于《密码法》定义的商用密码检测认证体系，另一个是基于 GB/T 18336 系列标准《信息技术 安全技术 信息技术安全评估准则》开展的中国 CC 认证体系。

国家市场监管总局和国家密码管理局联合发布的 2020 年第 23 号公告，推出了《商用密码产品认证规则》以及《商用密码产品认证目录（第一批）》。与 SoC 密码模块相关的产品认证类别有第 20 项 安全芯片和第 22 项 其它密码模块。这两项所遵循的认证依据是密码行业标准化技术委员会（SCTC）发布的 GM/T 0008《安全芯片密码检测准则》和 GB/T 37092《信息安全技术 密码模块安全技术要求》。

GM/T 0008-2012 提出安全芯片定义，“含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片”，并为安全芯片依安全能力从低到高划分了安全等级 1、安全等级 2、安全等级 3。GB/T 37092 对密码模块的定义是“实现了密码运算、密钥管理等安全功能的硬件、软件、固件或组合，且被包含在密码边界内”，按照要保护的模块及敏感安全参数规定了四个等级。

中国 CC 认证体系源于上文提到的 ISO/IEC 15408 系列标准，认证流程与国际 CC 认证大体一致。与 SoC 密码模块相关的标准有全国信息安全标准化技术委员会 2016 年发布的 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》。此标准的测评对象是包含了处理单元、易失性存储器、非易失性

存储器、随机数发生器、密码协处理器和安全保护措施等电路的 IC 卡芯片，主要的应用场景是金融领域。参照保护轮廓的格式，此标准定义了测评对象的安全问题（如资产、威胁）、安全目的、安全要求和基本原理。

### 2.2.3 现有密码标准体系对 SoC 密码模块的适用情况分析

参考 2.1 节关于国内外 SoC 密码模块功能、技术应用现状的介绍，SoC 密码模块一般集成在 SoC 内部，搭载专属的 CPU、RAM、ROM、RNG 等组件，并且会运行操作系统向 SoC 其它部分提供服务，从逻辑框架的视角看包含了硬件、固件和运行环境，因此它也具有密码模块的特征。

按照 2.2.2 节推导， GM/T 0008《安全芯片密码检测准则》和 GB/T 37092《信息安全技术 密码模块安全技术要求》是当前商用密码产品认证的主要安全测评依据。依据这两个标准，梳理出 SoC 密码模块与安全芯片、密码模块的共性和特性，研究适配密码测评的方法，如商用密码产品认证。

考虑到 SoC 密码模块保护的资产和提供的功能/服务在 SoC 中属于非常敏感的级别，有必要从对标 GM/T 0008 和 GB/T 37092 高等级的测评内容角度，对 SoC 密码模块与安全芯片、密码模块进行比较。

1）SoC 密码模块与 GM/T 0008 安全芯片的差异

GM/T 0008 中安全芯片的定义是含有密码算法、安全功能，可实现密钥管理机制的集成电路芯片。SoC 密码模块包含但不限于以下功能，如提供对导入的固件解密、验证签名，对根密钥安全存储和传输等功能，一般也具备密码算法硬件协处理器、保护这些处理敏感数据的关键模块的硬件安全措施，为 SoC 应用处理器或其它子系统提供密钥管理、安全升级、生命周期管理等服务。具体定义和功能在 3.1 节进行详细阐述。

测评内容上，GM/T 0008 对安全芯片提出了 8 大项安全要求，如下表。

表 2-3 安全芯片测评要求

| 测评要求 | 具体项目 | SoC 密码模块差异点 |
|---|---|---|
| 密码算法类别 | 分组、公钥、杂凑 | / |
| 密钥管理 | 密钥生成、存储、使用、更新、导入、导出、清除 | 第 2 级要求安全芯片须支持带校验的密钥存储，且密钥清除需要权限。SoC 密码模块有一些密钥存储在 eFuse，由于 eFuse 特性，烧写后不可更改。 |
| 敏感信息保护 | 存储、清除、运算、传输 | / |
| 固件安全 | 固件存储、执行、导入 | 固件导入的第 2 级要求安全芯片固件不可再次导入。SoC 密码模块的固件以加密+签名的方式存储在外置的存储器，每次上电会通过受保护的方式安全导入。 |
| 自检 | 上电、复位、外部指令、主动 | / |
| 审计 | 安全芯片标识、生命周期标识 | / |
| 攻击削弱与防护 | 具备对非侵入式、故障注入等攻击形式的防护 | / |

| | | |
|---|---|---|
| 生命周期保证 | 文档管理、开发环境安全、人员安全、开发流程、源文件等 | / |

从上表可以看到，SoC 密码模块在密钥存储、固件导入等多个测评项难以适配现有要求的描述，对标高等级时存在困难。

2）SoC 密码模块与 GB/T 37092 密码模块的差异

GB/T 37092 中密码模块的定义是实现了安全功能的硬件、软件/固件的集合，并且被包含在密码边界内。这与 SoC 密码模块的结构组成非常相似。

然而，SoC 密码模块由于其功能、形态特殊性，在商用密码产品认证的实际测评中，对现有测评方法产生了挑战。

以下分别就 GB/T 37092《信息安全技术 密码模块安全技术要求》的 11 个安全域进行 SoC 密码模块的讨论点阐述。

表 2-4 GB/T 37092 密码模块安全要求

| 测评域 | 安全要求 | SoC 密码模块讨论点 |
|---|---|---|
| 密码模块规格 | 模块类型、密码边界、工作模式 | 模块类型、密码边界与产品级密码模块的划分存在特殊性，详见下文**讨论点 1** |
| 密码模块接口 | 接口类型、接口定义、可信信道 | |
| 角色、服务和鉴别 | 角色、服务、旁路能力、自启动密码服务能力、软件/固件加载 | |
| 软件/固件安全 | / | |
| 运行环境 | 可变的运行环境、受限/不可变运行环境 | |
| 物理安全 | 物理安全实体、环境失效保护/测试 | SoC 密码模块的形态导致其 EFP/EFT 与密码模块要求存在特殊性，详见下文**讨论点 2** |
| 非侵入式安全 | 针对能量、计时、电磁等攻击的缓解措施和有效性 | |
| 敏感安全参数(SSP)管理 | 随机数生成器，SSP 生成、建立、输入输出、存储、置零 | SoC 密码模块的 SSP 置零与密码模块的置零要求存在特殊性，详见下文**讨论点 3** |
| 自测试 | 运行前自测试、条件自测试 | |
| 生命周期保障 | 配置管理、设计、有限状态模型、开发、厂商测试、配送与操作、生命终止、指南文档 | |
| 对其它攻击的缓解 | 其它未定义的攻击缓解措施 | |

讨论点1：密码模块类型有5种，硬件模块、软件模块、固件模块、混合软件模块和混合固件模块。按照硬件模块的定义，密码边界是指明确定义的边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件、和/或固件部件。SoC密码模块是SoC的一部分，其一般拥有专属的处理器、

易失性存储器等器件，存储SoC密码模块固件的非易失性存储器（NVM）可能是在SoC内，也可能在SoC外。因此，SoC密码模块适合定义为硬件密码模块，其密码边界包含硬件（如专属的处理器、易失性存储器、密码算法引擎、真随机数发生器等），固件（如子系统用于启动、运行的固件等）。以NVM外置的SoC密码模块举例，列出如下示意图，更详细的边界划分见3.1.2节。

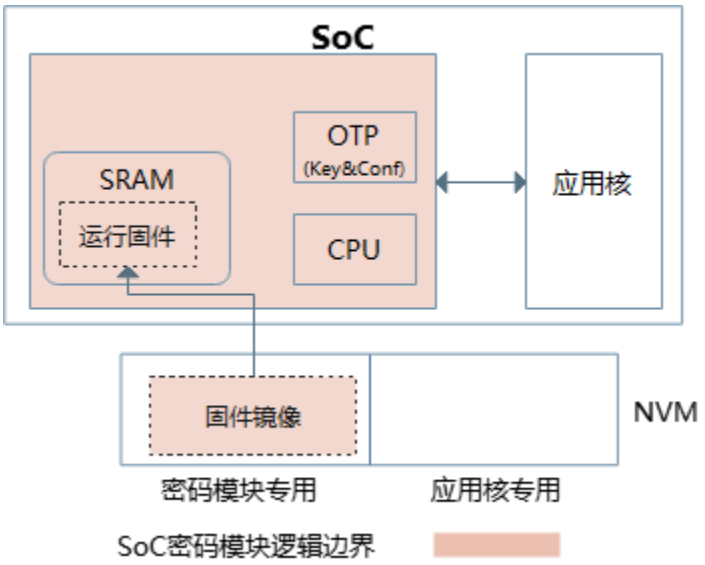


图 2-5 SoC 密码模块（NVM 外置）示意图

讨论点 2：GB/T 37092 第 7.7.4 节物理安全提到面向安全三级和四级的密码模块应具备环境失效保护（EFP）特性或经过环境失效测试（EFT）。

与标准课题组的商密检测中心检测专家讨论后，认为 SoC 密码模块只有在 SoC 上电时才能启动和运行，其电压和温度范围与 SoC 关联，单独对 SoC 密码模块进行 EFT 测试无法执行。类似 SoC 密码模块这类非独立运行的密码模块在集成式或嵌入式安全产品上的应用越来越广泛，可考虑以下 EFP/EFT 评测方法，以解决具体产品设计或检测时的困扰。将集成 SoC 密码模块的 SoC 按照 GB/T 37092 标准要求执行 EFT，当超出声称的工作电压或温度范围内，如果 SoC 停止工作或销毁所有未受保护的 SSP，则认为 SoC 密码模块满足 EFP/EFT 要求。

讨论点 3：GB/T 37092 第 7.9.7 节提到敏感安全参数(SSP)管理要求，对未受保护的 SSP 应执行置零。SSP 有两种，一种是公共安全参数 PSP，另一种是关键安全参数 CSP。PSP 如果不可修改或修改后能够被密码模块发现，可认为是受保护的；CSP 采用核准的密码算法进行加密，可认为是受保护的。SoC 密码模块有一些 CSP（如根密钥），用于密钥派生。这些 CSP 存储在 eFuse，使用硬件加扰算法保护，且只能由密钥派生硬件模块读取访问，没有其它任何访问通道。因 eFuse 特性是烧写后不可更改，导致无法满足上述置零要求。这些作为根密钥的 CSP，在硬件层次通过加扰和访问控制的措施进行保护，是否可认可为一种受保护的方法。

注：当前已知苹果 SEP 产品的 UID key 存放在 eFUSE 中，该部分数据只能被 AES 硬件 IP 使用，无法被任何固件/软件读写使用。苹果 FIPS CMVP 二级认证的处理方式是：在安全策略明确说明 UID key 无法清零作为例外情况，通过认证。

### 2.2.4 车载领域 SoC 密码模块标准化情况

针对智能网联汽车呈现强势发展劲头，国内外标准组织陆续将汽车的信息安

全列为标准化的重点。

国际标准化组织 ISO 下属道路车辆技术委员会 TC22 成立 SC32/WG11 信息安全工作组，并通过建立跨组织的联合工作组加强标准适用性，如 ISO/IEC JTC1/SC27/JWG6。

联合国世界车辆法规协调论坛（WP.29）成立汽车信息安全任务组（TFCS/OTA），提出关于网络安全和信息保护措施的指南草案。

全国汽车标准化技术委员会 TC114 于 2017 年成立智能网联汽车分技术委员会（SAC/TC114/SC 34），负责归口管理我国智能网联汽车领域的国家标准和行业标准。为落实有关政策法规要求，充分发挥标准在保障车辆信息安全、推动产业健康有序发展的引领和支撑作用，同年 SC34 专门设立汽车信息安全标准工作组，开展汽车信息安全标准体系框架研究以及标准制定工作。SC34 主导的多个汽车信息安全相关国标发布，同时有多项国标在制订中。

中国工业与信息化部 2022 年发布了《车联网网络安全和数据安全标准体系建设指南》[12]，在指南中划分了 6 种标准类别，如下图。

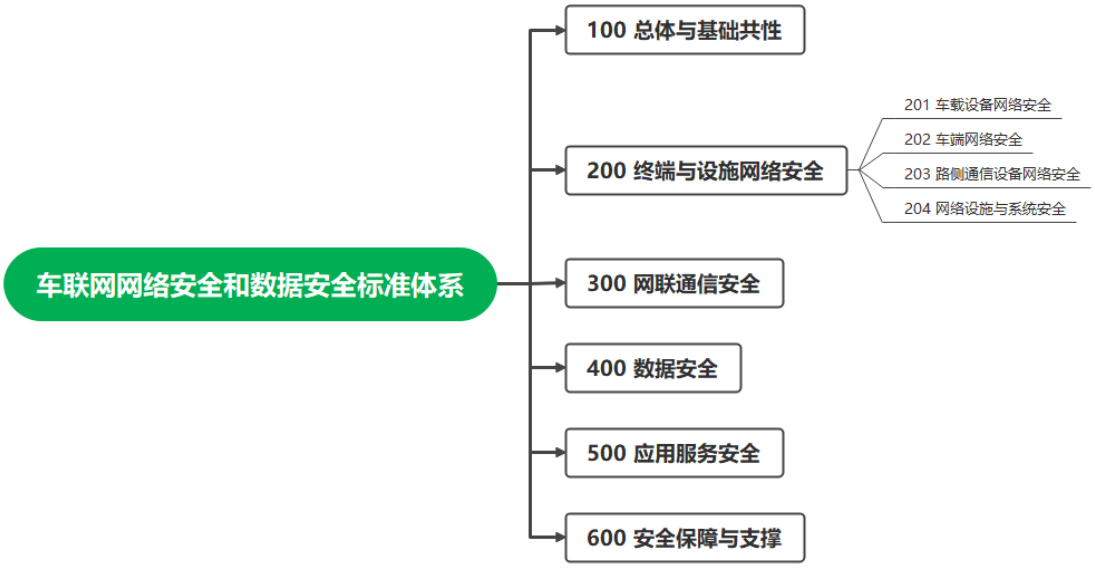


图 2-6 车联网网络安全和数据安全标准类别

终端与设施网络安全方向主要规范车联网终端和基础设施等相关网络安全要求，包括车载设备网络安全、车端网络安全、路侧通信设备网络安全、网络设施与系统安全等 4 类标准，当前有 4 项国家标准已发布，10 余项在制定或立项中，当前还没有专门针对车载领域的 SoC 密码模块设计和测评标准。

