

嵌入式操作系统信息系统测评技术研究与实践

陈飞然，刘瑞杰

中国电子科技集团公司第三十二研究所，上海

摘要：嵌入式操作系统信息系统测评技术围绕功能、性能、安全性、接口和强度五个方面开展研究与实践。针对任务管理需求，提出多任务状态切换、优先级动态调整和延时控制的测试方法，验证任务调度机制的正确性与稳定性。安全性测试聚焦时间保护与空间保护，评估系统在时间资源管理与栈空间防护中的容错机制与响应能力。强度测试通过高负荷任务并发与长时间运行，验证系统稳定性与数据传输的完整性。结果表明，所提出的测评方法有效支持嵌入式操作系统功能实现及其在复杂应用环境中的可靠运行。

关键词：嵌入式操作系统；信息系统测评；任务管理；安全性测试；强度测试

Research and Practice on Evaluation Technology of Embedded Operating System Information System

Feiran Chen, Ruijie Liu

32nd Research Institute of China Electronics Technology Group Corporation, Shanghai

Abstract: The embedded operating system information system evaluation technology conducts research and practice around five aspects: function, performance, security, interface and strength. According to the requirements of task management, the test methods of multi-task state switching, priority dynamic level adjustment and delay control are proposed to verify the correctness and stability of the task scheduling mechanism. The security test focuses on time protection and space protection, and evaluates the fault tolerance mechanism and response ability of the system in time resource management and stack space protection. The strength test verifies the system stability and the integrity of data transmission through the concurrent and long-time operation of high-load tasks. The results show that the proposed evaluation method effectively supports the function realization of embedded operating system and its reliable operation in complex application environment.

Keywords: Embedded operating system; Information system evaluation; Task management; Security test; Strength test

1 引言

随着信息技术的快速发展，嵌入式操作系统作为支撑各类智能设备与应用的核心平台，其性能与稳定性对于系统的整体表现至关重要。在复杂多变的应用环境中，如何确保嵌入式操作系统能够高效、安全地运行，成为当前研究的热点之一。本研

究聚焦于嵌入式操作系统信息系统的测评技术，旨在通过全面、系统的测评手段，揭示系统在不同维度上的表现与潜在问题，为系统的优化与改进提供科学依据。研究从功能、性能、安全性、接口和强度五个核心方面入手，构建了完整的测评体系。功能测评关注系统的基础功能与任务管理能力，通过

设计针对性的测试用例，验证系统在不同场景下的行为是否符合预期。性能测评则重点考察系统的响应时间、资源占用等指标，以评估其在实际应用中的效率与效能。

2 信息系统测评的理论基础

信息系统测评是通过科学方法和手段，对系统的功能、性能、安全性、稳定性等方面进行验证与评估。测评的目的是发现系统可能存在的问题，验证系统是否符合设计需求和技术指标。测评结果为系统的优化改进提供依据，同时支撑系统在实际应用中的稳定运行。

信息系统测评的内容主要包括功能测试、性能测试、安全性测试、接口测试和强度测试等方面。功能测试侧重于验证系统功能的完整性与正确性。性能测试评估系统在不同负载条件下的响应能力和资源利用情况。安全性测试关注系统在错误、异常或恶意攻击情况下的防护能力和容错性。接口测试验证系统各功能模块间、系统与外部环境之间的交互是否准确。强度测试通过高负荷、长时间运行评估系统的稳定性和耐久性。

测评工作的开展需要依托明确的需求规格、标准化的测评方法以及完善的测试环境。需求规格为测试提供依据，测评方法指导测试过程，测试环境为系统验证提供运行条件。

信息系统测评的理论基础涉及相关标准和技术规范，顶层技术文档为测评提供框架指导。例如，《嵌入式操作系统及开发环境定制技术协议》和《嵌入式操作系统软件设计说明》等文件明确了软件的功能要求与设计原则。此外，被测软件的《嵌入式操作系统软件需求规格说明》作为直接依据，详细描述了系统的具体需求和技术指标。

在管理类文件中，《军用软件测试指南》（GJB/Z 141-2004）和《软件工程化管理体系》（CEPREI-RC-2015）提供了系统化的测评方法和质量管理要求。这些文件与标准构建了完整的测评依据，使得测试活动有章可循，结果可信可用[1]。

3 测评技术与实施方案

3.1 测评技术概述

测评技术是对信息系统各方面指标进行科学

验证和分析的手段，具体包括功能测试、性能测试、安全性测试、接口测试和强度测试等方法。功能测试主要采用黑盒测试技术，验证系统功能的完整性和正确性，重点检查任务调度、数据处理及用户交互功能。性能测试侧重系统负载与响应，通过压力测试、负载测试及并发测试评估系统资源利用率和稳定性。安全性测试通过故障注入和攻击模拟等手段，分析系统在异常情况下的防护能力及容错机制。接口测试验证系统内部模块与外部接口的输入输出准确性，采用接口调用与协议一致性检查技术。强度测试评估系统在长时间高负荷运行条件下的稳定性，观察系统故障率与资源恢复能力[2,3]。

