基于智能网联汽车质量与安全要求的全融合研发体系研究

蔡丛

（南京航空航天大学计算机科学与技术学院，南京 210012）

【欢迎引用】蔡丛. 基于智能网联汽车质量与安全要求的全融合研发体系研究[J]. 汽车文摘，2025(3): 32-36.

【Cite this paper】CAI C, Research on Integrated R&D System Based on Quality and Safety Requirements of Intelligent and Connected Vehicles[J]. Automotive Digest (Chinese), 2025(3): 32-36.

【摘要】为了满足车规级质量与安全要求，同时降低实施质量和安全流程体系的复杂度和研发成本，探讨了基于汽车软件开发全过程，融合实施汽车软件过程改进及能力评定、功能安全、预期功能安全、信息安全等研发体系的方法，提出了一种基于智能网联汽车质量与安全要求的全融合研发体系方法，采用该方法可以降低智能网联汽车质量与安全开发难度和成本。

关键词：质量；ASPICE；功能安全；预期功能安全；信息安全；软件工程

中图分类号：U461.91　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20240251

Research on Integrated R&D System Based on Quality and Safety Requirements of Intelligent and Connected Vehicles

Cai Cong

（School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210012）

【Abstract】In order to meet the requirements of vehicle quality and safety, and reduce the complexity and Research and Development(R&D) cost of implementing quality and safety process system, this paper discusses the method of integrated implementation of Automotive Software Process Improvement and Capability Determination(ASPICE), Functional safety, Safety of the intended functionality, Security and other R&D systems based on the whole process of automotive software development. A fully integrated research and development system method based on the quality and safety requirements of intelligent networked vehicles is proposed. It reduces the difficulty and cost of quality and safety development of intelligent networked vehicles.

Key words: Quality, ASPICE, Functional safety, Safety of the intended functionality, Security, Software engineering

0　引言

随着智能网联汽车的发展，汽车电子系统日益复杂，单台车辆可能包含超过1亿行代码，配备多达100个电子控制单元[1-2]。汽车代码量的增加和软件复杂度的提升，显著增加了产品的安全和质量风险。当前集中化和域融合的智能网联汽车行业发展趋势进一步加剧了汽车软件复杂度，对智能网联汽车的质量与安全性提出了更为严峻的挑战[3-4]。此外，汽车高度智能化、网联化带来新的安全要求，功能安全、预期功能安全、信息安全和网络安全成为智能网联汽车安全性的关键要素[5-7]。

我国工业和信息化部明确智能网联汽车生产企业及产品准入的安全保障能力要求包括功能安全保障、预期功能安全保障、网络安全保障、数据安全保障、软件升级管理、风险与突发事件管理[8]。我国正加快建设智能网联汽车标准体系，2025年，系统修订智能网联汽车相关标准超过100项，贯穿功能安全、预期功能安全、网络安全和数据安全等安全标准，满足智能网联汽车技术、产业发展和政府管理对标准化的需

求[9-10]。在汽车质量与安全融合方面，主要为面向被动安全技术、新能源安全技术、主动安全技术及其相关的功能安全、预期功能安全融合关系的研究[11]，以及面向单个开发过程如软件单元测试、配置管理等，将汽车软件开发流程与功能安全融合实施的研究[12-13]，但是面向汽车软件开发全过程的、全体系的质量与安全标准融合方法研究较少。本文探讨了汽车软件过程改进及能力评定（Automotive Software Process Improvement and Capacity Determination，ASPICE）、功能安全、预期功能安全、信息安全等研发标准体系融合方法，以期对智能网联汽车满足繁杂的质量与安全标准研发要求，降低研发成本，提供指导与支持。

1 国际、国内智能网联汽车研发体系

汽车质量和安全问题是汽车研发体系关注的重点，为了确保软件产品的可靠性，国际、国内制定了ASPICE、功能安全、信息安全以及预期功能安全标准体系。

（1）ASPICE。ASPICE是一种满足高质量开发要求的汽车软件过程改进及能力评定的过程参考模型和过程评估模型，其起源于1994年的ISO/IEC 15504《信息技术-软件过程评估》（Information Technology-Software Process Assessment）系列标准[14]。2005年，由德国汽车行业联合会针对汽车行业，从ISO体系中分离，独立运营并发展成为现在的ASPICE。ASPICE为奥迪、宝马、大众以及通用等欧美主要汽车制造商对软件供应商的准入要求。供应商必须达到ASPICE二级水平才可以进入其供应商体系。最新版本的ASPICE于2023年发布，在原有基础上扩展了硬件和人工智能等领域过程要求。

