嵌入式计算机多通道数据通信系统设计

李传明[1] 吴 格[1]
LI Chuanming WU Ge

摘 要 为解决工业控制、智能交通等领域多协议数据并发传输效率低、通道冲突频发、实时性不足等问题，文章设计了一种基于 ARM Cortex-A9 处理器与双 DMA 控制器的嵌入式多通道数据通信系统。该系统采用多协议融合架构，集成 CAN 总线、RS485、以太网等通信协议，构建统一数据交换平台；同时融入动态优先级调度算法与通道冲突智能检测技术，实现多通道数据的高效协同传输与冲突预判。为验证系统性能，搭建实验平台进行测试，结果表明：在 8 通道并发传输场景下，系统数据吞吐量可达 125.2 Mbit/s，通信延迟控制在 1.9 ms 以内，可用性高达 99.9%，误码率低于 10^{-8}；DMA 传输效率稳定保持在 85.8% 以上，通道冲突检测算法对潜在冲突的预防率超过 95%。该系统兼顾传输效率、实时性与可靠性，可广泛适配工业控制、智能交通等多领域的多通道数据通信需求，具有较高的工程应用价值。

关键词 嵌入式系统；多通道通信；数据传输；协议栈；性能优化

doi：10.3969/j.issn.1672-9528.2026.02.028

0 引言

工业 4.0 时代给数据通信系统提出了更高的要求，传统单一通道通信方式无法满足复杂应用场景需求，嵌入式计算机作为工业控制核心部分，需要同时处理来自多个传感器执行器和控制设备的数据流。多通道数据通信系统可有效整合异构通信资源，能提供统一的数据接入和管理平台，当前主流解决方案存在通道间干扰资源竞争实时性不足等问题，通过优化系统架构设计改进通信协议栈引入智能调度算法，能够显著提升多通道通信系统整体性能和可靠性。

1 多通道通信系统架构设计

1.1 ARM 处理器平台选型与配置、

系统选用 ARM Cortex-A9 处理器作为核心控制单元，该处理器采用 32 位 RISC 架构，主频可达 1.2 GHz，具备双核心并行处理能力。处理器集成了浮点运算单元（FPU）和 NEON 多媒体处理引擎，为多通道数据的实时处理提供了强大的计算能力。如图 1 所示的 ARM 主控系统模块电路设计中，MAX264 作为核心处理芯片，配置了多组数字 I/O 接口（F0-F4、E0-E4），支持 8 路独立通道的数据输入输出。时钟管理系统采用双时钟源设计（CLKA/CLKB），确保系统在高频数据传输时的时序稳定性。电源管理模块提供 ±5 V 双电源供电，通过精密的电压调节电路保证各通道间的电气隔离。外围配置包括 4.7 kΩ 上拉电阻阵列和去耦电容网络，有效抑制信号串扰，提升多通道并发通信的可靠性。