表 2-5 车联网终端与设施网络安全方向标准清单

| 序号 | 标准名称 | 状态 |
|---|---|---|
| **201 车载设备网络安全** | | |
| 1 | 汽车网关信息安全技术要求及试验方法 | 已发布 |
| 2 | 车载信息交互系统信息安全技术要求及试验方法 | 已发布 |
| 3 | 汽车电子控制单元网络安全防护技术要求 | 待制定 |
| 4 | 车载计算平台网络安全技术要求 | 待制定 |
| 5 | 车载可插卸物联网设备安全防护及检测要求 | 待制定 |
| **202 车载网络安全** | | |

| | | |
|---|---|---|
| 6 | 汽车电子系统网络安全指南 | 已发布 |
| 7 | 汽车信息安全通用技术要求 | 已发布 |
| 8 | 电动汽车充电系统信息安全技术要求及试验方法 | 制定中 |
| 9 | 汽车软件升级通用技术要求 | 制定中 |
| 10 | 汽车整车信息安全技术要求 | 制定中 |
| 11 | 汽车诊断接口网络安全技术要求 | 制定中 |
| 12 | 汽车网络安全域及防护层级化定义 | 待制定 |
| 13 | 车载总线系统网络安全技术要求 | 待制定 |
| 14 | 车载以太网网络安全技术要求 | 待制定 |
| 15 | 车载操作系统及应用软件安全防护要求 | 待制定 |
| 16 | 汽车电子外部接口网络安全技术要求 | 待制定 |
| **203 路侧通信设备网络安全** | | |
| 17 | 车联网网络关键设备安全技术及检测要求 路侧无线通信设备 | 待制定 |
| 18 | 车联网网络关键设备安全技术及检测要求 路侧检测与信息服务设备 | 待制定 |
| **204 网络设施与系统安全** | | |
| 19 | 车联网网络设施与系统安全防护要求 | 待制定 |
| 20 | 车联网网络设施与系统安全检测要求 | 待制定 |

## 2.3 车载领域 SoC 密码模块的技术和标准发展趋势

车载 SoC 密码模块为平台完整性和密钥管理方面提供有力支持，填补了无法通过软件方案或外部组件来解决的系统级保护的空白。汽车系统与应用以及车载 Soc 安全需求不断发展的同时，当前车载 SoC 密码模块相关的规范（如 SHE、EVITA 等）没有得到进一步维护或更新。从当前许多汽车制造商的宣传或技术介绍可以看出，车载 SoC 密码模块在技术和标准化方面有以下发展趋势。

- 安全分级

综合考虑生产成本、安全性以及功能需求，SoC 密码模块将会趋向于划分为多个安全等级下的变体。例如 EVITA 把 SoC 密码模块等级从高到低划分为三个等级：EVITA full HSM、EVITA medium HSM 和 EVITA light HSM，分别面向 V2X 与中央网关的通信场景，ECU 之间的通信场景以及传感器、执行器与 ECU 的通信场景。

- 平台安全性保护

随着车载系统与应用不断发展，除了向应用程序提供安全服务外，保护车载平台关键资产的机密性与完整性也逐渐成为了 SoC 密码模块的重点功能。车载平台关键资产包括硬件部分知识产权、存储的代码或其他机密。为了保护平台的完整性，SoC 密码模块需要对 IC 架构进行控制，并实施验证机制，如安全引导、硬件强制隔离和运行时监控服务等。同时 SoC 密码模块需要能够监控和验证应用侧的完整性，并对资源进行永久或临时控制，以实施相关的安全策略。

- 标准发展趋势

SoC 密码模块在车载领域的应用越来越广泛，然而当前针对 SoC 密码模块的标准化动作仍较缺乏。随着汽车业界对信息安全的重视，有必要推进 SoC 密

码模块在车载领域的标准化，为安全设计和测评提供参考。

# 3.车载 SoC 密码模块技术研究

上述章节详细描述了SoC密码模块在产业界的应用情况，标准化现状，同时展望了未来的发展趋势。

本章通过利用ISO/IEC 15408的方法学，总结业界SoC密码模块的技术应用情况，梳理出车载领域SoC密码模块的定义、边界和功能，进而识别SoC密码模块的资产、潜在威胁和攻击场景，明确安全目标和需求。

## 3.1 SoC 密码模块的构成定义

结合前文内容及业界材料，本节将提出车载领域SoC密码模块的定义，常见的物理和逻辑边界划分及特点，最后聚焦SoC密码模块的通用和特有功能，形成架构图。

### 3.1.1 定义

当前业界对SoC密码模块已经有一些定义描述。首先对这些业界的定义描述进行梳理。

- **Secure Sub-system in SoC**

欧洲标准组织Eurosmart在2022年3月发布《Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile》，其中关于安全子系统secure sub-system的定义描述如下：

安全子系统是SoC中的一个功能模块，由处理单元、安全组件、I/O端口和存储器组成，提供一系列安全功能（密码学运算，密钥管理，随机数等）以满足既定的安全目标。安全子系统基于物理或逻辑隔离机制，提供与其余SoC组件隔离的安全功能和安全服务。有些场景中，安全子系统是依赖于外部存储进行数据，代码的存储。示意图如下：

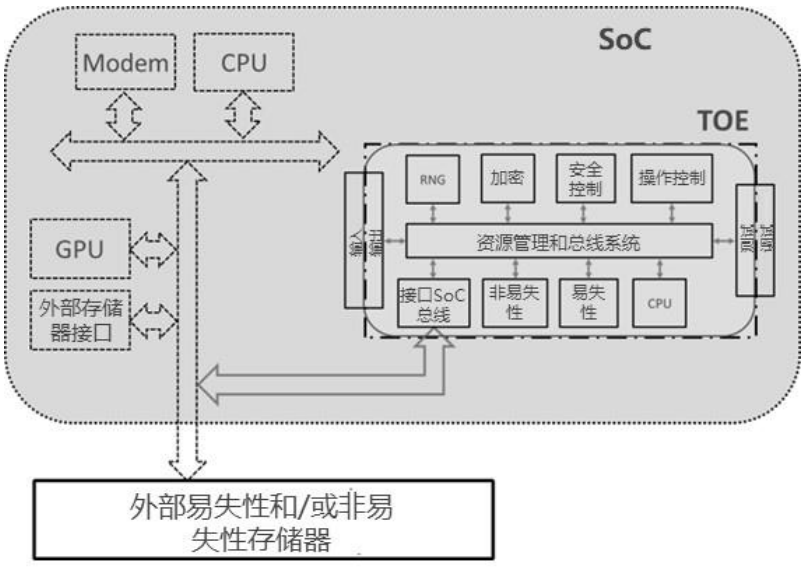


图 3-1 3S in SoC PP 定义的子系统框架

- **Dedicated Security Component -DSC**

2020年9月发布的《collaborative Protection Profile for Dedicated Security Component》由多家制造商、检测机构和CC发证机构主导编写，如苹果、Atsec和美国National Information Assurance Partnership等，里边提出了Dedicated Security Component，DSC，专用安全组件，定义描述如下：

专用安全组件是硬件组件和它控制的固件组成，为平台提供用于调配、保护和使用安全数据对象（security data object，SDO）的服务，其中包括密钥、身份、属性和其他类型的安全数据元素（security data element，SDE）。文中还提及，某些厂商已经集成该专用硬件组件到SoC中进行使用。

- **NIST标准中的HSM定义**

在NIST标准《NISTIR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases》、《NIST Special Publication 800-57 Part 2 Recommendation for Key Management》中涉及HSM定义描述，如下：

HSM进行密钥的保护和管理，且提供密码学运算包括加解密，签名验签等运算，很多具体实现中会为密码算法提供硬件加速机制。

- **学术专著中的SoC密码模块定义**

《The Cyber Security Body Of Knowledge,CyBOK》[15]，2019年10月发布，是网络安全的百科全书。

CyBOK的硬件安全领域知识体系是由硬件安全领域顶级学者，鲁汶大学Ingrid Verbauwhede撰写。这一部分对HSM的定义描述如下：

HSM通常会提供密码运算，安全密钥管理，包括密钥的安全生成、存储和删除，以及真随机数发生器等功能。HSM通常包括微处理器/微控制器、一组加密协处理器、安全易失性和非易失性存储器、TRNG、实时时钟和I/O。

最近在一些应用领域，如智能车领域，HSM功能不再作为独立模块提供，而是作为安全协处理器集成在较大的片上系统（SoC）中。

- **Security Hardware Extension – SHE**

AUTOSAR（汽车开放系统架构）联盟成立于 2003 年，该联盟致力于为汽车电子控制装置开发一个开放的、标准化的架构。AUTOSAR发布了SHE（Security Hardware Extension）规范，针对硬件模块的规范。汽车网络安全的实现不仅需要软件支持，还需要硬件的支持，所以奥迪和宝马合作制定了这个硬件密码模块规范，主要包括密码模块的硬件、硬件软件接口。这个规范已被广泛接受，很多针对汽车行业的微处理器都支持这个规范。SHE最早提出与2009年，最新版本于2020年11月发布，《Specification of Secure Hardware Extensions》。安全硬件扩展SHE规范中的定义描述为：

SHE可集成到任意微控制器中，SHE的主要作用是由硬件来控制保护密码学密钥，免受软件层面的攻击。总结来说，SHE是具备密码学功能，以及密钥管理，密钥存储等安全功能的安全子系统。示意图如下：

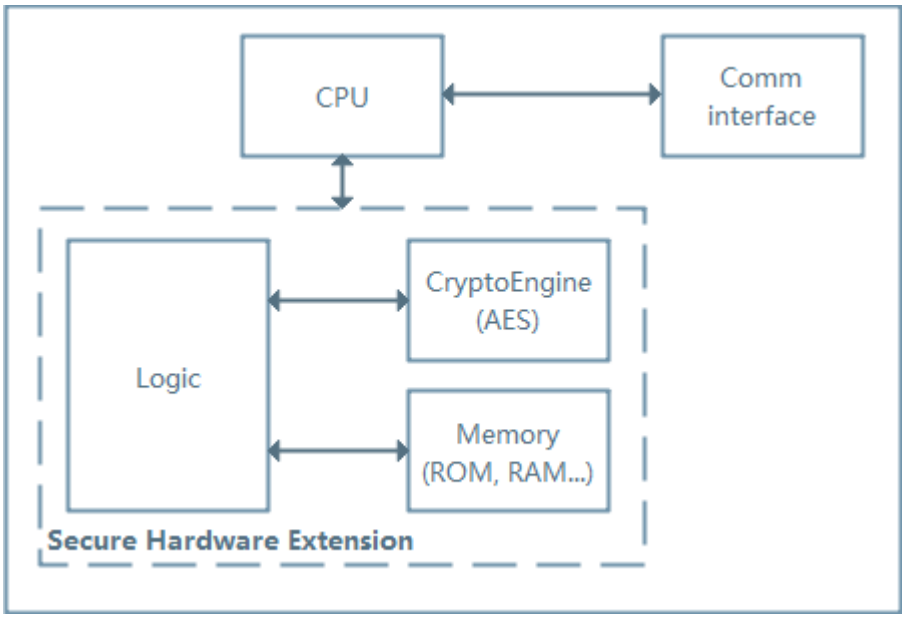


图 3-2 SHE 在控制器的位置及逻辑框架

- **Hardware Security Module - HSM**

EVITA，是欧盟组织的项目（https://evita-project.org/objectives.html），（2008年至2011年）。目标是设计、验证和原型汽车车载网络的体系结构，在这种体系结构中，安全相关组件受到保护，防止篡改，敏感数据在车辆内部传输时受到保护，防止泄漏。在EVITA项目，基于SHE规范提出了HSM硬件规范，该规范到目前为止也被广泛接受，很多针对汽车行业的微处理器都支持这个规范。其中对硬件安全模块HSM的定义描述如下：

HSM集成于车载SoC芯片，它的功能是安全并高效的实现密码运算以及确保自身安全的实施，例如随机数生成，敏感数据的安全存储，与应用CPU之间的安全访问控制机制等。总结来说，HSM是具备密码学功能，以及安全存储，随机数生成，访问控制机制等安全功能的安全子系统。示意图如下

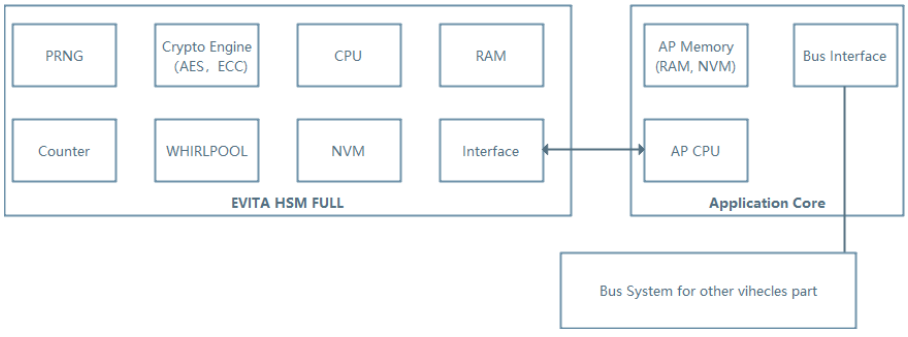


图 3-3 EVITA 定义的 HSM Full 框架

- **V2X HSM**

2019年9月，发布了车载V2X通信中使用的HSM的保护轮廓要求，《Protection Profile V2X Hardware Security Module》。在该保护轮廓中的定义描述如下：

