Embedded Technoloy and Intelligent Systems 嵌入式技术与智能系统, 2025, 2(4), 268-275
Published Online August 2025 in Hans. https://www.hanspub.org/journal/etis
https://doi.org/10.12677/etis.2025.24025

嵌入式系统安全与可信技术发展趋势

张凯龙[1]，马萌旭[1]，何周灿[1]，樊弈辰[1]，周世钰[2]，闫琳珊[1]

[1]西北工业大学软件学院，陕西 西安
[2]西北工业大学国家卓越工程师学院，陕西 西安

收稿日期：2025年10月28日；录用日期：2025年11月20日；发布日期：2025年12月1日

摘　要

作为信息世界与物理世界的桥梁，嵌入式系统发展呈现出网络化、智能化、协同化发展特征与趋势，其安全、可信问题日益突出。首先分析、讨论了面向嵌入式系统的安全、可信计算体系与技术。进而，重点从国内与国外、学术与技术、可信本体与计算架构等多个维度，对增强、提升嵌入式系统安全、可信性的相关理论与技术进展进行了梳理、分析与对照。

关键词

嵌入式系统，安全，可信计算，体系，技术，趋势

Development Trend of Security and Trusted Technologies for Embedded Systems

Kailong Zhang[1], Mengxu Ma[1], Zhoucan He[1], Yichen Fan[1], Shiyu Zhou[2], Linshan Yan[1]

[1]School of Software, Northwestern Polytechnical University, Xi'an Shaanxi
[2]National Institute of Excellence in Engineering, Northwestern Polytechnical University, Xi'an Shaanxi

Received: October 28, 2025; accepted: November 20, 2025; published: December 1, 2025

Abstract

As a bridge between the information world and the physical world, embedded systems are evolving toward greater connectivity, intelligence, and coordination, and their security and trustworthiness issues have become increasingly prominent. This paper first analyzes and discusses security and trusted computing frameworks and technologies tailored for embedded systems. It then systematically reviews, compares, and critically analyzes theoretical and technological advances for enhanc-

文章引用: 张凯龙, 马萌旭, 何周灿, 樊弈辰, 周世钰, 闫琳珊. 嵌入式系统安全与可信技术发展趋势[J]. 嵌入式技术与智能系统, 2025, 2(4): 268-275. DOI: 10.12677/etis.2025.24025

ing the security and trustworthiness of embedded systems from multiple perspectives—domestic and international, academic and industrial, and with respect to trust ontologies and computing architectures.

Keywords

Embedded Systems, Security, Trusted Computing, Architecture, Technologies, Trends

1. 引言

如我们所知，嵌入式系统日益广泛应用于工业控制、智能家居、医疗设备、航空航天、智能交通等诸多领域。同时，随着与物联网、人工智能等新兴技术的快速融合，嵌入式系统应用场景和规模不断扩大且日益呈现出突出的网络化、智能化、分布化、复杂化发展趋势，其安全性问题随之而来也日益突出。鉴于嵌入式系统连接信息、物理/社会的跨域融合特性，一旦在信息域遭受攻击或是计算系统出现故障，其信息域中产生的安全问题更会通过装备(如车辆、电力等实体)传递、放大到物理世界，产生危及生命财产安全乃至国家社会稳定的灾难性后果。

近年来，其已成为学术界和工业界关注的焦点[1]。据 WISE 统计，2023 年全球嵌入式安全市场规模为 49.7 亿美元，预计到 2032 年将达到 94 亿美元，2025~2032 年的复合年增长率为 7.32% [2]。根据 QYResearch 预测，2030 年全球可信计算芯片市场销售额预计将达到 22.9 亿元，年复合增长率为 5.2% (2024~2030) [3]。