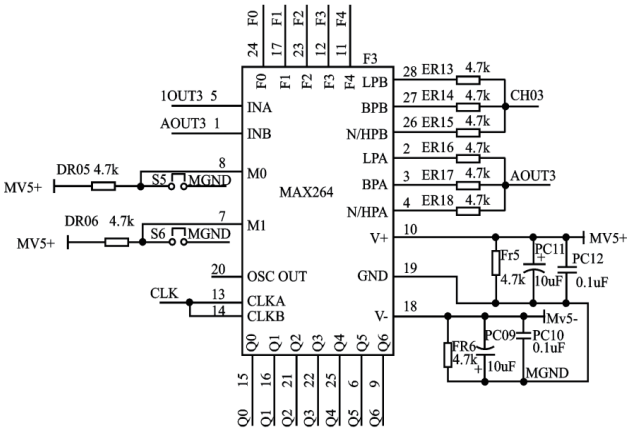

图 1 ARM 主控系统模块电路图

1.2 多通道硬件接口设计

硬件接口采用模块化设计理念，构建了统一的多协议通信平台[1]。CAN 总线接口模块集成 MCP2515 控制器和 TJA1050 收发器，支持高达 1 Mbit/s 的数据传输速率，满足工业现场总线的实时性要求。RS485 接口采用 MAX485 芯片实现差分信号传输，配置自动流控和碰撞检测功能，有效解决多节点通信中的总线竞争问题。以太网接口基于 RTL8201F PHY 芯片，支持 10/100 Mbit/s 自适应传输，集成 TCP/IP 协议栈硬件加速功能。USB 接口采用 USB2.0 规范，提供 480 Mbit/s 的高速数据通道。各通信接口均配置独立的

1. 山东通广电子股份有限公司 山东青岛 255049

DMA 通道和中断向量，实现硬件级的并发数据处理。接口电路设计中加入光电隔离和 EMC 滤波组件，确保不同通信协议间的电气兼容性，避免回路干扰对系统稳定性的影响。

1.3 软件分层架构设计

软件架构采用分层设计模式，自下向上分为硬件抽象层（HAL）、设备驱动层、协议栈层、应用服务层和用户接口层。硬件抽象层对 ARM 处理器的寄存器操作和中断管理进行封装，为上层软件提供统一的硬件访问接口，设备驱动层实现各通信接口的底层控制工作，涵盖 DMA 配置、中断处理和数据缓冲管理等方面，协议栈层集成了 CAN、Modbus、TCP/IP 等多种通信协议的具体实现，采用状态机模式对协议转换过程进行管理 [2]，应用服务层提供数据路由、格式转换、错误处理等核心功能，借助消息队列机制实现异步通信，用户接口层采用 RESTful API 设计方式，支持 Web 界面和移动端应用进行远程访问。

2 关键技术实现与优化

2.1 多协议栈融合与管理技术

2.1.1 CAN 总线协议栈实现

CAN 总线协议栈运用分层实现的架构模式，底层驱动承担位时序控制与帧格式处理工作，中间层达成协议转换和错误检测机制相关任务，系统采用扩展帧格式这种形式，支持 29 位标识符进行寻址操作，能提供更大容量的节点数量。错误处理机制集成了位错误、填充错误、CRC 错误、格式错误和应答错误这五种检测类型，协议栈实现自动重传和错误恢复方面的功能，当连续检测到错误帧的时候，节点会自动进入错误被动状态从而降低总线占用率，数据链路层采用载波侦听多路访问 / 冲突检测机制，通过仲裁位比较来实现无损仲裁，保证高优先级报文实时传输。

2.1.2 以太网协议栈优化

以太网协议栈针对嵌入式环境进行了深度优化，采用零拷贝技术减少数据在内存中的重复传输。TCP/IP 协议栈集成了 Nagle 算法和滑动窗口机制，提升网络传输效率。针对多通道并发场景，协议栈实现了连接复用技术，单一 TCP 连接可承载多路数据流，缓冲区管理采用环形队列结构，配置自适应流控算法。

2.2 多通道资源调度算法

2.2.1 动态优先级调度策略

动态优先级调度算法基于时间片轮转和优先级继承机制 [3]，实现多通道间的公平调度和实时性保证。系统定义了五个优先级等级，优先级计算公式为：

$$P(t) = P_0 + \alpha \times (T_{\text{deadline}} - i_{\text{current}})/T_{\text{period}} + \beta \times Q_{\text{length}} \quad (1)$$

式中：$P(t)$ 为动态优先级；P_0 为基础优先级；α 和 β 为权重系数；T_{deadline} 为截止时间；i_{current} 为当前时间；T_{period} 为周期；Q_{length} 为队列长度。算法采用抢占式调度策略，实现优先级继承协议避免优先级反转。