（2）功能安全。功能安全旨在管理由电子电气系统失效导致的危害，以减少不合理风险。该概念贯穿产品整个生命周期，包括需求设计、生产、运行、维修和报废阶段，目的是最大程度降低由软件、硬件和系统导致的安全隐患。ISO 26262《道路车辆-功能安全》（Road Vehicles- Functional Safety）系列标准[15]已成为欧洲主要汽车制造商以及国内大型整车企业对安全强相关的软件和硬件产品的准入要求。在新能源电子电气与辅助驾驶等领域，ISO 26262趋于强制应用，国内对应标准为GB/T 34590《道路车辆-功能安全》[16]。

（3）信息安全。信息安全是指保护车辆和车辆中的电子系统免受未经授权的访问、使用、披露、干扰和破坏的威胁，目标保护财产、隐私信息以及生命安全，其所需应对的威胁和攻击具有不可预测及动态的特性。ISO/SAE 21434《道路车辆-网络安全工程》（Road Vehicles-Cybersecurity Engineering）标准[17]于2021年正式发布，对应的全局性标准为2005年正式发布的ISO/IEC 15408《信息安全 网络安全和隐私保护信息技术安全评估准则》（Information Security-Cybersecurity and Privacy Protection-Evaluation Criteria for IT Security）系列标准[18]。

（4）预期功能安全。预期功能安全是指不存在由于预期功能不足或人为的合理可预见的误用所引起的危害造成的不合理风险。预期功能安全关注系统功能的可靠性，确保系统在发生故障或异常情况时仍保持安全，其强调在充满变量的环境中，系统执行其预期功能时保持安全的能力。ISO 21448《道路车辆-预期功能安全》（Road vehicles- Safety of The Intended Functionality）标准[19]于2022年发布。

ASPICE、功能安全、信息安全以及预期功能安全构成了国际汽车行业广泛认可的智能汽车软硬件研发流程标准，近年来在我国汽车企业得到了大力推广和应用。

2 智能网联汽车质量与安全风险分析

由于面向问题场景和发展历程存在差异，ASPICE、功能安全、信息安全以及预期功能安全标准形成了相对独立的标准体系，本节将基于智能网联汽车产品内部和外部质量安全风险对上述标准进行详细分析。

2.1 内部风险分析

产品内部面临的主要风险来自功能失效和功能不足。功能失效是指汽车整车、主要系统或零部件在规定的条件下和规定的时间内，因某种原因（如损坏、老化和设计缺陷）丧失原定功能。功能失效风险可分为产品系统性失效风险和硬件随机失效风险。系统性失效可以通过设计变更消除，其涉及的对象既包括硬件也包括软件。软件中的缺陷、硬件元器件的参数设计或选择错误均属于系统性失效范畴。该失效模式与产品设计、制造或操作中的错误紧密相关，因此，通过改进设计、优化流程等措施，可以有效降低系统性失效的风险。硬件随机失效是指在硬件要素的生命周期中，非预期发生并服从概率分布的失效，其具有偶发性且不可避免，影响对象仅限于硬件。内存数据位翻转、电阻开路、短路或阻值漂移等现象均属于

硬件随机失效。该类失效主要由物理因素导致(如腐蚀、热应力和老化),难以完全避免,但可以通过加强质量控制或采用可靠性工程的方法降低发生概率。系统性失效和硬件随机失效是软件开发和硬件设计中必须考虑的重要因素。通过深入理解上述失效模式并采取相应措施可以降低风险,显著提高产品质量和可靠性。

功能不足风险主要是指由于系统设计或性能局限性,系统可能无法在所有预期的工作环境和条件下正常运作,进而可能引发安全事故。尽管系统在大多数情况下可以正常运行,但在某些特定情况下(如极端天气条件、特殊的交通流场景或其他非寻常的操作环境中),系统可能表现出无法做出正确判断或响应的缺陷。该局限性不仅可能降低系统整体效能,还可能直接导致潜在安全风险,对人身和财产安全构成威胁。为确保系统功能完备性,最大限度地降低功能不足风险并保障预期功能安全,在设计和开发阶段必须综合考虑并测试系统在预期和非预期情况下的表现,有效识别并缓解潜在功能不足问题,确保系统维持其安全性和可靠性。

