doi:10.11920/xnmdzk.2025.05.009

基于电机保护控制器的多通信协议的设计与实现

润　泽[1,2],徐　明[1,2],钟　俊[3],袁　欢[1,2]

(1.西南民族大学电子信息学院,四川 成都 610041;2. 西南民族大学信息材料四川省高校重点实验室,四川 成都 610041;
3. 四川大学电气工程学院,四川 成都 610065)

摘　要:随着工业自动化和智能制造的快速发展,电机作为关键的动力源,其安全性和可靠性直接影响生产效率以及设备的运行寿命.为应对日益复杂的工业环境和多样化的应用需求,提出了一种基于 STM32F103ZET6 和 IMX6ULL 芯片联合开发的多通信协议下电机保护控制器的设计与实现的基本方案.该控制器支持 Modbus、Profibus 以及 IEC 61850 等多种工业通信协议,并且在使用 STM32F103ZET6 芯片实现 Profibus 通信协议时,并没有使用西门子公司所生产的 Profibus 专用通信报文处理芯片,而是采用 STM32F103ZET6 内部资源,在采集数据后直接以 Profibus 报文形式进行发送,能够大幅度降低通信成本.

关键词:MCU;modbus;Profibus;IEC 61850

中图分类号:TP273　　**文献标志码**:A　　**文章编号**:2095-4271(2025)05-0542-08

Design and implementation of multi-communication protocol based on motor protection controller

RUN Ze[1,2], XU Ming[1,2], ZHONG Jun[3], YUAN Huan[1,2]

(1. School of Electronic Information, Southwest Minzu University, Chengdu 610041, China;
2. Key Laboratory of Information Materials of Sichuan Province, Southwest Minzu University, Chengdu 610041, China;
3. School of Electrical Engineering, Sichuan University, Chengdu 610065, China)

Abstract: With the rapid development of industrial automation and smart manufacturing, the safety and reliability of electric motors as critical power sources have directly impacted the production efficiency and operational lifespan of equipment. To address the increasingly complex industrial environments and diverse application requirements, this paper proposed a basic scheme for the design and implementation of a motor protection controller based on the joint development of the STM32F103ZET6 and IMX6ULL chips, supporting multiple communication protocols. The controller was compatible with various industrial communication protocols, including Modbus, Profibus, and IEC 61850. Notably, when implementing the Profibus communication protocol using the STM32F103ZET6 chip, it did not rely on Siemens' dedicated Profibus communication message processing chip; instead, it utilized the internal resources of the STM32F103ZET6 chip to directly transmit data in Profibus message format after data acquisition, significantly reducing communication costs.

Keywords: MCU; modbus; Profibus; IEC 61850

现代电机保护控制器的设计必须考虑多方面的因素,包括实时监测、故障诊断、环境适应性及设备间的互联互通等.观察已有研究,发现现有电机保护控制器设计多聚焦于电机保护算法的精度提升,但普遍存在协议单一、适用场景有限的问题[1-4].在此背景下,通信协议的选择与集成成为设计中的关键因素.

收稿日期:2024-12-20

通信作者:徐明(1969-),男,教授,研究方向:光电功能材料与器件,新一代电子信息技术.E-mail:hsuming_2001@aliyun.com

基金项目:国家自然科学(61901401);西南民族大学中央高校基本科研业务费专项(ZYN2023030)

每个设备制造商都有常用通信协议,但不同厂商之间的协议仍然存在差异,导致多个生产设备无法直接对接.这也使得新设备的引入和现有系统的升级面临诸多挑战.因此,设计一款兼容市面上应用广泛的几种协议的电机保护控制器,不仅能够提高设备间的互操作性和兼容性,还能有效解决现有系统中的通信障碍.

与其他文献的各类电机保护控制器设备相比,本文研究在通信方面完全兼容其他设计版本,并且推出了更多的通信方式. 从可行性分析的角度上来看,设备算法以及保护逻辑会有些许不同,但是对于通信原理而言并没有太多的冲突,完全可以匹配使用.

本文将重点介绍三种主要的工业通信协议:Modbus、Profibus 和 IEC 61850. Modbus 协议因其简单性和广泛性成为工业自动化领域的标准之一,适用于多种设备的互联;Profibus 协议则在高速数据传输和实时性要求高的应用中表现出色,特别适合于复杂的自动化系统;IEC 61850 协议则专注于电力行业,具备强大的数据建模能力和通信效率.这些协议的结合,能够为电机保护控制器提供多样的通信方式,以适应不同的工业需求.