V2X HSM可集成于VCS（VCS，车内通信相关的设备），HSM的作用是为VCS提供高安全的密码学运算，密钥管理服务等。

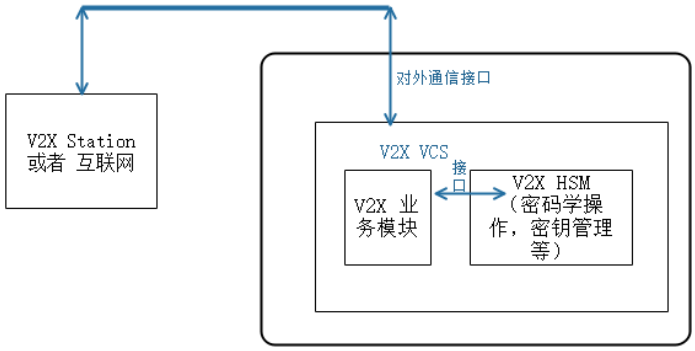


图 3-4 V2X HSM 逻辑边界

将上述对SoC密码模块的定义汇总到表格中。

表 3-1 SoC 密码模块的定义汇总

| 名称 | 定义描述 |
|---|---|
| Eurosmart 安全子系统<br>Secure Subsystem in SoC | 是SoC中的一个功能模块，由处理单元、安全组件、I/O端口和存储器组成，提供一系列安全功能（密码学运算，密钥管理，随机数等）以满足既定的安全目标。安全子系统基于物理或逻辑隔离机制，提供与其余SoC组件隔离的安全功能和安全服务。 |
| 专用安全组件保护轮廓<br>Dedicated Security Component, DSC | 是硬件组件和它控制的固件组成，为平台提供用于调配、保护和使用安全数据对象（security data object，SDO）的服务，其中包括密钥、身份、属性和其他类型的安全数据元素（security data element，SDE），可集成该专用硬件组件到SoC中进行使用。 |
| NIST标准中定义的硬件安全模块HSM | 进行密钥的保护和管理，且提供密码学运算包括加解密，签名验签等运算，很多具体实现中会为密码算法提供硬件加速机制。 |
| 学术专著CyBOK定义的硬件安全模块HSM | 通常会提供密码运算，安全密钥管理，包括密钥的安全生成、存储和删除，以及真随机数发生器等功能，可作为安全协处理器集成在较大的片上系统（SoC）中。 |
| AUTOSAR安全硬件扩展<br>Security Hardware Extension, SHE | 由硬件来控制保护密码学密钥，免受软件层面的攻击，具备密码学功能，以及密钥管理，密钥存储等安全功能，可集成到任意微控制器中。 |
| EVITA硬件安全模块<br>Hardware Security Module, HSM | 功能是安全并高效的实现密码运算以及确保自身安全的实施，例如随机数生成，敏感数据的安全存储，与应用CPU之间的安全访问控制机制等，集成于车载芯片SoC。 |
| 车载PP V2X HSM | 为VCS提供高安全的密码学运算，密钥管理服务等，可集成于VCS（VCS，车内通信相关的设备） |

综合上述的梳理和汇总，提炼SoC密码模块的定义，是具备密码学运算，密钥管理，真随机数发生器等安全功能的硬件、软件/固件的集合，可集成于SoC。

从上述定义看，其符合GB/T 37092《信息安全技术 密码模块安全技术要求》密码模块的定义。本研究报告借用CC的资产识别、威胁分析推导测评要求的方法学，进行边界、资产识别、安全功能测评等方面的研究，最后形成与国内密码标准体系兼容的标准建议。

### 3.1.2 边界和组成

SoC密码模块主要集成在车载领域SoC或MCU中，为T-Box、自动驾驶、车载网关、ECU等场景，提供密钥管理、密码服务、安全启动、安全升级、安全存储等能力。

GB/T 37092提到密码模块的密码边界是指明确定义的边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件、和/或固件部件。

车载SoC密码模块位于SoC内部，而存储其固件的非易失性存储器(NVM)有三种常见的部署形态。针对这些部署形态，其物理边界有差异，物理边界一般是指物理实体组成的边线；针对不同的部署形态，其逻辑边界是一致的，逻辑边界一般是指逻辑组成的边线。

依据NVM的位置，SoC密码模块一般划分成以下三类，如下图。

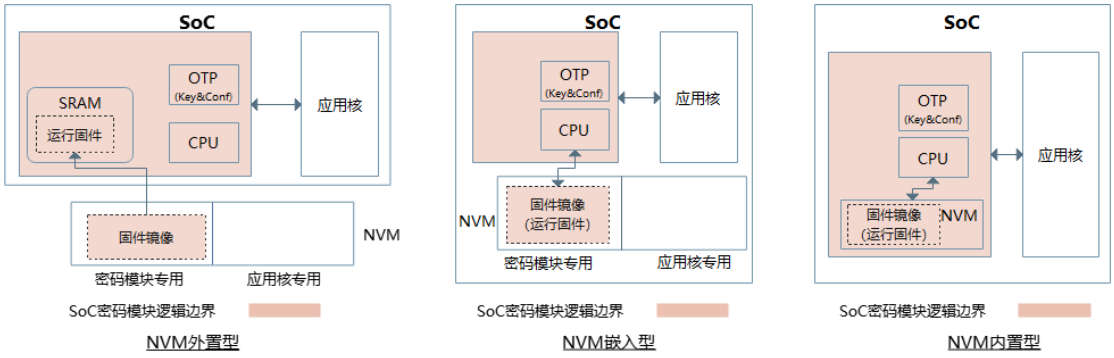


图3-5 车载SoC密码模块三种类型划分

- NVM位于SoC外（NVM外置型）
- NVM位于SoC内，SoC密码模块外（NVM嵌入型）
- NVM位于SoC密码模块内（NVM内置型）

依据GB/T 37092的模块类别划分，可将NVM内置型映射到硬件密码模块，另外两种映射到混合固件模块。

在本节，对这三类SoC密码模块进行物理和逻辑边界分析、特点介绍，同时通过逻辑视图，说明车载SoC密码模块可以提供的功能，及与SoC内CPU的交互，并体现出SoC密码模块涉及的密钥/SSP的存储与使用的要求及参考设计。

#### 3.1.2.1 车载 SoC 密码模块（NVM 外置型）

因为NVM放置在SoC外部，既可根据应用需求选择不同容量的NVM，也可通过访问控制机制为SoC密码模块和SoC其它部分隔离不同的容量，为SoC密码模块的设计提供了灵活性。

车载SoC密码模块的固件镜像以及部分密钥、SSP加密存储在外置NVM上，并进行了签名。在SoC上电时，SoC密码模块进行硬件初始化后，从外置NVM读

取固件镜像，加载到SoC密码模块并进行解密、校验，验证通过后在SoC密码模块内的SRAM运行。

从逻辑边界考虑，车载SoC密码模块包含位于SoC内的硬件部分、存储于SoC外置NVM的固件镜像、密钥及SSP。

物理边界的划分有两种可能，一种是仅包含SoC，如图3-6；另一种是包含SoC和外置NVM，如图3-7。

第一种划分：密码模块关于物理安全的要求可不适用于外置NVM，且SoC密码模块不与特定存储器绑定，可在量产时依据需求选择不同厂商、不同容量的存储器件。不过，因为SoC密码模块的固件镜像以及部分密钥、SSP存储在外置NVM，SoC应在固件镜像导入和密钥&SSP的导入/导出时提供机密性和完整性的保护措施。

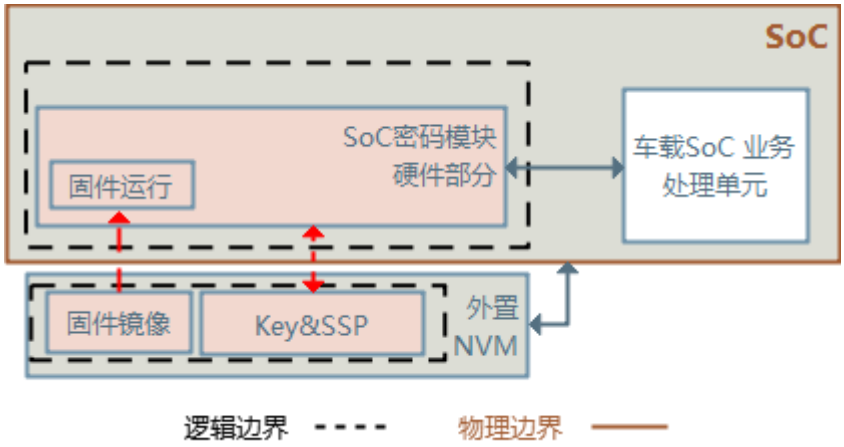


图3-6 SoC密码模块（NVM外置型）逻辑边界和物理边界（不含NVM）

第二种划分：如果物理边界包含SoC和外置NVM，密码模块关于物理安全的要求也适用于外置NVM，如要提供显式的拆卸证明。此时，SoC密码模块在量产时应使用声明的存储器件，可在认证后依据需求选择不同厂商、不同容量的存储器件。

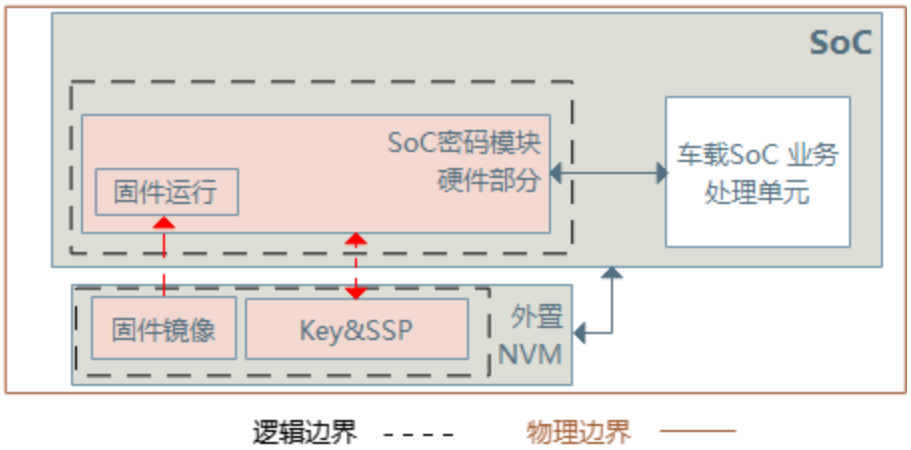


图3-7 SoC密码模块（NVM外置型）逻辑边界和物理边界（含NVM）

#### 3.1.2.2 车载 SoC 密码模块（NVM 嵌入型）

车载SoC密码模块（NVM嵌入型）与SoC其它业务单元共用NVM，可根据应用需求为SoC密码模块、SoC其它业务单元进行存储容量的配置，通过访问控制机制管理对NVM的读写。

车载SoC密码模块的固件镜像以及部分密钥、SSP存储在SoC内的NVM，并进行了签名。在SoC上电时，SoC密码模块进行硬件初始化后，对SoC内NVM上的SoC密码模块固件进行签名验证，通过后由SoC密码模块的CPU调用执行。

车载SoC密码模块的逻辑边界和物理边界可以这样划分，如下图。

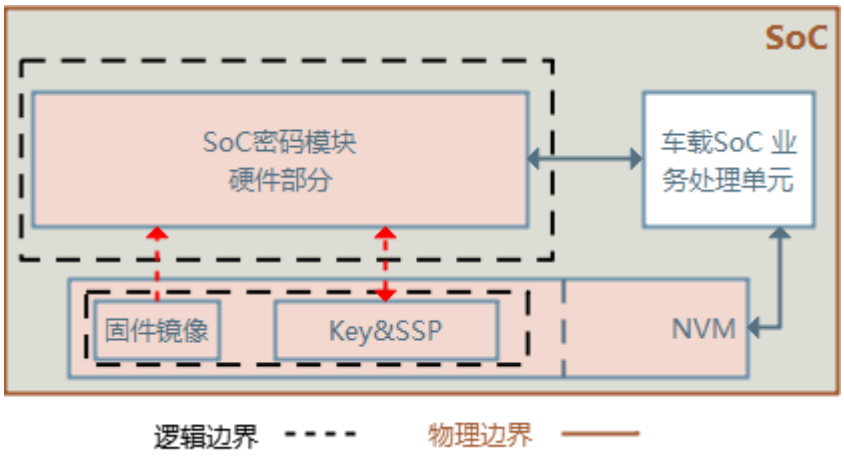


图3-8 SoC密码模块（NVM嵌入型）逻辑边界和物理边界

逻辑边界：包含位于SoC内的硬件部分、存储于SoC内NVM的固件镜像、密钥及SSP。由于NVM是整个SoC共用的，需要确保对NVM访问的控制机制设计保护SoC密码模块的固件镜像、密钥和SSP不会被非法读取、篡改。

物理边界：SoC的实体边界。由于车载SoC密码模块位于SoC内，SoC的顶层金属和外部封装同样也要覆盖SoC密码模块。

#### 3.1.2.3 车载 SoC 密码模块（NVM 内置型）

车载SoC密码模块（NVM内置型）拥有独立的NVM。

车载SoC密码模块的固件镜像以及部分密钥、SSP存储在SoC密码模块内NVM，可能会采用签名等安全措施进行保护。在SoC上电时，SoC密码模块进行硬件初始化后，从SoC密码模块内NVM读取固件镜像并交由SoC密码模块的CPU调用运行，如果镜像有签名，则会在上电时验证固件镜像，通过后再运行。

从逻辑边界考虑，车载SoC密码模块包含位于SoC内的硬件部分、存储于SoC密码模块内NVM的固件镜像、密钥及SSP。

物理边界则包含整个SoC的实体边界，如下图。由于车载SoC密码模块位于SoC内，SoC的顶层金属和外部封装同样也要覆盖SoC密码模块。

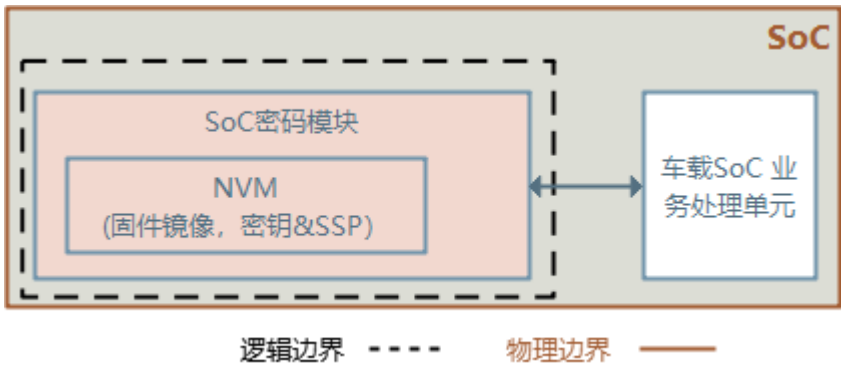


图3-10 SoC密码模块（NVM内置型）逻辑边界和物理边界

#### 3.1.2.4 三种 SoC 密码模块类型的主要差异汇总

综上所述，依据NVM的部署情况，SoC密码模块有三种类型。以下将三种类型的差异汇总在一起，见下表。

表 3-2 SoC 密码模块三种类型的差异

| SoC密码模块类型 | NVM内置型 | NVM嵌入型 | NVM外置型 | |
|---|---|---|---|---|
| 逻辑边界 | 位于SoC内的硬件部分、存储于NVM的固件镜像、密钥及SSP | | | |
| 物理边界 | SoC | SoC | SoC | SoC+NVM |
| 密码模块类型 | 硬件密码模块 | 硬件密码模块 | 硬件密码模块 | **混合**密码模块 |
| 物理安全实体类型 | 单芯片 | 单芯片 | 单芯片 | **多芯片嵌入式** |
| 存储器特点 | NVM：<br>1、位于SoC内<br>2、存储独享<br>3、容量固定 | NVM：<br>1、位于SoC内<br>2、SoC内共享存储<br>3、容量固定/可配（在生产/装备/启动阶段配置）<br>4、NVM控制器具备访问权限控制机制 | NVM：<br>1、位于SoC外<br>2、SoC内共享存储<br>3、容量可配<br>4、依据场景提供交付后存储器件更换的能力 | NVM：<br>1、位于SoC外<br>2、SoC内共享存储<br>3、容量可配<br>4、如器件更换，须重新认证<br>5、满足密码模块的物理安全要求 |
| 存储在NVM的数据/代码保护策略 | 完整性 | 完整性 | 完整性<br>机密性<br>防回滚<br>（防止攻击者对外部存储进行恶意窃取与篡改） | 完整性<br>机密性<br>防回滚<br>（防止攻击者对外部存储进行恶意窃取与篡改） |