2.2 外部风险分析

产品外部风险主要可以分为有意攻击风险和误用风险。有意攻击风险包括未经授权的访问、使用、披露、干扰和破坏,造成网络攻击风险和数据泄露风险。网络攻击风险方面,黑客可能通过网络攻击对智能网联汽车进行恶意操控(如恶意起动汽车或紧急制动等行为),威胁车辆和驾驶者的安全。此类攻击利用了智能网联汽车与外部网络通信的特性,通过渗透系统安全防护,实现对车辆的非法控制。数据泄露风险方面,智能网联汽车在运行过程中将产生大量用户数据,包括位置信息、驾驶习惯等敏感信息。若这些数据未得到妥善保护,将面临被黑客获取和滥用的风险。为了应对风险,可以采取以下安全措施:加强智能网联汽车的网络安全防护,包括使用防火墙、入侵检测系统等技术手段,防止黑客的渗透和攻击。对用户数据进行加密存储和传输,确保即使数据被窃取也无法被轻易解密和利用。定期进行安全漏洞扫描和修复,及时更新系统和应用程序,以修补已知的安全漏洞,降低被攻击的风险。

误用风险是指由于驾驶人员以制造商不期望的方式使用汽车系统可能引发的危害和不合理风险。这种误用可能源于对系统性能的过度信心,或者未按照系统的指定要求来操作车辆。误用风险涉及用户或操作人员对系统的误操作。例如,若用户在驾驶过程中错误地激活了自动驾驶模式,而在该模式下车辆无法应对当前的交通状况或道路环境,将有可能引发交通事故。同样,若用户在不了解系统限制和条件的情况下,过度依赖自动驾驶系统的某些功能,也可能会在遇到突发情况时无法做出正确的判断和应对,进而危及行车安全。为了降低误用风险,提高预期功能安全性,可以采取以下措施:加强用户培训和教育,提高用户对系统的理解和操作能力。优化系统设计,使其更加符合用户的认知习惯和操作逻辑。加强系统监控和预警机制,及时发现和纠正用户的误操作行为。通过实施以上措施,可以有效降低误用风险,提升系统整体安全性。

综上所述,包含功能失效、功能不足、误用以及有意攻击在内的产品内、外部风险是智能网联汽车产品必须解决的问题。为满足智能网联汽车安全与质量要求,建立解决上述问题的研发体系不可或缺。由于智能网联汽车标准体系的多样性和差异性,企业在实施过程中需投入专业团队和研发资源,增加了企业研发成本负担。为满足车规级质量与安全要求,建立融合执行质量与安全的研发体系已成为智能网联汽车行业的必然需求与重大挑战。

4 智能网联汽车质量与安全研发体系框架

功能安全体系旨在解决产品由于系统性失效和随机硬件失效引起的功能失效风险,预期功能安全体系旨在解决产品的功能不足风险和误用风险,信息安全体系旨在解决包含网络攻击风险和数据泄露风险的有意攻击风险,包含 ASPICE 在内的质量体系是以上体系实施的基础。ASPICE、功能安全、信息安全、预期功能安全标准体系分别针对各类风险提出了系统的理论框架和方法论。在此基础上,本研究提出了一套满足车规级要求的智能网联研发体系框架,如图 1 所示。

5 基于智能网联汽车质量与安全要求的全融合研发体系架构

ASPICE 包含 264 条基本实践,ISO 26262 系列标准需求超 1 000 条。此外考虑到信息安全和预期功能安全的实施,整体工作量巨大。通过对比分析 ISO 26262 和 ASPICE 流程过程概览,发现 ASPICE 与功能安全流程均基于软件工程和系统工程的 V 模型开发流程。最新发布的 ASPICE 加入硬件工程过程

后，其在系统工程过程、软件工程过程、硬件工程过程、支持过程以及确认过程，均支持ISO 26262流程过程的实施，覆盖了ISO 26262总流程过程的70%以上。

基于软件工程和系统工程的V模型开发流程，对ASPICE、功能安全、信息安全流程和预期功能安全流程进行融合，通过实践验证，提出基于ASPICE、功能安全、信息安全以及预期功能安全等全体系融合架构，如图2所示。