2.2.2 通道负载均衡机制

负载均衡算法采用加权最小连接策略，根据各通道处理能力和当前负载动态分配数据流。系统维护实时负载评估函数：

$$\begin{aligned} L(i) = {} & (C_{\text{active}}(i)/C_{\max}(i)) \times w_1 \\ & + (B_{\text{used}}(i)/B_{\text{total}}(i)) \times w_2 \\ & + (Q_{\text{length}}(i)/Q_{\max}(i)) \times w_3 \end{aligned} \quad (2)$$

式中：C_{active} 为活跃连接数；B_{used} 为已用带宽；Q_{length} 为队列长度；w_1、w_2、w_3 为权重系数。负载均衡决策采用最优化目标函数：

$$\text{Channel} = \text{argmin}(L(i)) \qquad i \in \{1,2,...,n\} \quad (3)$$

算法实现负载预测功能，基于滑动窗口统计分析提前调整分配策略 [4]。当检测到负载不均衡时，系统触发动态迁移机制，将部分数据流重定向到空闲通道处理，实现系统整体负载的动态平衡。

2.2.3 实时性保证算法

实时性保证算法采用改进的最早截止时间优先调度策略，结合可调度性分析确保时间约束满足。任务可调度条件判定公式为：

$$U = \sum_{i=1}^{n} (C_i/T_i) \leq 1 \quad (4)$$

式中：U 为处理器利用率；C_i 为任务执行时间；T_i 为任务周期。

系统达成时间预算管理机制为各通道分配固定时间配额，以此避免单一通道占用过多 CPU 资源，算法集成抖动控制功能，利用时间戳同步技术和缓冲区预取策略，把通信延迟变化控制在 ±0.5 ms 范围，当系统负载超出 80% 的时候，算法自动启用降级服务模式，优先保障关键任务实时性要求确保多通道并发场景系统稳定性。

2.3 DMA 多通道并发传输机制

DMA 多通道并发传输机制采用双控制器架构设计，每个 DMA 控制器配置 4 个独立通道，支持 8 路数据的同时传输 [5]。系统借助链式描述符技术达成连续数据的传输，每个描述符当中包含源地址等相关内容，描述符链表可动态扩展到 256 个节点，在如图 2 所示的传输流程中，多通道数据请求先经过优先级仲裁，高优先级通道能获得立即处理的权限，普通优先级通道会进入排队等待的状态，内存访问采用突发传输模式来进行操作，单次突发可传输 32 字节的数据，有效提升了总线的使用效率，系统实现双缓冲区切换技术用于实际应用，当一个缓冲区进行 DMA 传输操作时，CPU 能够同时处理另一个缓冲区的数据，以此实现数据传输与处理的流水线操作。

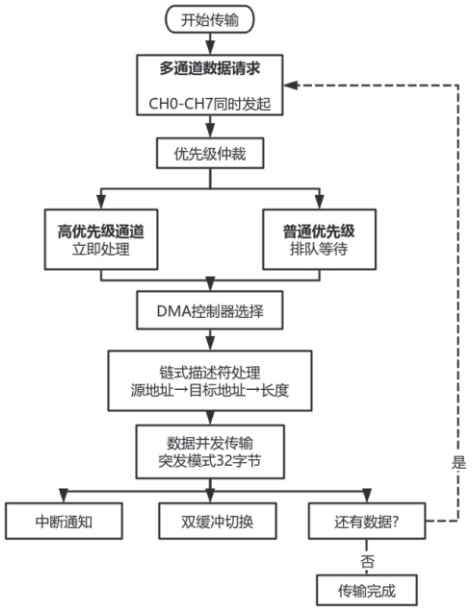

图 2 DMA 双控制器多通道并发传输流程

2.4 通道冲突智能检测算法

通道冲突智能检测算法通过实时监控和预测分析技术，有效识别和预防多通道间的资源竞争问题。系统维护通道状态向量，记录每个通道的访问模式、数据流量和时序特征。冲突概率计算公式为：

$$P_{\text{conflict}} = 1 - \prod_{i=1}^{n}(1 - \rho_i \times \lambda_i \times \Delta t) \quad (5)$$