1　通信协议概述

1.1　Modbus 协议

1979 年,德国 Modcion 公司发布了 Modbus 通信协议,其简单易用的特点马上受到了广泛关注.Modbus 协议演进分为两个阶段:

1)RS-232 阶段(1979—1983):点对点通信,最大速率 19.2 kbps.

2)RS-485 阶段(1984 至今):支持 32 节点组网,速率提升至 10 Mbps(EIA-485 标准)[5-7].

Modbus 通信采用“请求-响应”方式,适用于 RS-485 通信协议.当前,Modbus 协议可以在多种网络架构中进行通信,包括 PLC、HMI 及各种 I/O 接口等[8-12].

Modbus 协议数据帧结构相对简单,主要由以下几个部分构成(表 1):

地址域(Address Field):1 字节,指定从站(设备)的地址.

功能码(Function Code):1 字节,表示请求的功能类型,如读取或写入特定寄存器.

数据区(Data Field):可变长度,包含具体的数据内容.例如,读取寄存器的地址、数量等.

CRC 校验(CRC Checksum):2 字节,用于数据完整性校验,确保数据传输时没有错误.

表 1　Modbus 数据帧结构

Table1　Modbus data frame structure

地址	功能码	数据区	CRC
0x01	0x03	0x00 0x0A 0x02	0xC40E

1.2　Profibus 协议

Profibus(Process Field Bus)是一种先进的现场总线标准,能够实现高速、可靠的数据传输,适用于复杂的自动化系统.该协议支持多种通信模式,使电机保护控制器更好地融入工业自动化整体架构中.Profibus 在实时性、数据完整性和协议灵活性方面具备显著优势,是工业自动化领域的重要通信标准.Profibus 主要由以下几个部分构成(表 2):

起始码(Start Code):1 字节,用于标识帧的开始.

地址域(Address Field):1 字节,包含主站和从站的地址信息.

功能码(Function Code):1 字节,表示所请求的功能,例如读写操作.

数据区(Data Field):可变长度,包含具体的数据内容,如设备参数、状态信息等.

校验码(Checksum):1 字节,用于校验数据的完整性.

尾部(Footer):1 字节,结束符.

表 2　Profibus 数据帧结构

Table 2　Profibus data frame structure

起始码	地址	功能码	数据区	CRC	尾部
0x68	0x01	0x03	0x00 0x01	0xC40E	0x16

1.3　IEC 61850 协议

IEC 61850 通信协议是基于通用通信网络平台的变电站自动化系统所使用的唯一国际标准[13].该标准将设备(LD)抽象为多逻辑节点的服务器模型,每个 IED 智能设备由多个逻辑节点(LN)组成,而逻辑节点内部细分为数据对象(DO)和数据属性(DA).这些数据节点和对象共同构成一个服务器[14-15]. IEC 61850 数据帧主要由以下几部分组成(表 3):

版本号(Version):1 字节,版本标识.

消息类型(Message Type):1 字节,指定报文类型,比如请求或响应.

可变长度标头(Variable-length Header):包含消息长度及其他控制信息.

数据区(Data Field):根据具体请求进行数据封装,通常分为多个部分,包括数据对象、属性等.

尾部(Footer):包含校验信息或结束符.

表 3 IEC 61850 数据帧结构

Table 3 IEC 61850 data frame structure

版本	消息类型	可变长度标头	数据区	尾部
0x68	0x0001	0x03	0x00 0x01	0x16

2 各通信协议实现

2.1 Modbus 通信协议的实现

本节详细阐述电机作为 Modbus 从站的应用层通信流程.其主要涉及具体的应用和数据交互,包括功能码的定义、数据的类型以及设备的模型.从站协议栈的具体流程图如图 1 所示.