2. 嵌入式系统可信体系分析

图 1 所示为面向嵌入式系统的可信技术体系。该体系构建了一个从底层硬件根基到上层应用安全的垂直信任链条。其基础始于最下层的可信根，该层内置了加密引擎和白名单管理等核心安全功能；在此之上构建可信硬件层，集成了量子安全引擎或 PUF 等物理级安全防护机制；向上延伸至虚拟化与分区隔离层，通过可信的虚拟机监视器(VMM)启动和管理机制，确保不同计算环境之间的严格隔离；进一步加固可信系统软件层，包含安全的 BootLoader 引导程序等组件，为上层运行提供可信软件基础；最终抵达顶层的应用安全层，实施如应用白名单等机制，保障具体应用程序的可信执行。在整个可信技术体系中，可信开发部署工具涵盖从可信根到软件层面，提供安全的开发框架与工具链，确保所有组件在开发阶段即内嵌安全能力，并在部署时按预期运行。可信升级依赖可信根存储版本元数据，并在升级后验证新组件的完整性，保障系统可持续演进，避免升级成为安全突破口。而可信启动则是自下而上逐步构建的，可确保系统从启动伊始即处于已知可信状态，抵御 Bootkit 等底层攻击。可信运行是在系统启动完成后，通过技术手段保障系统在持续运行过程中始终处于安全可信状态的动态防护机制。

基于 TPM 芯片内置加密引擎实现关键数据加密防护，通过系统/应用软件哈希值校验及权限管理机制，在启动或运行前完成软件完整性验证，例如操作系统内核哈希比对机制，以此构建计算环境初始信任源，确保仅合法未篡改软件及操作被允许执行，为系统可信运行奠定基础[4] [5]。可信硬件借助量子密钥分发与 PUF 安全引擎，前者实现通信加密，后者通过设备唯一身份识别抵御物理层攻击与仿冒，同时依托手机启动时系统镜像验证等安全引导机制，保障硬件启动过程中加载软件的完整性，有效解决硬件

层面加密通信、身份认证及启动安全问题，提升物理层抗攻击能力。虚拟化与分区隔离通过 VMware ESXi 等 VMM 可信启动机制，完成虚拟机监控程序完整性验证以保障启动安全，并实施云计算平台租户虚拟机资源隔离等可信管理措施，阻断恶意攻击与数据泄露的跨虚拟机传播路径，在多业务多用户场景下实现资源隔离与环境可信，确保虚拟化实体的独立性与安全性。可信系统软件层通过应用分区技术，实现功能模块安全隔离以阻断故障与攻击扩散链，同时依托安卓 SELinux 强制访问控制等安全内核机制，限制应用对系统资源的越权访问行为，全面强化应用隔离与内核安全，提升系统整体稳定性与防御能力。应用层安全体系采用企业 MDM 办公 APP 白名单审核机制，从源头限制非法应用运行，结合 TLS 加密交易数据传输等安全通信技术，构建覆盖访问控制、通信安全与新兴技术防御的立体防护网，直接保障用户业务操作的可信性与数据安全。

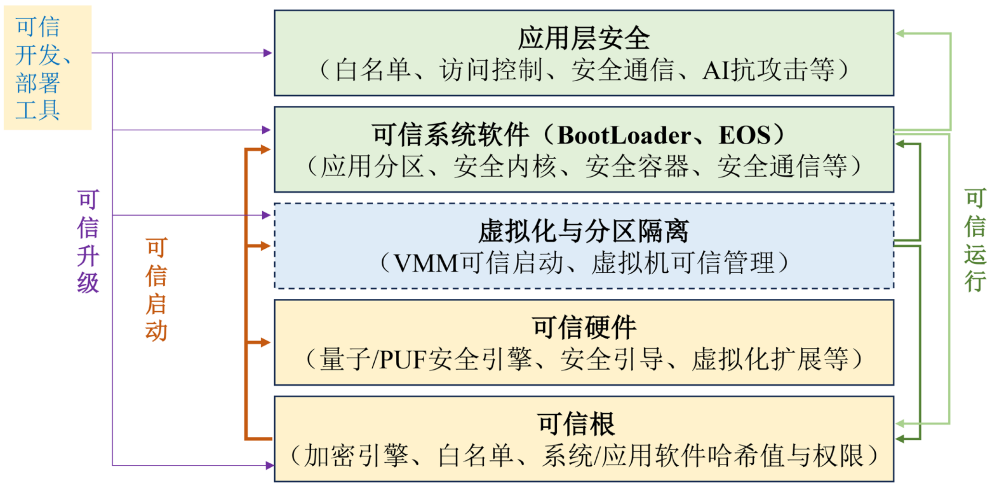

Figure 1. Architecture of trusted technology for embedded systems
图 1. 面向嵌入式系统的可信技术体系