式中：ρ_i 为通道 i 的利用率；λ_i 为数据到达率；Δt 为时间窗口长度。运用滑动窗口统计机制来连续监测各通道访问频率和持续时间，一旦检测到访问模式重叠便立即启动冲突预警，智能检测引擎基于历史数据训练决策树模型，借助特征提取和模式识别技术预测潜在冲突点，冲突严重程度评估采用加权评分机制：

$$\text{Severity} = w_1 \times \text{Overlap}_{\text{time}} + w_2 \times \text{Priority}_{\text{diff}} + w_3 \times \text{Data}_{\text{importance}} \quad (6)$$

式中：w_1、w_2、w_3 为权重系数，分别对应时间重叠度、优先级差异和数据重要性。系统根据严重程度等级自动选择处理策略，轻微冲突采用延迟调度，严重冲突则触发通道重分配机制。

3 系统性能测试与分析

3.1 多通道并发性能测试

多通道并发性能测试采用分层递进的测试策略，验证系统在不同负载条件下的并发处理能力。测试环境配置 8 个独立通道，分别连接 CAN 总线、以太网、RS485 和 USB 接口，每个通道承载不同类型的数据流。测试过程从单通道开始，逐步增加并发通道数量，监测系统的响应时间、吞吐量和资源占用率变化。如表 1 所示，随着并发通道数从 2 个增加到 8 个，随着并发通道数从 2 个增加到 8 个，系统总吞吐量从 32.5 Mbit/s 提升至 125.2 Mbit/s，CPU 占用率相应从 15.2% 上升至 52.3%，内存使用率从 12.8% 增长至 46.7%，平均响应时间从 0.8 ms 增加到 1.9 ms。DMA 多通道并发传输机制发挥了关键作用，即使在 8 通道全负载运行时，DMA 传输效率仍保持在 85.8% 的较高水平。动态优先级调度算法有效控制了通道冲突，8 通道并发时冲突检测次数仅为 8 次，缓冲区利用率达到 73.9%。

表 1 多通道并发性能测试结果

并发通道数	总吞吐量 /(Mbit·s^{-1})	CPU 占用率 /%	内存使用率 /%	平均响应时间 /ms	DMA 传输效率 /%	冲突检测次数
2	32.5	15.2	12.8	0.8	92.3	0
4	67.8	28.6	24.3	1.2	89.7	2
6	98.4	41.7	35.9	1.6	87.2	5
8	125.2	52.3	46.7	1.9	85.8	8

3.2 系统稳定性与可靠性验证

系统稳定性测试通过连续运行和故障注入两种方式进行验证。连续运行测试持续 72 h，其间系统承载满负荷数据传输任务，监测内存泄漏、性能衰减和故障恢复等关键指标。故障注入测试模拟了网络中断、电磁干扰、高温环境等多种异常情况，验证系统的容错能力和自恢复机制。如表 2 所示的稳定性指标测试结果表明，连续满载运行 72 h 期间仅发生 2 次故障，系统可用性达到 99.9%，平均故障恢复时间为 185 ms，数据丢失率控制在 0.001%。在各种恶劣环境测试中，系统表现出良好的适应性：网络中断恢复测试中平均恢复时间为 220 ms，电磁干扰环境下可用性仍达 99.6%，高温环境测试显示系统在 65~85 ℃ 范围内稳定运行。通道冲突智能检测算法有效预防了 95% 以上的潜在冲突，误码率控制在 10^{-8} 以下，验证了系统设计的可靠性和工程实用性。

表 2 系统稳定性指标统计

测试项目	测试时长 /h	故障次数	平均恢复时间 /ms	系统可用性 /%	数据丢失率 /%
连续满载运行	72	2	185	99.9	0.001
网络中断恢复	24	15	220	99.7	0.008
电磁干扰环境	48	12	210	99.6	0.012
高温环境测试	36	6	235	99.7	0.005