3.2 测评实施环境与工具

测评实施环境包括硬件平台、软件工具及配套调试设备，依据被测系统需求进行配置。硬件环境使用核芯二号硬件平台作为目标运行平台，搭载C9000处理器，主频200MHz，内存1MB，片上FLASH 1MB。软件环境包括嵌入式操作系统软件、集成开发环境、串口调试工具和网络调试工具。JTAG调试器用于目标程序的下载与调试，测试PC机运行编译工具与测试管理平台。软件版本控制及问题跟踪使用JIRA工具进行统一管理。测试环境的搭建严格遵循需求规格说明和技术协议，模拟真实应用场景，保证测试结果的有效性和可复现性。各项工具协同工作，实现测试数据采集、问题定位及结果分析，支撑测试任务的顺利执行。

3.3 测评实施方案

测评实施方案依据系统需求及技术指标，通过需求分析、测试设计、测试执行及结果验证四个阶段进行。需求分析阶段，对系统功能、性能、安全性等要求进行分解，提取测评需求。测试设计阶段，结合需求规格与技术协议，编写测试用例，设计覆盖各项功能和异常场景的测试方案。测试执行阶段，基于配置项测试环境，依次进行静态测试、功能测试、安全性测试和强度测试，逐项验证系统各指标的实现情况。在测试执行过程中，使用串口终端与调试工具监控测试状

态，记录测试数据与异常信息。结果验证阶段，分析测试数据，评估系统的正确性、稳定性与可靠性，生成测试报告。

4 任务管理需求测试的具体实践

4.1 任务管理功能需求概述

任务管理功能是信息系统操作系统核心模块之一，主要用于实现任务的创建、调度、挂起、恢复和删除等管理操作。任务调度通过优先级机制与时间分片实现资源分配与控制，保证各任务按设计需求执行。任务的生命周期管理涉及任务的状态切换，包括就绪、运行、挂起和终止等状态。任务优先级调整与调度控制实现任务执行顺序的动态管理，适应复杂应用场景的需求。任务管理功能还提供任务延时、取消延时、获取任务信息等接口，支持任务间的信息交互与状态监控。任务管理功能需求明确了系统在多任务环境下的执行逻辑与响应行为，通过测试验证这些功能的完整性、正确性和稳定性，为系统任务调度机制提供技术支持。

4.2 测试用例设计与步骤

任务管理需求测试设计包括多任务创建、调度切换、优先级调整 and 状态管理等方面。测试用例根据任务管理需求规格说明编写，覆盖任务各生命周期状态与调度行为。用例设计基于最小内核系统，配置任务最大个数大于10，验证系统在多任务条件下的运行表现。具体步骤包括：创建测试工程并编写任务管理测试代码；在测试主任务中依次创建6个子任务，设置优先级递减，模拟任务的动态调度。测试中调用task_self、task_suspend、task_resume等接口，实现任务挂起与恢复功能；通过task_set_priority调整任务优先级，验证调度控制逻辑；调用task_info接口获取任务状态信息，检查任务管理功能的准确性。测试结束后，记录任务状态、接口返回值与调度结果，为功能验证提供依据[4,5]。

4.3 测试过程与结果分析

任务管理需求测试过程严格按照测试用例执行，测试环境基于核芯二号硬件平台和嵌入式操

作系统集成开发环境。测试开始时，主任务创建6个子任务，优先级设置为16到11。测试主任务延时后，CPU控制权交由子任务。子任务依次调用task_get_priority接口获取自身优先级，任务成功挂起，验证任务创建与优先级管理功能。恢复操作调用task_resume接口，Task1优先级被动态调整至17，验证调度机制响应优先级变更。Task6调用task_delay延时2000个ticks，随后通过task_delay_cancel接口取消延时，检查延时控制逻辑。最终，任务依次恢复、删除，主任务完成测试流程，返回执行结果。测试结果显示，各项任务管理接口执行正常，任务状态与优先级变更符合预期。无错误与异常发生，串口终端输出验证了任务调度的正确性与稳定性，任务管理功能需求测试通过。

5 安全性测试的实施与分析

5.1 时间保护安全性测试

时间保护安全性测试验证操作系统在多任务环境下的时间隔离机制，评估任务执行时间控制的正确性与系统容错能力。测试通过设置任务的时间预算，检测任务执行时间是否符合预期，避免任务间因时间资源争夺导致的异常行为。在测试环境中，系统使能时间保护功能与系统致命错误钩子，配置任务最大个数大于3，建立测试工程并加载镜像文件。测试用例包括两种情况：任务执行时间未超预算和任务执行时间超预算。任务B设置时间预算，通过task_budget_set配置执行时间；在正常情况下，任务循环执行，钩子函数不触发，系统状态正常。在异常情况下，任务执行时间超过预算，系统调用钩子函数输出错误信息，验证系统对时间违规的响应能力。