以上策略为嵌入式系统安全提供了较为全面的保障，然而，现有的嵌入式系统安全解决方案仍面临诸多挑战。(1) 硬件安全机制虽然能够提供底层保障，但在面对复杂的攻击手段时，仍存在被绕过的风险。(2) 软件层面的安全措施如实时操作系统和微服务架构虽然增强了系统的灵活性和可靠性，但其复杂性也带来了新的安全漏洞和管理难度。(3) 工具链虽然在开发效率和代码质量方面发挥了重要作用，但在安全漏洞检测和修复方面仍存在不足。(4) AI 时代，复杂神经网络模型的不可解释性为嵌入式设备带来新的安全隐患，如代码篡改难以追溯等。(5) 5G、边缘计算等新兴技术与嵌入式系统的融合，可能带来新的安全需求，如终端设备数量与攻击面的扩大、数据隐私保护、边缘计算中的数据完整性和一致性等等。为此，在可信 3.0 的基础上，面向嵌入式系统日益呈现的云－边－端协同形态，进一步融合多端协同、零信任和保密计算的新一代计算架构进化出新的可信 4.0 计算体系。其特质在于，强调在多云－边－端融合环境中，通过硬件隔离、持续认证、动态策略和去中心化信任等手段，实现跨域、全生命周期、分级渐进的安全可信保障。

3. 国内研究现状

近年来，随着相关政策、项目的不断推进落地，对国内嵌入式系统安全发展起到了不可忽略的积极作用。由北京航空航天大学牵头，联合复旦大学、中山大学等多家单位协同攻关，旨在突破国内嵌入式智能计算软件关键技术，推动国产化智能芯片软件栈的持续完善，支持国产智能芯片生态建设[6]。由北

京和利时系统工程有限公司、中国科学院沈阳自动化研究所联合承担的国家“十二五”863 计划课题，针对工业测控系统的信息安全防护需求，突破可编程嵌入式电子设备开发与运行阶段的安全防护关键技术[7]。由华东师范大学牵头，与中国航发商发、中航工业 615 所、航天五院 502 所等单位合作，开发高安全嵌入式控制软件开发方法和支撑工具，成功应用于航空发动机控制软件研制、机载航空电子系统研制以及“嫦娥五号”探测器软件开发等重要任务[8]。此外，工业界也有一批嵌入式可信相关的军用、民用产品落地。2024 年华北工控研发的国产化可信嵌入式主板，集成系统级安全机制(密码加速引擎、抗物理攻击)，适配统信 UOS、银河麒麟等国产操作系统亮相军博会[9]。同年，国民技术研发并推出第四代可信计算芯片 NS350 系列，支持 SM2/SM3/SM4 国密算法，兼容 TPM 2.0，通过商用密码认证，适用于工业计算和嵌入式系统[10]。

