新能源汽车整车控制软件的功能安全与信息安全协同防护策略

黄 丹 雷 强
吉利汽车研究院（宁波）有限公司 浙江 宁波 315000

摘 要：随着汽车智能化、网联化和电动化的深度融合，新能源汽车的整车控制软件（Vehicle Control Unit, VCU）已从传统的机械控制单元演变为一个高度复杂、深度互联的网络物理系统（CPS）核心。这一转变使得功能安全与信息安全两大风险维度前所未有地交织在一起。传统的、各自为政的安全防护体系已无法应对由网络攻击引发的功能失效等新型复合型威胁。本文深入剖析了新能源汽车VCU软件在功能安全与信息安全方面面临的独特挑战，揭示了二者之间存在的内在耦合关系与潜在冲突。在此基础上，创新性地提出了一套贯穿系统全生命周期的“协同防护”策略框架。该框架强调在概念设计、系统架构、软件开发、集成测试及运行维护等各个阶段，同步考虑并融合功能安全与信息安全的需求，通过构建统一的风险评估模型、设计具备纵深防御能力的软硬件架构、采用形式化验证与模糊测试相结合的验证方法，以及建立实时联动的监控与响应机制，实现对复合型威胁的有效抵御。研究表明，唯有打破功能安全与信息安全之间的壁垒，实施协同防护，才能从根本上保障新能源汽车在复杂网络环境下的可靠、可信运行。

关键词：新能源汽车；整车控制软件；功能安全；信息安全；协同防护

引言

全球碳中和推动下，新能源汽车产业迅猛发展。整车控制软件（VCU）作为“大脑”，协调管理多个关键子系统，其决策关乎车辆性能与驾乘人员安全。随着V2X、OTA等技术普及，VCU软件网络暴露面扩大，成为网络攻击高价值目标。国际标准ISO 26262提供功能安全开发流程，新兴标准ISO/SAE 21434聚焦防范网络攻击。但实践中，功能安全与信息安全团队常割裂处理问题，存在致命缺陷，如攻击者入侵车载信息娱乐系统后渗透到VCU，篡改扭矩输出指令致车辆失控，既是安全漏洞也是功能安全失效。因此，在新能源汽车VCU软件开发与运维中，有效协同功能安全与信息安全，构建综合防护体系，是行业亟待解决的核心课题，本文将探讨并提出协同防护策略。

1 新能源汽车 VCU 软件的安全挑战与耦合分析

要制定有效的协同策略，必须首先厘清VCU软件面临的安全挑战及其内在关联。

1.1 功能安全的独特挑战

新能源汽车VCU的功能安全风险相较于传统燃油车更为突出。其核心在于能量流的高度电气化与集中化。VCU需要实时、精确地管理高压动力电池的能量输出与回收。任何软件层面的逻辑错误或时序紊乱，都可能引发一系列连锁反应。例如，若VCU在再生制动过程中错误地计算了电机的回馈扭矩，可能导致电池过充，触发热失控甚至起火爆炸[1]。同样，在加速过程中，若扭矩分配算法出现偏差，可能造成驱动轮打滑，严重影响车辆稳定性。这些危害场景的严重度（S）和可控度（C）通常被评估为最高级别（ASIL D），对软件的可靠性提出了极致要求。

1.2 信息安全的严峻威胁

VCU的信息安全威胁主要源于其日益增长的网络连接性。攻击面遍布多个入口：通过OBD-II诊断接口的物理接入、利用蓝牙/Wi-Fi与手机配对的近场攻击、经由蜂窝网络进行的远程渗透，以及通过V2X通信接收的恶意消息。一旦攻击者突破外围防线，便可能对VCU发起多种攻击。典型的包括：注入攻击，向VCU发送伪造的传感器数据（如虚假的车速信号），诱使其做出错误决策；篡改攻击，直接修改VCU内存中的关键参数（如最大功率限制），使其超出安全边界；拒绝服务攻击，通过洪泛请求耗尽VCU的计算资源，导致其无法及时响应真实的控制指令。这些攻击的最终目的，往往是利用VCU的控制权限，制造物理世界的危害。