5.2 空间保护安全性测试

空间保护安全性测试主要评估系统对任务栈溢出与代码段访问的防护能力，验证系统的空间隔离机制。测试环境配置任务栈保护与代码段保护功能，任务最大个数大于3，系统使能MMU管理模块，设置地址空间访问权限。栈保护测试中，测试任务分配固定大小的栈空间，逐步增加局部变量大小，模拟栈溢出场景。系统通过printf输出溢出错误

信息，并自动挂起异常任务，防止系统崩溃。代码段保护测试中，高优先级任务尝试写入代码段所在地址，系统触发访问权限异常，验证代码段的只读与可执行属性。低优先级任务正常运行，输出正确的信息，证明空间保护机制未影响其他任务的执行。

5.3 测试过程中的难点与解决方案

安全性测试实施过程中，任务执行时间控制和空间访问权限验证是两大难点。任务时间保护测试中，任务执行时间的精确控制依赖硬件定时器与系统钩子函数的配合，测试过程中存在任务时间误差问题。为解决该难点，测试通过重复多次执行任务，并对时间预算设置合理的容差范围，确保测试数据的稳定性与准确性。空间保护测试中，栈溢出触发点的精确定位是关键，局部变量的逐步递增与编译优化参数影响测试结果。为此，测试在编译过程中禁用优化设置，并通过边界值测试法逐步逼近栈空间极限，验证系统的检测与防护机制。代码段保护测试需要合理设置MMU访问权限，测试过程需严格规范任务操作，避免干扰其他测试模块。

6 强度测试的设计与验证

6.1 测试需求与场景设计

强度测试旨在验证系统在高负荷运行条件下的稳定性，评估任务并发执行和长时间运行的可靠性。测试需求要求系统在高强度收发任务模式下，保持稳定运行8小时，并同时支持128个任务无故障并发执行。测试场景以串行收发通道为核心，模拟数据传输的高负载状态，检验任务创建、调度及通信的稳定性与正确性。核芯一号与核芯二号硬件平台被选作测试平台，任务分别在两个平台上进行数据收发操作。任务task_send和task_recv交替执行，持续进行数据传输。测试重点观察系统是否存在任务中断、数据丢失、异常重启等现象，以验证操作系统的稳定性与长时间承载能力。

6.2 测试过程与环境搭建

强度测试环境搭建在核芯一号与核芯二号

硬件平台上，系统加载最小内核配置，任务最大数被设置为127，形成128个任务的并发运行环境。测试数据通过串口传输，核芯一号平台作为数据发送端，核芯二号平台作为数据接收端，反向任务亦同步进行。测试过程依次创建数据发送任务task_send和数据接收任务task_recv，通过循环机制维持数据的连续传输。系统通过JTAG调试器加载镜像文件，测试结果通过串口终端实时输出。测试持续8小时，期间记录系统的运行状态、任务切换情况和数据传输完整性。

6.3 系统稳定性验证与结果分析

测试结果显示，在连续8小时的高强度任务运行中，系统运行状态稳定，各任务均按预期执行。串行通道数据传输未出现丢包、延迟或错误信息，任务切换与调度正常完成，资源占用符合设计要求。系统日志记录显示，128个任务的并发执行过程中，CPU利用率与内存资源保持在可控范围内。测试过程中，未发生系统崩溃、任务死锁或异常重启现象，验证了系统在高负荷运行下的稳定性和可靠性。通过对测试数据的比对分析，串口通道收发任务准确完成，数据传输结果与预期一致。测试结果表明，操作系统具备长时间高负载环境下的稳定运行能力，满足系统设计指标与应用需求。

7 结语

通过系统化的测评技术与实践，本文验证了嵌入式操作系统在功能、性能、安全性及稳定性方面的可靠性。任务管理功能测试确保了任务调度、状态切换及优先级控制的准确性。安全性测试揭示了系统在时间和空间保护机制中的防护能力，有效应对异常条件下的资源分配问题。强度测试进一步验证了系统在高负载与长时间运行条件下的稳定性和数据传输的完整性。

参考文献

- [1] GB/T 43206-2023, 信息安全技术 信息系统密码应用测评要求[S].
- [2] 漆桃. 基于风险分析的信息系统等级测评[J]. 网络安

- 全和信息化, 2024 (04) :18-21.
- [3] 周军强. 网络安全防御系统自动测评与优化技术研究[J]. 电子元器件与信息技术, 2022, 6 (06) : 141-144.
- 教育信息技术, 2023 (09) :68-72.
- [4] 李静, 孙睿. 基于云计算的政务信息系统安全防护体系研究[J]. 电子技术, 2022, 6 (06) : 141-144.
- [5] 牛勇, 李泽, 马麟, 周玉熬. 嵌入式技术在电子信息系统中的应用[J]. 电子技术, 2023 (09).

