

基于 IEC60870-5-104 远动规约的 PLC 通信模块的设计与实现^①

孙俊男^{②***} 刘明哲^{*} 徐皑冬^{*} 郭廷廷^{***} 韩晓佳^{***}

(^{*} 中国科学院 沈阳自动化研究所 工业控制网络与系统研究室 沈阳 110016)

(^{**} 中国科学院大学 北京 100049)

摘 要 为了实现对分布在很广地域的变电站或设备进行监视和控制的以太网规约 IEC60870-5-104 远动规约在工业通信领域的应用,首先深入分析了该远动规约的结构模型,设计了一种主要由 ARM7 内核的主控制器和以太网控制器构成的通信模块硬件平台,以及通过嵌入式实时操作系统来实现多任务调度的软件平台,并针对规约要求以及工业现场需求设计了主要任务的有限状态机模型。还通过实验对该模块的一致性、互操作性和系统性能进行了测试,结果表明,该通信模块具有系统独立、通讯稳定、互操作性强、可靠性高等特点。

关键词 嵌入式系统, IEC60870-5-104, 以太网通信, 状态机, 规约

0 引 言

IEC60870-5-104 规约由国际电工委员会(IEC)于 1998 年 8 月制定,我国于 2002 年也制定了相应的配套标准 DL/T634.5104-2002。它是基于现代电子技术和电子计算机技术,应用远程通信技术对远方变电站或者电厂的设备进行监视和控制,主要实现远程测量、远程控制和远程调节等各项功能。该规约目前在电力领域已经得到了比较广泛的应用^[1]。

随着计算机技术、网络技术、通信技术的发展,加之我国“中国制造 2025”、“互联网+”等发展理念的推动^[2],现代工业控制系统越来越复杂,工业设备逐渐增多,设备分布范围越来越广,设备与控制中心交换的数据量也急剧增加,因此,人们对工业控制系统的数据通信性能提出了越来越高的要求,通过发展网络来实现工业控制系统远动信息的快速、高效、可靠的传输成为了现在工业通信技术的发展

趋势。所有这些新需求都离不开网络化控制领域的技术和产品。对于 IEC60870-5-104 远动规约,国内基于该规约的研究大多针对于电力控制系统。本文将该规约应用在工业通信领域,以满足上述工业控制系统的新需求。

本文通过深入分析 IEC60870-5-104 远动规约,总结出该规约的层次结构模型,实现工业现场数据与调度主站按照 104 规约格式进行通信,并通过使用数据交换格式 JSON 对模块参数进行配置,以满足不同的工业现场的需求,同时,配置过程也定义了 104 规约的监测点、控制点地址与可编程逻辑控制器(PLC)所连设备地址的对应关系,实现了 PLC 与 104 通信模块的数据交换,另外,该模块还将周期地向上位机发送设备运行状态信息,以便实时监控设备的运行状况,增强了设备的可靠性。本文还通过使用 104 规约测试工具 IEC104 TESTER 模拟调度中心,即 104 主站,对 PLC 实际工作现场数据进行测试,并通过软件编写测试模块,针对数据量大、数据变化快等极端使用环境以及网络连接故障、启停

① 工业和信息化部智能制造专项(Y5C8150801)资助项目。
② 男,1992 年生,硕士生;研究方向:工业通信技术,嵌入式系统等;联系人,E-mail: sunjunnan@sia.cn
(收稿日期:2016-02-25)

控制无效、报文丢失、报文冗余等常见问题进行模拟,对该通信模块的 104 功能项以及模块性能进行全面的测试。

1 IEC60870-5-104 规约分析

1.1 规约模型

图 1 所示为终端系统上的 104 规约模型,其主要模型源于国际标准化组织(ISO)为网络通信制定的协议 ISO-OSI 参考模型^[3]。

根据IEC 60870-5-101从IEC60870-5-5中选取的应用功能	初始化	用户层
从IEC60870-5-101和IEC60870-5-104中选取的ASDU		应用层
APCI（应用规约控制信息） 传输接口（用户到TCP的接口）		
TCP/IP协议子集（RFC2200）		传输层
		网络层
		链路层
		物理层
注：第5、第6层未使用		

