 DOI: https://doi.org/10.12349/iser.v7i3.9474

Reliability and Verification System of Embedded Computing Hardware Solutions in Industrial Scenarios

Laiyou Liu

Shenzhen Jiexingtong Technology Co., Ltd., Shenzhen, Guangdong, 518107, China

Abstract

In the context of the deep integration of Industry 4.0 and intelligent manufacturing, industrial grade embedded computing hardware, as a key infrastructure, needs to achieve long-term stable operation in complex electrical environments and harsh working conditions. Its reliability design has become a core challenge that restricts the development of the industry. This article focuses on the multidimensional requirements of industrial scenarios for computing performance, real-time performance, security, and environmental adaptability. The system proposes a reliability assurance system that covers hardware architecture design, software fault tolerance enhancement, full lifecycle verification, and supply chain risk management. By constructing a three in one framework of "design verification management" and combining verification methods such as functional simulation, accelerated life testing, and electromagnetic compatibility analysis, a reusable industrial grade embedded hardware development paradigm has been formed, providing theoretical support and practical reference for the independent research and development of highly reliable industrial equipment.

Keywords

Industrial grade embedded computing; Hardware reliability; Verification system; System architecture design; Whole life cycle management

嵌入式计算硬件方案工业场景下的可靠性与验证体系

刘来友

深圳市杰星通科技有限公司，中国 · 广东 深圳 518107

摘　要

在工业4.0与智能制造深度融合的背景下，工业级嵌入式计算硬件作为关键基础设施，需在复杂电气环境与严苛工况下实现长周期稳定运行，其可靠性设计已成为制约行业发展的核心挑战。本文聚焦工业场景对计算性能、实时性、安全性及环境适应性的多维度需求，系统提出覆盖硬件架构设计、软件容错增强、全生命周期验证及供应链风险管理的可靠性保障体系。通过构建“设计-验证-管理”三位一体框架，结合功能仿真、加速寿命测试、电磁兼容分析等验证方法，形成了一套可复用的工业级嵌入式硬件开发范式，为高可靠工业装备的自主化研发提供理论支撑与实践参考。

关键词

工业级嵌入式计算；硬件可靠性；验证体系；系统架构设计；全生命周期管理

1 引言

在工业自动化与智能化加速演进的当下，工业级嵌入式计算硬件作为连接物理世界与数字系统的核心载体，其可靠性直接决定了工业装备的运行效能与安全等级。相较于消费级电子设备，工业场景对硬件系统提出了更为严苛的要求：需在 -40℃ ~85℃宽温范围、强电磁干及高频振动等极端条件下，实现微秒级实时响应、99.999% 以上可用性及功能安全认证合规。然而现有研究多聚焦于单一技术维度优化，缺乏对硬件架构设计、软件容错机制、全生命周期验证及供应链管理的系统性整合。本文针对上述挑战，提出一种覆盖“需求分析 - 设计实现 - 验证测试 - 生产维护”全流程的工业级嵌入式硬件可靠性保障体系，通过多学科交叉方法与工程实践结合，为轨道交通、能源电力等关键领域的高可靠硬件开发提供理论框架与技术路径。

【作者简介】刘来友（1975–），男，中国江西吉安人，从事工业级嵌入式计算与定制化硬件方案领域研究。

2 工业级嵌入式计算硬件架构设计

工业级嵌入式计算硬件架构设计需在性能、功耗、可靠性及成本之间实现多目标优化，其核心在于通过系统级权衡与模块化设计，满足工业场景对实时性、环境适应性和长生命周期的严苛要求。

2.1 系统级设计权衡

工业场景的多样性决定了硬件架构需具备高度可配置性。例如轨道交通信号控制需满足 SIL4 安全等级，需采用双冗余处理器架构；而能源电力监测设备则更注重低功耗与宽温运行能力 [1]。设计初期需通过需求分析矩阵明确计

