自动化测试在嵌入式系统安全性验证中的应用探索

闫 腾 郭新伟

中国电子科学研究院 北京 100041

摘 要：伴随嵌入式系统于航空航天、汽车电子、医疗设备等关键领域的大量应用，对其安全性进行验证极为关键，本文以自动化测试在嵌入式系统安全性验证中的应用为聚焦点，解析嵌入式系统安全需求及传统测试存在的局限，解读自动化测试的技术优势及实施框架内容，对代码静态分析、动态功能测试、形式化验证等自动化测试方法的实际应用展开探讨，且凭借汽车电子ECU系统案例验证其成效性，志在为增强嵌入式系统安全性验证效率与质量提供理论参考和实践帮扶。

关键词：自动化测试；嵌入式系统；安全校验；动态测试

嵌入式系统集计算机、电子、自动化技术于一体，广泛应用于现代社会。在智能汽车、医疗设备等场景中，其安全关乎人身与社会稳定。但传统手工测试面对复杂架构和庞大代码，效率低、覆盖差、偏差大，难满足安全验证需求。自动化测试高效、精准、可重复，成为重要发展路径，研究其对维持系统可靠运行意义重大。

一、嵌入式系统安全性需求与传统测试局限性

（一）嵌入式系统安全性需求分析

嵌入式系统安全需求涵盖功能安全与信息安全。功能安全要求系统在规定条件下实现功能且无危险故障，如飞机飞控系统需在极端气象下稳定运行，避免软件故障引发事故。信息安全关注系统抵御攻击、保护数据隐私，如智能电网嵌入式控制单元要防黑客入侵、数据泄露。物联网发展使嵌入式系统互联，安全风险更复杂，对安全性验证要求更高[1]。

（二）传统测试方法的局限性

传统手工测试在嵌入式系统安全性验证中缺陷明显。它效率低下，处理海量测试用例困难，10万行代码的软件基础功能测试就需数月。且难以保证测试覆盖率，易漏掉边界条件与异常场景，导致安全漏洞难察觉。此外，手工测试受人员经验和状态影响大，结果缺乏可重复性与一致性，难以满足安全性验证对精准性和可靠性的严苛要求。

二、自动化测试在嵌入式系统安全性验证中的技术优势

（一）提高测试效率与覆盖率

自动化测试可迅速执行海量测试用例，大幅增进测试作业效率，利用编写测试脚本途径，可达成24小时无间断的测试，跟手工测试相比，效率能提升数倍乃至几十倍，自动化测试工具可自动生成覆盖各类场景的测试用例，有正常操作表现、边界条件设定、异常输入情形等，有效扩大测试覆盖范畴，启用以模型为依据的测试工具，可依照系统需求模型自动产生覆盖全部状态转换路径的测试用例，保证系统功能的完整度。

（二）降低人为误差与成本

自动化测试消除了手工测试因人为不小心或操作失误引发的误差，保证测试结果既准确又连贯一致，测试脚本一旦起草完成，可反复开展执行，杜绝因人员变动或劳累造成的测试质量起伏，从成本维度去看，尽管自动化测试前期需花费一定的工具采购及脚本开发方面的成本，然而从长远考量，借助高效性与复用性，能大幅降低测试的人力及时间成本，优化项目综合收益。

（三）支持持续集成与持续测试

处在敏捷开发以及DevOps模式搭建的架构里，持续集成（CI）与持续测试（CT）流程可达成自动化测试的无缝集成，只要代码出现了变动，自动化测试工具自动唤起测试任务，实时反馈代码的安全性与质量状态，此快速反馈机制帮助开发团队及时找到并修复安全上的漏洞，缩短问题定位及解决的时间跨度，保障系统开发阶段的安全与稳定[2]。

三、嵌入式系统安全性验证的自动化测试实施框架

（一）测试需求分析与用例设计

按照嵌入式系统安全性需求的相关规范，明确测试目标与界限，把如ISO 26262的功能安全标准跟IEC 62443这样的信息安全标准结合，剖析系统潜藏的安全风险点，设计具针对性的测试用例集，以汽车电子系统的制动控制模块为对象，需设计囊括正常制动、紧急制动、制动无法正常工