图 1 IEC60870-5-104 规约结构图

IEC60870-5-104 规约底层采用的是 TCP/IP 的协议子集,通过用户到传输控制协议(TCP)的接口连接到应用层,该规约的应用层分为应用规约控制信息(application protocol control information, APCI)和应用服务数据单元(application service data unit, ASDU)。

1.2 应用规约控制信息 (APCI)

图 2 所示为应用规约控制信息 (APCI) 的报文结构图^[3]。

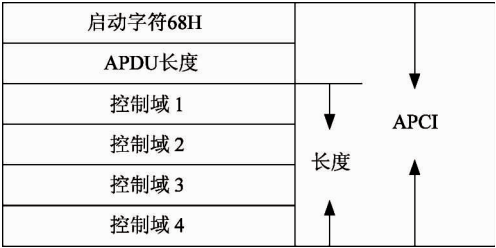


图 2 APCI 结构图

在 APCI 中,第一个字节是启动字符 68H,标志着本报文是 IEC104 规约的报文,同时启动字符也标记了 IEC104 规约的报文起始位置。

第二个字节是应用规约数据单元 (APDU) 的长度,其值不能超过 253。

接下来是 4 个字节的控制域,根据控制域 4 个字节的不同编码规则,APDU 又被分为编号的信息传输报文(I 格式)、编号的监视功能报文(S 格式)、未编号的控制功能报文(U 格式)三种报文,S 格式与 U 格式报文不包含数据信息,只有在 I 格式报文的 APDU 中包含了应用服务数据单元(ASDU)。

1.3 应用服务数据单元 (ASDU)

1.3.1 报文结构

图 3 所示为应用服务数据单元 (ASDU) 的报文结构图^[3]。

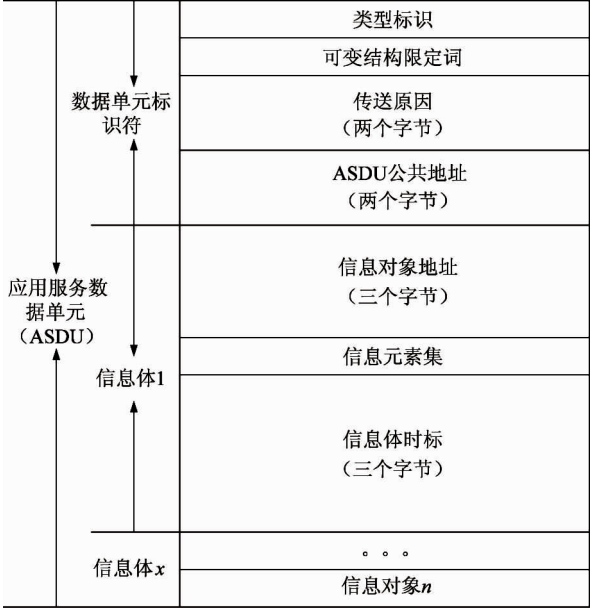


图 3 ASDU 结构图

在 ASDU 中,第一个字节是类型标识,它定义了信息对象的结构、类型和格式。

可变结构限定词,占用一个字节。它定义了信息对象的个数和信息对象的排列方式。

传输原因,占用两个字节。它定义了信息报文传输的具体原因。

服务数据单元公共地址和信息对象地址的结构,分别占用两个字节和三个字节。它们分别用来

表示站号和具体的信息对象点号。

信息对象时标,占用 7 个字节。104 规约规定可以采用 2 字节时标、3 字节时标和 7 字节时标。现在通常采用 7 字节时标,可以表示毫秒到年的时间。

1.3.2 报文类型

104 规约规定应用报文的类型主要有 4 种:监视方向的过程信息、控制方向的过程信息、监视方向的系统信息、控制方向的系统信息^[3]。

监视方向上的过程信息,包括单点遥信、双点遥信、步位置信息、归一化测量值、标度化测量值、短浮点测量值等。遥信用来表示信息对象分、合状态的数字量信息;测量值用不同的数据类型来表示信息对象的数值的模拟量信息。

