面向未来的汽车整车信息安全架构设计

童 芸 高花兰 康 佳 周 超 蒋娴文
陕西汽车集团股份有限公司技术中心 陕西 西安 710200

摘 要：随着汽车产业的智能化与互联化，信息安全已成为行业面临的关键挑战。本文旨在探讨汽车正向开发过程中，如何通过能力构建、体系保障和技术手段，全面提升汽车信息安全保障和管理水平，以满足当前国际、国内针对汽车信息安全法规的实施要求和趋势。

关键词：汽车信息安全；整车架构设计；信息安全体系

引言

在智能网联汽车时代，信息安全问题日益凸显，对汽车行业提出了新的挑战。为了保障用户数据的安全、车辆的稳定运行以及行业的可持续发展，全面了解和应对信息安全风险至关重要。本研究将深入探讨国内外信息安全法规与标准，分析汽车信息安全核心能力的构建方法，提出多层次的信息安全保障策略，并探讨信息安全管理体系的认证与实践。通过这一系列研究，旨在为汽车行业提供一套科学、实用的信息安全解决方案。

1 国际与国内汽车信息安全法规及标准解读

1.1 国际法规及标准要求

UN R155：专注于车辆网络安全，设定了各类车辆的网络安全要求，包括电子和电气架构的网络安全相关部分，强调车辆需配备网络安全管理系统（CSMS）。UN R156：规定了软件更新和软件更新管理系统的要求，确保软件更新的安全可靠[1]。ISO/SAE 21434：提供道路车辆网络安全工程的核心指导，覆盖全生命周期的各个阶段，强调风险识别及应对流程。

1.2 国内法规及标准要求

GB/T 40861-2021：中国汽车信息安全通用技术要求，规范汽车信息安全的技术要求，包括基本概念、术语、原则、危险源评估、防护技术体系结构等，对保障汽车信息安全和用户隐私有重要意义。

2 汽车信息安全核心能力建设

2.1 信息安全管理体系的构建

2.1.1 制定全面的信息安全政策与流程

首先要确立信息安全目标和原则：明确信息安全的重要性，制定保护信息资产、确保业务连续性和减少信息安全风险的目标。确立信息安全的基本原则，如保密性、完整性和可用性。其次，制定详细的信息安全政策：涵盖信息安全管理的各个方面，包括数据保护、网络安全、物理安全等。规定员工和其他相关方的信息安全行为准则[2]。此外，还要建立信息安全流程：制定应对信息安全事件的流程，包括事件报告、响应和恢复程序。设立定期的信息安全风险评估和审计流程。

2.1.2 设立专门的信息安全管理部门与职责划分

一是成立信息安全管理部门：设立专门的信息安全团队，负责监控、管理和应对信息安全风险。确保团队具备专业的信息安全知识和技能。二是明确职责划分：为信息安全团队的每个成员分配明确的职责和权限。确保各个部门和员工都了解自己在信息安全管理体系中的角色和责任。三是建立协作机制：促进信息安全团队与其他部门之间的沟通和协作。确保信息安全政策和流程在整个组织中得到有效执行。

2.2 信息安全技术研发与应用

在信息安全领域，技术研发与应用是保障信息安全的重要手段。以下将重点讨论先进加密技术的研发与应用，以及身份认证与访问控制技术的创新。

2.2.1 先进加密技术的研发与应用

加强对称加密算法（如AES）和非对称加密算法（如RSA）的研究，提高算法的安全性和效率。探索基于量子计算的加密算法，以应对未来量子计算机对当前加密体系的潜在威胁。研究同态加密、零知识证明等新型加密技术，以满足特定场景下的安全需求。应用场景包括：在车联网通信中，使用加密技术保护车辆与基础设施、其他车辆之间的通信数据安全。在车载系统中，对敏感数据进行加密存储，防止数据泄露或被非法访问。在远程车辆控制和诊断中，利用加密技术确保指令和数据的完整性和真实性。

2.2.2 身份认证与访问控制技术的创新

研发基于生物特征（如指纹、虹膜等）的身份认证技术，提高认证的准确性和安全性。探索多因素身份认证方法，结合密码、动态令牌、手机短信验证码等多种手段，增强身份认证的可靠性。发展基于角色的访问控

制（RBAC）技术，实现细粒度的权限管理，确保用户只能访问其角色所允许的资源。应用场景包括：在车联网服务平台上，实施严格的身份认证和访问控制，防止未经授权的访问和操作。在车载信息娱乐系统中，通过身份认证技术保护用户隐私和个性化设置。在车辆远程监控和诊断系统中，确保只有经过授权的人员才能访问敏感数据和执行关键操作。