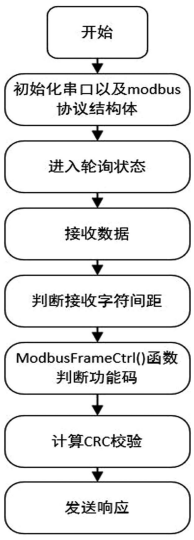

图 1 Modbus 应用层流程图

Fig. 1 Modbus application layer flow chart

在与 Modbus 通信协议相关的各类函数中,通过结构体内容判断是否执行函数操作.在 AD 采样阶段和有效值计算结束后,将有效值存储在 MCU 内存中.此期间,通信单元保持接收状态.当主机发送读取当前值命令后,MCU 进入串口中断,启动 Modbus 标志位,检查通信状态是否忙碌.若处于忙碌状态,则直接返回;若不忙,则进行状态设置和计数器初始化,完成前期配置,进入命令解析阶段.解析功能根据报文功能码分配相应功能函数,如读线圈、读输入状态、读保持寄存器等.根据报文内容提取数据长度和地址位后,将返回报文存入发送消息缓冲区,进行 CRC 校验并发送响应,具体流程图如图 2 所示.

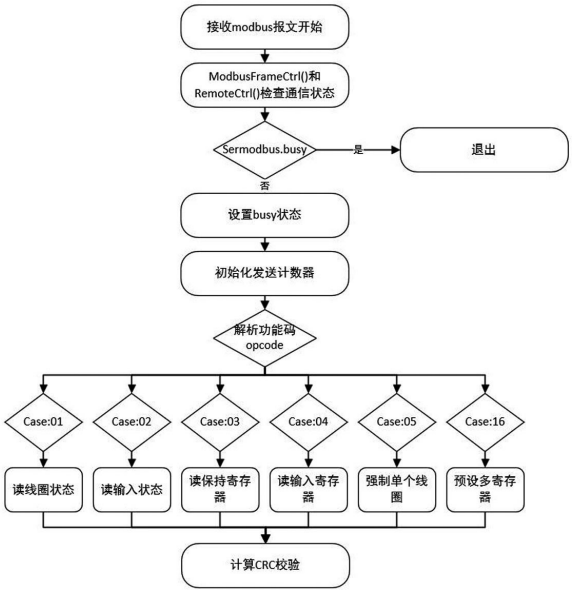

图 2 Modbus 具体功能流程图

Fig. 2 Modbus specific function flow chart

2.2 Profibus 通信协议设计

目前,Profibus 已在许多工业系统中应用,但由于成本和复杂性问题,尚未大规模使用.目前的 Profibus-DP 均使用西门子公司的 VPC3 芯片作为协议封装.截止至 2024 年 5 月,VPC3 芯片价格约为 150 元,已成为产品开发中的一项高昂成本.本文设计的基于 Modbus-Profibus 的电机保护控制器采用 STM32 内部资源进行协议封装,显著降低了成本.整体流程图如图 3 所示.

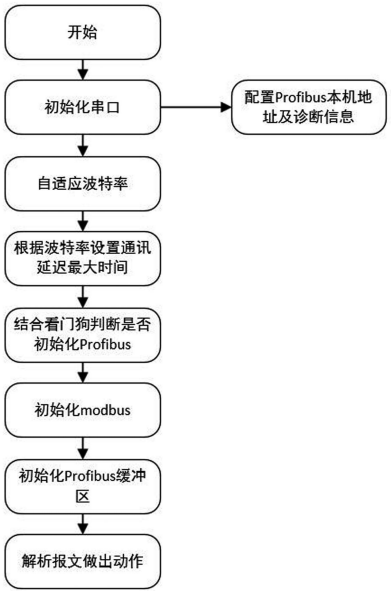

图 3 Profibus 整体流程图

Fig. 3 Profibus overall flow chart

通过通信稳定性检测后,将 485 通信模块调整为接收状态并设置接收计数器.每接收到一个字节,计时器自增一,用于判断后续 Profibus-DP 报文的有效性.在主站与从站进行数据交换前,需进行组态、诊断及参数化相关配置. 首先需发送 FDL 状态请求,明确主站与从站的通信关系,类似于电话拨打前明确通话双方.主站通过广播形式发送连接请求报文 SD1,其内容包括主站地址、从站地址及功能码.所有从站均可接收到该报文,当接收到以 10 开头、16 结尾的完整帧数据时,从站开始进行解析.若接收地址与自身地址不匹配,则不进行任何动作;仅当匹配时,从站便发送回应报文,表示准备接收报文.随后,主站发送组态报文和参数化报文,三类报文同时通过后,才会响应发送的数据请求,具体流程图如图 4 所示.