1.3 功能安全与信息安全的耦合与冲突

功能安全与信息安全并非简单的叠加关系，二者之间存在着深刻的耦合与潜在的冲突。耦合性体现在，信息安全事件是功能安全危害的一种新型诱因。一个原本

在功能安全分析中被认为“残余风险可接受”的系统，一旦引入网络攻击的可能性，其整体风险水平将急剧升高。反之，功能安全机制（如看门狗定时器）有时也能在无意中增加攻击者的难度。冲突性则更为棘手。例如，为了满足ASIL D级别的高可用性要求，系统可能会采用冗余设计，但这同时也增加了潜在的攻击面。再如，信息安全措施中的强加密和身份认证会引入额外的计算开销和通信延迟，这可能与功能安全对实时性（Timing）的严苛要求相矛盾。如何在保障安全的同时，不牺牲性能，是协同设计中必须权衡的关键问题。

2 协同防护策略框架

针对上述挑战，本文提出一个覆盖系统全生命周期的协同防护策略框架，其核心思想是“同步规划、融合设计、联合验证、联动响应”。

2.1 统一的风险评估与管理（TARA + HARA）

协同防护的起点是统一的风险评估。传统的危害分析与风险评估（HARA）专注于识别因功能失效导致的危害，并确定相应的ASIL等级。而威胁分析与风险评估（TARA）则用于识别潜在的网络威胁及其影响。协同策略要求将这两种分析过程深度融合[2]。具体而言，在进行HARA时，应主动考虑“被网络攻击”作为一种新的、独立的危害诱因。例如，对于“非预期加速”这一危害事件，其诱因不仅要包括传感器故障、软件bug，还必须明确包含“VCU接收并执行了来自攻击者的恶意加速指令”。通过这种整合，可以生成一个更全面的危害-威胁矩阵，并据此为每个资产（如VCU的扭矩控制功能）同时分配ASIL等级和网络安全等级（CAL），为后续的设计提供统一的输入。

2.2 融合式系统架构设计

在系统架构层面，必须摒弃“先做功能安全，再打信息安全补丁”的旧思路，转而采用一种原生融合的设计方法。为此，可以构建“1+3+4”的立体化纵深防御体系。该体系以1个核心——硬件信任根（Root of Trust）为基础，在VCU的微控制器（MCU）中集成硬件安全模块（HSM），作为整个安全体系的信任锚点，为安全引导（Secure Boot）提供保障，确保只有经过签名的、未被篡改的代码才能运行。体系的3大支柱——分区隔离、动态微隔离与物理层屏蔽，共同构筑了多层次的防护屏障。通过硬件内存保护单元（MPU）实现关键控制任务与非关键通信任务的严格分区隔离；利用软件定义的策略实施动态微隔离，限制服务间的横向移动；并辅以物理层屏蔽措施，抵御针对硬件接口的直接攻击。在此基础上，体系集成了4维能力：安全引导、认证加密、主动诱捕与实时检测。其中，安全引导建立了完整的信任链；在车内网络上对关键指令采用认证加密（AEAD）机制，确保其真实性与完整性；同时，通过部署主动诱捕机制来感知攻击意图，并结合实时检测技术对异常行为进行快速响应。这样的架构设计既保持了底层的硬件安全，又具备了上层的智能攻防，真正实现了功能安全与信息安全的深度融合。

2.3 协同的软件开发与验证

软件是安全策略落地的关键载体，其开发与验证过程必须体现协同思想。（1）安全编码规范：制定并强制执行同时涵盖功能安全（如MISRA C）和信息安全（如CERT C）的编码规范，从源头上减少漏洞。（2）形式化方法与模糊测试结合：对于ASIL等级高的核心控制算法，可采用形式化验证方法，数学化地证明其在所有可能输入下均能满足安全属性[3]。同时，对软件接口（特别是网络接口）进行大规模的模糊测试（Fuzz Testing），通过向其输入大量随机或畸形的数据，主动挖掘潜在的缓冲区溢出、空指针解引用等安全漏洞。这两种方法互为补充，前者保证逻辑正确性，后者发现实现缺陷。（3）端到端的安全测试：构建包含真实ECU和仿真环境的硬件在环（HIL）测试平台。在该平台上，不仅要测试功能安全场景（如模拟传感器失效），更要模拟真实的网络攻击场景（如注入恶意CAN报文），验证整个系统在复合威胁下的鲁棒性和安全机制的有效性。