3 多层次的信息安全保障策略

3.1 硬件层面的安全保障

3.1.1 安全芯片的选择与集成策略

选择标准应遵循：一是安全性：优先选择经过严格安全测试和认证的安全芯片，确保其具有强大的防御能力，能够有效抵御各种安全威胁。二是性能：考虑芯片的运算速度和处理能力，以确保在保障安全的同时，不影响系统的整体性能。三是兼容性：选择与现有系统架构相兼容的安全芯片，以降低集成难度和成本。集成策略包括：一要将安全芯片与系统硬件紧密集成，确保其能够实时监控和保护系统的关键部件和数据[3]。二要加强安全芯片与其他系统组件之间的通信安全，采用加密和认证机制，防止数据泄露和篡改。三要定期更新安全芯片中的安全策略和算法，以应对不断变化的安全威胁。

3.1.2 硬件加密模块的设计与实现

在设计硬件加密模块时，应优先考虑其安全性，确保加密算法的强度和密钥管理的安全性。其次设计应具有一定的灵活性，以适应不同应用场景下的加密需求。此外还要通过优化加密算法的实现，提高加密和解密的速度，以减少对系统性能的影响。实现策略方面：一是根据具体需求选择适合的加密算法，如AES、RSA等，并确保其实现的安全性。二是建立完善的密钥管理体系，包括密钥的生成、存储、分发和更新等环节，确保密钥的安全性和可用性。三是针对特定的硬件平台进行优化，提高加密模块的性能和效率。例如，可以利用硬件并行处理能力来加速加密和解密操作。四是对硬件加密模块进行严格的测试和验证，确保其在实际应用中的稳定性和安全性。

3.2 软件层面的安全保障

3.2.1 安全编程实践

首先，需采用安全编码标准：遵循如OWASP等安全编码标准，确保在软件开发过程中减少安全漏洞的引入。其次是输入验证与清洁。对所有用户输入进行严格的验证和清洁，防止SQL注入、跨站脚本（XSS）等攻击。此外要遵循最小化权限原则：在软件设计中实施最小化权限原则，确保每个组件或服务仅具有完成其功能所需的最小权限。再者是错误处理与日志记录：实施恰当的错误处理和日志记录机制，以便及时检测和响应潜在的安全事件。

3.2.2 代码审计流程

一是确定审计目标和范围：明确审计的目的是发现潜在的安全漏洞、错误或不合规的编码实践，并确定审计的具体范围，如特定的应用程序、系统或代码库。二是制定审计计划：根据审计目标和范围，制定详细的审计计划，包括审计方法（如手动审查、自动化工具等）、时间表和资源分配。三是实施审计：按照计划进行代码审计，记录所有的问题和发现。这可能包括对源代码的逐行审查、函数和方法的分析，以及对安全最佳实践的遵守情况。四是报告与修复：在审计结束后，提供详细的审计报告，并指出需要修复的问题。开发团队应根据报告及时修复发现的安全问题。

3.2.3 软件漏洞管理与修复机制

第一，建立完善的漏洞管理流程，包括漏洞的发现、报告、验证、修复和验证等环节。确保每个漏洞都能得到及时有效的处理。第二，使用自动化工具定期扫描软件系统，以发现潜在的安全漏洞。同时，对扫描结果进行评估，确定漏洞的严重性和修复优先级。第三，一旦发现安全漏洞，应立即启动修复流程。修复过程中要确保修复措施的有效性和安全性，并在修复后进行充分的测试以确保系统的稳定性。第四，在软件运行过程中持续监控安全状况，并根据新的安全威胁和漏洞情报及时更新安全策略和防护措施。

3.3 网络通信层面的安全保障

3.3.1 车载网络通信的加密与认证技术

加密技术方面：采用高级的加密算法（如AES、RSA等），对车载网络通信中的数据进行加密，确保数据的机密性和完整性。实施端到端的加密策略，保证数据在传输过程中的安全性，即使数据被截获，也无法被轻易解密。认证技术方面：利用公钥基础设施（PKI）进行身份认证，确保通信双方的身份真实有效。通过数字签名技术验证信息的完整性和真实性，防止数据在传输过程中被篡改。

3.3.2 防止网络攻击与入侵的检测与防御系统

（1）入侵检测系统（IDS）：部署IDS以实时监控网络流量，检测异常行为和潜在的攻击模式。IDS能够识别并报告任何可疑活动，为安全团队提供及时的警报和响应机会。（2）入侵防御系统（IPS）：与IDS相比，IPS不仅能检测攻击，还能主动阻止或减轻攻击的影响。IPS可以配置为自动阻断恶意流量或隔离受感染的系统，防