#### 3.1.2.5 车载 SoC 密码模块的组成

基于前三小节的描述可看出，3种类型的车载SoC密码模块，其逻辑边界都是一致的，即包含SoC密码模块硬件部分，存储于NVM的固件镜像、部分密钥及SSP。

对车载SoC密码模块的层次关系和对外交互进行分析时，可以梳理出它的逻辑视图，如下。

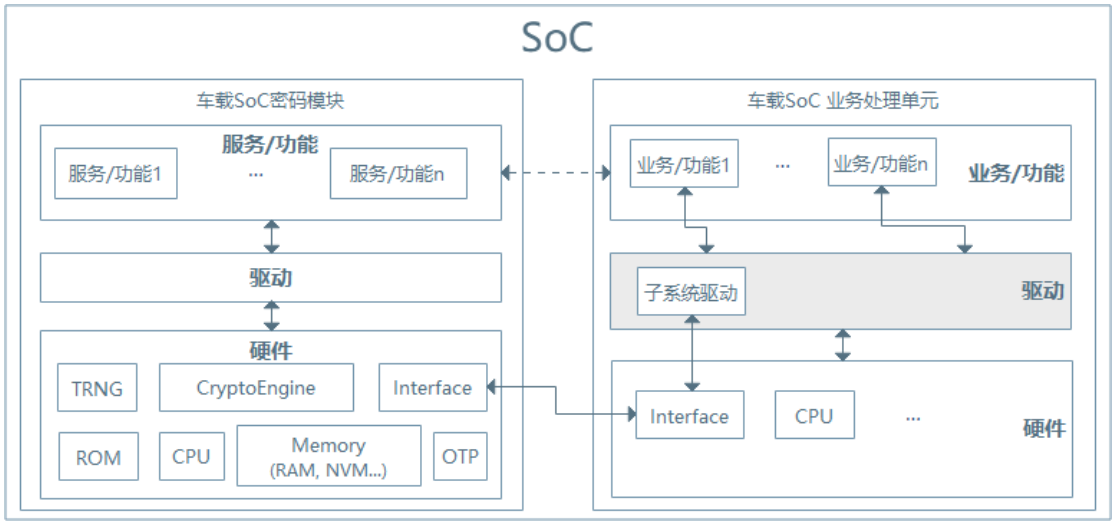


图3-11 车载SoC密码模块逻辑视图

从上图可以看出，车载SoC密码模块的组成包含：

**硬件**：处理器，密码学运算引擎，真随机数发生器，易失性存储SRAM，非易失性存储ROM、OTP、Flash，与车载SoC业务处理单元交互的通信接口模块等

**驱动**：将硬件提供的能力封装成可被车载SoC密码模块运行环境调用的驱动，如密码算法、存储器读写、随机数生成等

**服务/功能**：在运行阶段，可向车载SoC提供的服务或功能，如密码学服务（加/解密、签名/验证）、安全升级、安全存储、安全时间等

**物理端口/逻辑接口**：SoC密码模块至少拥有一个物理端口，如Mailbox，可与SoC业务处理单元通信;在SoC密码模块的运行环境，会有多种逻辑接口，向SoC业务处理单元输出服务/能力。这些通信接口需要具备访问控制机制，防止非法读写，保证数据安全。

同时，车载SoC密码模块一般需要使用到的代码、敏感安全参数SSP，经过分析这些内容的存储位置、功能，推导出其应具备的安全要求，并提供了一些参考的保护措施，如下表。

表3-3 车载SoC密码模块涉及的代码、SSP

| 名称 | 存储在 | 功能 | 安全要求 | 保护措施 |
|---|---|---|---|---|
| 运行态固件 | SRAM | 运行在 SoC 密码模块，向 SoC 提供车载相关的安全服务 | 完整性 | 访问控制 |
| 固件镜像 | NVM | 存储在 NVM，在 SoC 密码模块运行时加载的文件 | 真实性<br>完整性 | 数字签名、加密（增强） |

| | | | | |
|---|---|---|---|---|
| 固件镜像验证根公钥 | eFuse | 用于安全启动/安全升级过程中固件导入时进行签名验证 | 真实性<br>完整性 | 不可篡改，eFuse 特性 |
| 加密用的根密钥 | | 用于 SoC 密码模块持久化数据安全存储 | 真实性<br>完整性<br>机密性 | 访问控制、加扰，不可篡改（eFuse 特性） |
| 资产导入的根密钥 | | 用于导入 SoC 密码模块过程的资产保护 | | |
| 镜像加解密的根密钥 | | 用于对镜像加解密 | | |
| UID | | UID 可以作为 ECC 的私钥 | | |
| 密钥传输的加密密钥 | SRAM | 用于在业务 CPU 和安全 SoC 密码模块之间进行密钥的传输保护 | 真实性<br>完整性<br>机密性 | 访问控制<br>加扰<br>下电擦除 |
| 车载 SoC/ECU 的主密钥 | NVM/<br>SRAM | 更新业务密钥、调试鉴权等 | 真实性<br>完整性<br>机密性 | （NVM）加密和完整性保护 |
| 车载 SoC/ECU 的业务密钥 | NVM/<br>SRAM | 提供对业务数据的解密 | 真实性<br>完整性<br>机密性 | （NVM）加密和完整性保护 |
| 安全时间 | SRAM | 为 HSM 内部业务提供时间戳，如密钥有效期 | 真实性<br>完整性 | 访问控制<br>下电擦除 |
| 安全计数器 | NVM | 单向计数器用于向 SoC/ECU 提供服务 | 真实性<br>完整性 | 访问控制 |

### 3.1.3 车载 SoC 密码模块的功能

考虑到车载领域的应用场景要求，车载SoC密码模块在常见SoC密码模块的功能外，还具备特别的应用特性。

#### 3.1.3.1 通用功能

**密码学运算**

提供常见的密码学运算服务，包含非对称算法SM2，哈希算法SM3，对称算法SM4。基于密码运算操作来构建相关的安全功能，例如基于公钥验签运算构建安全启动功能，基于对称加密运算构建安全存储功能等等。

**密钥管理**

SoC密码模块可以安全地处理和保护各类密钥信息，其中根密钥信息存储于SoC密码模块内的OTP组件，其他密钥可通过多种途径生成。

1、SoC密码模块内直接基于真随机数进行密钥生成，生成的密钥由加密存储保护。

2、密钥派生，基于根密钥信息来派生得到临时使用的密钥，在SoC密码模块中可能涉及多层级的密钥派生。

3、密钥导入、导出，作为本地密钥生成的一种补充方案，SoC密码模块允许导入和导出加密密钥等。在密钥导入、导出过程中，密钥仅允许以受保护的方式导入导出，确保密钥的机密性和完整性。

**随机数生成**

子系统内有真随机数发生器，提供随机数生成功能，用于密钥生成，密码算法对随机数的需求等等。

**安全存储**

车载SoC密码模块对静态数据存储时，为了防止攻击者对存储在flash的数据的机密性和完整性进行破坏，需要对静态存储在flash中的数据进行加密处理，确保存储于flash中的敏感数据的机密性和完整性得以保护。

#### 3.1.3.2 车载特有功能

**唯一身份标识**

车载SoC密码模块提供唯一身份，可基于唯一身份对SoC密码模块进行身份认证等功能，确保子系统的合法身份。

**安全启动**

安全启动提供必要的安全特性，来保证车载SoC要加载的固件或者软件的机密性、真实性和完整性，确保车载SoC运行前的固件安全。

**回滚保护**

车载SoC密码模块的回滚保护可防止攻击者利用旧版本（有合法签名，但存在代码漏洞）替换新版本以实施攻击，需要考虑此类攻击的保护。

**固件韧性**

车载SoC密码模块内固件是受密码学保护的，涉及车载领域的高可靠性，需要构建固件韧性的能力，如主从备份，防止单个固件失效后可能导致系统的崩溃。

**安全升级**

保障车载SoC安全升级包的机密性、完整性和真实性。提供安全升级功能，需要升级的固件或软件，在升级到SoC的存储介质之前，做真实性和完整性校验，在安全校验完成后，密文的固件或软件才能被烧写到SoC的存储介质。

**安全时间**

车载SoC密码模块提供安全时间的能力，用于生成签名的时间戳、密钥生命周期的时间管理。下电后安全时间会清零，上电后会从外部加载同步可信时间源。

**安全存储（对外）**

对业务处理单元提供安全存储能力，用于保护数据防回滚，只能单向递增。

**生命周期标识管理**

车载领域ECU各阶段都有独特的生命周期标识，如制造、集成、在线运行等。这些标识会在SoC密码模块进行管理，并由子系统提供保护。

**单向计数器**

车载SoC有些服务会向车载SoC密码模块申请一个计数值，保护服务的需求方数据防回滚；此计数值的刷新需要进行鉴权。

## 3.2 SoC 密码模块技术安全需求

“资产”在网络安全威胁分析中表示需要保护的内容。站在攻击者的角度，资产有助于帮助其实施下一步攻击以破坏目标系统或者获得进一步的经济利益。

SoC密码模块中具备大量对恶意攻击者具备吸引力的内容。这些内容具有多种表现形式，从密钥、证书、侧信道信息，到系统提供的服务、数据的访问权限等。

本节借鉴CC对2.2.1节提到的多个SoC密码模块保护轮廓（Protection Profile）的定义方法。通过识别SoC密码模块中的关键数据资产及其面临的威胁，从中分析和制定SoC密码模块应具备的安全目标。这些安全目标用于消除或降低所识别到的安全威胁。依据这些安全目标，我们从中推导出SoC密码模块的安全需求。

本章节中涉及到的资产、威胁、安全目标、安全需求具体编号中的英文缩写，其具体含义可参考附录中的缩略语表。

### 3.2.1 资产识别和威胁分析

为保障 SoC 密码模块的功能要求，系统中需要对其运行的固件进行安全加载，对其中产生、存放、传递、使用的敏感数据进行保护。针对这些关键数据资产，我们从三方面定义其安全防护要求：机密性（防窃取等），完整性（防篡改等），真实性（防伪造等）。

下表中列出了 SoC 密码模块中可能涉及的关键资产表。

表 3-4 SoC 密码模块涉及的资产

| 资产列表 | | | | | |
|---|---|---|---|---|---|
| 代号 | 名称 | 描述 | 安全要求 | | |
| | | | 机密性 | 完整性 | 真实性 |
| AS.PublicKey | 公开密钥 | 系统执行密钥运算所需的公钥、公钥证书等可公开的密钥 | | √ | √ |
| AS.SecretKey | 机密密钥 | 系统执行密钥运算所需的对称密钥、签名私钥等非公开的密钥 | √ | √ | √ |
| AS.Firmware | 固件 | 系统启动引导程序及加载运行的功能固件 | | √ | |
| AS.ConfPara | 关键配置参数 | 系统运行所需的关键配置参数 | | √ | √ |
| AS.ID | 系统唯一硬件身份 ID | 用于表示模块唯一身份，生成设备绑定的密钥等功能 | | √ | √ |
| AS.TRNG | 真随机数生成器 | 用于产生密码运算功能所需的安全随机数 | √ | | √ |
| AS.UserData | 用户数据 | 存储在 SoC 密码模块中的用户数据 | √ | √ | √ |
| AS.Service | 功能服务 | SoC 密码模块向外部提供的功能服务，如加解密、安全存储、单向计数器等 | 正确可用 | | |

安全威胁指 SoC 密码模块中资产所面临的被攻击风险，根据攻击者接入位置的不同，将可能的攻击者划分为两类。

表 3-5 SoC 密码模块涉及的攻击者类型

| 类型 | 描述 |
|---|---|

| | |
|---|---|
| 近端攻击者 | 攻击者能够近端物理接触SoC密码模块，尝试物理手段提取、监听或篡改系统中的资产及对应处理过程。 |
| 远程攻击者 | 攻击者通过SoC芯片应用侧软件漏洞获取整个系统的远程控制权限，能够通过恶意传参、功能调用来实施对SoC密码模块的攻击。 |

通常情况下，攻击者首先可以通过近端攻击的方式获得 SoC 密码模块的相关实现信息和可能脆弱点，之后尝试远程利用近端获得的信息对 SoC 密码模块展开攻击。近端攻击每次通常只能影响一个设备，远程攻击可简单地将特定攻击方式向多个设备进行实施。