控制方向上的过程信息,包括单点命令、双点命令、升降挡命令、归一化设点命令、标度化设点命令、短浮点设点命令等。单、双点命令是用来控制被控信息对象的分、合状态的数字量命令;设点命令是用不同的数据类型来设置被控信息对象的数值的模拟量命令。

监视方向上的系统信息,主要是初始化命令,负责向主站传送具体的初始化原因。

控制方向上的系统信息,包括总(组)召唤命令、电能脉冲召唤、时钟同步等。总(组)召唤命令用于召唤该站所有点或者一组点的状态与数值;电能脉冲召唤用于召唤该站所有累积量点的数值;时钟同步命令用于同步该站与主站的时钟。

2 通信模块设计与实现

2.1 硬件平台介绍

本文所设计的通信模块,硬件平台主要由 ARM7 内核的主控制器和以太网控制器构成,通过 PLC 的背板总线技术与 PLC 模块连接,实现 PLC 电源模块统一供电、模块与 PLC 控制器通过背板总线传输文件、数据等功能。该模块作为 PLC 的外接扩展模块,具有系统独立性。

2.2 系统的架构

本文所设计的通信模块系统架构如图 4 所

示^[4-8]。该模块采用嵌入式实时多任务操作系统 Nucleus PLUS 实现初始化线程、配置文件读取线程、网络线程、数据线程、104 规约主逻辑线程^[9]、状态信息反馈线程等任务的调度。

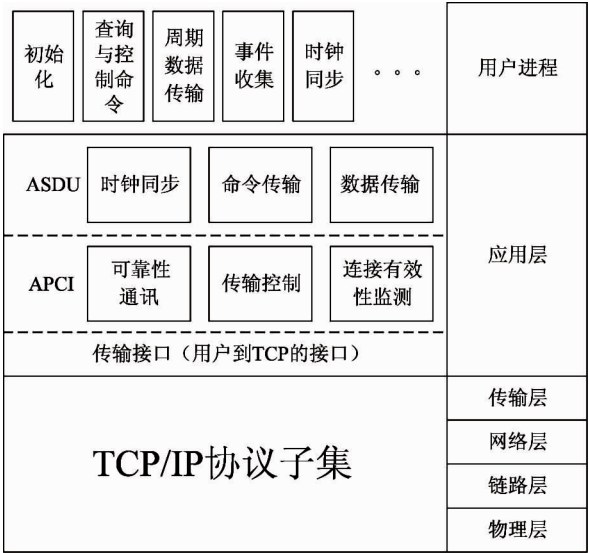


图 4 通信模块系统架构

2.2.1 初始化线程

设备上电、复位动作后,104 通信模块要首先执行初始化线程,该线程需要完成的功能主要有:初始化背板驱动、测试和清空 RAM,为其后配置文件的写入和数据交换做准备。

2.2.2 配置文件读取线程

由于 PLC 可以应用在不同场合,工业现场的数据量与通信性能参数也会不同,这时就需要选取不同的模块参数,需要配置的信息对象个数也不同,所以,本文所述模块采用上位机配置工具来对这些参数进行配置,并将配置文件发送给模块。

本文所设计的 104 通信模块的配置文件,使用 JSON 编写。JSON (JavaScript Object Notation) 是一种轻量级的数据交换格式。它易于人阅读和编写,同时也易于机器解析和生成,有利于提升网络传输速率^[10]。

该配置文件由上位机配置工具生成,一份发送给 PLC 的组态软件,该组态软件读取配置文件中的信息对象点数和点号,用于对应 104 规约应用中的点号与 PLC 的 I/O;另一份经由 PLC 控制器通过背