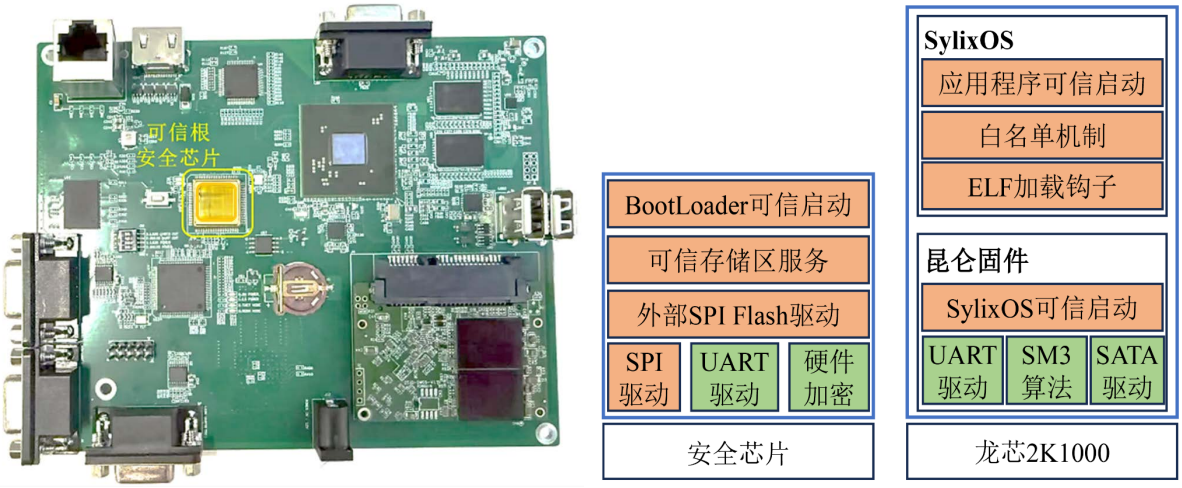

Figure 2. A trusted embedded platform developed by the authors' team on a domestically-developed software-hardware stack
图 2. 作者团队基于国产软硬件技术栈研制的可信嵌入式平台

针对嵌入式设备的安全启动需求，Zhao 等人[11]设计了一种轻量级的基于安全模块的可信启动方法，通过在嵌入式设备启动前验证预设信息，确保设备按照预定方式启动，并利用安全模块对启动过程中的数据完整性进行度量，从而实现可信嵌入式系统。为保证电力系统嵌入式装置能够安全可信启动，张翔等人[12]提出了一种基于可信平台控制模块(TPCM)的轻量型可信启动方法。Liu 等人[13]提出了一种将区块链的链上信任扩展到链下物理世界的框架，以可信疫苗追溯为例进行了实现，包含基于可信执行环境(TEE)的可信环境监测系统和一致性协议两部分。Ma 等人[14]从高可信嵌入式系统、人工智能嵌入式模型、智能芯片嵌入式操作系统三个方面展开，通过将区块链共识机制与特定方法结合来提升系统性能，设计异构计算平台和混合嵌入式训练系统，利用智能芯片增强功能并完成相关硬件设计。在基于量子计算的加密方法上，Yu 等人[15]研究了部分可信中继量子密钥分发(QKD)网络中的密钥分发路由问题，提出了一种基于协作路由的秘密密钥分发(SKP-CR)算法。Wang 等人[16]提出一种面向无 TPM 嵌入式智能设备的可信启动模型，以解决此类设备的安全启动及系统执行环境可信性问题。在航空航天领域，为了提升机载嵌入式计算机的安全防护能力，杨子怡等人[17]在将可信计算平台引入到机载计算机的基础上，设计并实现了基于机载嵌入式可信计算平台的安全配置管理系统。Yang 等人[18]提出基于区块链的 BC-UTSON 机制，通过 U-PBFT 共识、BMWSL 信任评估和 TPDR 可信路由技术，构建无人机群可信自组织网络以抵御内部恶意攻击并提升安全性。此外，基于可信 3.0 思想，作者团队面向特种装备可信需求，基于“自主可信根 + 龙芯 + 昆仑固件 + SylixOS”的全自主技术栈，研究并设计了一种基于双芯片架构的

可信执行环境，实现了可信启动、可信加载、可信运行、可信升级等核心能力，如图 2 所示。针对嵌入式系统混合部署与功能安全需求，何瑞琦等人[19]提出 DHR-OS 架构，在多核 CPU 上以 Linux 为主系统、动态部署 RTOS 从系统，利用 OpenAMP 实现通信及驱动复用、RPC 调用、中断路由等协同机制；设计调度–分发–裁决一体的安全执行机制，通过 Linux 池化 RTOS 核心、加权投票共识算法裁决任务结果。基于飞腾 D2000 的测试表明，该架构在差模/多模攻击下可靠性高，为嵌入式系统提供了兼具灵活性与抗攻击性的新方案。吉晨等人[20]提出基于轻量级虚拟化环境的可信多级安全容器机制，划分系统安全域并制定多级安全策略规则，通过形式化方法证明其安全性，利用联合文件系统技术和以 Docker 为代表的容器技术说明技术可行性，从来源和运行两方面保证可信性，可改善传统多级安全机制实用性差的问题。

