● 特种铸造 Special Casting ●
DOI:10.16410/j.issn1000-8365.2019.12.021

Modbus TCP/IP 协议在反重力铸造数据记录与处理系统中的应用

李 建,郝启堂,李新雷
(西北工业大学 材料学院,陕西 西安 710072)

摘 要:反重力铸造过程中数据产生多且快,如何高效精确采集生产数据对于提高铸件产品质量以及后续铸件质量跟踪有着至关重要的作用。将 Modbus 协议与当下广泛应用的 TCP/IP 网络技术结合起来,基于 Modbus TCP/IP 协议与 Socket 技术,采用 C# 高级语言完成反重力铸造数据记录与处理系统以太网通信设计。结果表明,基于以太网通信的数据记录与处理系统在实际生产数据记录过程中通信稳定,数据传输能力强,具有很高的实用性。

关键词:Modbus TCP/IP 协议;反重力铸造;以太网通信
中图分类号:TG249.9 **文献标识码**:A **文章编号**:1000-8365(2019)12-1315-05

Application of Modbus TCP/IP Protocol in Counter-gravity Casting Data Recording and Processing System

LI Jian, HAO Qitang, LI Xinlei
(School of Materials Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: In the process of counter-gravity casting, data was generated more and faster. How to collect production data efficiently and accurately plays an important role in improving casting quality and follow-up casting quality tracking. Combining Modbus protocol with TCP/IP network technology widely used at present, based on Modbus TCP/IP protocol and Socket technology, the Ethernet communication design of counter-gravity casting data recording and processing system was completed by using C# high-level language. The results show that the data recording and processing system based on Ethernet communication has stable communication, strong data transmission ability and high practicability in the process of actual production data recording.

Key words: Modbus TCP/IP protocol; counter-gravity casting; ethernet communication

反重力铸造数据记录与处理系统是反重力铸造设备中的重要组成部分,用于记录与处理反重力铸造过程参数,例如上下罐体压力、金属液温度、组合阀开度,以及多个开关量输入输出信号等[1,2]。这些过程数据在一次短暂的铸造生产过程中被数据记录系统快速准确获取是较为困难的,往往需要一个稳定可靠的通信系统来支持。当前,国内应用在反重力铸造数据记录与处理系统上的通信方式大多是 Modbus 串行通信,但在"工业 4.0"以及"中国制造 2025"战略方针提出信息化智能制造理念后,串行通信在网络技术上的应用短板显现出来[3,4]。而基于 Modbus TCP/IP 协议的以太网通信相比于 Modbus 串行通信,其硬件接口由 RS-232/RS-485 串口变为以太网端口,通信报文通过以太网完成传输。通信模式以及硬件支持的变化,使得以太网通信可以很好的与各种网络技术结合,同时在通信距离、通信稳定性和通信速度上较串行通信有着很大的提升[5]。所以在本文中将研究如何把 Modbus TCP/IP 协议应用到反重力铸造数据记录与处理系统中,实现铸造过程数据信息化、网络化收集记录。

1 Modbus TCP/IP 通信分析

1.1 Modbus TCP/IP 以太网通信系统结构

图 1 中给出 Modbus TCP/IP 协议下的以太网通信系统结构,其结构为 C/S(客户端/服务器)架构,客户端与服务器通过 TCP/IP 网络或由网关、路由器等设备形成的串行链路子网实现通信连接。图中客户端向服务器发送 Modbus 请求报文,服务器接收来自客户端的请求报文,并根据请求报文指示向客户端回复响应报文,客户端再接收验证响应报文。Modbus 报文在客户端和服务器之间被循环进行请求、指示、响应、验证四种处理,处理的过程中完成了

收稿日期:2019-08-16
作者简介:李 建(1995-),安徽合肥人,硕士生.研究方向:反重力铸造数据记录与处理系统的研究.
E-mail:2995477994@qq.com