作等情形的测试用例，让功能维持安全水平；同时设计对网络攻击进行模拟的测试用例，证实系统对信息安全的防护实力。

（二）自动化测试工具选型与环境搭建

依照测试需求选定恰当的自动化测试工具，Coverity、PC - Lint 是代码静态分析的常用工具，动态功能测试可借助 VectorCAST、LDRA Testbed 完成，UPPAAL、Spin等可用于形式化验证。在搭建测试环境这个阶段，需把目标嵌入式系统跟测试工具、仿真器、调试器等设备进行联合集成，保证测试数据实现精准的传输和交互，处于汽车ECU测试的阶段，需借助CAN总线模拟器实现车辆各部件通信信号的模拟，为测试缔造逼真的运行态势。

（三）测试脚本开发与执行

采用Python、Shell之类的脚本语言，抑或运用测试工具自带的脚本编写能力，生成自动化测试脚本，脚本应做到测试用例的自动载入、实施、结果记录及剖析，处于执行流程期间，实时把控系统运行状态变化，采集日志内容与错误相关数据，开展医疗设备嵌入式系统测试工作期间，脚本需实时针对设备输出的生理参数数据进行监测，若发现有异常存在，马上中断测试并记录相关信息。

（四）测试结果分析与反馈

待测试操作结束，对测试结果开展深度剖析，对比预期结果跟实际输出，找出系统所存在的安全漏洞，凭借测试工具生成的如覆盖率报告、缺陷分析报告之类的文档，厘定问题代码的位置及产生缘故，马上把分析结果反馈至开发团队，以便实施针对性的修补，然后重新开展回归测试工作，保障安全漏洞实现有效治理[3]。

四、嵌入式系统安全性验证的自动化测试方法

（一）代码静态分析

代码静态分析在代码不运行的情形下进行，开展对源代码的语法审查、语义分析及安全规则排查，通过排查代码里像未初始化变量、内存泄漏、越界访问这类潜在的缺陷，发掘也许造成安全问题的编程差错，采用Coverity工具对嵌入式C代码进行剖析，可识别出缓冲区溢出的漏洞，杜绝数据越界写入引发系统崩溃或遭恶意侵害，静态分析还可查验代码是否符合既定编码规范，增强代码质量与安全水平。

（二）动态功能测试

在系统运行状态下开展动态功能测试，采用输入不同测试数据，审视系统功能是否符合安全需求范畴，采用黑盒、白盒、灰盒的测试方式，采用边界值分析、等价类划分等技术设计测试所用案例，当对智能家居控制系统的嵌入式网关实施动态测试时，对不同网络环境（包括弱网、断网）与用户操作（如频繁开关设备、并发发起请求）进行模拟，考察系统稳定性及响应本领，保障在不同场景下不出现安全上的漏洞。

（三）形式化验证

形式化验证凭借严格的数学逻辑开展，开展对系统模型的精确验证，保障系统实现安全性属性要求，以建立系统的数学模型（诸如有限状态机、时序逻辑公式）的方式，借助模型检测工具或定理证明器，核查系统是否存在死锁、非法状态转换这类安全隐患，处于航空航天嵌入式系统范畴中，借助UPPAAL开展飞行控制系统实时性与安全性的形式化验证工作，确认系统在所有潜在状态下皆可满足安全约束条件。

（四）安全性渗透测试

基于嵌入式系统的信息安全诉求，推进安全性的渗透测试实施，仿效黑客的攻击举措，诸如网络扫描、漏洞攻破、数据窃取等方式，审视系统安全防护的综合实力，依靠渗透测试途径，找出系统在网络通信、数据加密、用户认证等方面存在的安全漏洞，且给出针对性加固方案，实施对工业控制领域嵌入式系统的渗透测试，审视其抵御DDoS攻击、SQL注入攻击的实力，维护系统在网络环境下信息的安全可靠。

五、自动化测试在嵌入式系统安全性验证中的前沿发展与挑战

（一）人工智能与机器学习的融合应用

随着AI和ML技术成熟，其在自动化测试领域应用渐深。AI算法可分析历史数据预判隐患、优化用例优先级；机器学习模型经训练能识别嵌入式系统潜在隐患点以提前测试。强化学习使测试脚本执行时自主调策，适应系统变化。在智能交通系统测试中，采用强化学习的脚本能依交通流量生成最佳序列，验证系统安全性。

（二）物联网与边缘计算场景下的测试扩展

边缘计算与物联网快速发展，使嵌入式系统呈分布式、异构化，安全性验证面临新挑战。自动化测试需拓展至设备通信协议、边缘节点安全防护等范畴。在智慧城市物联网传感器网络中，自动化测试工具要模拟多场景，检验系统抗干扰与数据完整性。同时，因边缘计算节点资源受限，自动化测试应具备轻量化、低功耗特性以适配环境。