4. 国外研究现状

STMicroelectronics 于 2023 年 9 月推出了一款新的安全微控制器，具备高级加密和认证功能，可有效保护物联网设备的安全[21]。一年后，该公司基于零信任安全模型，推出 STM32L5 系列 MCU，支持安全启动、硬件加密，功耗低至 33 nA [22]。Infineon Technologies AG 在 2023 年 2 月推出了 SECORA Connect 产品组合，包含小型芯片，适用于多种嵌入式设备[23]。此外，英特尔的 Gaudi 3 AI 加速器、至强 6 处理器液冷方案、酷睿 Ultra 系列均支持硬件级隔离(鲲鹏 TEE)、机密计算[24]。

Bognar 等人[25]以 SancusV 和 VRASED 系统为例，讨论了在嵌入式可信执行架构中，形式化方法证明的安全性与实际系统安全性之间的差距。Aaraj 等人[26]研究了在资源受限的嵌入式系统中实现 TPM 的硬件/软件协同设计，提出了一种基于软件的 TPM (SW-TPM)实现方案，通过在嵌入式处理器上执行受保护的代码域来实现 TPM 功能。Fedorov 等人[27]提出了一种基于隐藏软件代理和隐写术的方法，用于构建可信环境并保护信息系统免受内部攻击。在医疗设备的嵌入式系统可信认证方面，Gebreab 等人[28]提出了一种基于非同质化代币(NFT)的解决方案，用于确保翻新医疗器械的可信追溯和认证。该方案利用动态可组合的 NFT 作为医疗器械及其翻新过程的数字表示，通过将替换部件和认证文件嵌入到父子 NFT 层次结构中，并通过动态令牌的演变记录翻新步骤，从而实现对翻新医疗器械的认证、追踪和所有权管理。在新一代量子计算方面，Trochatos 等人[29]提出了一种量子计算机可信执行环境(QC-TEE)的硬件架构，旨在保护用户量子电路和数据免受诚实但好奇的云服务提供商的窥探。该架构通过在用户端软件添加诱饵控制脉冲混淆真实量子门操作，在量子计算机端的稀释制冷机内使用简单的 RF 开关衰减诱饵脉冲，并由硬件安全管理器控制开关。Phalak 等人[30]提出两种量子物理不可克隆函数(QuPUF)，以解决嵌入式设备量子计算中基于云平台的量子硬件安全与信任问题。面对 AI 时代对嵌入式系统安全冲击，Seng 等人[31]围绕嵌入式智能(EI)展开全面研究，指出其在安全、隐私和信任方面存在显著挑战，EI 服务器加速器和边缘设备在安全需求上可能存在差异。基于人工智能物联网(AIoT)的概念，Alkhoori 等人[32]讨论了 AI 决策与物联网设备结合的安全性挑战，被篡改的深度学习算法可能会操控 AIoT 的运行，进而威胁到整个系统的安全态势。此外，由于设备间持续进行通信和数据共享，保护这些信息免受泄露、篡改或中断至关重要。Raja 等人[33]提出 Secured UAV 模型，以 UAV 位置为输入、借助集中控制器形成无线网状网络，利用 A*搜索算法实现高效通信，并运用高级加密标准和 Blowfish 等加密技术及安全认证机制，保障多无人机通信的可信性与安全性，有效应对各类安全攻击。Nawshin 等人[34]提出 DP-RFECV-FNN 方法，将差分隐私与前馈神经网络结合，用于安卓恶意软件检测，遵循零信任安全模型对应用严格验证，在保障用户数据隐私的同时实现对已知和新型恶意软件的准确检测。Holmes 等人[35]提出了 SEVeriFast，一种针对 AMD SEV 微虚拟机的新型引导方案，其通过引入最小引导验证器、利用内核压缩减少测量开销、优化预加密等方式，在保证通过硬件强制信任根建立信任、借助测量直接启动和远程认证确保 VM 初始化完整性的前提下，将 SEV VM 冷启动性能提升 86%~93%。