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

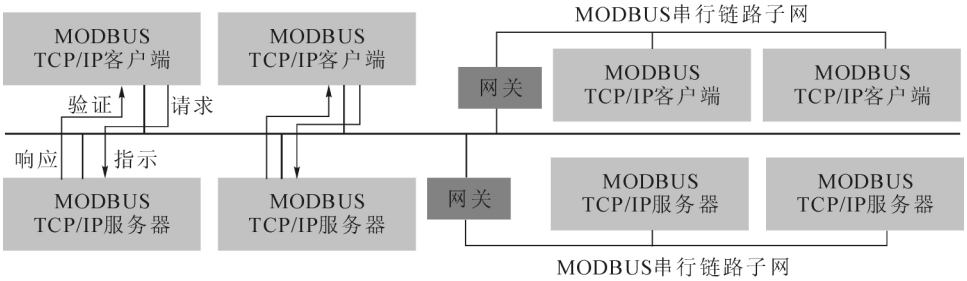

图 1 Modbus TCP/IP 以太网通信系统结构图

Fig.1 Modbus TCP/IP protocol Ethernet communication system diagram

客户端与服务器之间的数据交换。

1.2 Modbus TCP/IP 通信帧格式

Modbus 协议下数据被封装成应用数据单元(ADU)在总线或其他网络上传输,在不同类型通信模式下应用数据单元结构存在差异,如图 2 中所给出的在 Modbus 串行链路和 Modbus TCP/IP 下的 ADU 结构[6,7]。对比图中两种通信模式的 ADU 可看出,在 Modbus TCP/IP 协议下 ADU 少了地址域和差错校验域,多了一个 MBAP 报文头,其 ADU=MBAP 报文头 +PDU。

MBAP 报文头其作用是方便在 TCP/IP 网络上传输和提取报文,保证报文的完整性。结构上主要包括事务处理标识符、协议标识符、长度以及单元标识符 4 个域。表 1 中列出了 MBAP 报文头中每个字段所占字节长度及作用描述。

表1 MBAP报文头组成及描述

Tab.1 Composition and description in MBAP Header

字段	所占字节长度	描述
事务处理标识符	2 字节	请求 / 响应事务处理的识别码,常用 0x00 0x00
协议标识符	2 字节	0 表示 Modbus 协议,设置为 0x00 0x00
长度域	2 字节	长度字段其后字节数目,等于单元标识符+功能码+数据字段字节总和,用于限定报文的范围
单元标识符	1 字节	总线或其他网络上远程从站连接的识别码(从站站号)

协议数据单元(PDU)由功能码和数据字段两部分组成。功能码用于客户端指示服务器执行何种行为,而数据字段则是存放在某一功能码下,服务器执行该功能时,所需的数据或服务器响应功能时采集到的数据。

2 数据记录与处理系统以太网通信的实现

2.1 数据记录与处理系统结构

图 3 中给出反重力铸造数据记录与处理系统结构组成,客户端与服务器通过网线、光纤、交换机等通信介质实现物理连接,以 Modbus TCP/IP 协议作为通信协议实现数据交换。其中客户端是采用 C# 高级编程语言自行开发并运行在 Windows 操作系统上的应用软件,包括参数设置、过程监控、数据处理和故障定位等操作界面,可以实现工艺参数下载至 PLC 以及采集读取 PLC 数据并显示客户端界面上。服务器是配置以太网端口的 PLC,铸造生产中上传实时数据给客户端,同时也作为反重力铸造设备动作执行控制器控制设备运行。

