

工业机械手示教器与 PLC 通信协议设计实现

樊聪远

国能准能集团有限责任公司, 内蒙古 鄂尔多斯 010300

DOI:10.61369/EPTSM.2026010025

摘 要 : 为应对工业机械手示教器同 PLC (可编程逻辑控制器) 之间数据传送的稳定性、实时性以及兼容性事项, 本文以中小型工业机械手应用场景为根基, 选用 Modbus RTU 作为核心通信协议, 完成从硬件接口匹配、协议帧结构改进至软件编程达成的全流程规划。借助 STM32F407 芯片搭建示教器控制核心, 搭配西门子 S7-1200 PLC, 构建半双工 RS-485 通信链路, 改进数据帧的地址域、功能码以及校验机制, 达成示教指令、位置数据与状态反馈的双向交互。测试结果显示, 该设计在波特率 9600bps、传输距离 10m 的工业环境里, 通信误码率低于 0.01%, 指令响应延迟控制在 50ms 以内, 契合工业机械手精准控制的实际需要, 具备较强的工程实用性。

关 键 词 : 工业机械手; 示教器; PLC; Modbus RTU 协议; RS-485 通信

Design and Implementation of Communication Protocol between Industrial Manipulator Teaching Pendant and PLC

Fan Congyuan

Guoneng Zhuneng Group Co., Ltd., Ordos, Inner Mongolia 010300

Abstract : To address the stability, real-time performance, and compatibility issues of data transmission between the industrial manipulator teaching pendant and PLC (Programmable Logic Controller), this paper is based on the application scenarios of small and medium-sized industrial manipulators. It selects Modbus RTU as the core communication protocol and completes the entire process planning from hardware interface matching, protocol frame structure improvement to software programming. Using the STM32F407 chip to build the core of the teaching pendant control, and combining with the Siemens S7-1200 PLC, a half-duplex RS-485 communication link is constructed. The address field, function code, and error-checking mechanism of the data frame are improved to achieve two-way interaction of teaching instructions, position data, and status feedback. The test results show that this design has a communication bit error rate of less than 0.01% at a baud rate of 9600bps and a transmission distance of 10m in an industrial environment. The instruction response delay is controlled within 50ms, meeting the actual needs of precise control of industrial manipulators and having strong engineering practicability.

Keywords : industrial manipulator; teaching pendant; PLC; Modbus RTU protocol; RS-485 communication

引言

工业机械手作为自动化生产线的核心执行单元, 其动作精准度与控制灵活性径直决定生产效率^[1]。示教器作为人机交互终端, 担负着动作示教、参数设定、状态监测的核心功能, 而 PLC 则负责协调机械手与周边设备 (传送带、夹具、传感器) 的联动逻辑, 二者的通信品质是保障整个自动化系统稳定运转的关键。目前中小型企业应用中, 普遍存在示教器与 PLC 通信协议不统一、数据传送延迟高、抗干扰能力弱等状况, 致使机械手动作卡顿、定位偏差等故障。鉴于此, 本文结合工业现场实际需求, 选用成熟通用的 Modbus RTU 协议, 设计适配机械手与 PLC 的通信方案, 通过硬件接口改进与软件逻辑编程, 实现二者高效可靠的双向通信, 为工业自动化生产线的稳定运行提供技术支撑。

一、通信协议选型与方案设计

(一) 常见通信协议对比与选型

工业场景中, 示教器与 PLC 的通信协议类型多样, 各有适

配场景与优缺点。Profinet、EtherNet/IP 等以太网协议传送速率快、支持节点多, 但硬件成本高、配置繁杂, 适用于大型自动化生产线; CAN 总线协议抗干扰能力强、实时性好, 但协议解

作者简介: 樊聪远 (1970.10-), 男, 内蒙古乌兰察布人, 本科, 高级工程师。

析难度大，多用于汽车制造等特殊场景；Modbus协议作为开源通用协议，分为RTU（串口）与TCP（以太网）两种模式，其中Modbus RTU通过串口传送，硬件成本低、解析简易、兼容性强，广泛应用于中小型工业设备通信。

结合本文中小型工业机械手的应用场景，综合考量成本控制、现场布线复杂程度及设备兼容性，最终选用Modbus RTU作为核心通信协议，传输介质采用RS-485总线，实现示教器与PLC的半双工双向通信，既满足数据传送的实时性需求，又降低系统搭建成本，契合工业现场的应用需求^[2]。

