

学校编码: 10384

分类号____密级____

学号: 22320051302477

UDC _____

厦 门 大 学

硕 士 学 位 论 文

EtherNet/IP 通信适配器的软件设计与实现

The design and realization of the software based on
EtherNet/IP communication adapter

谢维盛

指导教师姓名: 刘瞰东副教授

专 业 名 称: 系 统 工 程

论文提交日期: 2008 年 5 月

论文答辩时间: 2008 年 月

学位授予日期: 2008 年 月

答辩委员会主席: _____

评 阅 人: _____

2008 年 5 月

厦门大学博硕士学位论文摘要库

厦门大学学位论文原创性声明

兹呈交的学位论文是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年 月 日

摘要

本文以上海捷准工业自动化公司委托开发的“EtherNet/IP 通信适配器开发”项目为背景，设计并实现一种基于 EtherNet/IP 工业以太网的通信适配器，该通信适配器作为 EtherNet/IP 控制网络与其他技术之间的一个网关，可将工业控制设备集成到 EtherNet/IP 工业以太网中，提高控制系统的灵活性和兼容性。

工业以太网技术和嵌入式技术都是当前应用研究的热点。本文在分析 EtherNet/IP 工业以太网技术和嵌入式系统发展的基础上，提出了一种工业以太网设备开发方案。该方案既满足了运行网络协议的功能要求，又适应了嵌入式系统采用 32 位微处理器及嵌入式操作系统的发展趋势，满足 Ethernet/IP 通信处理器对通信实时性、可靠性的近乎苛刻要求。

本文构建了以 S3C2410 ARM9 为核心的 EtherNet/IP 通信适配器的硬件系统，设计开发了该通信适配器的 Boot Loader、I/O 接口驱动程序等底层软件，成功移植 Windows CE.NET 嵌入式操作系统到该 EtherNet/IP 通信适配器的硬件平台。Boot Loader 与硬件高度相关，担负着初始化系统硬件和引导操作系统的双重任务，是操作系统和硬件之间的联结纽带；而 I/O 接口驱动程序使操作系统自动识别外围数据采集设备，并为应用程序对底层设备的操控提供服务。

此外，本文在 EADK (EtherNet/IP Adapter Developers Kit) 软件协议栈的基础上编写了该 EtherNet/IP 通信适配器的应用程序，在应用层实现了 CIP (控制与信息协议)，保证网络上实时 I/O 数据和显式信息的有效传输，进行正确的控制；借助 EIPScan 软件、EDITT 软件、ControlLogix PLC 和 PCU-ETHIO EtherNet/IP 扫描器等工具对该通 EtherNet/IP 信适配器进行了完整的通信测试，结果表明该 Ethernet/IP 通信适配器在数据传输的实时性、稳定性、可靠性等方面有良好的性能。

关键字：工业以太网；EtherNet/IP；通信适配器

Abstract

Using “EtherNet/IP Communication Adapter development” commissioned by Shanghai Hurco industrial automatic company as background, this thesis designs and realizes a communication adapter of Industrial Ethernet based on EtherNet/IP, this communication adapter is used as a gateway between EtherNet/IP control network and other technologies, it can integrate industrial control equipments to EtherNet/IP industrial Ethernet, and make the control system more flexible and compatible.

Industrial Ethernet technology and embedded technology are the hottest topic of recent application and research. According to the analysis of the evolution concerning about Industrial Ethernet technology and embedded system, a comprehensive scheme for Industrial Ethernet intelligent equipment was presented in this thesis. This design not only satisfies the functional requirements for Ethernet protocol, but also fits the developmental tide of the embedded system progress of adopting 32-bit microprocessor and embedded operating system (OS), and satisfies the rigorous request of the Ethernet/IP communication adapter's real-time and reliable communication.

Aimed at the design of the EtherNet/IP communication adapter, this thesis adopts S3C2410 ARM9 microprocessor and Windows CE.NET operating system, and develops the communication processor's Boot Loader program and I/O interface's driver. The Boot Loader program, which is highly relevant to the hardware, initializes hardware platform and boots Windows CE.NET OS. While the I/O interface's driver makes the OS detect peripherals automatically, and provides services for the applications to control the bottom equipments.

Furthermore, the thesis also concentrates on the design of the application of this communication adapter based on the EADK (EtherNet/IP

Adapter Developers Kit) , and realizes CIP in application layer, which guarantees the effective transmission of the real-time I/O data and explicit message in network. In addition, EIPScan, EDITT, ControlLogix PLC and PCU-ETHIO EtherNet/IP scanner have been used to test this communication adapter completely, and it has been demonstrated that this Ethernet/IP communication adapter has excellent real-time property, stability and reliability in data transmission.