算性能、实时性、功耗、成本及安全性的优先级。在处理器选型方面，MCU 适用于低功耗控制场景，SoC 可支持异构计算，FPGA 则用于高速信号处理。总线架构需根据数据带宽需求选择：低速外设采用 I²C/SPI，高速存储接口选用 DDR4/LPDDR5，实时控制总线优先选择 EtherCAT 或 PROFINET。此外，电源架构设计需兼顾效率与动态响应，例如采用多相 DC-DC 转换器降低瞬态压降，并通过 LDO 为敏感模拟电路提供低噪声供电。

2.2 关键硬件模块设计

存储体系是影响系统可靠性的关键因素。工业级 Flash 需支持 -40℃ ~105℃宽温工作，并通过 ECC 校验实现单比特错误纠正。DDR 存储器需采用多通道交错访问设计，结合 PLL 锁相环优化时钟抖动，确保高速信号完整性。对于高速数字电路，需通过 HyperLynx 等工具进行 SI/PI 仿真，重点解决差分对阻抗匹配、串扰抑制及电源完整性优化。例如在 10Gbps SerDes 接口设计中，需通过预加重与均衡补偿信道损耗。抗恶劣环境设计方面，需选用 AEC-Q200 认证的被动器件，并通过三防涂覆提升防潮防腐蚀能力。对于振动场景，需采用金属化安装孔与减震橡胶垫降低机械应力，并通过有限元分析优化 PCB 叠层结构。

2.3 可制造性与可测试性设计

可制造性设计需从 PCB 布局阶段融入工艺约束。如 BGA 器件焊盘需满足 IPC-7351 标准，0402 封装电阻的间距应大于 0.2mm 以避免连锡。为提升生产良率，需在关键信号层设置测试点，并通过 JTAG 边界扫描实现芯片级功能测试。可测试性设计需覆盖从器件到系统的全链条：在 MCU 内部集成硬件看门狗与 CRC 校验模块，通过 I²C 接口外接温度传感器实现板级健康监测。对于高速总线，需设计 PRBS 发生器与误码检测器，支持眼图分析与抖动测试。

3 嵌入式计算平台软件与可靠性增强

工业级嵌入式计算平台的软件设计需兼顾实时性、功能安全与长期稳定性，其核心在于通过全链路开发流程优化、通信协议栈可靠性实现及系统级容错机制构建，形成覆盖软件全生命周期的可靠性保障体系。

3.1 底层软件全链路开发

底层软件作为硬件与上层应用的桥梁，需实现从引导加载到实时操作系统的完整功能链。Bootloader 需支持多启动模式，并通过 CRC 校验与数字签名确保固件完整性。例如 U-Boot 可扩展为支持双镜像备份，主镜像故障时自动切换至备用镜像，切换时间需控制在 10ms 以内以满足 IEC 61508 SIL3 级要求。RTOS 选型需综合考虑任务调度效率与确定性，VxWorks 因其微秒级中断响应与优先级继承机制广泛应用于轨道交通控制，而 FreeRTOS 凭借轻量化设计更适合资源受限的传感器节点 [2]。任务划分需遵循“单一功能原则”，将实时控制任务与数据采集任务分离，并通过邮箱或消息队列实现低耦合通信。内存管理需禁用动态分配，采用静态内存池与内存保护单元防止堆栈溢出，例如通过 ARM Cortex-M 的 MPU 配置实现任务级内存隔离。

3.2 工业通信协议栈实现

工业通信协议栈的可靠性直接影响系统互联能力。以 EtherCAT 为例，其分布式时钟同步机制可实现 μs 级同步精度，但需在从站设备中实现精确的本地时钟补偿算法。协议栈开发需遵循 IEC 61158 标准，通过状态机管理协议生命周期，并在数据链路层集成 CRC-16 校验与自动重传机制。对于 PROFINET IO，需实现实时通道与等时同步实时通道的双模式支持，其中 IRT 需通过时间触发以太网实现确定性传输。在软件实现层面，可采用分层架构：物理层驱动通过 DMA 加速数据收发，数据链路层实现帧封装 / 解封装，应用层通过回调函数向上层传递有效数据。例如，在 Modbus TCP 协议栈中，需在 TCP/IP 协议栈与 Modbus 应用层之间插入看门狗定时器，防止因网络阻塞导致协议栈死锁。此外，需通过 Wireshark 抓包分析验证协议交互时序，确保符合 IEC 61784 规范。