（二）通信协议核心方案构建

此构建运用“示教器主动生成请求—PLC被动作出回应”的通信样式，核心完成三类数据交互：其一为示教器向PLC传送控制命令（像机械手启动/停止、关节运动方位、速度调整）；其二为示教器向PLC上传示教完毕的位置参量（例如各关节角度、坐标数值）；其三为PLC向示教器回馈设备状况（比如机械手运行情形、故障编码、周边设备联动状况）。通信链路采用主从构造，示教器作为主站，PLC作为从站，从站地址设定为0x01（能够借助软件修改适配多设备），波特率默认9600bps，数据位8位，停止位1位，校验位为偶校验，契合工业现场RS-485通信的常规布置，有效增强抗干扰本领^[3]。

二、系统硬件架构构建

（一）示教器硬件模块构建

示教器硬件把STM32F407VET6单片机作为控制核心，该芯片具备高性能ARM Cortex-M4内核，主频可达到168MHz，拥有丰富的串口资源，能够满足多通道数据传输需求。硬件模块主要涵盖：核心控制模块、RS-485通信模块、显示模块、按键输入模块以及电源模块^[4]。其中，RS-485通信模块选用MAX485芯片，该芯片支持半双工通信，工作电压范围较宽（3.3V—5V），能够直接与STM32的USART2串口相连，通过DI、RO引脚完成数据的发送与接收，RE与DE引脚并联之后由STM32的GPIO引脚操控，实现发送与接收状态的转换。显示模块选用4.3英寸TFT液晶显示屏，通过SPI接口与核心芯片通信，实时展示机械手位置参量、运行状况以及故障信息；按键输入模块采用矩阵按键，实现示教指令、参数调整等操作的输入^[5]。

（二）PLC硬件接口配置

PLC选用西门子S7-1200系列的CPU 1214C，该型号PLC具备2个RS-485通信接口，支持Modbus RTU协议，能够通过集成接口与示教器的RS-485模块建立通信链路，无需额外扩展通信模块，降低硬件成本。PLC的数字量输入接口连接机械手的限位开关、急停按钮等传感器，数字量输出接口连接机械手驱动模块、夹具控制模块等执行机构，通过接收示教器指令，实现对机械手动作的精确控制，并将传感器采集的状态数据回馈给

示教器^[6]。

（三）通信链路搭建

示教器的MAX485模块与PLC的RS-485接口通过屏蔽双绞线连接，采用A、B两根信号线对应连接，同时在总线两端并联120Ω终端电阻，抑制信号反射，提升长距离传输的稳定性。硬件接线时，严格划分信号线与电源线，避免电磁干扰，电源线采用24V直流电源，为示教器与PLC提供稳定供电，符合工业现场的布线规范^[7]。

（四）通信协议与软件流程构造

通信协议选用Modbus RTU规范，该协议具有构造紧密、实时性剧烈、兼容性广阔的特征，尤其适配于工业现场设施之间的串行通信。示教器充作主站角色，PLC担当从站角色，通信地址设定为1数值。数据帧格式涵盖地址码要素、功能码要素、数据域要素和CRC校验要素，其中功能码03（读取保持寄存器）用于示教器获取PLC内部的机械手状态数据信息，功能码06（写入单个寄存器）用于向PLC下发控制指令内容。软件维度，示教器端程序依托Keil MDK平台运用C语言开展开发作业，采用模块化设计理念。主程序接通电源之后首先完成系统时钟装置、GPIO装置、USART2装置及SPI外设装置的初始化操作。USART2配置成为波特率9600bps参数、8位数据位参数、1位停止位参数、无奇偶校验参数。随后进入主循环环节，循环内部依次施行按键扫描作业、指令解析作业、数据发送/接收作业及显示刷新作业任务^[8]。

按键扫描模块运用状态机算法模式，对4×4矩阵按键实施行列扫描举措，达成去抖操作并辨识“示教”指令、“运行”指令、“参数+”指令等具体键值信号。指令解析模块依照键值组合状况，生成相应的Modbus指令数据包。比如，当用户按压“X轴+”按键之时，该模块会生成功能码为06数值、目标寄存器地址为0x0002（对应X轴正向位移情况）、写入值为固定步长（像0x000A代表10个脉冲单位数量）的数据帧结构。数据发送/接收模块通过操控GPIO引脚电平实施MAX485发送模式切换操作，将数据帧借助USART2进行发出动作；发送作业完成之后即刻切换为接收模式状态，启动定时器等候PLC响应信号。若在设定超时时间范围之内接收到完整且CRC校验准确的应答帧体，则判定通信作业成功，反之开展重试操作（最多3次频次）并记录故障码信息^[9]。