5. 国内外研究现状对比

通过对国内外研究现状的系统性梳理可知，国内研究以国家重大科技专项为牵引，聚焦自主可控技术体系构建，重点开展国产操作系统与国密算法的适配应用研究。在研究模式上，强调高校与军工、航天等单位的产学研协同，围绕高安全等级嵌入式软件开发、可信启动机制、双芯片异构架构等关键技术展开攻关，研究成果直接服务于国防安全与关键信息基础设施建设。国外研究则呈现企业主导的技术创新特征，侧重集成硬件级安全模块的系统性解决方案研发，致力于构建零信任安全模型。其研究热点集中于形式化方法验证、量子计算可信执行环境架构设计、区块链技术与物联网融合应用等领域，注重技术创新与产业应用的深度耦合。

综合调研显示，当前国内外研究均在量子安全技术体系、人工智能与嵌入式系统安全融合、硬件可信根技术以及零信任安全架构等方向加速战略布局，体现出技术交叉融合与场景化应用的显著趋势。

6. 发展趋势与展望

从国内外研究动态来看，嵌入式可信安全领域正呈现技术深度融合与场景化需求驱动的发展趋势。在技术层面，量子安全技术(如量子密钥分发、量子可信执行环境)与传统可信计算体系加速融合，推动国密算法体系向量子抗毁方向升级；AI 与区块链技术赋能嵌入式可信架构，通过联邦学习实现设备间安全协同与未知攻击检测，基于区块链的链上链下信任传递机制(如可信疫苗追溯、无人机群自组织网络认证)逐步落地；硬件级可信根(国产可信计算芯片、集成安全模块的 MCU)与轻量级软件可信链深度协同，结合形式化验证方法构建资源受限环境下的全栈可信执行环境，成为高安全嵌入式系统(如航空发动机控制软件、工业测控设备)的核心支撑。在应用层面，边缘计算与物联网的泛在化催生轻量化可信认证需求，无人机群、智能医疗设备等场景推动分布式信任架构研发；国防军工、航天装备领域则加速自主可控可信技术栈的生态构建，聚焦异构架构、可信启动机制等关键技术的工程化应用。

展望未来，嵌入式可信安全研究一方面需突破国产软硬件协同优化瓶颈，建立从芯片级可信根到应用级可信开发部署工具的全流程体系，完善适应高安全场景的可信技术标准；在另一方面，针对量子计算威胁、资源受限设备安全效率平衡等挑战，需加强跨学科交叉创新，推动零信任模型与动态信任评估技术的轻量化改造，构建覆盖设备启动、运行、交互全生命周期的嵌入式可信安全体系，为国防安全、关键基础设施等领域提供坚实的可信保障。

参考文献

[1] 赵波, 倪明涛, 石源, 等. 嵌入式系统安全综述[J]. 武汉大学学报(理学版), 2018, 64(2): 95-108.

[2] WISE GUY. 全球嵌入式安全市场研究报告[EB/OL]. https://www.wiseguyreports.com/cn/reports/embed-ded-security-market, 2023-09-01.

[3] QYResearch. 可信计算芯片行业总体规模、市场占有率排名报告 2025 [EB/OL]. https://www.gelonghui.com/p/1576665, 2025-01-08.

[4] Morris, T. (2024) Trusted Platform Module. In: Jajodia, S., Samarati, P. and Yung, M., Eds., *Encyclopedia of Cryptography, Security and Privacy*, Springer, 1-5. https://doi.org/10.1007/978-3-642-27739-9_796-2

[5] Perez, R., Sailer, R. and van Doorn, L. (2006) vTPM: Virtualizing the Trusted Platform Module. *Proceedings of the* 15*th conference on USENIX Security Symposium*, San Jose, 31 July-4 August 2006, 305-320.