板发送给 104 通信模块,104 通信模块对其参数进行解析。

2.2.3 网络线程

IEC60870-5-104 规约是基于 TCP/IP 的规约。在初始化线程与配置文件读取线程完成以后,初始化 TCP/IP 协议栈,并启动网络线程,该线程状态机模型如图 5 所示,状态转换表如表 1 所示。

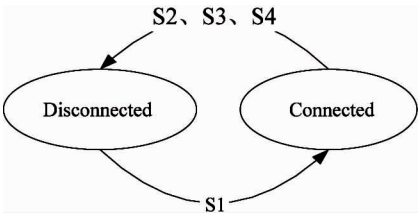


图 5 网络线程状态机模型

表 1 网络线程状态转换表

#	当前状态	事件/动作	下一状态
S1	Disconnected	Connect. req/ NetConnect()	Connected
S2	Connected	T1. timeout/ NetClose()	Disconnected
S3	Connected	K. exceeded/ NetClose()	Disconnected
S4	Connected	N(R). discontinu-ous/ NetClose()	Disconnected

2.2.4 数据线程

设备运行过程中,PLC 需要将现场设备的过程的数据发送给 104 通信模块,并通过模块将这些数据按照 104 规约的要求发送给主站,并且主站还需要将控制命令发送给 PLC 的设备,这就需要自定义一种 PLC 控制器与 104 通信模块的数据传输规则。

本文所设计的通信模块与 PLC 控制器数据传输规则如图 6 所示。在 PLC 中定义 3 块独立的存储区,即输入数据存储区、输出数据存储区、状态信息存储区,104 通信模块通过配置文件的地址偏移量对应表将规约的监视方向过程信息与 PLC 控制器输出存储区对应,将规约的控制方向的过程信息与 PLC 控制器输入存储区对应,将模块运行过程中

的状态信息与 PLC 的状态信息存储区对应,通过周期轮询的方式,向 PLC 控制器请求或发送数据的镜像。从而实现了 PLC 控制器与 104 通信模块的数据交换。

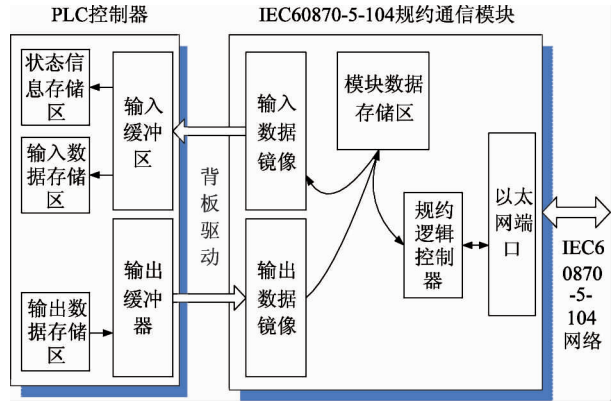


图 6 系统数据流图

该线程作为独立运行的系统模块,在系统运行的过程中始终保持数据的周期发送与接受,数据交换的周期通过配置文件进行配置。

2.2.5 104 规约主逻辑线程

在数据线程启动之后,且主站与该 104 通信模块 Socket 连接完成,将启动 104 规约主逻辑线程,该线程是模块实现 104 规约的核心部分。

该线程的状态机模型如图 7 所示,状态转换表如表 2 所示。

该线程启动以后,网络线程一直处于监听网络数据的状态,直到收到主站的传输控制报文 STARTDT 之后,模块的数据收发进入准备状态,数据传输功能启动,当收到主站的传输控制报文 STOPDT 之后,模块停止与主站的数据传输,直到主站再次发送 STARTDT 报文。