Keywords: Industrial Ethernet; Ethernet/IP; Communication Adapter

厦门大学博硕士学位论文摘要库

目 录

第一章 绪论	1
1.1 工业以太网是控制网络发展的方向	1
1.2 Ethernet 应用于工业现场的关键技术	3
1.2.1 通信确定性与实时性	3
1.2.2 稳定性与可靠性	3
1.2.3 安全性	4
1.2.4 总线供电问题	4
1.3 主要的工业以太网解决方案	5
1.3.1 HSE	5
1.3.2 Profinet	5
1.3.3 Modbus/TCP	5
1.3.4 EtherNet/IP	6
1.4 本文的主要工作以及研究的内容	6
第二章 EtherNet/IP 协议简介	8
2.1 EtherNet/IP 协议体系结构	8
2.2 EtherNet/IP 的物理层与数据链路层	9
2.3 网络层和传输层使用标准的 TCP/IP	9
2.4 应用层协议 CIP——控制与信息协议	10
2.5 EtherNet/IP 的优势	12
第三章 CIP 协议规范	13
3.1 CIP 的对象模型 (Object Model)	13
3.1.1 CIP 对象分类	13
3.1.2 基于对象的 CIP 对象模型	15
3.2 CIP 连接和报文协议	17
3.3 设备描述	18
3.4 电子数据文档 EDS	20
第四章 EtherNet/IP 通信适配器的硬件结构与底层软件	22
4.1 通信适配器的硬件结构	22
4.2 基于 Windows CE 的 Boot Loader 程序	23
4.2.1 Boot Loader 启动代码	24
4.2.2 Boot Loader 的主代码	27
4.3 I/O 接口驱动程序的设计与实现	30

4.3.1 流接口驱动模型.....	30
4.3.2 驱动程序的中断处理.....	31
4.3.3 驱动程序的设计与实现.....	32
第五章 EtherNet/IP 通信适配器的应用软件开发.....	36
5.1 EADK 简介	36
5.2 应用程序与 EADK 之间、EADK 各组件间的联系	37
5.2.1 UCMM Server.....	38
5.2.2 UCMM Client.....	39
5.2.3 CIP 连接的建立.....	40
5.2.4 Class 3 server.....	41
5.2.5 Class 1 (I/O) Data.....	42
5.3 基于 CIP 对象的软件实现	43
5.3.1 通信适配器的实现要求.....	43
5.3.2 应用软件的整体架构.....	44
5.3.3 程序的编写.....	46
5.4 EDS 文件的编写	50
第六章 EtherNet/IP 通信适配器的验证测试.....	51
6.1 使用 EIPScan 和 EDITT 进行测试	51
6.2 与 ControlLogix 之间的通信测试	53
6.3 Woodhead scanner 的完整测试	55
总结与展望	57
参考文献	59
作者硕士期间发表的论文	62
附录一	63
致 谢.....	77

Contents

Chapter 1 Introduction.....	1
1.1 Industrial Ethernet is the development direction of the control network.....	1
1.2 The key technologies of using Ethernet in factory.....	3
1.2.1 Determinacy and real-timing of the communication.....	3
1.2.2 Stability and reliability.....	3
1.2.3 Safety.....	4
1.2.4 The problems of bus-powered.....	4
1.3 Some Industrial Ethernet solutions.....	5
1.3.1 HSE.....	5
1.3.2 Profinet.....	5
1.3.3 Modbus/TCP.....	5
1.3.4 EtherNet/IP.....	6
1.4 The main works and research of the paper.....	6
Chapter 2 The brief introduction of EtherNet/IP.....	8
2.1 EtherNet/IP architecture.....	8
2.2 Physical layer and data link layer.....	9
2.3 Network layer and transport layer.....	9
2.4 The brief introduction of CIP.....	10
2.5 The advantages of EtherNet/IP.....	12
Chapter 3 CIP specifications.....	13
3.1 Object Model.....	13
3.1.1 Object.....	13
3.1.2 The Object Model based on object.....	15
3.2 CIP Connections and message protocol.....	17
3.3 Device profile.....	18
3.4 EDS.....	20
Chapter 4 The hardware and low-level software of the EtherNet/IP communication adapter.....	22
4.1 The hardware software of EtherNet/IP communication adapter...22	22
4.2 The Boot Loader based on Windows CE.....	23