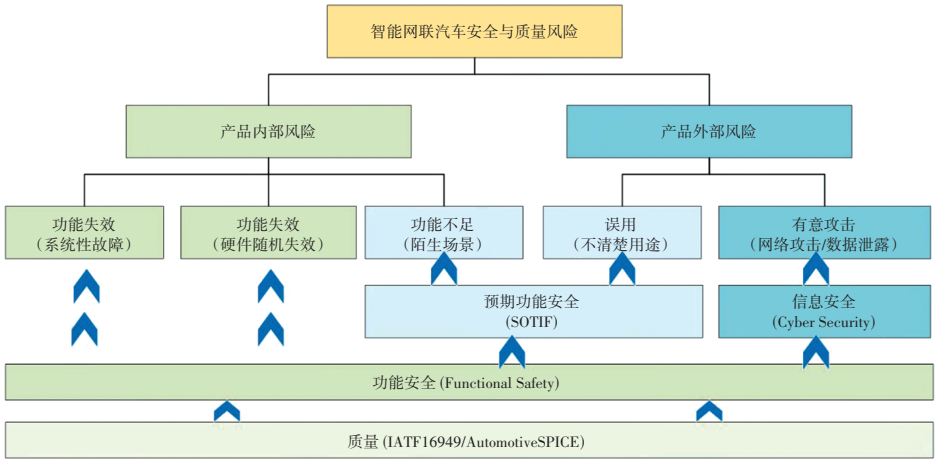

图1　满足车规级要求的智能网联研发体系框架

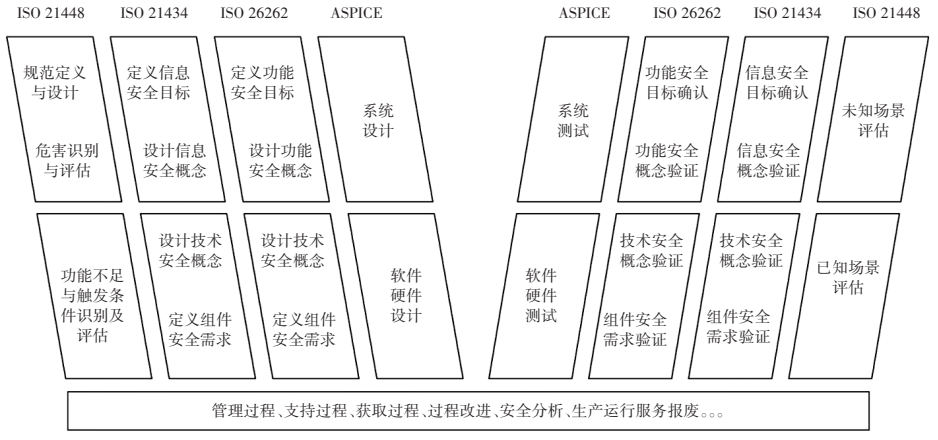

图2　基于智能网联汽车质量与安全要求的全融合研发体系架构

基于ASPICE，将开发过程分为4个阶段：系统设计阶段、软件硬件设计阶段、软件硬件测试阶段以及系统测试阶段。在系统设计阶段，对于功能安全开发和信息安全开发，开展安全目标定义和安全概念设计工作。对于预期功能安全开发，开展功能规范定义设计与危害识别评估工作。在软件硬件设计阶段，对于功能安全开发和信息安全开发开展技术安全概念设计和组件安全需求定义工作。对于预期功能安全开发，开展功能不足与触发条件识别及评估工作。在软件硬件测试阶段，对于功能安全开发和信息安全开发，开展组件安全需求验证和技术安全概念验证工作，对于预期功能安全开发，开展已知场景评估工作。在系统测试阶段，对于功能安全开发和信息安全开发，开展安全概念验证和安全目标确认工作，对于预期功能安全开发，开展未知场景评估工作。

V模型开发流程基础主要包括管理过程（项目管理、风险管理、度量、复用管理）、支持过程（质量保证、配置管理、问题解决管理、变更管理、数据管理）、获取过程（供应商监控）、安全分析过程（功能安全分析、预期功能安全分析、信息安全分析）、生产运行服务报废过程以及过程改进。上述过程共同支撑V模型开发流程的各阶段运行，确保产品质量。