下表列出 SoC 密码模块中的数据资产可能涉及的威胁列表。

表 3-6 SoC 密码模块涉及的威胁

| 名称<br>T.Name | 威胁描述 |
|---|---|
| 数据泄漏<br>T.DataLeakage | 攻击者尝试通过调试接口、恶意调用功能接口、或存储器物理接口，获取存储在系统中的敏感数据 |
| 数据篡改<br>T.DataForge | 攻击者尝试通过篡改SoC密码模块的启动镜像、关键配置、存储敏感信息等数据，导致系统执行异常，进而获取系统中的敏感数据 |
| 侧信道泄漏<br>T.SideChannel | 攻击者尝试通过密码算法运行过程中的侧信道信息来获取密码算法模块的敏感信息。 |
| 故障注入<br>T.FaultInjection | 攻击者尝试通过故障注入手段来影响SoC密码模块功能的正常运行，从而绕过限制访问敏感数据，或者破解密码运算过程中的敏感信息等。 |
| 随机数缺陷<br>T.BadRNG | 攻击者尝试使用或者诱发随机数产生器的弱随机性（低熵），从而预测随机数产生器的产生的信息。 |
| 回滚攻击<br>T.Rollback | 攻击者通过对固件、安全配置等关键代码和数据进行版本回退，以利用旧版本中安全漏洞。 |
| 身份伪造<br>T.Impersonation | 攻击者通过伪造身份绕过SoC密码模块对特定角色的访问控制机制，进而获取特定角色权限之外的功能或数据访问权限。 |
| 功能滥用<br>T.AbuseFunctionality | 攻击者通过错误流程、错误参数等方式恶意调用SoC密码模块的功能接口，尝试篡改系统工作状态或安全配置，获取敏感数据，或导致系统崩溃无法工作等 |
| 内存破坏<br>T.MemCorruption | 攻击者通过构造恶意输入，导致SoC密码模块运行堆栈中内存数据被破坏，进而劫持系统执行流程，读取或篡改系统中敏感数据 |
| 设备克隆<br>T.Clone | 攻击者通过将A设备中加密保护的敏感数据资产克隆到已经成功攻击的B设备中，通过对B设备的攻击获取A中的明文敏感数据资产 |
| 拒绝服务<br>T.DOS | 攻击者通过网络对SoC密码模块所在的系统进行拒绝服务攻击，导致服务不可用 |

资产和威胁的对应关系见下表。

表 3-7 SoC 密码模块涉及的资产和威胁对应关系

| | T.DataLeakage | T.DataForge | T.SideChannel | T.FaultInjection | T.BadRNG | T.Rollback | T.Impersonation | T.AbuseFunctionality | T.MemCorruption | T.Clone | T.DOS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| AS.PublicKey | | X | | X | | | | | | | |
| AS.SecretKey | X | X | X | X | X | | | X | | X | |
| AS.Firmware | | X | | X | | X | | | X | X | X |
| AS.ConfPara | | X | | | | X | X | | X | | |
| AS.ID | | X | | | | X | | | | X | |
| AS.TRNG | | X | | | X | | | | | X | |
| AS.UserData | X | X | X | X | X | X | X | X | | X | |
| AS.Service | | | X | X | X | X | X | X | X | | X |

### 3.2.2 安全目标和安全需求推导

根据上一节中SoC密码模块中的资产定义和威胁，可以定义SoC密码模块的安全目标，如下表所示。

表 3-8 SoC 密码模块安全目标

| 目标名称 O.Name | 描述 |
|---|---|
| O.Confidentiality | SoC密码模块需保护敏感数据资产不被泄漏 |
| O.Integrity | SoC密码模块需保护敏感数据资产不被恶意篡改 |
| O.Authentication | SoC密码模块需支持对管理员的认证，以及对交互的外部实体进行身份认证 |
| O.State | SoC密码模块在设计预期的状态下运行 |
| O.AccessControl | SoC密码模块需支持对外部交互实体的访问控制 |
| O.KeyManagement | SoC密码模块对系统中的密钥，应具备安全产生/导入、派生、传递、使用、销毁等密钥全生命周期的管理功能 |
| O.CryptoFunction | SoC密码模块应具备正确完成相应密码学运算的能力 |
| O.RandomNumber | SoC密码模块应具备正确产生安全随机数的能力 |
| O.Functionality | SoC密码模块应确保在不同环境条件下的正确使用及不泄漏敏感数据资产，包括外部恶意的输入、恶意调 |

| | |
|---|---|
| | 用顺序、环境因素如温度、电压、辐射改变等。<br>SoC密码模块需具备在异常条件下维持核心功能可用的能力 |
| O.SecureIO | SoC密码模块应支持部分关键数据资产的安全导入导出功能 |
| O.AntiSCA | SoC密码模块需具备侧信道防护能力 |
| O.AntiFI | SoC密码模块需具备故障注入防护能力 |
| O.UID | SoC密码模块需具备防篡改能力的唯一身份ID |
| O.SelfTest | SoC密码模块需具备自检能力，以防护功能被篡改 |

以上安全目标覆盖了前文中识别到的安全威胁，具体对应关系见下表。

表 3-9 SoC 密码模块的威胁与安全目标对应关系

| | T.DataLeakage | T.DataForge | T.SideChannel | T.FaultInjection | T.BadRNG | T.Rollback | T.Impersonation | T.AbuseFunctionality | T.MemCorruption | T.Clone | T.DOS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| O.Confidentiality | X | | X | | | | | | | X | |
| O.Integrity | | X | | | | X | | | | | |
| O.Authentication | | X | | | | | X | | | X | |
| O.State | X | X | | | | X | | | | X | |
| O.AccessControl | X | | | | | | X | | | | |
| O.KeyManagement | X | X | | | | | | | | | |
| O.CryptoFunction | X | X | | | X | | | | | | |
| O.RandomNumber | | | | | X | | | | | | |
| O.Functionality | | | | | | | | X | X | | X |
| O.SecureIO | X | | | | | | | X | | | |
| O.AntiSCA | X | | X | | | | | | | | |
| O.AntiFI | X | X | | X | | | | | | | |
| O.UID | | | | | | | | | | X | |
| O.SelfTest | | | | | X | | | X | | | |

根据以上安全目标，分解SoC密码模块的安全需求如下。

表 3-10 SoC 密码模块的安全需求

| 缩写 | 描述 |
|---|---|

| | |
|---|---|
| Class FCS: Cryptographic Support | |
| FCS_CKM.1/PK | 密钥生成/公钥算法中公私钥对 |
| FCS_CKM.1/KEK | 密钥生成/生成密钥保护密钥 |
| FCS_CKM.1/KDF | 密钥生成/KDF算法派生得到临时密钥 |
| FCS_CKM.2 | 支持密钥交换 |
| FCS_CKM.4 | 支撑密码销毁 |
| FCS_COP.1/Hash | 密码学操作/哈希 |
| FCS_COP.1/HMAC | 密码学操作/消息认证 |
| FCS_COP.1/KAT | 密码学操作/密钥协商及传输 |
| FCS_COP.1/KeyEnc | 密码学操作/密钥加密保护 |
| FCS_COP.1/SKC | 密码学操作/对称密钥加解密 |
| FCS_COP.1/SignGen | 密码学操作/签名 |
| FCS_COP.1/SignVer | 密码学操作/验签 |
| FCS_RNG | 基于真随机数的随机数产生 |
| Class FDP: User Data Proteciton | |
| FDP_ACC.2 | 完整的访问控制机制 |
| FDP_SDC.1 | 存储数据机密性保护 |
| FDP_SDI.2 | 存储数据的完整性保护 |
| FDP_UCT.1 | 传输数据的机密性保护 |
| FDP_UIT.1 | 传输数据的完整性保护 |
| FDP_RDE.1 | 运行态数据的硬件隔离（如SoC密码模块与外部的隔离） |
| FDP_RDC.1 | 运行态数据机密性保护 |
| FDP_RDI.1 | 运行态数据完整性保护 |
| FDP_RIP.2 | 硬件支持残余数据保护 |

| | |
|---|---|
| FDP_ROL.1 | 安全存储的回滚保护 |
| Class FIA: Identification and Authentication | |
| FIA_UAU.2 | 用户执行操作前先进行认证 |
| FIA_UAU.5 | 多种不同的鉴权认证方法 |
| Class FMT: Security Management | |
| FMT_MSA.1 | 安全属性管理 |
| FMT_SMR.2 | 安全角色维护及权限设置 |
| FMT_LIM.1 | 安全功能权限最小化 |
| FMT_LIM.2 | 安全功能可用性约束 |
| Class FPT: Protection of the TSF | |
| FPT_SCP.1 | 防侧信道攻击 |
| FPT_PHP.3/FAL | 抵抗故障注入攻击 |
| FPT_PRO_EXT.1 | 信任根 |
| FPT_ROT_EXT.2 | 安全存储根 |
| FPT_RPL_EXT.1 | 防重放攻击 |
| FPT_TST.1 | 安全功能可测 |
| FPT_STM.1 | 可靠时间戳 |
| FPT_UID.1 | 不可篡改唯一身份ID |
| FPT_LCS.1 | 生命周期标识 |
| FPT_INT.1 | 安全启动/可信启动 |
| FPT_Update | 安全升级（包含镜像真实性和镜像版本的校验，防止非法或旧版本的镜像加载） |
| Class FRU: Resource Utilization | |
| FRU_FLT.2 | 有限的故障容忍（如固件韧性，关键固件备份） |

安全需求和安全目标的对照关系见下表。

表 3-11 安全需求和安全目标的对应关系

| 安全目标与安全需求对应关系 | |
|---|---|
| 目标名称 O.Name | 对应的安全需求 |
| O.Confidentiality | 通过基于密码学运算、密钥管理构建的数据加密保护体系实现机密性<br>FCS_CKM.1/PK：密钥生成公钥算法的公私钥对<br>FCS_CKM.1/KEK：密钥生成/生成密钥保护密钥<br>FCS_COP.1/KeyEnc：密码学操作/密钥加密保护<br>FCS_CKM.1/KDF：密钥生成/KDF算法派生得到临时密钥<br>FCS_CKM.2：支持密钥交换<br>FCS_CKM.4：支撑密码销毁<br>FCS_COP.1/SKC：密码学操作/对称密钥加解密<br>FPT_ROT_EXT.2: 安全存储根<br>FDP_SDC.1：存储数据机密性保护<br>FDP_UCT.1：传输数据的机密性保护<br>FDP_RIP.2：硬件支持残余数据保护 |
| O.Integrity | 通过基于密码学运算构建的认证和保护体系实现机密性<br>FCS_CKM.1/PK：密钥生成公钥算法的公私钥对<br>FCS_COP.1/Hash：密码学操作/哈希<br>FCS_COP.1/HMAC：密码学操作/消息认证<br>FCS_COP.1/SignGen：密码学操作/签名<br>FCS_COP.1/SignVer：密码学操作/验签<br>FDP_SDC.2：存储数据的完整性保护<br>FDP_UIT.1：传输数据的完整性保护<br>FDP_RDI.1：运行态数据完整性保护<br>FDP_ROL.1: 安全存储的回滚保护 |
| O.Authentication | FCS_CKM.2：支持密钥交换<br>FCS_COP.1/HMAC：密码学操作/消息认证<br>FIA_UAU.2: 用户执行操作前先进行认证<br>FIA_UAU.5: 多种不同的鉴权认证方法 |
| O.State | FPT_INT.1: 安全启动/可信启动<br>FPT_Update：安全升级<br>FPT_PRO_EXT.1: 信任根<br>FDP_ROL.1: 安全存储的回滚保护<br>FPT_STM.1: 可靠时间戳<br>FPT_LCS.1：生命周期标识 |

| | |
|---|---|
| O.AccessControl | FIA_UAU.2: 用户执行操作前先进行认证<br>FIA_UAU.5: 多种不同的鉴权认证方法<br>FMT_MSA.1: 安全属性管理<br>FMT_SMR.2: 安全角色维护及权限设置<br>FMT_LIM.1: 安全功能权限最小化<br>FMT_LIM.2: 安全功能可用性约束 |
| O.KeyManagement | FCS_CKM.1/KEK：密钥生成/生成密钥保护密钥<br>FCS_COP.1/KeyEnc：密码学操作/密钥加密保护<br>FCS_CKM.1/KDF：密钥生成/KDF算法派生得到临时密钥<br>FCS_CKM.2：支持密钥交换<br>FCS_CKM.4：支撑密码销毁<br>FCS_COP.1/SKC：密码学操作/对称密钥加解密 |
| O.CryptoFunction | Class FCS: 密码学功能支持 |
| O.RandomNumber | FCS_RNG: 基于真随机数的随机数产生<br>FPT_PHP.3/FAL: 抵抗故障注入攻击<br>FRU_FLT.2：有限的故障容忍 |
| O. Functionality | FDP_RDE.1：运行态数据的硬件隔离（如SoC密码模块与外部的隔离）<br>FPT_RPL_EXT.1: 防重放攻击<br>FPT_SCP.1: 防侧信道攻击<br>FPT_PHP.3/FAL: 抵抗故障注入攻击<br>FRU_FLT.2：有限的故障容忍 |
| O.SecureIO | FDP_UCT.1：传输数据的机密性保护 |
| O.AntiSCA | FPT_SCP.1: 防侧信道攻击 |
| O.AntiFI | FPT_PHP.3/FAL: 抵抗故障注入攻击<br>FRU_FLT.2：有限的故障容忍 |
| O.UID | FPT_UID.1：不可篡改唯一身份ID |
| O.SelfTest | FPT_TST.1: 安全功能可测 |

# 4. 车载 SoC 密码模块测评要求研究

## 4.1 SoC 密码模块的现有测评方法研究

国内外对 SoC 密码模块的认证测评规范以密码模块为主，如美国的 FIPS140 系列标准，欧洲 CC 认证体系。

### 4.1.1 FIPS 140 系列标准测评方法

美国联邦信息处理标准FIPS PUB 140系列标准，是NIST（美国国家标准和技术委员会）所发布的针对密码模块的安全要求。该系列标准每5年进行审计更新，其中FIPS140-1于1994年正式实施，FIPS140-2于2001年正式发布，FIPS140-3于2019年正式发布。FIPS认证是美国国家标准和技术委员会（NIST）和加拿大通讯安全局(CSEC)共同建立了加密模块验证体系的认证，CMVP(Cryptographic Module Validation Program) 验证密码模块对FIPS140-3及相关标准的符合程度。美国政府采购的密码模块必须要有FIPS140-3认证，加拿大政府推荐优先采购通过FIPS认证的产品。

FIPS140-3标准针对用于计算机和电信系统(包括语音系统)的敏感信息保护的密码模块，规定了安全性性依次递增的4个安全等级，分别为Level 1、Level 2、Level 3、Level 4。这些安全级别目标是涵盖加密模块可能使用的的各种潜在环境和场景，涉及的安全需求覆盖密码模块从设计到实现的诸多方面。四个安全等级如下：