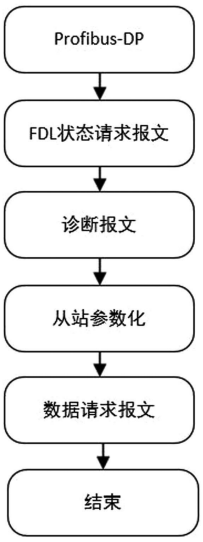

图 4　Profibus 通信流程

Fig. 4　Profibus communication flow

2.3　61850 服务器通信协议设计

本节将阐述 61850 服务器实现逻辑.代码开始部分引入了必要的头文件并定义外部变量,包括 IEC 61850 设备模型和各类数据列表.这些数据列表用于存储不同类型的数据,例如遥测(YC)、遥信(YX)、控制(YK)和电度(YM)信息.同时,使用信号处理函数捕获终止信号,以便在需要关闭服务器程序时能安全地完成关闭操作.

在主函数中,首先加载配置文件(CFG 文件),该文件定义了设备的逻辑架构及其功能.通过调用“ConfigFileParser_createModelFromConfigFileEx”函数,程序将 CFG 文件解析为设备模型.接着,创建服务器配置实例并设置多个参数,如报表缓冲区大小、MMS 文件服务基本路径、动态数据集服务启用状态以及最大客户端连接数.这些配置确保服务器以最佳性能运行并满足未来的扩展需求.

在代码的主循环中,服务器周期性更新遥测、遥信和电度值的状态.每次迭代中,程序首先获取当前时间戳并清空其标志位.然后,通过锁定数据模型,确保在更新过程中不被其他线程修改,以保证数据的一致性和安全性.在更新数据时,程序遍历各类数据列表,更新相应的属性值和时间戳.更新完成后,数据模型被解锁,并通过睡眠机制控制更新频率.

当服务器接收到终止信号时,主循环结束,服务器停止运行并清理相关资源,包括销毁服务器实例和设备模型.整体流程图如图 5 所示.

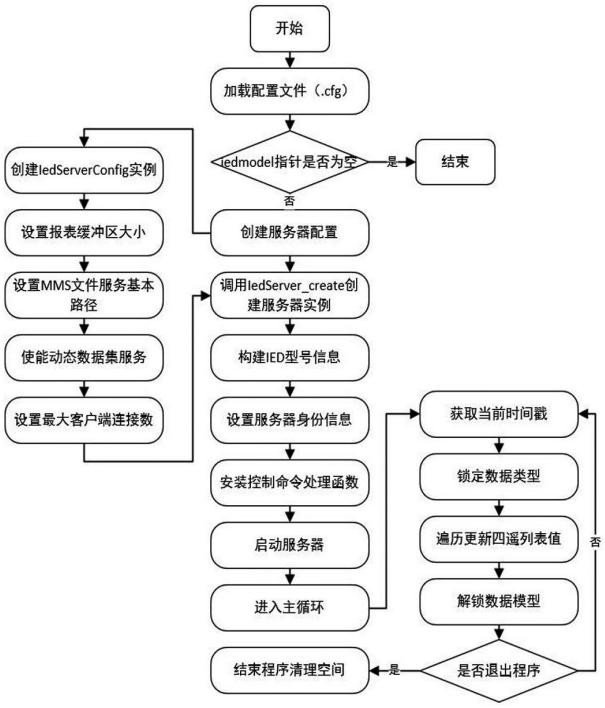

图 5　61850 服务器通信设计流程图

Fig. 5　Flow chart of 61850 server communication design

在建立 61850 服务器后,还需解决如何将数据通过客户端发送至服务端并返回的问题.61850 是基于对象的行业标准,其通信由 MMS 报文进行数据传递.当服务器完成 61850 与 MMS 的映射关系后,客户端将向服务端发送请求报文.在此过程中,MMS 通信服务由 MMS PDU 构成,并通过 ASN.1 编解码接口实现报文的编解码,最终通过 TCP/IP 协议在以太网上传输.具体的 MMS 流程图如图 6 所示.