三、通信协议的软件层面实现路径

（一）示教器端的软件编程实施方式

示教器端软件依托Keil MDK开发环境体系，运用C语言开展编程工作，其核心构成涵盖串口初始化操作、Modbus RTU协议帧的构建过程、数据的发送与接收环节、数据解析处理以及状态反馈处置共五大模块内容。串口初始化模块针对USART2的工作参数进行配置设定，将波特率确定为9600bps，数据位设置

为8位，停止位设定为1位，采用偶校验方式，同时对串口中断功能进行使能操作，以此实现数据的异步接收过程。Modbus RTU 协议帧构建模块依据数据交互的类型差异，生成相对应的协议帧结构，该帧结构包含从站地址信息（1字节）、功能码内容（1字节）、数据域部分（N字节）、CRC 校验码数据（2字节）。其中，功能码选取 0x03（用于读取保持寄存器，实现对 PLC 状态数据的读取操作）、0x06（用于写入单个保持寄存器，完成控制指令的发送任务）、0x10（用于写入多个保持寄存器，进行位置参数的上传工作），从而覆盖三类核心的数据交互需求类型。数据发送模块通过对 MAX485 的 RE/DE 引脚实施控制操作，切换至发送工作状态，将构建完成的协议帧通过串口通道发送至 PLC 设备；数据接收模块借助串口中断功能接收 PLC 反馈的响应帧信息，切换至接收工作状态，同时开展 CRC 校验工作，若出现校验失败情况则重新发起请求操作。数据解析模块对校验通过的响应帧进行解析处理，提取 PLC 反馈的状态数据信息，并将其更新至显示屏进行显示操作^[10]。

（二）PLC端的软件编程实现形式

PLC 端软件基于 TIA Portal V15 编程环境平台，采用结构化文本（ST）编程方式，其核心部分包括 Modbus RTU 从站初始化操作、数据接收与解析处理、指令执行与状态反馈共三大模块内容。Modbus RTU 从站初始化模块对 PLC 的 RS-485 接口进行配置操作，使能 Modbus RTU 从站功能，设置从站地址为 0x01，与示教器的通信参数达成匹配状态，同时对保持寄存器地址映射表进行定义，将控制指令信息、位置参数数据、状态数据内容分别映射至不同的寄存器地址位置，例如：0x0000 寄存器对应着机械手启动 / 停止指令内容，0x0001-0x0004 寄存器对应着各关节位置参数数据，0x0005 寄存器对应着故障代码信息。数据接收与解析模块对串口数据进行实时监测，接收示教器发送的协议帧信息，开展 CRC 校验以及功能码识别工作，依据功能码内容执行相应的操作任务：当接收到 0x03 功能码时，读取对应寄存器的状态数据信息，并生成响应帧反馈给示教器设备；当接收到 0x06、0x10 功能码时，解析数据域中的指令内容或者参数信息，写入对应寄存器位置，进而控制机械手执行相关动作。指令执行模块根据寄存器中的指令具体内容，驱动机械手关节产生运动动作、夹具完成开合操作等，同时对传感器数据进行采集处理，更新状态寄存器的数值内容，为状态反馈提供数据层面的支撑条件。

（三）数据校验与抗干扰构建

工业场景存有电磁影响、电压起伏等状况，易造成数据传递差错，所以于软件内增强校验同抗干扰构造。除 Modbus RTU 协议自带的 CRC-16 校验之外，于数据范畴中增添冗余校验位，对关键参量（像位置坐标）实施双重校验。同时，于示教器一端设定超时重发机制，倘若传送请求之后 50ms 之内未获取 PLC 回应，则再次传送，最多再次传送 3 回，依旧无回应则判定通信故障，发出报警提示。另外，于软件中纳入数据滤波处置，对 PLC

反馈的状态数据开展滑动平均滤波，去除异常波动数据，提升数据的稳定程度；借助 GPIO 引脚操控 MAX485 的状态转换，规避发送与接收冲突，保障通信链路的顺畅态势。

四、系统测试与性能解析

（一）测试环境搭建

为验证设计规划的可行性质与稳定性质，搭建工业现场模拟测试环境，核心设施涵盖：STM32F407 示教器、西门子 S7-1200 PLC、六轴工业机械手、限位开关、急停按钮、24V 直流电源以及屏蔽双绞线。测试环境模拟中小型生产线情景，通信间距设定为 10m（工业现场常见间距），环境温度 25℃，湿度 60%，同时引入轻微电磁影响（模拟车间电机启停影响）。