- Level-1：对密码模块的基本安全要求（如至少包含1个符合NIST要求的密码算法或功能），无物理安全要求。该等级为使用密码模块的产品提供了最低安全要求。
- Level-2: 在level-1基础上增加了物理安全要求，要求模块具备防拆封条或涂覆，以防御未授权的物理拆解攻击。另外要求模块具备基于角色的授权功能，确保对合法角色提供相应服务。
- Level-3: 在level-2基础上,有以下要求的增强和新增。增强鉴别、物理安全、敏感安全参数等方面的要求，如要求模块具备非法访问敏感安全参数（SSP）时的检测能力，被物理拆解时主动清零模块内的关键安全参数（CSP），并要求模块具备基于身份的鉴权功能。新增可信信道/知识拆分，以传输未加密的CSP。同时新增对外部环境变化的保护要求，具备对温度、电压等外部环境的监测EFP或进行严格的环境失效测试EFT，以保证模块在异常环境下的运行安全。
- Level 4：该等级为最高安全等级，在物理安全方面要求密码模块具备完整的封装保护，可检测从任何方向的物理入侵企图，并在检测到封装破坏后清零所有的关键安全参数。当模块检测到运行环境中温度或外部电压发生波动时数清零CSP，或模块通过严格的环境失效测试以确保环境波动不会影响模块的安全性。

各安全等级对应的具体要求见下表。

表 4-1 FIPS 140-3 安全分析要求

| | **Level 1** | **Level 2** | **Level 3** | **Level 4** |
|---|---|---|---|---|
| **密码模块规格** | 密码模块规格、加密范围边界、经批准的算法、经批准的操作模式，密码模块的描述（包括所有硬件、软件和固件），模块安全策略描述 | | | |
| **密码模块端口和接口** | 必选和可选的接口，对所有接口和输入/输出数据通道进行描述 | | 可信信道 | |
| **角色，服务和鉴权** | 必选和可选的角色和服务逻辑上应分开 | 基于角色或基于身份的操作员鉴权机制 | 基于身份的操作员鉴权机制 | 多因素鉴权 |
| **软件/固件** | 核准的完整性 | 核准的数字签名 | 核准的数字签名完整性测试 | |

| | | | | |
|---|---|---|---|---|
| **安全** | 技术或基于 EDC 的完整性测试 | 或基于密钥的 MAC 完整性测试 | | |
| **操作环境** | 不可修改、受限或可修改的 | 可修改的 | | |
| **物理安全** | 工业级别设备 | 加锁或篡改可留迹象 | 对外壳和门的入侵检测与响应。具备 EFP 或 EFT | 入侵检测及响应封装，具有 EFP，错误注入防护 |
| **非入侵式安全** | 模块应可抵御附录 F 中指定的非入侵式攻击 | | | |
| | 应提供附录 F 指定的消减措施的文档，以及有效性 | | 攻击测试 | |
| **密钥管理** | 随机数发生器，SSP 产生、建立、导入、导出、存储、清零 | | | |
| | 利用核准的方法，进行自动的 SSP 传输或 SSP 交换 | | | |
| | 利用人工手段建立的 SSP 可以用明文方式导入/导出 | | 利用人工方式建立的 SSP 应该通过加密或可信信道或知识拆分机密等方式导入/导出 | |
| **自检** | 运行前：软件/固件完整性测试、旁路测试以及关键功能测试 | | | |
| | 条件：密码算法、配对一致性、软件/固件加载、手动输入、旁路以及关键功能测试 | | | |
| **生命周期保障-配置管理** | 配置管理系统应覆盖密码模块、组件和文档。每一项在整个生命周期都能唯一标识并可追踪 | | 自动化的配置管理系统 | |
| **生命周期保障-设计** | 模块应设计成可允许对所有提供的安全相关服务进行测试 | | | |
| **生命周期保障-有限状态模型** | 有限状态模型 | | | |
| **生命周期保障-开发** | 带注释的源代码、版图或 HDL | 软件的高级语言；硬件高级描述语言 | | 文档注明模块部件的前置条件，以及当组件执行完毕时预期为真的后置条件 |
| **生命周期保障-测试** | 功能测试 | | 底层测试 | |
| **生命周期保障-配送和操作** | 初始化流程 | 配送流程 | | 使用厂商提供的鉴别信息进行操作员鉴别 |
| **生命周期保障-指导文档** | 管理员和非管理员指南 | | | |
| **其它攻击的缓解** | 缓解其他攻击的说明，目前对这些攻击还没有可测试要求 | | | 验证缓解技术的有效性 |

根据产品实际情况，上述11个类别中的某些项如果不适用，可不做评估认证。

FIPS认证测试首先需要确定认证范围，可纳入认证范围的服务和密码功能必须是基于符合标准的密码算法，部分符合标准的服务可自主选择不纳入认证范围。核心密码功能模块（如随机数生成器）必须纳入认证范围。

FIPS认证时，评估实验室会从6个维度展开测试，以评估认证对象与标准的符合度。

这6个维度分别为：

1. 算法测试：确认密码算法实现是否遵从标准，算法执行结果是否正确等
2. 设计评估：评估产品设计实现中的一些安全要求是否得到满足，如安全敏感参数管理、开机自检等
3. 熵源评估：评估熵源是否满足SP 800-90B相关要求
4. OP测试：Operational Test，验证密码模块/认证产品是否能正常执行所有的安全功能设计，甚至业务服务
5. 代码审计：评估密码模块中服务相关的代码实现是否正确
6. 物理安全测试：评估密码模块的物理安全是否符合对应等级的安全要求

认证实验室从以上6个维度评估测试对象与标准的符合度。每一类会根据实际情况给出可满足的最高等级，产品最后的FIPS等级由11类要求对应等级的最低等级决定。

实际产品在进行FIPS140-2认证时，部分设计特性可能和认证标准存在差异。以“Apple 安全密钥库加密模块 v10.0”为例，该模块设计安全等级为Level-2，该等级要求密钥管理具备密钥清零能力，但在苹果产品中部分密钥材料存放在eFUSE中，该部分数据无法清零。Apple在其安全策略中明确说明该场景下无法清零。该方案已成功获得FIPS140-2认证。

**7.5 Key / CSP Zeroization**

Cleartext keys and CSPs are zeroized immediately after their usage is completed or when the device is powered down. Additionally, the user can zeroize the entire device directly (locally) or remotely, returning it to the original factory settings.

The exception is the key called the device UID which is stored in a specially protected hardware component. The UID key is programmed during manufacturing process and cannot be directly read or written by any software/firmware. It can only be used for an AES encryption or decryption operation. The UID is used to wrap the file system Class D key or keys that are intended to be bound to the current device. For wrapping the remaining Class keys, a key is derived using the KDF from the UID and a key derived from the User's password. Therefore, the UID is required for the lifetime of the device. The UID stored in hardware exists as “blown fuses” and cannot be zeroized.

### 4.1.2 CC 认证测评方法

CC认证（Common Criteria for Information Technology Security Evaluation）是计算机安全认证的国际标准(ISO/IEC 15408)。 CC认证是一整套的认证，包括操作系统，接入控制系统，数据库和密钥管理系统等，所以相比FIPS 140-2认证来说，CC认证更加全面通用。

CC认证对评估对象（TOE）安全设计的多个方面，以及对TOE进行脆弱性评估，从而给出TOE的安全等级（EAL），CC将EAL划分为7个等级，从EAL1到EAL7安全性递增，EAL等级越高，评估要求的证据更多、评估也更严格加。

CC 安全认证对 TOE 的安全评估维度包括以下六个大类：

1. ASE：评估 TOE 的安全边界、资产及威胁、安全问题解决方案等，确保所有相关的安全问题都得到有效解决。
2. ADV：从功能规格、架构设计、模块设计、源码等层面评估 TOE 开发过程的安全性，确保 TOE 实现正确。
3. ATE：评估 TOE 安全测试设计与执行，确保 TOE 得到充分的安全测试
4. AGD：评估使用手册是否能指导用户正确接收、配置及使用 TOE，确保 TOE 被用户正确使用。
5. ALC：评估 TOE 开发生命周期管理，确保开发过程中，员工遵循并采用规范、工具保障开发质量，设计信息安全等，EAL3 及以上安全性还需进行现场稽查评估，确保 TOE 从生产到交付的安全性。
6. AVA：从攻击者视角对 TOE 进行脆弱性评估

在 CC 的通过评估方法文档（CEM）中对以上 6 个大类进行了详细展开，给出了每个子类不同分值对应的不同测评要求。根据各项达成的分值，最终给出整个 TOE 达到的 EAL 安全等级。

| Assurance class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Development | ADV_ARC | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 |
| | ADV_IMP | | | | 1 | 1 | 2 | 2 |
| | ADV_INT | | | | | 2 | 3 | 3 |
| | ADV_SPM | | | | | | 1 | 1 |
| | ADV_TDS | | 1 | 2 | 3 | 4 | 5 | 6 |
| Guidance documents | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_PRE | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life-cycle support | ALC_CMC | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Security Target evaluation | ASE_CCL | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 |

图 4-1 CC 认证的 EAL 安全等级

CC 认证中不要求 SoC 密码模块中“固件不可升级”，在 BSI 最新发布的 3S（Secure Sub-System in System-on-Chip） PP 中，运行子系统的固件存放在外部

存储器中以支持固件升级，在固件加载时 TOE 需具备足够的安全保护，如提供签名校验机制。

to be in the scope of the evaluation. The external memory is manufactured in Phase 3. After manufacturing, the firmware and software, as well as composite software, might be loaded to the external memory. In the case firmware, software and/or composite software are stored in the external memory, they should be protected.

The secure external memory can be evaluated as part of the TOE or may have been evaluated separately, with evaluation results re-used during the evaluation of the TOE, based on the composition approach.

- The passive external memory can also store a firmware image to enable updates of the firmware. Loading Firmware images require a similar security service than the loading of software images.

## 4.2 SoC 密码模块的测评和管理需求研究

### 4.2.1 安全功能测评的指导要求

本节主要覆盖SoC密码模块功能部分的安全测评，主要目标为评估系统中的安全功能是否正确实现，如密码学计算是否正确等。

具体的测评项见下表。

表 4-2 车载 SoC 密码模块安全功能测评项

| 编号 | 描述 |
|---|---|
| Testcase.Cryptographic Functionality | |
| TSF_PK | 测试公钥算法生成公私钥对是否安全正确，加解密、签名验签功能是否正确实现 |
| TSF_SKC | 测试对称密钥加解密功能是否正确 |
| TSF_KDF | 测试KDF算法派生临时密钥功能是否正确 |
| TSF_KE | 测试密钥交换功能是否正确 |
| TSF_RNG | 测试系统产生的随机数是否具备足够的随机性 |
| TSF_Hash | 测试杂凑算法计算结果是否正确 |
| TSF_HMAC | 测试HMAC计算结果是否正确 |
| TSF_KAT | 测试密钥协商及传输功能是否正确 |
| TSF_KEK | 测试密钥保护密钥结果是否正确 |
| TSF_KeyEnc | 测试密钥加密保护功能是否正确 |
| TSF_KeyDel | 测试密钥删除功能是否正确 |

| | |
|---|---|
| Testcase.Data Protection | |
| TDP.AC | 测试SoC密码模块是否具备访问控制机制 |
| TDP.DC | 测试SoC密码模块的存储数据是否具备机密性保护 |
| TDP.DI | 测试SoC密码模块的存储数据是否具备完整性保护 |
| TDP.CT | 测试SoC密码模块的传输数据是否具备机密性保护 |
| TDP.IT | 测试SoC密码模块的传输数据是否具备完整性保护 |
| TDP.DE.1 | 测试SoC密码模块的运行态数据是否具备硬件隔离（如SoC密码模块与外部的隔离） |
| TDP.DC.1 | 测试SoC密码模块的运行态数据是否具备机密性保护 |
| TDP.DI.1 | 测试SoC密码模块的运行态数据是否具备完整性保护 |
| TDP.ROL | 测试SoC密码模块的安全存储是否具备回滚保护能力 |
| Testcase. Identification and Authentication | |
| TIA_UAU | 测试用户执行操作前是否有角色权限认证 |
| Testcase.Security Management | |
| TMT_MSA | 测试SoC密码模块是否具备安全属性管理功能 |
| TMT_SMR | 测试SoC密码模块是否具备安全角色维护及权限管理功能 |
| TMT_LIM | 测试SoC密码模块是否符合安全功能权限最小化 |
| Testcase.Protection of the TSF | |
| TPT_Port | 测试SoC密码模块的调试接口是否正确关闭，物理接口是否存在数据泄漏 |
| TPT_Secboot | 测试SoC密码模块是否具备安全启动/可信启动功能 |
| TPT_Update | 测试SoC密码模块是否具备安全升级功能 |
| TPT_RPL | 测试SoC密码模块是否具备固件版本防重放攻击能力 |
| TPT_STM | 测试SoC密码模块是否能够提供可靠的时间戳 |

### 4.2.2 安全保障要求测评的指导要求

根据3.2.1章节内容，可以从资产识别和威胁分析导出对于SoC密码模块的测评要求。测评的主要目的是为了评估SoC密码模块在面临攻击的情况下，能否满足机密性、完整性和可用性的安全防护要求。

根据SoC密码模块涉及的威胁，可从故障注入、侧信道和逻辑攻击导出测评项，如下表。因为SoC密码模块集成在芯片内部，此处不考虑物理侵入式攻击手段。

表 4-3 SoC 密码模块安全保障要求测评项

| 测评项 | 描述 |
| --- | --- |
| **故障注入测评：尝试通过故障注入手段来影响SoC密码模块功能的正常运行，从而绕过限制访问敏感数据，或者破解密码运算过程中的敏感信息等。** | |
| 时钟故障注入 | 通过控制单板时钟源，利用外部信号产生设备，在单板运行过程中干扰时钟信号，导致时序错乱，影响单板正常运行，概率性可以绕过安全机制、泄漏敏感信息 |
| 电压故障注入 | 对攻击目标的供电电源进行干扰，影响设备的正常运行，引起设备的工作异常 |
| 电磁故障注入 | 通过在目标设备表面产生电磁脉冲信号，干扰设备内部的电路运行，引起设备故障 |
| 激光故障注入 | 通过对单板电路照射特定波长的激光，导致电路逻辑出错，单板运行异常，有一定概率可以绕过安全机制、泄漏敏感信息 |
| **侧信道分析测评：尝试通过密码算法运行过程中的侧信道信息来获取密码算法模块的敏感信息。** | |
| 泄漏检测分析 | TVLA 泄漏检测是一种基于 Welch’s t-test 的统计假设检测。它通常用于侧信道分析前泄漏的检测，是当前有效地寻找可能被利用的安全薄弱点的方法 |
| 计时分析 | 利用加解密算法执行相应操作时所表现出来的时间特征，分析运算时间与密钥和敏感信息之间的关联性，进而恢复密钥或敏感信息。 |
| 功耗分析 | 利用加解密算法执行相应操作时所泄漏的功耗侧信道信息，分析能量消耗特征与密钥和敏感信息之间的相关性，结合侧信道分析算法，尝试恢复密钥或敏感信息。 |
| 电磁分析 | 利用加解密算法执行相应操作时所泄漏的电磁侧信道信息，分析电磁泄漏特征与密钥和敏感信息之间的相关性，结合侧信道分析算法，尝试恢复密钥或敏感信息。 |
| **逻辑漏洞分析测评：利用TOE中存在的逻辑缺陷，改变其正常执行流程或触发异常行为，达到窃取或篡改关键资产的目的。主要是基于设计或代码中存在的逻辑薄弱点进行攻击** | |
| 绕过 | 利用逻辑漏洞避开安全保护机制，进而篡改或窃取关键资产的测评方式 |
| 篡改 | 利用TOE逻辑漏洞篡改TOE的安全功能，进而篡改或窃取关键资产的攻击方式 |
| 直接攻击 | 直接攻击针对的对象主要是涉及概率性（密码学强度）、排列组合的安全特性，例如密钥、密码、随机数等。评估者通过分 |

| | |
|---|---|
| | 析密码构造机制（长度、元素组成等）、密钥更新时间、随机数产生机制等信息，判断是否能在攻击时间窗内，通过遍历所有可能性的方式即可破解密钥、密码或随机数规律。 |
| 泄漏 | TOE在运行过程中会通过接口通信、单板信号、操作时间反应出各种操作信息，评估者需要分析这些信息中是否会泄漏出敏感信息 |