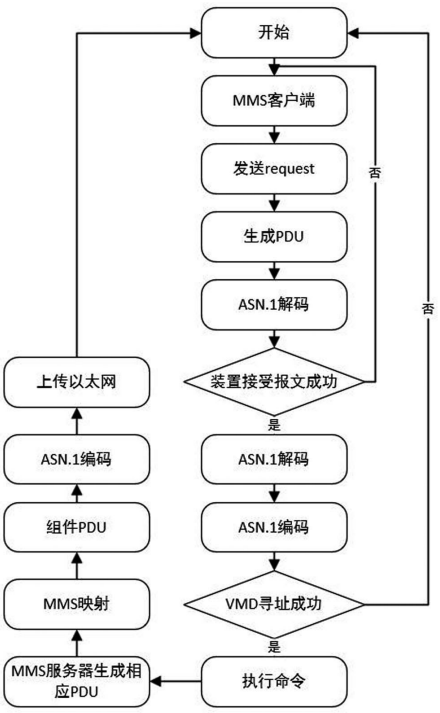

图 6 61850 MMS 流程图

Fig. 6 Flow chart of 61850 MMS

3 多通信协议协同实现与软硬件实现

3.1 多协议协同与数据共享设计

在电机保护控制器使用环境中,实现 IEC 61850、Modbus 及 Profibus 协议的高效协同是系统设计的核心挑战.本文通过统一数据存储、地址映射引擎及硬件协同机制,构建了跨协议数据交互框架,显著提升了系统的兼容性与扩展性.系统的核心是位于共享内存区的全局数据池,其物理地址映射至 IMX6ULL 的 0x80000000 区域,STM32 通过 FSMC 总线直接访问.数据池采用结构化的存储方式,包含模拟量、数字量、电度量及互斥锁等字段,通过内存对齐优化确保跨处理器访问的一致性.

地址映射引擎是多协议协同的核心模块,其功能包括静态映射表解析、动态数据类型转换及数据有效性校验.映射表通过 XML 配置文件定义协议地址与共享内存偏移量的对应关系,支持浮点型、整型及布尔值的格式转换,并检查数值范围、信号品质及更新时间,过滤无效或超时数据.以下表 4 为映射表示例.

表 4 通信协议映射

Table 4 Communication protocol mapping

物理量	IEC 61850 对象	Modbus 地址	共享内存偏移	转换系数
母线电	MMXU1. PhV. mag. f	0x4001	0x0000	0. 1
断路器位置	XCBR1. Pos. stVal	0x0001	0x0040	1;1
有功功率	MMXU1. TotW. mag. f	0x4003	0x0008	0. 01

STM32 功能模块负责数据采集、协议处理及实时控制,通过滤波与滑动窗口算法消除噪声;运行 FreeModbus 协议栈响应主站轮询,处理 03/04 功能码请求;接收 IMX6ULL 下发的控制命令,驱动光耦隔离输出模块,响应时间低于 500 μs.IMX6ULL 功能模块通过多线程管理 MMS 服务、数据同步及事件报告任务,采用优先级继承协议(PIP)解决线程优先级反转问题,为频繁访问的数据属性(如保护定值)分配专用缓存区,减少内存访问延迟.数据流采用分层缓冲设计,通过硬件缓冲、协议缓冲和应用缓冲实现高效数据传输.硬件缓冲由 STM32 的 DMA 控制器实现采集数据的零拷贝传输;协议缓冲采用双缓冲机制,确保 Modbus 事务处理无中断;应用缓冲为每个客户端分配独立报告缓冲区,防止数据覆盖.多协议并发访问可能导致数据不一致,系统通过两级机制保障数据完整性:

硬件信号同步:利用 RS-485 接口的时钟同步引脚(CLK)实现微秒级时间对齐;

事务回滚机制:在检测到冲突时自动恢复至一致状态,确保系统的可靠性与稳定性.

通过上述设计,系统实现了 IEC 61850 与 Modbus、Profibus 协议的高效协同,为电机保护控制器的运行提供了强有力的支持.

3.2 多协议协同软硬件设计

本文设计的电机保护控制器采用双核协同架构,由 STM32F103 微控制器与 IMX6ULL 应用处理器共同构成.其中,STM32F103 作为主控单元承担核心监测功能:通过内置 12 位 ADC 实现三相电流、电压信号的同步采集(采样频率设置为 16 倍工频即 800 Hz),完成包括短路保护(响应时间<30 ms)、堵转保护(动作延时 1~10 s 可调)等九大保护算法的实时计算;同时管理 8 路光耦隔离数字量输入(支持干/

湿接点自适应检测)和 4 路继电器输出(触点容量 10 A/250 VAC,配备灭弧电路).