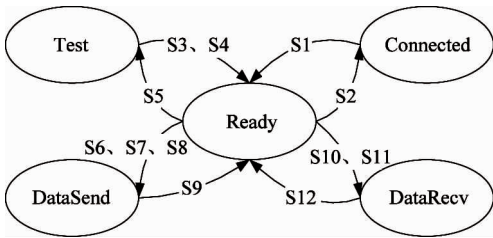


图 7 主逻辑线程状态机模型

表 2 主逻辑线程状态转换表

#	当前状态	事件/动作	下一状态
S1	Connected	STARTDT. req/ STARTDT. con/ ProcessDTRrecv() ProcessDT()	Ready
S2	Ready	STOPDT. req/ STOPDT. con	Connected
S3	Test	TESTFR. req/ TESTFR. con/ ProcessDTRrecv() ProcessDT()	Ready
S4	Test	TESTFR. con/ ProcessDTRrecv() ProcessDT()	Ready
S5	Ready	T3. timeout/ TESTFR. req	Test
S6	Ready	TeleSignal. chg TeleMetering. chg/ NetWrite() T2. reset/N(S) + 1	DataSend
S7	Ready	W. exceeded/ NetWrite() T2. reset/ N(S) + 1	DataSend
S8	Ready	Command. req/ NetWrite() T2. reset/ N(S) + 1	DataSend
S9	DataSend	Send. success/ ProcessDTRrecv() /ProcessDT()	Ready
S10	Ready	Command. req/ ProcessDTRrecv() T3. reset/ N(S) + 1	DataRecv
S11	Ready	Data. refresh/ ProcessDTRrecv() T3. reset/ N(S) + 1	DataRecv
S12	DataRecv	Recv. success/ ProcessDTRrecv() ProcessDT()	Ready

104 通信模块与主站通信主要分为两部分内容,一是响应主站的命令,二是从站变化数据主动上

送。

主站的命令主要有总召唤、组召唤、电能累计量总召唤(遥脉总召唤)、对时命令、控制命令。收到主站总召唤与组召唤命令后,根据所配置的点的数量以及地址排列方式,分单帧和连续多帧向主站应答;收到对时命令后,则根据收到的主站时间来校对该 104 通信模块的时间,并以对时命令的镜像向主站发送确认应答;收到控制命令则先判断命令类型,若为选择命令,则先选中命令点,若为执行命令,则将控制命令发送给 PLC 控制器的输入缓冲区,执行该命令,若为撤销命令,则以原状态应答,撤销该命令。

从站变化数据主动上送主要有遥信变位和遥测数据跨越死区两种情况。遥信变位即该遥信点的状态由分变为合,由合变为分,则产生一个事件,并将该变位的遥信点号地址、变位信息、变位时间上送至主站;遥测数据跨越死区即该遥测点本次数据的变化范围大于为该点配置的死区数值范围,则产生一个事件,并将该变化的点的点号信息、当前值、变化时间上送至主站。

另外,为了保证可靠性通讯和连接的有效性,在线程执行时启动 TCP 连接超时定时器 t0、帧确认超时定时器 t1、无 I 帧超时发送 S 帧定时器 t2 和超时监测定时定时器 t3,以及报文计数器 k、w。

3 实验结果

3.1 实验平台介绍

如图 8 所示,该实验平台包括电源模块、PLC 控制器、104 规约通信模块。电源模块通过背板给 PLC 控制器和 104 通信模块供电。104 通信模块的以太网接口与 PC 连接,在 PC 端使用 IEC104TESTER