4.2.1 OEM Startup Code.....	24
4.2.2 Main Code.....	27
4.3 The design and realization of the I/O interface' s Driver....	30
4.3.1 Streams Device Driver Model.....	30
4.3.2 The interrupt handler of the driver.....	31
4.3.3 The design and realization of the driver.....	32
Chapter 5 The development of the EtherNet/IP communication	
adapter' s application.....	36
5.1 The brief introduction of EADK.....	36
5.2 The relationship between application and EADK.....	37
5.2.1 UCMM Server.....	38
5.2.2 UCMM Client.....	39
5.2.3 The establishment CIP connections.....	40
5.2.4 Class 3 server.....	41
5.2.5 Class 1 (I/O) Data.....	42
5.3 The realization of the software based on CIP objects.....	43
5.3.1 The designing requirements of the communication adapter	
.....	43
5.3.2 The architecture of the application.....	44
5.3.3 Programming.....	46
5.4 Writes the EDS.....	50
Chapter 6 The tests of the EtherNet/IP communication adapter	
.....	51
6.1 Testing via EIPscan and EDITT.....	51
6.2 Testing via ControlLogix.....	53
6.3 Testing via Woodhead scanner.....	55
Summary and prospect.....	57
Reference.....	59
Published papers of author.....	62
Appendix 1.....	63
Acknowledgement.....	77

厦门大学博硕士学位论文摘要库

第一章 绪论

1.1 工业以太网是控制网络发展的方向

工业控制网络作为一种特殊的网络，直接面向生产过程，肩负着工业生产运行现场测量与控制信息传输的特殊任务，因此它通常应满足强实时性、高可靠性、恶劣的工业现场环境适应性、总线供电等特殊要求和特点。它的发展经历了集散控制系统(Distributed Control System——DCS)、现场总线控制系统(Fieldbus Control System——FCS)、工业以太网(Industrial Ethernet)等几个阶段^[1-3]。

在DCS中，工业控制网络是一种数字—模拟混合系统，其核心思想是集中管理、分散控制。这种分布式的控制系统克服了集中控制对控制器处理能力和可靠性要求高的缺陷，但其自身也有难以消除的缺点。首先，不同的DCS制造商为达到垄断经营的目的而对其控制网络采用各自专用的封闭形式，不同的制造商的DCS之间以及与上层Intranet、Internet信息网络之间难以实现网络互联和信息共享；其次，DCS的控制站仍然是集中的，现场信号的检测、传输和控制并没有彻底做到分散控制、集中管理；最后，DCS采用的是普通商业网络的通信协议和网络结构，在解决工业控制系统的可靠性方面并没有做出实质性的改进，布线复杂，费用高。因此总体来讲，DCS是一种封闭专用的、不具有可互操作性的、不彻底的分布式控制系统。

在过去的十几年间，在工厂自动化和过程自动化领域中，FCS是现场级通信系统的主流解决方案。然而，随着技术的不断进步和发展，现场总线技术越来越多的表现出其本身的局限性和不足。首先，现有的现场总线技术标准过多，仅IEC61158标准就包含了CAN、LonWorks、Profibus、Devicenet、ControlNet等8个类型，未能统一到单一标准，不同总线之间不能兼容；其次，随着现场设备智能程度的不断提高，控制系统变得越来越分散，现场设备之间以及现场设备和工厂控制层设备之间的数据的交换量飞速增长，而现场总线的传输速率较低；最后，随着计算机技术的发展，企业希望能够将底层的生产信息整合到统一的全厂信息管理系统中，实现信息的透明互访和无缝集成，并使工业控制网络能够与Intranet、Internet相集成。

为解决现场总线所带来的问题，国际上各厂商开始采用以太网来作为控制网

络^[4-6]。20 世纪 90 年代开始,因特网开始了爆炸性的发展。因特网的基础是 TCP/IP 协议族,以太网是应用最为广泛的一种局域网,TCP/IP 和以太网的结合是当前最为流行的网络解决方案。将以太网应用于控制网络,具有较多的优点,主要包括:

(1) 成本低廉

以太网技术成熟,具有统一的国际标准,网络设备价格相对较低,基于以太网的控制网络性价比大大提高。

(2) 通信速率高

以太网的带宽在逐渐增加,出现了百兆、千兆、万兆以太网,这些以太网的速率比目前的现场总线快得多,使控制网络的数据传输速度大大提高。

(3) 软硬件资源丰富

以太网得到了广泛的技术支持。由于以太网应用多年,人们对以太网的设计、应用等方面有很多的经验,对其技术也十分熟悉。大量的软件资源和设计经验可以显著降低系统的开发和培训费用,从而可以显著降低系统的整体成本,并大大加快系统的开发和推广速度。

(4) 便于解决现场总线中的互操作性问题

基于以太网的网络大多采用 TCP/IP 协议,各种工业以太网方案也都在网络层和传输层上采用 TCP/IP 协议,这就为解决控制系统中各厂商间的产品互不兼容或可操作性差等问题带来了极大的方便。

(5) 能够实现办公自动化网络,企业管理网络以及工业控制网络的无缝集成。

以太网由于其开放性好、应用广泛以及价格低廉等特点,不但基本垄断了商业领域的网络市场,而且在工业控制领域(主要是在企业管理层)也得到了大规模的应用。目前许多大公司的工业控制系统都是采用以太网来统一管理层的通信,而且各种现场总线也大多开发出以太网接口,可以建立一个从现场控制到企业管理层都采用的以太网的控制网络。