[6] 北京航空航天大学. 北航牵头的国家重点研发计划“高安全强实时嵌入式智能软件系统”项目启动暨实施方案论证会顺利召开[EB/OL]. https://scse.buaa.edu.cn/info/1092/11559.htm, 2024-03-29.

[7] 中国科学院沈阳自动化研究所. 国家 863 课题“可编程嵌入式电子设备安全防护技术”通过技术验收[EB/OL]. https://sia.cas.cn/xwzx/kydt/201810/t20181031_5152011.html, 2024-10-24.

[8] 华东师大软件工程学院. 喜报！华东师大牵头研发项目获上海市技术发明一等奖保障关键设备安全可信

[EB/OL]. https://sei.ecnu.edu.cn/da/cf/c33170a645839/page.htm, 2024-10-23.

[9] 深圳华北工控股份有限公司. 第十届中国(北京)军事智能技术装备博览[EB/OL]. https://m.gkong.com/news/121541.html, 2025-05-12.

[10] Nations 加油站. 国民技术第四代可信计算芯片 NS350 正式投入量产[EB/OL]. https://mcu.eetrend.com/content/2024/100580225.html, 2024-10-05.

[11] Zhao, H., Xu, C. and Zhou, F. (2021) Research on Embedded Startup Method of Trusted Module. 2021 *IEEE* 5*th Information Technology, Networking, Electronic and Automation Control Conference* (*ITNEC*), Xi'an, 15-17 October 2021, 953-957. https://doi.org/10.1109/itnec52019.2021.9587096

[12] 张翔, 王元强, 聂云杰, 等. TPCM 的轻量型安全可信启动方法[J]. 单片机与嵌入式系统应用, 2023, 23(6): 36-39, 44.

[13] Liu, C., Guo, H., Xu, M., Wang, S., Yu, D., Yu, J., *et al.* (2022) Extending On-Chain Trust to Off-Chain—Trustworthy Blockchain Data Collection Using Trusted Execution Environment (TEE). *IEEE Transactions on Computers*, **71**, 3268-3280. https://doi.org/10.1109/tc.2022.3148379

[14] Ma, Q. (2022) Design of High-Confidence Embedded Operating System Based on Artificial Intelligence and Smart Chips. 2022 *Second International Conference on Artificial Intelligence and Smart Energy* (*ICAIS*), Coimbatore, 23-25 February 2022, 58-62. https://doi.org/10.1109/icais53314.2022.9742917

[15] Yu, X., Liu, Y., Zou, X., Cao, Y., Zhao, Y., Nag, A., *et al.* (2022) Secret-Key Provisioning with Collaborative Routing in Partially-Trusted-Relay-Based Quantum-Key-Distribution-Secured Optical Networks. *Journal of Lightwave Technology*, **40**, 3530-3545. https://doi.org/10.1109/jlt.2022.3153992

[16] Wang, R. and Yan, Y. (2022) A Novel Trusted Boot Model for Embedded Smart Device without TPM. 2022 24*th International Conference on Advanced Communication Technology* (*ICACT*), PyeongChang Kwangwoon Do, 13-16 February 2022, 228-233. https://doi.org/10.23919/icact53585.2022.9728958

[17] 杨子怡, 李亚晖, 王中华, 等. 基于机载嵌入式可信计算平台的安全配置管理系统[J]. 航空计算技术, 2023, 53(2): 123-126.

[18] Yang, J., Liu, X., Jiang, X., Zhang, Y., Chen, S. and He, H. (2023) Toward Trusted Unmanned Aerial Vehicle Swarm Networks: A Blockchain-Based Approach. *IEEE Vehicular Technology Magazine*, **18**, 98-108. https://doi.org/10.1109/mvt.2023.3242834

[19] 何瑞琦, 张凯龙, 吴金飞, 等. 基于多核异构操作系统的动态冗余可靠机制研究[J]. 计算机科学, 2025, 52(4): 33-39.

[20] 吉晨, 石勇, 戴明, 等. 基于轻量级虚拟化环境的可信多级安全容器机制[J]. 计算机应用研究, 2017, 34(6): 1770-1773.