止攻击扩散。（3）防火墙与访问控制：利用防火墙技术过滤不安全的网络流量，阻止未经授权的访问。实施严格的访问控制策略，确保只有经过授权的设备和服务才能访问车载网络。（4）持续的安全监控与更新：建立安全运营中心（SOC），持续监控网络安全状况，及时发现并响应安全事件[4]。定期更新安全策略和防护措施，以适应不断变化的威胁环境。

4 信息安全管理体系的认证与实践

4.1 国内外信息安全认证标准与流程

4.1.1 国内外主要的信息安全认证要求对比

在中国，信息安全产品的认证主要依据《信息安全技术网络安全等级保护管理办法》等国家标准。需要通过国家信息安全测评中心（CNITSEC）等权威机构的测试和评估。人员资质认证方面，有注册信息安全员（CISM）和注册信息安全专业人员（CISP）等认证体系。国际上，常见的信息安全认证标准包括ISO 27001（信息安全管理体系）和ISO 15408（通用标准化评估方法）等。这些标准被广泛应用于全球各种信息系统的评估与认证。

4.1.2 认证流程的具体步骤与注意事项

具体步骤：（1）申请阶段：根据相关认证机构的要求，准备详细的申请资料，包括产品介绍、技术文档等，并缴纳相关费用。（2）测试和评估阶段：产品需送往认证机构或授权的测试实验室进行功能、性能、安全性等多方面的测试。此阶段需要提供产品的设计文档、源代码等材料。（3）认证阶段：测试通过后，提交评估报告和其他所需资料给认证委员会进行审核。审核通过后，将进行认证决策。（4）颁发证书阶段：如果产品通过所有评估和测试，认证委员会将颁发认证证书，标明产品的认证类别和有效期限等信息。

在整个认证过程中，应严格遵守保密协议，确保产品信息和相关资料的保密性。申请人需要密切配合认证机构的工作，及时提供所需资料和响应测试评估过程中的问题。认证证书具有时效性，通常有效期为一年。在证书到期前，应重新进行测试和评估，以确保产品持续符合认证要求。

4.2 认证的价值与意义

4.2.1 认证对汽车企业品牌形象与市场信任度的影响

通过获得信息安全管理体系认证，汽车企业能够展示其对信息安全的高度重视和承诺，从而提升品牌形象。这种认证相当于一个权威的“标签”，能够增强消费者和合作伙伴对企业的信任。信息安全管理体系认证是由独立的第三方机构进行的，具有客观性和公正性。因此，获得认证的汽车企业在市场上会更容易获得消费者的信任和认可。

4.2.2 认证在促进汽车技术研发与管理体系完善中的作用

一是推动技术研发创新：为了达到信息安全管理体系认证的标准，汽车企业可能需要对现有的技术架构和系统进行升级或改进。这一过程往往会激发企业的技术研发创新，推动企业在信息安全领域的技术进步。二是完善管理体系：信息安全管理体系认证要求企业建立一套完整的信息安全管理制度和流程。这不仅有助于企业更好地保护敏感数据和客户信息，还能促进企业内部管理体系的完善和规范。通过认证过程，企业可以发现并修正管理中存在的漏洞和不足，从而提高整体运营效率。三是增强风险应对能力：信息安全管理体系认证强调对潜在信息安全风险的识别、评估和控制。通过这一认证过程，汽车企业能够提升自身的风险应对能力，确保在面临各种信息安全威胁时能够迅速、有效地作出反应。

结语

本研究探讨了国内外信息安全法规与标准，汽车信息安全核心能力的构建，多层次的信息安全保障策略，以及信息安全管理体系的认证与实践。通过对比分析、技术研发、策略制定及认证流程的梳理，为汽车行业提供了一套全面的信息安全保障方案。这不仅有助于提升汽车企业的品牌形象和市场信任度，还能推动技术研发与管理体系的持续完善，为智能网联汽车的健康发展和社会公共安全提供坚实保障。

参考文献

[1]蔡方博,李钰莹.智能网联汽车信息安全风险研究[J].智能网联汽车,2024,(02):72-74.

[2]严锦伟,郭秋华,李冀,等.汽车企业研发机构信息安全体系构建方法研究[J].重型汽车,2023,(04):38-40.

[3]贾文伟.汽车控制芯片信息安全技术研究[J].汽车科技,2023,(05):81-86.

[4]史宁,高荣刚,李景剑.汽车产品信息安全认证关键技术研究[J].汽车工业研究,2018,(11):33-35.