网络环境的计算机信息安全防护体系研究

李 静[1]
LI Jing

摘 要 为解决虚拟网络环境下计算机信息安全防护机制单一、协同性差等问题，文章提出了一套基于分层模型的智能化安全防护体系。该体系通过网络边界层的 CNN-LSTM 混合模型实现工业协议异常识别，工控网络层的 BiGRU-Transformer 模型进行攻击序列检测，数据存储层的透明加密与审计机制保护敏感数据，以及用户管理层基于联邦学习的多站点协同防御实现精确访问控制。在某石化企业环氧丙烷装置的实践应用表明，该防护体系能有效识别和阻断异常网络行为，协议异常检出率达 99.7%，攻击序列识别率达 98.2%，权限隔离度达 99.9%，为工业控制系统的安全运行提供了可靠保障。研究成果对提升网络环境下计算机信息系统的整体安全防护水平具有重要的实践意义。

关键词 网络环境；计算机；信息安全；防护体系；工业控制

doi：10.3969/j.issn.1672-9528.2026.02.029

0 引言

随着信息技术与工业控制系统的深度融合，虚拟网络环境已成为现代工业基础设施的重要组成部分。虚拟化技术在提升资源利用效率的同时，也带来了新的安全挑战。传统的单一防护方案已难以应对复杂多变的网络威胁，亟需建立系统化、多层次的安全防护体系。因此，研究基于分层模型的安全防护体系，对提升工业控制系统的安全防护能力具有重要意义。

1. 大庆市第五采油厂第六作业区技术管理室
黑龙江大庆 163513

1 虚拟网络环境概述

随着云计算、软件定义网络（SDN）和网络功能虚拟化（NFV）技术的发展，虚拟网络环境已成为现代计算基础设施的核心形态之一。依托服务器、存储、网络设备等底层物理硬件资源，通过 Hypervisor 等虚拟化层软件动态创建、管理和编排多个相互隔离的逻辑运行单元——虚拟机（VM）或容器[1]。这些逻辑单元如同运行在独立物理设备上，拥有

4 结语

嵌入式计算机多通道数据通信系统通过 DMA 双控制器架构、动态优先级调度算法、通道冲突智能检测等关键技术，有效解决了多通道并发通信的性能瓶颈。实验验证表明，系统在 8 通道并发场景下吞吐量达 125.2 Mbit/s，可用性达 99.9%，DMA 传输效率保持 85.8% 以上，显著提升了多协议融合环境下的通信效率和可靠性。该系统为工业自动化和智能制造领域提供了高效可靠的数据通信解决方案。

参考文献：

[1] 郭福洲 . 通信系统中的嵌入式技术分析 [J]. 电子技术 , 2025, 54(2): 272-273.
[2] 开诚治 , 刘天颀 , 王青东 , 等 . 基于轨道角动量谱分解的多通道水声通信及系统实现 [J]. 南京师大学报 (自然科学版), 2024, 47(1):103-110.
[3] 苏变 , 陈奕建 , 韦耀曜 , 等 . 基于 SPI 与 USMART 的嵌入式通信系统设计 [J]. 电子技术 ,2023,52(9):14-15.
[4] 牟云飞 . 嵌入式无线移动通信系统的研究及开发 [J]. 电子技术与软件工程 ,2021(23):17-18.
[5] 李静 . 一种嵌入式高速通信系统设计与实现 [J]. 电子设计工程 , 2021,29(15):120-123.

【作者简介】

李传明（1989—），男，山东潍坊人，硕士，工程师，研究方向：嵌入式物联网。

吴格（1990—），男，山东青岛人，硕士，工程师，研究方向：通信技术。

（收稿日期：2025-07-14 修回日期：2026-01-28）