（三）标准化与合规性验证的强化

在航空航天、医疗这类对安全性要求近乎苛刻的行业，国际标准跟法规不断在细化，自动化测试要紧密围绕ISO

26262、IEC 62304（医疗设备软件）等标准去落实，研制标准化测试流程及工具，处于医疗植入式设备安全性验证阶段时，自动化测试不只是要对设备功能安全加以验证，还得保证它符合数据隐私相关法规，采用设立标准化测试框架，可提升测试结果的通用属性与权威性，让产品合规认证进程加速[4]。

（四）面临的主要挑战

虽说自动化测试发展十分迅猛，但依旧得克服众多挑战，不同厂商所采用的嵌入式系统架构差异大，测试工具的兼容适配性存在短板，加深了测试实施的难度级别，AI及机器学习技术在测试应用方面仍处于探索阶段，模型可靠性、可解释性需进一步提高，伴随嵌入式系统功能复杂程度持续升高，测试数据量呈指数形式迅猛增长，对测试数据管理与分析能力的要求进一步提高。

六、案例分析：自动化测试在汽车电子 ECU 系统中的应用

（一）案例背景

某车企着手开发新一代发动机控制单元，此ECU充当汽车动力系统的核心机件，其安全性直接关乎车辆行驶的安全，ECU软件包含的代码数量为20万行，应符合ISO 26262功能安全ASIL - D等级的要求，采用传统手工测试难以契合验证需求，为此引入自动化测试手段。

（二）自动化测试实施过程

1.测试需求分析与用例设计：依照ISO 26262相关标准，识别出ECU系统的安全目标，诸如预防发动机意外停转、防止错误喷油调控等，筹备覆盖正常工况、故障注入、边界条件等场景的测试用例，合计有1200条。

2.工具选型与环境搭建：采用VectorCAST当作自动化测试工具，搭建以ECU硬件、CAN总线模拟器、实时操作系统仿真器为组成部分的测试环境，对车辆运行过程里不同信号的交互做模拟。

3.测试脚本开发与执行：采用VectorCAST的脚本开发功能做，构建自动化测试脚本，达成测试用例自动开展与结果收集，在测试进行的阶段内，采用故障注入工具模拟传感器出现失效、通信发生中断等故障场景，考查ECU对故障的反应能力。

4.结果分析与反馈：完成所有测试后，代码覆盖率报告、缺陷分析报告由 VectorCAST 生成，检测到代码里有3处潜在内存越界风险以及2个逻辑判断失误，把检测结果反馈给开发团队做修复处理，再重新实施回归测试，直至测试过关[5]。

（三）实施效果

凭借自动化测试途径，从手工测试的65%起步，ECU系统代码覆盖率提升到92%，实现缺陷发现率40%的提升，测试周期实现60%的缩短，该ECU系统最终成功迈过ISO 26262功能安全认证门槛，说明自动化测试在嵌入式系统安全性验证时的有效性及可靠性。

结语

自动化测试在嵌入式系统安全性验证领域体现出显著优势，依靠增强测试效率、降低人为失误、支持持续检测等特性，高效填补了传统测试方法的漏洞，综合采用代码静态分析、动态功能测试、形式化验证等自动化测试方法，能从多维度保障嵌入式系统的功能安全与信息安全水平。伴着技术的发展，人工智能、物联网等前沿领域的融合，为自动化测试开启新机遇之门，也对标准化、兼容性等方面提出了更为苛刻的挑战，应进一步强化技术革新与实践钻研，促进自动化测试技术在嵌入式系统安全性验证里达成更智能、更高效的运用，为嵌入式系统的广泛铺开筑牢安全壁垒。

参考文献:

[1]赵昶宇.嵌入式软件安全性测试技术研究[J].科技与创新,2023(21):81-83.

[2]范娜,李全洲.面向安全性分析的嵌入式软件测试方法浅析[J].信息系统工程,2023(6):80-83.

[3]肖蕾,卢倩,冉毅德,等.基于功能安全的汽车嵌入式软件单元验证技术研究[J].汽车电器,2023(10):64-66,69.

[4]董丽,赵琪,周健.嵌入式软件安全性分析和测试方法研究[J].信息系统工程,2021(5):70-71.

[5]张宝斌.面向安全性分析的嵌入式软件测试方法研究[J].电子测试,2020(11):117-118.