2.2 客户端通信设计

本文在客户端通信设计上主要利用 Socket 技术实现以太网通信[8]。客户端以太网通信设计流程如图 4 所示,具体实现过程如下。

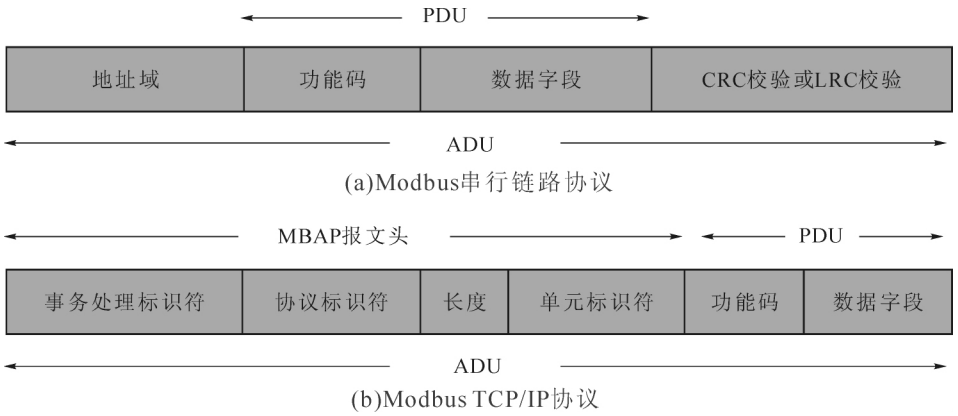

图 2 不同通信协议下 ADU 格式

Fig.2 ADU format under different communication protocol

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

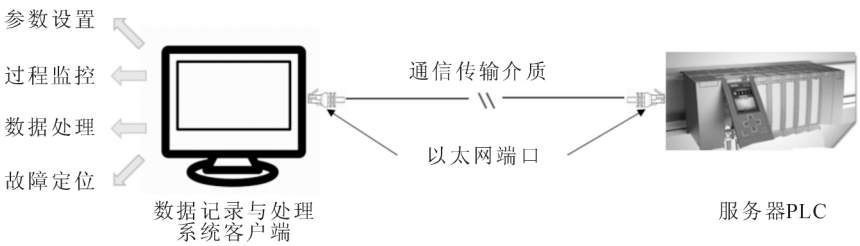

图 3 数据记录与处理系统结构示意图

Fig.3 Schematic structure diagram of data record and processing system

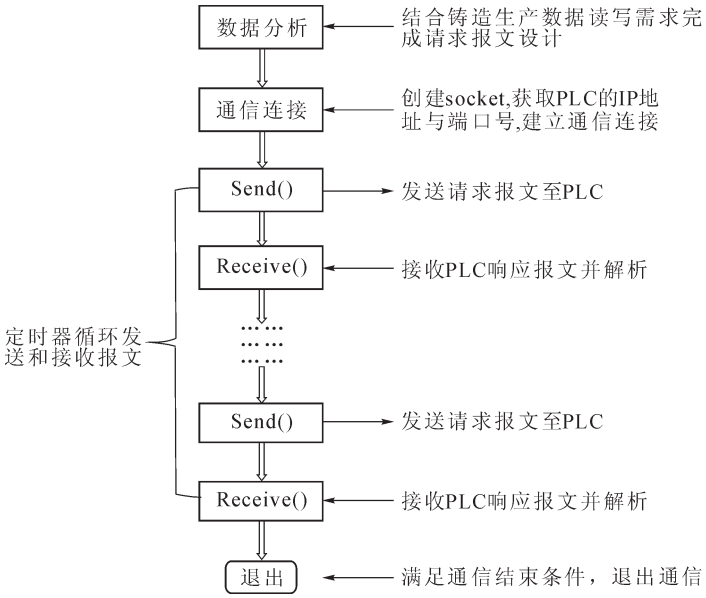

图 4 客户端通信流程图

Fig.4 Communication flow diagram of Client

(1)**通信数据分析**　客户端服务器通信连接前对反重力铸造数据记录过程进行数据读写需求分析，确定客户端需要从 PLC 各个变量表中采集记录的线圈量、离散量和保持寄存器量。再根据读写的 PLC 变量类型、个数及起始地址，选择相应的 Modbus 功能码完成请求报文设计。表 2 中给出客户端所读写的部分铸造过程数据介绍。

表2 铸造过程参数介绍

Tab.2 Casting process parameters introduction

PLC 变量	描述	Modbus 地址	数据类型
线圈变量	组合阀状态信号、触点信号等	00001-0xxxx	位
离散量输入	充型开始按钮、同步建压按钮、紧急停止按钮等	10001-1xxxx	位
保持寄存器变量	同步压力、设定压力、给定压力、实测压力、实测时间、组合阀开度、上罐 / 下罐压力等	40001-4xxxx	实数 / 整型

(2)**通信连接**　通信连接过程中客户端先实例化一个 Socket 对象，随后利用 IPEndPoint 通信类完成对服务器 IP 地址和端口号的组合，创建客户端连接服务器的连接点。再通过 Socket 对象调用 Connect()通信连接函数，建立客户端与连接点的通信连接，从而实现对服务器的通信连接。其实现核心代码如下：

```
Socket socket=new Socket (AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
IPEndPoint newserver=new IPEndPoint (IPAddress, Port);
socket.Connect(newserver);
```

(3)**循环发送请求命令**　通信连接完成后，客户端采用定时器通过 socket 对象定时调用 send()函数循环发送请求报文至 PLC，实时记录铸造过程数据。实现代码如下：

```
void timer_Tick_1 ( )
{
  Byte  [] byte=new Byte  [] {·····请求报文·····};
  Socket.send(byte);
}
```

(4)**接收验证解析响应命令**　当客户端发送请求报文后，PLC 会回复一条响应报文，客户端需要接收验证并解析响应报文。报文接收是通过 socket

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

对象调用 Receive()函数实现。报文验证是通过判断响应报文功能码是否与原报文功能码完成的，正常响应报文功能码与原报文功能码相同，异常响应功能码则是将原报文功能码最高位置位所得。最后，通过验证的正常响应报文在字节转 8 位二进制、双字节转整型和四字节转实数型等方法下被解析，解析获取的输入输出开关量数据和保持寄存器数据被用于客户端界面显示和客户端本地保存。部分代码如下：

```
Byte [] data=new Byte [1024];
Socket.Receive(data);
if(data[7]==01){···响应报文解析···};
if(data[7]==02){···响应报文解析···};
if(data[7]==03){···响应报文解析···};
```