3.3 系统级容错与安全机制

系统级容错需从硬件抽象层到应用层构建多级防御体系。在硬件故障检测方面，可通过 ADC 周期性采样电源电压与温度传感器数据，结合阈值比较与滑动窗口算法识别异常。对于处理器故障，需实现双核锁步或看门狗管理器，例如 TI Hercules 系列 MCU 通过内置比较器实时监测两核运算结果一致性。软件容错方面，可采用 N- 版本编程实现关键算法冗余，如通过三模冗余投票机制提高传感器数据可信度。安全机制需覆盖功能安全与信息安全：功能安全通过 IEC 61508 认证的 Safety Library 实现安全输入 / 输出处理，信息安全则需集成 AES-128 加密与 TLS 1.3 协议栈，防止数据篡改与中间人攻击。例如在轨道交通信号系统中，需同时满足 SIL4 级功能安全与 IEC 62443 信息安全标准，通过安全启动与安全存储构建信任链，并通过定期安全审计消除潜在漏洞。

4 定制化硬件方案的验证体系构建

工业级嵌入式硬件的定制化开发需构建覆盖全生命周期的验证体系，以确保其在极端工况下的长期可靠性。该体系需融合功能验证、环境适应性测试、寿命评估及供应链风险管理，形成“设计 - 验证 - 生产”闭环。

4.1 功能验证与仿真测试

功能验证是硬件设计的首要环节，需通过虚拟仿真与物理测试结合实现全链路覆盖。在数字电路设计阶段，采用 ModelSim 进行 RTL 级功能仿真，验证逻辑正确性；通过 VCS 或 QuestaSim 实现门级仿真，检查时序约束是否满足设计要求 [3]。对于高速信号，需利用 HyperLynx 或 ADS 进行信号完整性仿真，优化阻抗匹配、串扰抑制及眼图质量。模拟电路验证需通过 Cadence Virtuoso 进行 SPICE 仿真，重点分析电源完整性噪声、ADC 线性度及运放增益带

宽积。硬件描述语言验证需构建 UVM 测试平台，通过随机约束生成覆盖所有边界条件的测试向量，确保功能覆盖率达 100%。物理原型验证阶段，需开发 FPGA 原型系统或硬件仿真器，通过实际 I/O 接口与外设交互，验证硬件 - 软件协同性能。例如在轨道交通控制器开发中，需通过 CANoe 模拟列车网络通信，验证 EtherCAT 从站同步精度是否满足 μs 级要求。

4.2 环境可靠性测试

环境适应性测试需模拟工业场景的极端条件，包括温度循环、振动冲击、电磁兼容及防护等级验证。温度测试需覆盖 -40℃ ~85℃宽温范围，采用步进应力法确定器件失效阈值，并通过 HALT 快速暴露设计薄弱点。例如对 BGA 封装器件进行 -55℃ ~125℃热冲击测试，验证焊点可靠性。振动测试需根据 IEC 60068-2-64 标准执行随机振动与正弦扫描，通过应变片监测 PCB 应力分布，优化器件布局与减震设计。EMC 测试需满足 IEC 61000-4 系列标准，包括 ESD、EFT 测试，通过磁环、TVS 二极管及屏蔽罩提升抗干扰能力。防护等级验证需按 IP67 标准进行 1m 水深浸泡试验与粉尘箱测试，确保外壳密封性。

4.3 老化与寿命评估

寿命评估需结合加速老化试验与实际工况建模，预测硬件在长期运行中的失效概率。对于半导体器件，采用 Arrhenius 模型与 Coffin-Manson 模型分别计算高温与振动导致的寿命损耗。例如电解电容需在 105℃下进行 1000h 加速老化试验，通过 ESR 变化推算实际工况下的 MTBF。对于 Flash 存储器，需通过 JEDEC JESD218 标准进行 P/E 循环测试与数据保持测试，验证其耐久性与数据保留能力。PCB 寿命评估需关注焊点疲劳，通过 Miner 线性累积损伤法则计算温度循环与振动共同作用下的损伤值。系统级寿命预测需构建蒙特卡洛仿真模型，输入器件失效率与应力参数，输出整机可靠性指标。