该融合体系已应用于某智能制动系统产品开发项目。项目软件测试分析报告表明，软件静态分析遵循了国际机动车工业软件可靠性联盟（The Motor Industry Software Reliability Association，MISRA）的C语言编码规范，其中强制性及必需类别的测试缺陷数量为0。在软件测试阶段，测试通过率为100%，并且软件分支覆盖率、修正判定条件覆盖率、函数覆盖率与函数调用覆盖率均达到功能安全汽车安全完整性

等级（Automotive Safety Integrity Level，ASIL）最高等级D级要求。此外，该产品公司内部评审满足ASPICE L2级要求，研发周期缩短了4个月。同时该项目还通过了第三方认证机构评审，获得了功能安全ASIL最高等级D级产品认证，产品质量与安全性能明显提高，市场竞争力大幅提升。

6 结束语

本研究基于智能网联汽车流程体系的独特视角，深入研究智能网联汽车研发适用的全部质量与安全标准体系，基于V模型开发全流程，提出一套满足智能网联汽车质量与安全要求的全融合研发体系架构，以融合实施ASPICE、功能安全、预期功能安全、信息安全等研发体系，不仅满足了车规级质量与安全要求，还有效降低了研发成本，提高了研发效率，这是对业界研究的重要补充和发展。

然而，本研究在全融合研发体系的应用细节和优化方面仍有待进一步实践验证。同时，随着智能网联汽车技术的不断发展，新的安全和质量挑战将不断涌现，如何持续更新和优化全融合研发体系以应对这些挑战，将成为未来研究的关键方向。

参 考 文 献

[1] MCCONNELL S. Code Complete: A Practical Handbook of Software Construction[M]. 电子工业出版社, 2004.

[2] KOLHAPURKAR A , KAISERSLAUTERN U O. Functional Safety: ISO26262[S]. [2024-12-24].

[3] 董碧成, 石春, 吴刚. 基于AUTOSAR的电动汽车中央控制单元CAN通信软件开发[J]. 仪表技术, 2021(4): 65-67.

[4] 高庆, 陈静, 许平, 等. 工业嵌入式软件开发安全漏洞模式研究[J]. 信息安全研究, 2022(6): 595-604.

[5] 李骏. 中国预期功能安全的挑战与解决方案 [J]. 智能网联汽车, 2021(05): 12-13.

[6] 张云, 李茹, 焦伟赟, 等. 自动驾驶功能安全标准化研究[J]. 中国标准化, 2020(11): 109-112.

[7] 张骁, 陈海龙, 杨思佳, 等. 自动驾驶网络安全政策与标准化研究[J]. 中国信息安全, 2024(2): 26-29.

[8] 工业和信息化部. 工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见（工信部通装〔2021〕103号）[J]. 科学与信息化, 2021(24): 6-8.

[9] 刘丽亚, 宋琨, 孔晓霜, 等. 智能网联汽车标准体系建设概述[J]. 汽车文摘, 2019(3):13-15.

[10] 吴胜男, 朱云尧, 杨志成, 等. 我国智能网联汽车产业管理体系与思路研究[J]. 汽车文摘, 2022(10): 1-5.

[11] 杨帅, 张金换, 钱占伟, 等. 汽车安全多领域融合的研究与展望[J]. 汽车安全与节能学报, 2022(1): 29-47.

[12] 王爱菲, 禹营, 刘雯. ASPICE和ISO 26262标准要求的软件单元验证实践[J]. 质量与认证, 2021(11): 57-60.

[13] 曹旭, 王璐洋. 一种适用于功能安全和ASPICE流程实施的配置管理策略[J]. 质量与认证, 2021(11): 64-67.

[14] ISO. Information Technology-Software Process Assessment: ISO/IEC 15504: 2012[S]. ISO. 2012.

[15] ISO. Road vehicles-Functional safety: ISO 26262: 2018[S]. ISO. 2018.

[16] 中国国家标准化管理委员会. 道路车辆 功能安全: GB/T 34590-2022[S]. 北京: 中国标准出版社, 2022.

[17] ISO. Road Vehicles-Cybersecurity Engineering: ISO/SAE 21434: 2021[S]. ISO. 2021.

[18] ISO. Information Security-Cybersecurity and Privacy Protection-Evaluation Criteria for IT Security: ISO/IEC 15408: 2022[S]. ISO.2022.

[19] ISO. Road vehicles-Safety of The Intended Functionality: ISO 21448: 2022[S]. ISO.2022.

（责任编辑 **梵玲**）