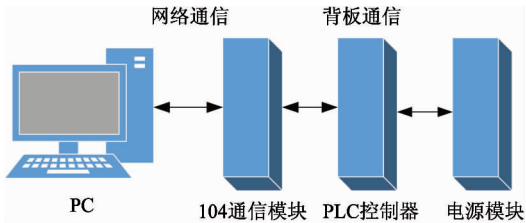


图 8 实验平台架构

软件来模拟 104 主站,对该通信模块的一致性、互操作性和系统性能进行了测试。

3.2 一致性测试

使用 IEC104 TESTER 软件,选择“模拟主站”选

项,此时该软件会模拟 104 通信网络的主站,定期的发送命令与接受数据。结果如图 9 所示,该模块满足一致性。

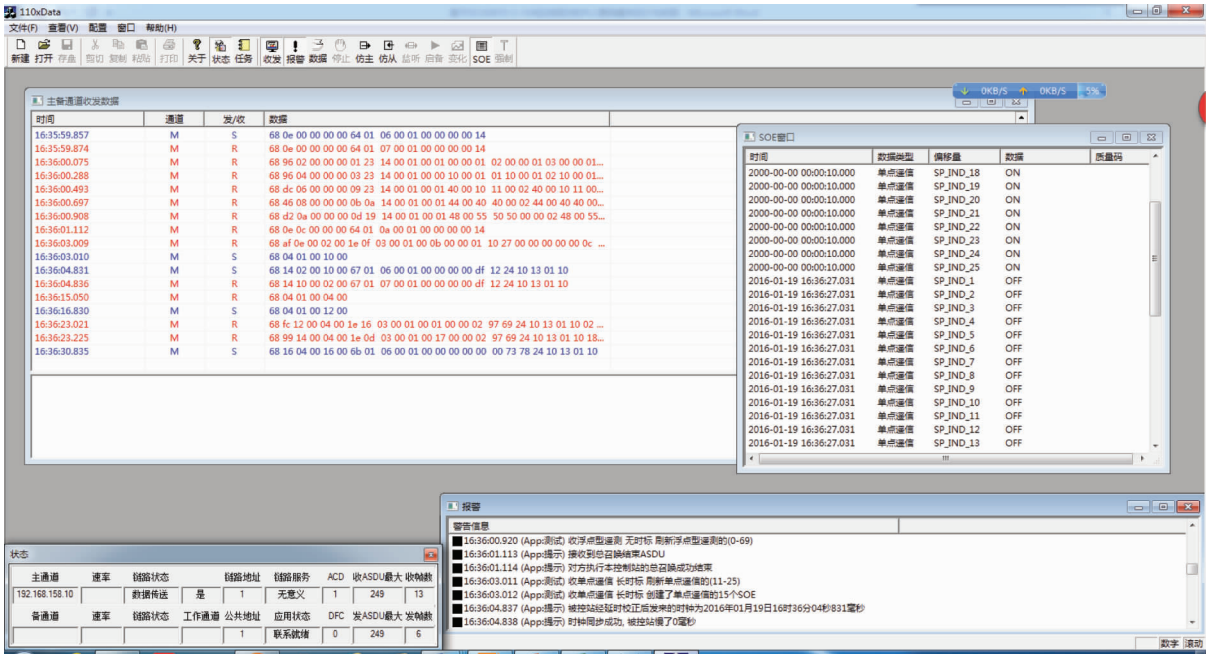


图 9 实验结果

3.3 互操作性测试

更改测试软件参数,同时相应的修改 104 通信模块的配置参数,以模拟不同规格和不同使用情景下的主站,实验结果表明,该模块满足互操作性。

3.4 系统性能测试

考虑到工业现场存在数据量大,数据变化快等极端环境,本文通过编写测试模块,针对这两种情况对该 104 模块在不同数据量、不同数据变化速率的情况下的平均时延进行了统计分析。结果如图 10 所示。横轴为同一时刻产生的待发送报文的数量,

4 条曲线自下向上依次为数据刷新速率为 10 秒、5 秒、1 秒、0.1 秒的平均时延情况。

经过对工业现场需求数据量和时间精度的调研,该模块的性能能够满足绝大多数工业现场的需求。

4 结 论

本文通过深入分析 IEC60870-5-104 远动规约的结构模型,提出了一种实现 IEC60870-5-104 远动规约的通信模块的设计方案,并予以实现。硬件平台能够很好地支持 PLC 的架构。软件平台通过嵌入式实时多任务操作系统来实现任务的调度,并且针对每个任务分别提出了状态机模型,来实现各个模块的功能。

本文所设计的通信模块,作为 PLC 的扩展模块,具有独立的软硬件平台,PLC 与模块协同工作,模块的改动不会影响 PLC 性能,具有系统独立的特点;模块系统参数与性能参数可以通过配置文件进