4.4 供应链风险管理

供应链可靠性直接影响硬件的长期可维护性。需建立供应商评估体系，从质量体系、生产能力及交付周期三个维度评分，优先选择 AEC-Q200 认证的被动器件与车规级主动器件。对于关键器件，需实施“一主两备”策略，与至少两家供应商签订长期供货协议，并储备 6 个月安全库存。物料清单管理需通过 PLM 系统实现版本控制，防止因器件停产导致设计冻结。例如，在轨道交通信号系统开发中，需提前 3 年与芯片厂商锁定产能，并通过替代料验证降低断供风险。

5 工程化实施与全生命周期管理

工业级嵌入式系统的工程化实施需贯穿需求分析、设计开发、批量生产到长期运维的全生命周期，通过系统化管理能力、生产质量控制及持续技术支持实现可靠性闭环。

5.1 系统工程管理能力

系统工程管理是确保多学科协同的核心手段，需基于 V 模型开发流程构建需求 - 设计 - 验证的映射关系。在需求分析阶段，通过 QFD 将用户功能需求转化为技术特性参数，例如将轨道交通控制器的“实时响应”需求转换为 RTOS 中断延迟≤ 5μs 的量化指标。设计阶段需采用 MBSE 方法，通过 SysML 语言构建系统架构模型，明确硬件、软件及机械的接口定义与交互逻辑。验证阶段需执行多层级测试：模块级通过 JTAG/SWD 调试接口验证硬件功能，系统级通过 HIL 仿真测试 ECU 与传感器 / 执行器的协同性能，整车级通过实车路试验证电磁兼容性与环境适应性。

5.2 批量生产导入与质量控制

生产导入需完成从工程样机到量产产品的工艺转化，重点解决可制造性与质量控制问题。工艺文件开发需明确 SMT 贴片温度曲线、波峰焊导轨速度及 AOI 检测阈值。产线建设需配置自动化设备：通过 SPI 设备控制锡膏印刷厚度，利用 X-Ray 检测 BGA 焊点空洞率，采用 ICT 验证电路通断。质量控制需实施 APQP 流程，在 PPAP 阶段提交 CPK 报告，并通过 SPC 监控产线波动。

5.3 长期技术支持与优化

全生命周期管理需覆盖产品退役前的持续服务，包括故障修复、功能升级及备件供应。故障管理需建立 FRACAS，通过 FTA 定位根因，并通过 8D 报告推动设计改进。功能优化需响应市场需求，通过 OTA 技术实现软件远程升级，或通过硬件改版提升算力。备件管理需基于 Weibull 分布预测器件寿命，对电解电容、Flash 存储器等易损件建立安全库存，并通过替代料验证降低断供风险。需定期发布技术通告，向用户提供硬件维护指南及软件补丁。

6 结语

本文针对工业级嵌入式系统定制化开发需求，系统构建了涵盖功能验证、环境可靠性测试、老化寿命评估及供应链风险管理的硬件验证体系，提出了基于系统工程管理、批量生产质量控制与长期技术支持的全生命周期管理方案。通过 MBSE 方法实现需求 - 设计 - 验证的闭环追溯，采用 HALT 试验与 Weibull 分析提升硬件可靠性，结合 FRACAS 系统与 OTA 技术保障产品持续优化。未来研究可进一步融合数字孪生技术，实现硬件设计 - 生产 - 运维的虚拟映射与实时优化，同时探索 AI 驱动的失效预测模型，为工业互联网场景下的嵌入式系统开发提供更高效的工程化解决方案。

参考文献

[1] Kamal R. Embedded Systems: Architecture, Programming and Design [M]. 陈曙晖, 译. 北京: 清华大学出版社, 2005.

[2] Noergarrd T. Embedded Systems Hardware and Software Architecture [M]. 北京: 人民邮电出版社, 2005.

[3] Zhang H, Li X, Wang Y, et al. Digital Thread-Based Full Lifecycle Management Optimization for Smart Manufacturing Embedded Devices [J]. IEEE Transactions on Industrial Informatics, 2022, 18(6): 4235-4246.