### 4.2.3 生命周期安全管理的指导要求

生命周期安全管理，是指厂商在SoC密码模块的开发、生产制造、运行等各个阶段，使用相关管理措施，以保障SoC密码模块被正确地开发、测试、配置、配送、安装、运行，并保障模块配有适当的操作员管理文档。对于SoC密码模块的生命周期安全管理，需要明确SoC密码模块包含的阶段以及在全生命周期的各阶段需要实行的安全管理措施。

SoC密码模块最终以物理形态集成在SoC芯片中交付客户使用，其整个生命周期从开发到投入使用可分为以下阶段：

1) **SoC密码模块的硬件开发：**

SoC密码模块的硬件开发主要包含SoC密码模块内部的硬件开发、SoC密码模块与SoC其它组件的接口开发。

向SoC开发者交付的SoC密码模块成果应包括硬件IP、SoC密码模块集成到SoC的相关指南以及准备集成在ROM中的二进制代码。通常，该阶段开发人员会在SoC模拟环境中运行SoC密码模块。

在向掩模车间或晶圆厂交付完整的SoC之前，需要完成SoC的SoC密码模块集成，因此SoC密码模块硬件的SoC集成也在该生命周期阶段完成。

最终需要向掩模车间或晶圆厂交付的成果包括生产SoC所需的所有组件，这包括了SoC密码模块、固件等。

对于这一阶段的安全管理，需要保障SoC密码模块的开发环境安全、配置管理安全、人员管理安全等。考虑到有两次交付，需要重点关注传输安全和SoC密码模块接口说明，以保护SoC密码模块的机密性和完整性。

2) **SoC密码模块的固件开发：**

本阶段主要包含SoC密码模块的固件开发，固件通常存储在SoC密码模块的内部存储或者外部非易失性存储中。

对于这一阶段的安全管理措施，主要包含软件开发环境的保护、配置管理、人员管理、固件/软件的完整性保护以及传递给下一阶段的过程安全保护等。其中配置管理应保障SoC密码模块的开发过程及其相关文档都使用配置管理系统进行管理，并且每个配置条目的每个版本，都应被分配并标注一个唯一身份标识码。在SoC密码模块的整个生命周期中，配置管理系统应当追踪并维护标识和版本的更改。

**3) SoC密码模块的集成：**

该阶段主要是指导SoC密码模块进行硬件和固件的集成，调试接口的管理。一方面，要输出指导文档，以确保SoC密码模块的用户能够准确理解，使得硬件、固件被正确地集成在SoC；另一方面，对于已完成SoC密码模块的

相应测试后，要提供合适的调试接口管理方法，以保证在出厂前，SoC密码模块的调试接口被有效地管理，调试功能不能被非法使用。

参考相关评测标准，如GM/T 0008《安全芯片密码检测准则》，对SoC密码模块的生命周期管理，可以分别从源文件安全、重要文档安全和重要制度保障三个方面提出安全要求：

**(1) 源文件安全**

a) SoC密码模块的源文件应安全存放
b) SoC密码模块的源文件的设计应有规范的格式
c) 在保密协议的约束下，SoC密码模块有关密码部分的源文件应进行审查
d) SoC密码模块源文件及相关设计文档的变更应可追溯
e) 在保密协议的约束下，SoC密码模块与密码技术相关的硬件版图应进行审查

**(2) 重要文档安全**

a) SoC密码模块的配置管理、交付运行、开发安全和工具技术等各类文档齐全，并定期更新
b) 提交给检测机构的所有文档应采用符合相关规范的中文编写；如使用英文编写，应同时具备对应的中文版本
c) 送检单位应提供SoC密码模块操作用户安全指南类文档，确保SoC密码模块的安全使用
d) SoC密码模块的各类文档分级管理，分开存放，访问不同级别的文档应具有相应权限
e) 送检单位应提供SoC密码模块研发设计环节的相关文档，文档中应详细描述SoC密码模块的架构设计、模块划分、安全策略等开发质量要求相关描述
f) SoC密码模块在生命周期的各个阶段应具有追踪记录文档

**(3) 重要制度保障**

a) SoC密码模块开发环境应具有相应的规章制度及安全配置
b) SoC密码模块的生命周期的各个阶段所涉及的工作人员应具有明确的职能划分。
c) SoC 密码模块开发环境的访问应具有严格的人员控制。
d) SoC 密码模块的开发环境应确保安全，且与外网物理隔离。
e) SoC 密码模块开发环境应有研发规章制度和安全配置指导。
f) SoC 密码模块的开发流程的各个阶段应明确界定。
g) SoC 密码模块开发过程中各阶段完成的任务及相应的输出应具有明确要求。
h) SoC 密码模块设计、研发、加工、销售、交付各阶段应具备基本安全管理制度。
i) 送检单位应提供采用的各种 IP 核安全可控的自证明声明。
j) 工作人员仅能接触与本人工作相关的信息。
k) 接触敏感信息的工作人员应签署相关的保密协议。
l) SoC 密码模块生命周期中应具备安全资产清单，包括但不限于信息、源文件、外部关键数据、测试工具等，采取安全资产保护措施。
m) SoC 密码模块应具备国家认可的芯片设计评估、生产质量保障体系。

n) SoC 密码模块全生命周期应对代码实现进度、设计文档、测试文档、安全缺陷、用户文档进行跟踪，并根据记录进行定期审计。
o) SoC 密码模块应提供采用的各种 IP 核安全可控的供应商安全保障协议书。
p) SoC 密码模块应提供全生命周期供应链的长期保障机制书面文档，确保芯片供应安全。
q) 送检单位应支持对包括但不限于全生命周期设计、管理文档、资产清单、质量保障体系、人员安全管理、安全组织、安全工作流程、数据安全管理、环境安全管理等方面进行文档检查和现场检查。

## 4.3 SoC 密码模块和 GB/T 37092 密码模块安全域的映射关系

在 3.2 和 4.2 两个小节内，分别对 SoC 密码模块的资产、威胁和安全目标进行了分析，并给出对应的安全需求和测评需求。

结合 2.2 标准化现状及 3.1 节 SoC 密码模块定义的描述，SoC 密码模块更接近于密码模块。为更好地与密码模块匹配对标，接下来从安全需求与测评需求两个维度分析与密码模块的 11 个安全域的映射关系。

### 4.3.1 SoC 密码模块安全需求与 GB/T 37092 密码模块安全域的对应

依据 4.1 和 4.2 节的内容，车载 SoC 密码模块的以下安全需求可映射到 GB/T 37092《信息安全技术 密码模块安全技术要求》12 个安全域，如下表。

表 4-4 SoC 密码模块对应 GB/T 37092 密码模块安全域的安全需求

| GB/T 37092 安全域 | 安全域的安全要求 | SoC 密码模块的安全需求 |
|---|---|---|
| 密码模块规格 | 模块类型、密码边界、工作模式 | SoC 密码模块应具备正确完成相应密码学运算的能力，如密钥生成、密钥交换、加解密、签名验签等 |
| 密码模块接口 | 接口类型、接口定义、可信信道 | 1、SoC 密码模块应支持关键数据的安全导入，即数据传输的机密性保护 |
| 角色、服务和鉴别 | 角色、服务、旁路能力、自启动密码服务能力、软件/固件加载、鉴别 | 1、SoC 密码模块应支持对用户的认证/鉴权 |
| 软件/固件安全 | 软件/固件要使用核准的完整性技术进行保护 | 1、SoC 密码模块应具备完整性保护能力，如固件不被恶意篡改 |
| 运行环境 | 可变的运行环境、受限/不可变运行环境 | 1、SoC 密码模块一般为受限的运行环境 |
| 物理安全 | 物理安全实体、环境失效保护/测试 | 1、SoC 密码模块集成于 SoC 内，天然具备芯片外部封装及芯片金属层的保护 |
| 非侵入式安全 | 针对能量、计时、电磁等攻击的缓解措施和有效性 | 1、SoC 密码模块应具备侧信道防护能力 |

| | | |
|---|---|---|
| 敏感安全参数(SSP)管理 | 随机数生成器，SSP 生成、建立、输入输出、存储、置零 | 1、SoC 密码模块应具备正确产生安全随机数，密钥安全产生/导入、派生、传递、使用、销毁的管理能力 |
| 自测试 | 运行前自测试、条件自测试 | 1、SoC 密码模块应具备自检能力 |
| 生命周期保障 | 配置管理、设计、有限状态模型、开发、厂商测试、配送与操作、生命终止、指南文档 | |
| 对其它攻击的缓解 | 其它未定义的攻击缓解措施 | SoC 密码模块应具备故障注入防护能力、防重放攻击能力 |

同时，车载 SoC 密码模块还有以下特有功能和安全需求。

表 4-5 SoC 密码模块面向车载领域的特有功能及安全需求

| 特有功能 | 安全需求 |
|---|---|
| **SoC 密码模块应具备唯一身份 ID** | 服务提到了要有模块版本号，未涉及具体细节。<br>而这个身份 ID 是利用公私钥机制产生，具有密码学的可验证性，须保护私钥部分的机密性，汽车生命周期长，还涉及转让等环节，此 ID 可提供真实性。 |
| **SoC 密码模块应支持系统安全启动的能力** | 密码模块提到“软件/固件要使用核准的完整性技术进行保护”，未涉及具体流程。车载 SoC 密码模块负责整个 SoC 的启动安全，整体的软件/固件安全性一般涉及多级校验，需要有更具体的指导流程 |
| **SoC 密码模块应支持回滚保护** | 密码模块当前没提及此要求。SoC 密码模块的回滚保护可防止攻击者利用旧版本（有合法签名，但存在代码漏洞）替换新版本以实施攻击，需要考虑此类攻击的保护。 |
| **固件韧性，主从备份** | 密码模块当前没提及此要求。车载 SoC 涉及高可靠性，固件是受密码学保护的，但如果没有类似主从备份构建固件韧性的能力，会导致固件失效，导致系统崩溃，因此在车载 SoC 须考虑此特性 |
| **SoC 密码模块应支持系统安全升级的能力** | 车载 SoC 密码模块负责整个 SoC 的固件升级 |

| | |
|---|---|
| **SoC 密码模块应支持安全时间** | 安全时间用来作签名的时间戳，密钥生命周期的时间管理。<br>下电后安全时间会清零，上电后会从外部加载同步可信时间源； |
| **SoC 密码模块应支持对外提供安全存储的能力** | 对外提供安全存储能力，用于保护数据防回滚，只能单向递增 |
| **SoC 密码模块应提供生命周期标识管理的能力** | 车载领域 ECU 各阶段的生命周期标识（如制造、集成、在线运行等等）在 SoC 密码模块中进行保护，可进行管理；一般只读，更改需要鉴权 |
| **SoC 密码模块应支持对外提供单向计数器的能力** | 单向计数器用于向外部提供服务，服务访问可向 SoC 密码模块申请一个计数值，保护服务访问方的数据防回滚；如果要更新，需要进行鉴权。 |

这些安全需求按照密码模块的四个等级进行划分，可形成以下安全要求概述。

表 4-6 特有功能对应密码模块四个等级的安全要求概述

<table>
<tr><th colspan="2">安全域</th><th>安全等级 1</th><th>安全等级 2</th><th>安全等级 3</th><th>安全等级 4</th></tr>
<tr><td rowspan="5">车载 SoC 密码模块特有功能</td><td>具备唯一身份 ID</td><td colspan="2">具有可防篡改的唯一身份 ID</td><td colspan="2">唯一身份 ID 利用公私钥机制产生，具有密码学的可验证性</td></tr>
<tr><td>支持安全启动的能力</td><td colspan="2">具备启动时对固件进行校验的能力，检测固件完整性和真实性</td><td colspan="2">启动过程使用核准的数字签名方法，并具备一定的防故障注入能力</td></tr>
<tr><td>支持回滚保护</td><td colspan="4">支持固件版本检查，对过往固件版本提供拒绝运行的能力</td></tr>
<tr><td>固件韧性</td><td colspan="3">固件具有备份机制</td><td>主动恢复</td></tr>
<tr><td>支持系统安全升级的能力</td><td>具备对升级镜像进行校验的能力，检测升级镜像的完整性和真</td><td>使用核准的校验方法</td><td colspan="2">升级过程出现错误，系统能够恢复到升级前状态</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| | | 实性 | | | |
| | 支持安全时间（如可用） | 具备向外部提供安全时间的能力 | SoC 密码模块内的安全时间应采用核准的算法进行保护 | 外部时间来源的导入应采用核准的数字签名算法进行真实性检查 | |
| | 支持对外提供安全存储的能力 | 关键数据需要进行加密存储 | 用于加密的密钥应被 SoC 密码模块内部进行保护 | 密钥应与设备绑定，一机一密 | 加密的数据防回滚 |
| | 提供生命周期标识管理的能力 | 生命周期标识应具备防篡改的保护措施，修改前应进行鉴权 | | | |
| | 支持对外提供单向计数器的能力（如可用） | 应向外部提供单向计数器，计数器的更新应具备鉴权机制 | | | 计数器应具备防回滚 |