IMX6ULL 处理器专用于处理 IEC 61850 通信协议栈,其选择基于协议栈的特殊需求:完整协议栈需占用约 256 KB RAM 空间,数据模型存储需要 512 KB Flash,远超 STM32F103 的 64 KB RAM/512 KB Flash 资源.双核间通过全双工 RS232 接口通信(波特率 115 200 bps,8N1 格式),设计专用通信协议包含 32 字节数据帧(含 2 字节 CRC 校验).系统电源采用宽压输入设计(AC85-264V),通过自研电源模块生成5 V(模拟电路供电)、3.3 V(数字电路供电)和 24 V(继电器驱动)三路隔离电源.通信模块使用 RS485 与网口联合设计,modbus、Profibus 部分使用 RS485、IEC 61850 部分使用网口进行通信,完成上位机与设备的网络系统功能.其余外设备包括液晶显示器、外置开关电源、隔离式按键输入等.方案模块如图 7 所示.

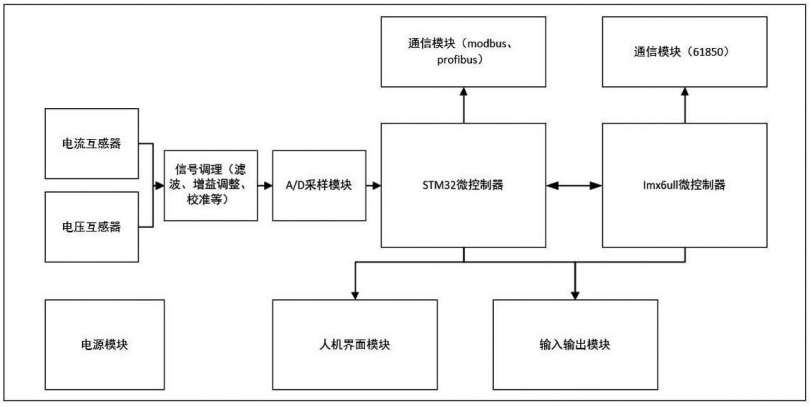

图 7　硬件模块框图

Fig. 7　Block diagram of the hardware module

4　结果与讨论

4.1　Modbus 通信协议测试

采用 RTU 模式的 Modbus 通信,通过 RS485 工业总线连接物理层,并使用串口调试助手配置串口波特率、8N1 的数据格式及校验模式开始通信实验.实验中,使用继电器保护控制仪作为电源输入.输入三相电压均为 50 V,使用 Modbus 功能代码 07 03 00 05 00 03 15 AC 进行数据回传验收.这表示设备地址为 07 的电机保护控制器回传遥测值,数据回传结果如图 8 所示.07 03 表示为地址 07 的电机保护控制器回传的遥测功能数据,06 为回传数据长度,13 78 十六进制数据转换为十进制为 4 984,精度为 0.01,因此具体数据为 49.84 V.

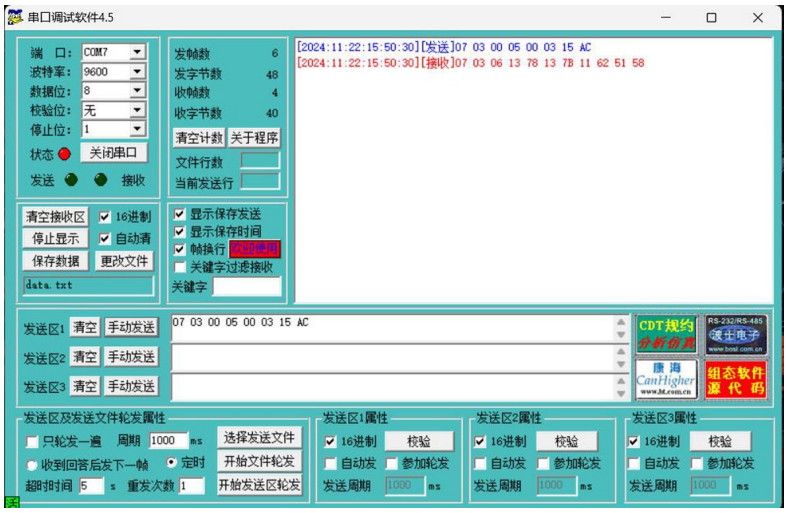

图 8　Modbus 通信结果

Fig. 8　Modbus communication results

4.2 Profibus 通信协议测试

通过上述方法完成 Modbus 与 Profibus-DP 的采集和转发功能后,以下将使用串口调试助手模拟 Profibus-DP 主站数据采集.对于 Profibus-DP,报文发送顺序至关重要,必须完整遵循顺序.本次通信中设定主站地址为 02,从站地址为 04,依次发送连接、组态、参数化和诊断报文,回传数据如图 9 所示.