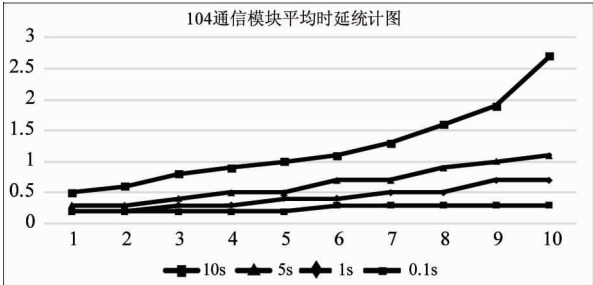


图 10 性能测试统计图

行修改,满足不同规格、不同使用情景下的主站要求,具有互操作性强的特点;模块选取高性能软硬件平台并设计良好的系统架构,使得模块具有通讯稳定、可靠性高的特点。接下来将针对该模块进行进一步的优化,提升系统性能与可靠性。

参考文献

- [1] 薛飞. IEC60870-5-104 协议的软件建模与实现:[硕士学位论文]. 北京:华北电力大学(北京)控制与计算机学院, 2012. 23
- [2] 贺正楚, 潘红玉. 德国“工业 4.0”与“中国制造 2025”. 长沙理工大学学报:社会科学版, 2015, 3: 103-110
- [3] International Electrotechnical Commission. IEC-60870-5-104 Network access for IEC 60870-5-101 using standard transport profiles. Geneva, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1998
- [4] International Electrotechnical Commission. IEC-60870-5-1 Telecontrol equipment and systems, Part 5: Transmission protocols, Section 1: Transmission frame formats. Geneva, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1990
- [5] International Electrotechnical Commission. IEC-60870-5-2 Telecontrol equipment and systems, Part 5: Transmission protocols, Section 2: Link transmission procedure. Geneva, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1990
- [6] International Electrotechnical Commission. IEC-60870-5-3 Telecontrol equipment and systems, Part 5: Transmission protocols, Section 3: General structure of application data. Geneva, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1990
- [7] International Electrotechnical Commission. IEC-60870-5-4 Telecontrol equipment and systems, Part 5: Transmission protocols, Section 4: Definition and coding of application information elements, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1990
- [8] International Electrotechnical Commission. IEC-60870-5-5 Telecontrol equipment and systems, Part 5: Transmission protocols, Section 5: Basic application functions, Switzerland: International Electrotechnical Commission, Technical Committee 57, Working Group 03, 1990
- [9] Fu Q C, Liu Z Y, Fu K J. Implementation of IEC60870-5-104 Protocol Based on Finite State Machines. In: Proceedings of the International Conference on Sustainable Power Generation and Supply, Nanjing, China, 2009, 45: 1-5
- [10] 胡晓锋. JSON 与 XML 在网络数据传输中的应用分析. 电脑编程技巧与维护, 2010, 10: 77-78

Design and implementation of PLC communication module based on IEC60870-5-104 protocol

Sun Junnan^{***}, Liu Mingzhe^{*}, Xu Aidong^{*}, Guo Tingting^{***}, Han Xiaojia^{***}

(^{*} Industrial Control Networks and systems Department, Shenyang Institute of Automation Chinese Academy of Sciences, Shenyang 110016)

(^{**} University of Chinese Academy of Sciences, Beijing 100049)

Abstract

In order to apply the IEC60870-5-104 telecontrol protocol, an Ethernet protocol for monitoring and controlling the substations or equipment in wide area to the field of industrial communication, this study analysed the structure of the IEC60870-5-104 telecontrol protocol, and presented a method for design and development of a PLC communication module based on this protocol. The hardware platform of this communication module mainly includes the processor based on the ARM7 kernel and Ethernet controller. The software platform uses the embedded real-time multi-task operating system to schedule the tasks of configuration file read, state feedback, module and PLC controller information exchange, data transformation according to the protocol request. The consistency, interoperability and system performance of the module were tested by experiments. The results showed that the communication module had the characteristics of independence, stability, strong interoperability, high reliability and so on.

Key words: embedded system, IEC60870-5-104, ethernet communication, finite state machine, protocol