### 4.3.2 SoC 密码模块测评需求与 GB/T 37092 密码模块安全域的对应

以下通过一个表格，将 4.2 节中提到的安全功能需求、安全保障需求和生命周期管理需求与密码模块的安全域进行映射。

表 4-6 SoC 密码模块对应 GB/T 37092 密码模块安全域的测评需求

| GB/T 37092 安全域 | 安全域的安全要求 | SoC 密码模块的测评需求 |
|---|---|---|
| 密码模块规格 | 模块类型、密码边界、工作模式 | TSF_PK，公钥算法的功能<br>TSF_SKC，对称算法的功能<br>TSF_KDF，派生算法功能<br>TSF_KE，密钥交换功能<br>TSF_Hash，杂凑算法功能 |

| | | |
|---|---|---|
| | | TSF_HMAC，HMAC 功能 |
| 密码模块接口 | 接口类型、接口定义、可信信道 | 1、SoC 密码模块应支持关键数据的安全导入，即数据传输的机密性保护<br>TPT_Port，调试接口的正确关闭<br>TDP.DC，存储数据的机密性保护<br>TDP.DI，存储数据的完整性保护<br>TDP.CT，传输数据的机密性保护<br>TDP.IT，传输数据的完整性保护<br>TDP.DE.1，运行时数据的硬件隔离保护<br>TDP.DC.1，运行时数据的机密性保护<br>TDP.DI.1，运行时数据的完整性保护 |
| 角色、服务和鉴别 | 角色、服务、旁路能力、自启动密码服务能力、软件/固件加载、鉴别 | 1、SoC 密码模块应支持对用户的认证/鉴权<br>TMT_SMR，安全角色维护及权限管理的功能<br>TIA_UAU，用户的角色权限认证<br>TPT_Update，安全升级 |
| 软件/固件安全 | 软件/固件要使用核准的完整性技术进行保护 | 1、SoC 密码模块应具备完整性保护能力，如固件不被恶意篡改<br>TPT_Secboot，安全启动/可信启动功能 |
| 运行环境 | 可变的运行环境、受限/不可变运行环境 | 1、SoC 密码模块一般为受限的运行环境<br>TDP.AC，SoC 密码模块的访问控制机制 |
| 物理安全 | 物理安全实体、环境失效保护/测试 | 1、SoC 密码模块集成于 SoC 内，天然具备芯片外部封装及芯片金属层的保护 |
| 非侵入式安全 | 针对能量、计时、电磁等攻击的缓解措施和有效性 | 1、SoC 密码模块应具备侧信道防护能力<br>覆盖侧信道分析测评，如泄漏检测、计时、功耗和电磁等分析手段 |
| 敏感安全参数(SSP)管理 | 随机数生成器，SSP 生成、建立、输入输出、存储、置零 | 1、SoC 密码模块应具备正确产生安全随机数，密钥安全产生/导入、派生、传递、使用、销毁的管理能力<br>TSF_RNG，随机数产生的功能 |

| | | |
|---|---|---|
| | | TSF_KAT，密钥协商及传输功能<br>TSF_KEK，密钥保护密钥结果的功能<br>TSF_KeyEnc，密钥加密保护的功能<br>TSF_KeyDel，密钥删除的功能 |
| 自测试 | 运行前自测试、条件自测试 | 1、SoC 密码模块应具备自检能力 |
| 生命周期保障 | 配置管理、设计、有限状态模型、开发、厂商测试、配送与操作、生命终止、指南文档 | 源文件安全<br>重要文档安全<br>重要制度保障 |
| 对其它攻击的缓解 | 其它未定义的攻击缓解措施 | TDP.ROL，安全存储是否具备回滚保护<br>TPT_RPL，固件防重放攻击能力<br>TMT_MSA，安全属性管理的功能<br>TMT_LIM，安全功能权限最小化<br><br>故障注入防护能力，覆盖时钟故障、电压故障、电磁故障和激光故障等注入手段<br><br>逻辑漏洞分析测评，覆盖绕过、篡改、直接攻击、泄漏等分析手段 |

# 5. 标准化研究

## 5.1 标准体系及本标准在体系中的位置

车载 SoC 密码模块被越来越多汽车厂商接受，应用在多种场景中，如自动驾驶、智能座舱等等。

根据 2.2.3 分析，车载 SoC 密码模块相关的设计、检测标准有 GB/T 37092《信息安全技术 密码模块安全技术要求》和 GM/T 0039《密码模块安全检测要求》，这些标准存在多处待讨论或完善的要求内容，如密码边界划分、未受保护的 SSP 执行清零等等。

国内车载领域芯片厂商的 SoC 密码模块大多遵从国外车载相关安全标准，如 EVITA HSM，来构建车载领域的安全。

因此，对车载 SoC 密码模块进行标准化，可为车载 SoC 密码模块、车载芯片和车载设备系统提供安全设计或检测上的参考，引导国内车载领域厂商选用更符合安全标准的产品，保障最终用户安全放心地使用。

从密码角度看，车载 SoC 密码模块涉及到密码基础、密码产品、密码检测等标准类型，因此依据 GM/Y 5001-2021，规划 SoC 密码模块的密码标准体系，如下图。

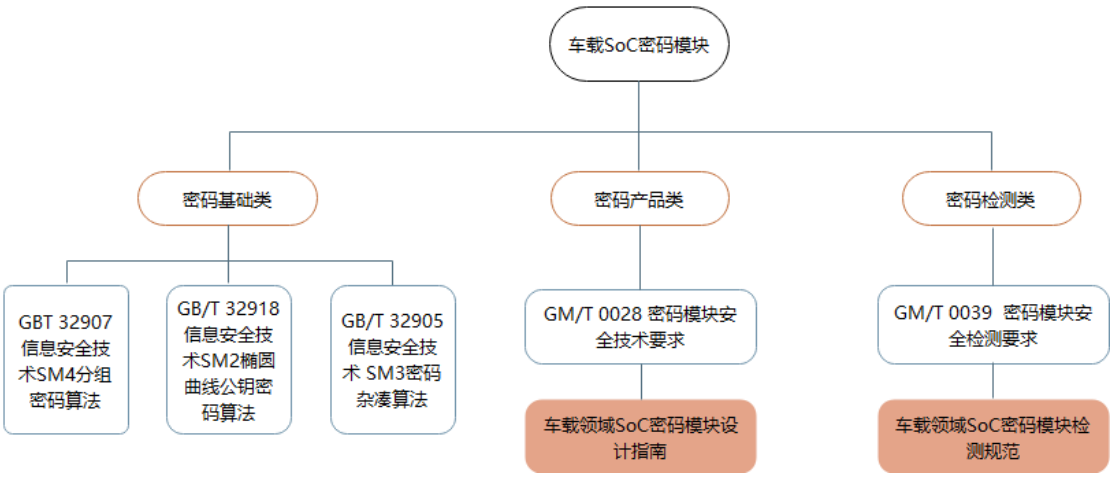


图 5-1 车载 SoC 密码模块标准体系

除了已发布标准外，车域 SoC 密码模块仍须在密码产品设计指南和检测两个维度载领进行标准化的推动，为此类产品在开发、检测时提供更适用的标准，形成新的商用密码产品认证类别，如下表。

表5-1 新增“车载SoC密码模块”认证类别

| 序号 | 产品种类 | 产品描述 | 认证依据 |
|---|---|---|---|
| … | … | … | … |
| **23** | 车载 SoC 密码模块（暂名） | 实现密码运算、密钥管理、安全存储，一般包含硬件、固件，为车载 SoC/ECU 提供安全启动、安全升级、安全通信、固件韧性、安全时间等功能 | GM/T 0028《密码模块安全技术要求》<br>GM/T 0xxx《车载领域 SoC 密码模块设计指南》 |

在下一节，具体描述以上两个维度标准化推动的考虑。

## 5.2 标准化建议

建议制定以下标准。

- **《车载领域 SoC 密码模块设计指南》**

SoC 密码模块作为 SoC 的关键子系统，承载整个 SoC 的密码学、密钥管理、安全升级等敏感操作，通常包含硬件、固件、运行环境。虽然当前 GB/T 37092《信息安全技术 密码模块安全技术要求》可以提供密码模块在设计和开发上的参考，然而考虑到车载领域 SoC 密码模块的形态、密钥存储和生命周期管理等方面的特殊性，有必要制订适用于车载领域 SoC 密码模块的设计方法，作为 GB/T 37092 的子集，形成评测方法的补充。

标准提纲如下：

--车载领域 SoC 密码模块逻辑框架

--车载领域 SoC 密码模块安全威胁

--车载领域 SoC 密码模块安全功能

--面向密码模块标准不同安全级别的设计指导

- **《车载领域 SoC 密码模块检测规范》**

依据国家市场监管总局 国家密码管理局联合发文【2020 年第 23 号】，当前商用密码产品认证目录有 22 项，每一项认证有对应的认证依据。密码模块类商用密码产品的认证依据一般包括功能性检测和安全性检测，其中安全性检测统一遵从 GB/T 37092《信息安全技术 密码模块安全技术要求》，功能性检测基于对应产品的检测标准。

本标准定位车载领域 SoC 密码模块的功能性检测，覆盖密码运算、唯一身份 ID、安全启动、回滚保护、固件韧性、安全升级、安全时间、安全存储、生命周期管理标识等功能。检测标准的制定为此类产品提供统一、有效的方法，在整车厂商、汽车芯片提供商、监管机构等汽车业界相关方形成对这类密码产品可感知、可衡量的尺子。

标准提纲如下：

--车载领域 SoC 密码模块检测项目

--车载领域 SoC 密码模块检测方法

# 6. 总结

本研究报告共分为六个章节，首先明确车载领域 SoC 密码模块的研究背景，从国家政策，产业趋势等阐述了研究的必要性和迫切性，以及研究对象和研究目标。然后从国内外 SoC 密码模块的技术现状和业界现有 SoC 密码模块的标准化现状进行了分析，归纳总结业界当前主流的 SoC 密码模块的技术发展趋势，并对现有密码标准体系对 SoC 密码模块的适用情况给出分析结果，识别出存在的差异点和问题。

基于现状分析，本研究报告通过梳理业界对 SoC 密码模块的各类描述，给出 SoC 密码模块的定义、组成、边界和主要功能，分析 SoC 密码模块的关键资产和主要威胁，推导出安全目标和安全需求。同时，开展对 SoC 密码模块的测评要求研究分析，提炼安全功能测评、安全保障测评和生命周期安全管理的指导要求。

最后，基于上述研究情况，给出关于后续车载领域 SoC 密码模块的设计与测评相关的标准化建议。

# 参考文献


[1] 工业和信息化部，车联网网络安全和数据安全标准体系建设指南，2022
[2] 工业和信息化部，车联网（智能网联汽车）产业发展行动计划，2018
[3] 发改委、工信部等 11 部委，智能汽车创新发展战略，2020
[4] Eurosmart, Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, 2022
[5] AUTOSAR, Specification of Secure Hardware Extensions, 2020
[6] EVITA, Secure On-board Architecture Specification, 2011
[7] Dedicated Security Components (DSC) international Technical Community, Collaborative Protection Profile for Dedicated Security Component, 2020
[8] CAR 2 CAR Communication Consortium, Protection Profile V2X Hardware Security Module by CAR 2 CAR Communication Consortium Version 1.0, 2020
[9] Common Criteria, Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, 2017
[10] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, 2012
[11] NIST, FIPS PUB 140-3 Security Requirements for Cryptographic Modules, 2019
[12] 工业与信息化部，车联网网络安全和数据安全标准体系建设指南，2022
[13] NIST, NISTIR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases, 2022
[14] NIST, Special Publication 800-57 Part 2 Recommendation for Key Management,2019
[15] Ingrid Verbauwhede, section Hardware Security in The Cyber Security Body of Knowledge，2019
[16] 密标委，GM/Y 5001 密码标准使用指南，2021

# 附录 A

考虑到缩略语篇幅较长，在本附录详细列出了本标准研究报告出现的缩略语、中文含义。

## A.1 缩略语

| 缩写 | 含义 | 中文 |
|---|---|---|
| SoC | System-on-Chip | 系统级芯片或片上系统 |
| MCU | Microcontroller Unit | 微控制器 |
| PK | Public Key | 公钥 |
| PKI | Public Key Infrastructure | 公钥设施 |
| TOE | Target of Evaluation | 评估对象 |
| HUK | Hardware unique Key | 硬件唯一密钥 |
| FW | Firmware | 固件 |
| HW | Hardware | 硬件 |
| SCA | Side Channel Analysis | 侧信道分析 |
| FI | Fault Injection | 故障注入分析 |
| IO | Input/Output | 输入输出 |
| UID | Unique Identification | 唯一身份ID |
| RNG | Random Number Generator | 随机数生成器 |
| FCS | Functionality of Cryptographic Support | 密码学功能支持 |
| TSF | TOE Security Functionality | 测试目标安全功能 |
| CKM | Cryptographic Key Management | 密码学密钥管理 |
| KEK | Key Encryption Key | 密钥加密密钥 |

| | | |
|---|---|---|
| KDF | key derivation function | 密钥派生函数 |
| COP | Cryptographic Operation | 密码学操作 |
| SKC | Symmetric Key Cryptographic operation | 对称密码操作 |
| KAT | Key Agreement and Transfer | 密钥协商及密钥传递 |
| FDP | Functionality of Data Protection | 数据保护功能 |
| ACC | Access Control | 访问控制 |
| SDC | Stored Data Confidentiality | 存储数据机密性 |
| SDI | Stored Data Integrity | 存储数据完整性 |
| UCT | User data Confidentiality during Transfer | 传递过程中用户数据机密性 |
| UIT | User data Integrity during Transfer | 传递过程中用户数据完整性 |
| RDE | Runtime Data Environment isolation | 运行态数据环境隔离 |
| RDC | Runtime Data Confidentiality | 运行态数据机密性 |
| RDI | Runtime Data Integrity | 运行态数据完整性 |
| RIP | Residual data Protection | 残留数据保护 |
| ROL | Roll-back protection | 回滚保护 |
| FIA | Functionality of Identification and Authentication | ID和认证功能 |
| UAU | User Authentication before Any Action | 用户操作前先认证 |
| FMT | Functionality of Security Management | 功能和安全管理 |
| MSA | Management of Secure Attributes | 安全属性管理 |
| MSR | Restrictions on Security Roles | 安全角色限制 |
| LIM | Limited capabilities and availability | 受限可用能力 |
| NVM | Non-Volatile Memory | 非易失性存储器 |