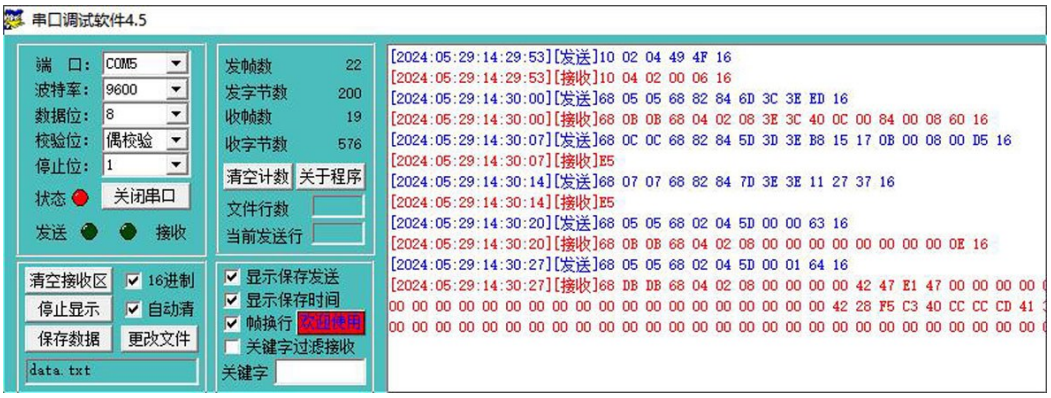

图 9 Profibus 通信结果

Fig. 9 Profibus communication results

4.3 61850 通信测试

本节旨在对 IEC 61850 通信协议在电机保护控制器系统实验当中进行测试,以验证其功能、性能和互操作性,通过三相电源进行供电,使设备能够进行正确的通信以及建模过程,例如遥测、遥信等基本功能,客户端使用的为 iec_61850_spy 国产客户端软件,三相电压均配置为 57 V,查看其通信效果,以及客户端的建立模型是否完整,具体效果图如图 10 所示.