由以上可见,将以太网应用于工业控制网络,具有较大的优势。它能够适应 Intranet/Internet 等信息技术的飞速发展,使企业能够实现从现场控制层到企业管理层全面的无缝信息集成,为实现工业企业完全信息化和管理控制网络一体化提供可能。随着以太网技术的日渐成熟,产生了一种新型的以太网——工业以

太网。

1.2 Ethernet 应用于工业现场的关键技术

1.2.1 通信确定性与实时性

工业控制网络不同于普通数据网络的最大特点在于它必须满足控制作用对实时性的要求，即信号传输要足够快和满足信号的确定性。实时控制往往要求对某些变量的数据准确定时刷新。由于 Ethernet 采用 CSMA/CD 方式，网络负荷较大时，网络传输的不确定性不能满足工业控制的实时要求，故传统以太网技术难以满足控制系统要求准确定时通信的实时性要求，一直被视为“非确定性”的网络^[7-9]。

工业以太网采取了以下措施使得该问题基本得到解决：

(1) 采用快速以太网加大网络带宽。以太网的通信速率从 10Mb/s、100 Mb/s 增大到如今的 1Gb/s、10Gb/s。在数据吞吐量相同的情况下，通信速率的提高意味着网络负荷的减轻和网络传输延时的减小，即网络碰撞机率大大下降，从而提高实时性。

(2) 采用全双工交换式以太网。用交换技术替代原有的总线型 CSMA/CD 技术，避免了由于多个站点共享并竞争信道导致发生的碰撞，减少了信道带宽的浪费，同时还可以实现全双工通信，提高信道的利用率。

(3) 降低网络负载。工业控制网络与商业控制网络不同，每个结点传送的实时数据量很少，一般为几个位或几个字节，而且突发性的数据大量传输也很少发生，因此可以通过限制网段站点数目，降低网络流量，进一步提高网络传输的实时性。

(4) 应用报文优先级技术。在智能交换机或集线器中，通过设计报文的优先级来提高传输的实时性。

1.2.2 稳定性与可靠性

传统的 Ethernet 并不是为工业应用而设计的，没有考虑工业现场环境的适应性需要。由于工业现场的机械、气候、尘埃等条件非常恶劣，因此对设备的工业可靠性提出了更高的要求。在工厂环境中，工业网络必须具备较好的可靠性、可恢复性及可维护性。

为了解决在不间断的工业应用领域，在极端条件下网络也能稳定工作的问题，美国 Synergetic 微系统公司和德国 Hirschmann、Jetter AG 等公司专门开发和生产了导轨式集线器、交换机产品，安装在标准 DIN 导轨上，并有冗余电源供电，接插件采用牢固的 DB-9 结构。此外，在实际应用中，主干网可采用光纤传输，现场设备的连接则可采用屏蔽双绞线，对于重要的网段还可采用冗余网络技术，以此提高网络的抗干扰能力和可靠性。

1.2.3 安全性

在工业生产过程中，很多现场不可避免地存在易燃、易爆或有毒气体等，对应用于这些工业现场的智能装置以及通信设备，都必须采取一定的防爆技术措施来保证工业现场的安全生产。

在目前技术条件下，对以太网系统采用隔爆、防爆的措施比较可行，即通过对 Ethernet 现场设备采取增安、气密、浇封等隔爆措施，使现场设备本身的故障产生的点火能量不外泄，以保证系统运行的安全性。对于没有严格的本安要求的非危险场合，则可以不考虑复杂的防爆措施。

工业系统的网络安全是工业以太网应用必须考虑的另一个安全性问题。工业以太网可以将企业传统的三层网络系统，即信息管理层、过程监控层、现场设备层，合成一体，使数据的传输速率更快、实时性更高，并可与 Internet 无缝集成，实现数据的共享，提高工厂的运作效率。但同时也引入了一系列的网络安全问题，工业网络可能会受到包括病毒感染、黑客的非法入侵与非法操作等网络安全威胁。一般情况下，可以采用网关或防火墙等对工业网络与外部网络进行隔离，还可以通过权限控制、数据加密等多种安全机制加强网络的安全管理。

1.2.4 总线供电问题

总线供电（或称总线馈电）是指连接到现场设备的线缆不仅传输数据信号，还能给现场设备提供工作电源。对于现场设备供电可以采取以下方法：

(1) 在目前以太网标准的基础上适当地修改物理层的技术规范，将以太网的曼彻斯特信号调制到一个直流或低频交流电源上，在现场设备端再将这两路信号分离开来。

(2) 不改变目前物理层的结构，而通过连接电缆中的空闲线缆为现场设备提供电源。

Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士学位论文摘要库