（二）功能测试

功能测试主要验证示教器与 PLC 之间三类数据交互的准确性质：其一为控制指令发送，通过示教器传送启动、停止、关节运动指令，PLC 能够准确接收并驱动机械手执行对应动作，动作响应与指令相符；其二为位置参量上传，示教器记录机械手的示教位置参量，上传至 PLC 之后，PLC 能够准确存储并调用该参量控制机械手复现动作，定位误差 ≤ ± 0.1mm；其三为状态反馈，机械手运行进程中，PLC 实时采集限位开关、急停按钮状态，反馈至示教器显示屏，显示准确无误，故障产生时能够及时反馈故障代码。

（三）性能测试

性能测试重点检测通信延迟与误码率，通过改变波特率（4800bps、9600bps、19200bps），记录不同条件之下的通信性能指标，测试成果如下表所示。

表 1 通信性能指标				
波特率 （bps）	通信延迟 （ms）	发送数据量 （帧）	错误帧数 （帧）	误码率
4800	85-95	10000	8	0.08%
9600	40-50	10000	1	0.01%
19200	20-30	10000	3	0.03%

从测试得出的数据来看，当处于 9600bps 的波特率状况时，系统在通信方面展现出最优性能，将通信延迟控制在 50ms 的范围之内，误码率仅仅为 0.01%，这种情况能够对工业机械手在实时控制方面的要求予以满足；当波特率处于 19200bps 的时候，延迟呈现出更低的态势，然而误码率却有小幅度的上升，此情形受到现场电磁干扰的影响较为显著；当波特率为 4800bps 时，延迟达到了过高的程度，没有办法满足快速响应的需要。基于此，本设计把 9600bps 选作默认波特率，对实时性和稳定性进行同时考量。

五、结论与展望

（一）结论

在本文中所设计的工业机械手示教器和 PLC 通信协议方案，

是以 Modbus RTU 协议以及 RS - 485 总线作为基础,借助合理的硬件挑选和软件编写程序,让示教指令、位置参数以及状态数据实现了高效的双向交互。测试结果显示,该方案在工业现场模拟的环境当中,具备通信延迟低、误码率低以及稳定性强的特点,定位精度和响应速度都能够符合中小型工业机械手在控制方面的需求,而且具有硬件成本低、兼容性强的优势,便于在工业现场进行推广和应用,解决了传统通信方案中所存在的兼容性差、抗干扰能力弱等实际问题。

（二）展望

在后续的工作中,可以从两个方面对方案进行优化和完善:

一方面是对通信协议的兼容性进行扩展,增加对 EtherNet/IP 协议的支持,以适配大型自动化生产线中多设备联动的需求;另一方面是引入无线通信模块,像 Wi-Fi、LoRa 等,用其替代有线链路,解决工业现场布线复杂以及设备移动不便的问题,进而进一步提升系统的灵活性和适用性。与此同时,还能够对软件算法进行优化,加入数据加密功能,保障通信数据的安全性,以适应智能化工厂的发展要求。

参考文献

[1]王玲玲.基于 MCGS 的 PLC 仿真实训系统设计 [J].电动工具,2025,(06):40-44.

[2]赵宏越.基于 PLC 与组态软件的工业机电控制系统智能化改造方案 [J].信息系统工程,2025,(12):84-87.

[3]于建成.PLC 变频电气组态发展原理分析 [J].内蒙古科技与经济,2025,(21):145-148.

[4]谢李洋,陈荷燕,王坤,刘树青.基于物联网和 PLC 的变频器远程调速控制系统设计 [J].自动化应用,2025,66(21):1-5.

[5]王昊邦,康朋飞,金宇鹏,杨佳成.电机负载物理模拟平台通信协议设计 [J].科技创新与生产力,2025,46(10):96-98.

[6]周升波.基于 ISO/IEC 15693 标准的 RFID 系统的实践 [J].大众标准化,2025,(18):4-6.

[7]林金晶.通信系统质量监管与功能测试研究——基于 TCP 协议的上位机与西门子 S7-1200PLC 通信设计与实现 [J].中国品牌与防伪,2025,(11):170-172.

[8]吕栋腾,黄旭.基于 PLC 的 Profinet 转 Modbus RTU 通信设计 [J].工业控制计算机,2025,38(09):96-97+100.

[9]郭祥飞.基于工业互联网的 PLC 远程监控系统设计 [J].电子技术,2025,54(09):112-114.

[10]李浩.基于 PLC 的汽车生产线自动化控制系统优化 [J].汽车维修技师,2025,(18):118-119.