2.4 运行时的联动监控与响应

车辆交付后，安全防护并未结束。需要建立一个运行时的联动机制。（1）入侵检测系统（IDS）与功能监控协同：在VCU中部署轻量级的入侵检测系统，持续监控网络流量和系统行为。当IDS检测到可疑活动（如异常的内存访问模式）时，不应仅记录日志，而应立即向功能安全监控模块发出警报。功能安全模块可根据预设的安全状态机，采取降级措施，例如将车辆动力限制在安全阈值内，或引导车辆进入安全停车状态，从而将信息安全事件的影响控制在功能安全的容错范围内[4]。（2）安全的OTA更新机制：OTA是修复漏洞的重要手段，但其本身也是一个高风险的攻击面。必须确保OTA过程的完整性和真实性，通过双签名、差分更新、回滚机制等多重保障，防止攻击者利用OTA通道植入恶意软件。

3 案例分析：协同防护在扭矩控制中的应用

为具体说明协同策略的有效性，我们以VCU中最核心的“扭矩控制”功能为例。该功能的ASIL等级通常为D级，其危害场景是“非预期加速”或“动力突然中断”。

3.1 统一风险评估

在HARA中，我们将“VCU接收并执行了伪造的加速踏板信号”明确列为“非预期加速”的危害诱因之一。通过TARA分析，确定攻击者可能通过入侵网关ECU来伪造此信号。综合评估后，该信号的传输路径被赋予高网络安全等级（CAL C）。

3.2 融合架构实现

在架构上，加速踏板信号的处理被置于一个由MPU严格保护的高安全域内。该域内的软件只能接收来自特定、经过认证的传感器源的数据。同时，VCU与网关之间的通信采用AUTOSAR SecOC（Secure Onboard Communication）标准，为每一个关键信号（包括踏板信号）附加一个基于共享密钥生成的消息认证码（MAC）。任何未经认证或被篡改的信号都将被接收方直接丢弃。

3.3 协同验证

在HIL测试中，测试用例不仅包括踏板传感器硬件失效，还包括模拟网关被攻破后发送伪造踏板信号的场景。测试结果表明，由于SecOC的保护，伪造信号被成功拦截，VCU的扭矩输出保持稳定，未发生非预期加速，验证了协同防护措施的有效性。

4 挑战与未来展望

尽管协同防护策略前景广阔，但在实践中仍面临诸多挑战。首先是人才的复合型缺口，既懂功能安全又精通信息安全的工程师极为稀缺。其次是工具链的整合难题，目前支持ISO 26262和ISO/SAE 21434协同开发的成熟工具尚不普及。此外，如何量化协同防护带来的安全增益，以证明其投入产出比，也是企业决策层关心的问题。展望未来，随着人工智能在汽车领域的应用，AI模型本身的安全性（包括对抗样本攻击）将成为新的协同防护焦点。同时，基于零信任架构（Zero Trust Architecture）的理念，未来的汽车安全体系将不再默认信任任何内部组件，而是对每一次访问请求都进行严格的身份和权限验证，这将进一步深化功能安全与信息安全的融合。最终，构建一个自适应、自学习、自愈合的智能汽车安全生态系统，将是行业不懈追求的目标。

5 结语

新能源汽车的快速发展将整车控制软件推向了安全风暴的中心。功能安全与信息安全不再是两个可以独立考量的维度，而是紧密交织、相互影响的统一体。本文提出的协同防护策略，通过统一风险评估、融合系统架构、协同软件验证和联动运行时响应，为破解这一难题提供了系统性的解决方案。该策略的核心在于打破专业壁垒，在产品开发的每一个环节都同步思考“防故障”与“御攻击”的双重需求。实践证明，唯有如此，才能构筑起真正坚固的防线，确保新能源汽车在享受智能化、网联化红利的同时，始终将用户的生命安全置于最高优先级。未来的研究与实践应继续深化这一协同理念，推动相关标准、工具和人才的协同发展，共同迎接智能网联汽车时代的安全挑战。

参考文献

[1]李翠萍,张巧.智能网联汽车软件安全治理国际化启示[J].中国信息安全,2025,(04):70-73.

[2]汽车产业要筑牢“软件安全”防线[N].第一财经日报,2025-07-09(A02).DOI:10.28207/n.cnki.ndycj.2025.002548.

[3]赵雄,方熙宇,邵文,等.汽车网络安全管理体系下的恶意软件防御技术研究[J].汽车知识,2025,25(12):254-256.

[4]方柯.智能网联汽车软件安全开发分析[J].时代汽车,2024,(13):22-24.