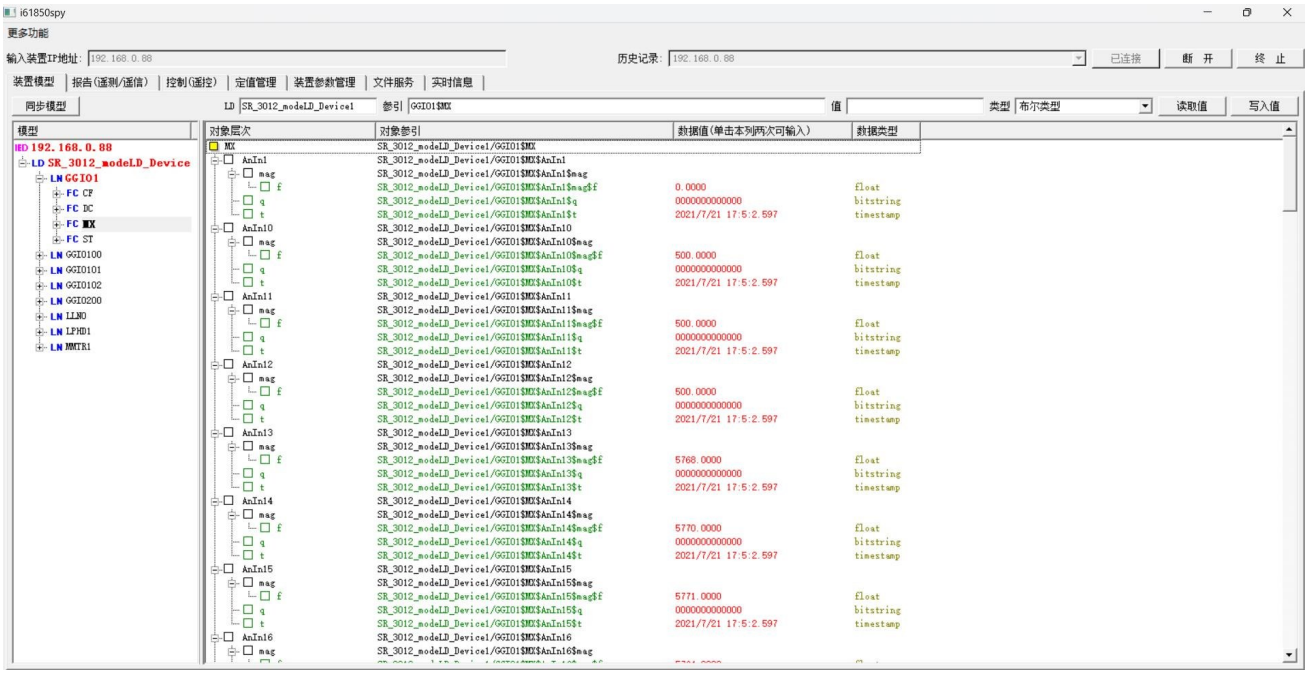

图 10 61850 通信结果

Fig. 10 61850 communication results

上述测试结果表明,本文所设计的电机保护控制器能够有效地进行数据采集与监测,确保电机的安全性与可靠性.Modbus 协议为控制器提供了简单易用的通信方式,适合不同设备的互联;Profibus 协议在高速数据传输和实时性要求方面表现出色,适合复杂的自动化系统;而 IEC 61850 协议则为电力管理提供强大的数据建模和通信效率,进一步增强了系统的灵活性和可靠性.

5　结论

针对电机保护控制器的设计与实现,提出了一种基于 STM32F103ZET6 和 IMX6ULL 芯片的多通信协议方案.通过对 Modbus、Profibus 和 IEC 61850 等多种工业通信协议的深入分析与实现,展现了该控制器在现代工业环境中的广泛适用性和高效性.该方案不仅提升了电机保护控制器的功能多样性,还为工业自动化领域的设备互联互通提供了有效的解决方案.

参考文献

[1]郁剑.船用电机保护与控制系统研究[D].镇江:江苏大学,2023.

[2]冯银飞.基于 DSP 的智能电机保护系统研究[D].南京:东南大学,2018.

[3]周向前.基于 ARM 的智能电机保护器设计[D].鞍山:辽宁科技大学,2015.

[4]冯辉.基于 RS-485 的电机保护系统的研究[D].西安:西安电子科技大学,2012.

[5]HAO Z J,ASADULLAH A,WAWALE S,et al.Application of MODBUS double-layer communication network technology in intelligent management of urban traffic equipment[J].International Journal of System Assurance Engineering and Management,2022,13(1):197-202.

[6]WANG Y,FENG X N,CHEN Y X,et al.A dual detection method for siemens inverter motor modbus RTU attack[J].Journal of Computer and Communications,2021,9(7):91-108.

[7]PALLAVI D.Design and Implementation of Circuit Analysis System for Industrial Watt-hour Meter based on MODBUS Protocol[J].International Journal of Power and Energy Engineering,2020,2(1):15-28.

[8]FENG W Q,LAI Y X,LIU Z H. Vulnerability mining for Modbus TCP based on exception field positioning[J].Simulation Modelling Practice and Theory,2020,102:101989.

[9]PARIAN C,GULDIMANN T,BHATIA S.Fooling the master:Exploiting weaknesses in the modbus protocol[J]. Procedia Computer Science,2020,171:2453-2458.

[10]宗镇彦.变频空调电控板故障自动诊断系统设计[D].青岛:山东科技大学,2020.

[11]王超.Modbus 通信协议研究及在油田控制系统中的应用[J].仪器仪表用户,2014,21(2):51-53.

[12]朱立朋.IEC 61850 智能变电站在线监测系统设计[D].济南:山东大学,2014.

[13]刘涛.基于 61850 规约的多协议转换技术研究[D].武汉:武汉理工大学,2018.

[14]范建忠.基于 IEC 61850 标准的变电站监控系统数据模型的建立与通讯实现[D].北京:中国电力科学研究院,2005.

[15]何磊.IEC 61850 应用入门[M].北京:中国电力出版社.

(责任编辑:张阳,殷锋,付强,和力新,肖丽;英文编辑:周序林,郑玉才)