2.3 服务器通信设计

服务器为配置以太网端口的 PLC，不同类型 PLC 需要采用相应的下位机程序编辑软件，完成对服务器端以太网通信设计。主要设计思路是利用下位机程序编辑软件在 PLC 主程序上添加以太网通信库中的服务器通信模块，在模块中完成本地 PLC 的 IP 地址和端口设置，添加通信客户端 IP 地址，并配置客户端读写保持寄存器中数据的起始位置及个数。最后，将配置好的通信模块与下位机程序装载到现场 PLC 中，即可完成服务器端以太网通信设计。

3 现场通信测试

3.1 通信稳定性测试

在完成客户端界面、通信程序设计后，在反重力铸造生产现场对数据记录与处理系统进行通信和运行测试，现场测试设备的动作执行控制器为西门子 S7-1500 PLC。测试前利用 Portal 软件完成服务器端通信配置，IP 地址设置为 192.168.116.240，端口为 502。再通过光纤、工业交换机和网线，将现场 PLC 与 200 米外控制室内电脑连接，最后给 PLC 上电并运行远端电脑上的数据记录系统客户端。测试过程中客户端定时发送请求报文给 PLC，发送周期设置为 30 ms。发送报文同时在客户端电脑上利用 Wirshark 网络封包分析软件，捕获客户端与 PLC 之间的通信报文，并测试通信过程速率，从而实现通信过程稳定性测试。

图 5 给出通过 Wirshark 软件在通信 8 h 内对通信数据包数量以及通信速率的稳定性测试的监测结果。从图中可看出，在测试中客户端发送接收报文数量与通信时间呈线性关系，接受发送报文总计大约 925 000 条，平均每秒发送接收报文数量稳定

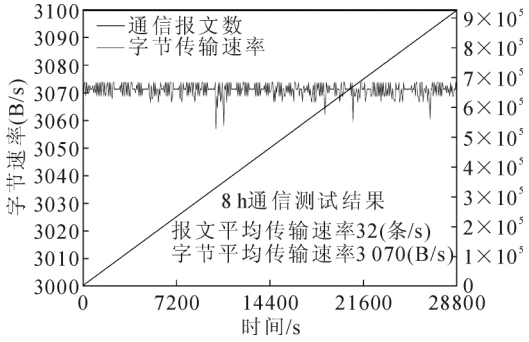

图 5 通信报文数和通信字节速率
Fig.5 Message number and byte rate

在 32 条左右，平均发送接收字节速率稳定在 3 070 B/s 左右。在整个测试过程中没有出现传输报文和字节数的突然性的增加或减少，表明通信测试过程中客户端服务器之间没有出现通信异常或数据丢失问题，通信稳定性良好，完全满足反重力铸造实际生产数据记录稳定性要求。

3.2 通信网络带宽测试

在完成现场通信稳定性测试后，利用微软公司的 PsPing 通信测试软件对控制室客户端与现场 PLC 之间网络带宽进行测试，测试以太网通信下数据传输能力是否可以满足反重力铸造实际生产中大数据量下的通信速率要求。表 3 中列出 PsPing 软件测试参数介绍，图 6 中给出通信测试参数设置与测试结果。测试过程中利用实际生产时通信稳定性测试结果作为本次带宽测试参数，客户端电脑发送 925 000 条长度为 3 070 字节的报文给现场 PLC。测试结果显示，在该条件下客户端电脑与 PLC 之间最小带宽为 783.49 kB/s，最大带宽达到 1.63 MB/s，全程平均带宽为 1.52 MB/s。从测试结果可得其数据传输能力相比 9.6 kbps 或 19.2 kbps 波特率下的串行通信有着明显的提升，也远远高于现场生产时的 3 070 B/s 通信速率要求。

表3 带宽测试参数描述
Tab.3 Parameter description in bandwidth test

参数	描述
-b	代表进行带宽测试
-l	定义测试过程中数据包字节长度
-n	代表测试过程中发送数据包个数
IP : Port	测试连接对象的 IP 地址及端口号

3.3 数据记录与处理系统现场监控界面

图 7 是现场通信测试过程客户端监控界面，包括了对实时压力、跟踪时间、组合阀开度等铸造过程数据的监控，以及实时压力曲线跟踪。在反重力铸造生产现场通信测试时，客户端完成通过 Modbus TCP/IP 以太网通信从 PLC 实时采集铸造过程数据，