[21] Marketsandmarkets. (2023) Embedded Security Market Size & Trends. https://www.grandviewresearch.com/industry-analysis/embedded-security-market-report

[22] STMicroelectronics (2025) STM32L5 Series. https://www.st.com/en/microcontrollers-microprocessors/stm32l5-series.html

[23] Business & Financial Press (2023) Infineon's SECORA™ Connect Can Make Anything a Wallet; New Technologies Will Make Contactless Payment Easier in the Future. https://www.infineon.com/press-release/2023/infxx202302-068

[24] Intel (2025) Intel Newsroom: Corporate. https://www.intel.cn/content/www/cn/zh/newsroom/corporate.html

[25] Bognar, M., Van Bulck, J. and Piessens, F. (2022) Mind the Gap: Studying the Insecurity of Provably Secure Embedded Trusted Execution Architectures. 2022 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, 22-26 May 2022, 1638-1655. https://doi.org/10.1109/sp46214.2022.9833735

[26] Aaraj, N., Raghunathan, A. and Jha, N.K. (2008) Analysis and Design of a Hardware/Software Trusted Platform Module for Embedded Systems. *ACM Transactions on Embedded Computing Systems*, **8**, 1-31. https://doi.org/10.1145/1457246.1457254

[27] Fedorov, V.K., Balenko, E.G., Shterenberg, S.I. and Krasov, A.V. (2021) Development of a Method for Building a Trusted Environment by Using Hidden Software Agent Steganography. *Journal of Physics*: *Conference Series*, **2096**, Article ID: 012047. https://doi.org/10.1088/1742-6596/2096/1/012047

[28] Gebreab, S.A., Salah, K., Jayaraman, R. and Zemerly, J. (2023) Trusted Traceability and Certification of Refurbished Medical Devices Using Dynamic Composable NFTs. *IEEE Access*, **11**, 30373-30389. https://doi.org/10.1109/access.2023.3261555

[29] Trochatos, T,. Xu, C., Deshpande, S., *et al.* (2023) Hardware Architecture for a Quantum Computer Trusted Execution Environment. arXiv: 2308.03897.

[30] Phalak, K., Saki, A.A., Alam, M., Topaloglu, R.O. and Ghosh, S. (2021) Quantum PUF for Security and Trust in Quan-

tum Computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, **11**, 333-342. https://doi.org/10.1109/jetcas.2021.3077024

[31] Seng, K.P. and Ang, L. (2022) Embedded Intelligence: State-Of-The-Art and Research Challenges. *IEEE Access*, **10**, 59236-59258. https://doi.org/10.1109/access.2022.3175574

[32] Alkhoori, A., Alkhoori, A., Alkhoori, A. and Ahmed, O. (2024) Security and Reliability Concerns of AI on Critical Embedded Systems. In: Rasheed, J., Abu-Mahfouz, A.M. and Fahim, M., Eds., *Forthcoming Networks and Sustainability in the AIoT Era*, Springer, 32-45. https://doi.org/10.1007/978-3-031-62871-9_4

[33] Raja, G., Anbalagan, S., Ganapathisubramaniyan, A., Selvakumar, M.S., Bashir, A.K. and Mumtaz, S. (2021) Efficient and Secured Swarm Pattern Multi-UAV Communication. *IEEE Transactions on Vehicular Technology*, **70**, 7050-7058. https://doi.org/10.1109/tvt.2021.3082308

[34] Nawshin, F., Unal, D., Hammoudeh, M. and Suganthan, P.N. (2024) AI-Powered Malware Detection with Differential Privacy for Zero Trust Security in Internet of Things Networks. *Ad Hoc Networks*, **161**, Article ID: 103523. https://doi.org/10.1016/j.adhoc.2024.103523

[35] Holmes, B., Waterman, J. and Williams, D. (2024) SEVeriFast: Minimizing the Root of Trust for Fast Startup of SEV MicroVMs. *Proceedings of the* 29*th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, *Volume* 2, La Jolla, 27 April-1 May 2024, 1045-1060. https://doi.org/10.1145/3620665.3640424