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

```
C:\Windows\system32>psping -b -l 3070 -n 925000 192.168.116.240:502

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Setting warmup count to match number of outstanding I/Os: 8
TCP bandwidth test connecting to 192.168.116.240:502: Connected
925008 iterations (8 warmup) sending 3070 bytes TCP bandwidth test: 227013100%

TCP sender bandwidth statistics:
  Sent = 925000, Size = 3070, Total Bytes: 2839771490,
  Minimum = 783.49 KB/s, Maximum = 1.63 MB/s, Average = 1.52 MB/s
```

图 6　带宽测试结果

Fig.6　Bandwidth test results

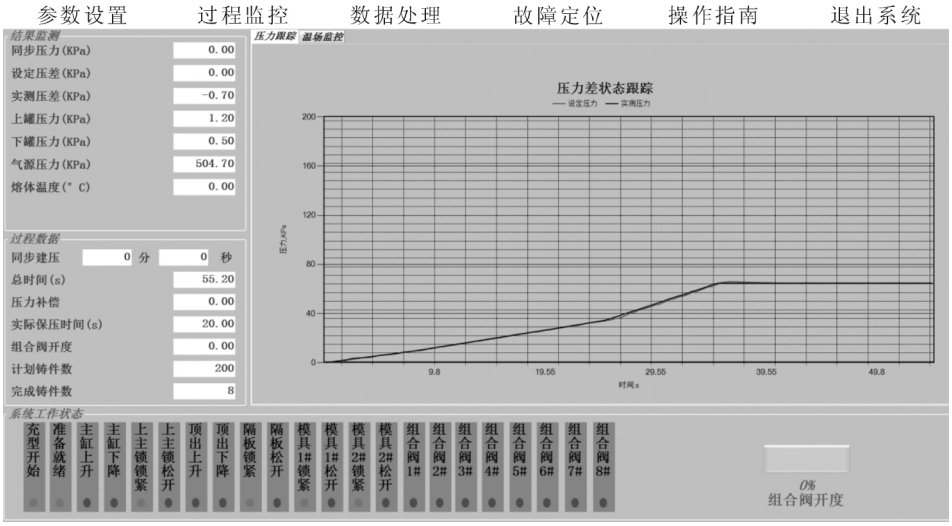

图 7　过程监控界面

Fig.7　Process monitor frame

并以数值和曲线形式直观展示在操作者面前，证明了 Modbus TCP/IP 协议应用于反重力铸造数据记录工作上的可行性和实用性。

4　结论

（1）分析了 Modbus TCP/IP 协议概念，对以太网通信过程数据交换的报文格式进行了解读。

（2）介绍了反重力铸造数据记录与处理系统整体的组成结构，分析了反重力铸造过程客户端数据记录实际需求，并依据客户端通信流程利用 Socket 技术和 C# 语言完成了对客户端通信程序设计，最后，给出了以太网通信服务器端通信设计的主要思路。

（3）在铸造生产现场对数据记录与处理系统进行长时间、多类型的以太网通信测试。利用 Wirshark 抓包软件测试了系统在生产过程中数据传输稳定性，结果表明在测试过程中通信过程稳定可靠。借助 PsPing 软件测试了系统客户端与服务器之间的网络带宽，证明以太网通信下数据传输能力相比串行通信有着较大提升，完全满足实际反重力铸造生产时数据传输速率要求。通过客户端界面运行结果，验证了 Modbus TCP/IP 协议在反重力铸造数据记录上应用的可行性和实用性。

参考文献：

[1]　柴艳，郝启堂，介万奇. 多功能铝合金反重力铸造装备的研制[J]. 特种铸造及有色合金，2009, 29(1)：33-35.

[2]　林海峰，任天庆. TP801 型微型计算机在低压铸造与差压铸造液面加压控制系统中的应用[J]. 铸造设备研究，1990(4)：30-33.

[3]　张曙. 工业 4.0 和智能制造 [J]. 机械设计与制造工程，2014(8)：1-5.

[4]　Ling Li. China's manufacturing locus in 2025: With a comparison of “Made-in-China 2025” and “Industry 4.0”[J]. Technological Forecasting & Social Change, 2017.

[5]　习博方，彦军. 工业以太网中网络通信技术的研究[J]. 微计算机信息，2005(2)：148-149.

[6]　倪建军. 嵌入式 Modbus/Modbus TCP 网关的设计与研究[D]. 北京：北京交通大学，2008.

[7]　闫素杰. MODBUS 通讯协议与仪表的数据采集[J]. 信息技术与信息化，2014(2)：99-103.

[8]　蒋东兴，林鄂华. Windows Sockets 网络程序设计大全[M]. 北京：清华大学出版社，1999.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net