工业控制以太网协议实现研究

庄晓燕,周森鑫
(安徽财经大学 信息工程学院,安徽 蚌埠 233041)

摘 要:基于以太网的工业控制网络是工业控制系统的发展趋势。研究高速以太网的关键技术,其中包括解决以太网通信的实时性、可互操作性、可靠性、抗干扰性和本质安全等问题,同时研究开发相关高速以太网技术的现场设备、网络化控制系统和系统软件等是目前工业控制理论界的一项重要任务。通过分析工业控制以太网的工作原理和相关的性能指标及目前常用的工业控制以太网协议实现细节得出以下结论:尽管各种工业以太网技术可能会像现场总线国际之争那样,出现多协议并存局面,但以太网协议的相融统一是工业控制以太网发展的必然趋势。

关键词:工业控制以太网;CSMA/CD;实时性;EPA
中图分类号:TP273^{+}.3 **文献标识码**:A **文章编号**:1673-629X(2009)12-0243-05

Research on Application of Ethernet Control Network Protocol

ZHUANG Xiao-yan, ZHOU Sen-xin
(Information Engineering School of Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: The development trend of industrial control system is industrial control network of the Ethernet. It is an important task for the industrial control theory field currently to study the key technique of the high-speed ethernet, including resolving real-time performance, operability, credibility, anti-interference and the essence safety etc. In the meantime researching and developing field equipments of control network, control system of network and control system software is also very important. Analyze the industrial control ethernet network principle, related performance and the industrial control ethernet protocols in common use. We draw a conclusion: though various industrial ethernet protocal may exist in the meantime like the field control bus, the mutually melt and overall usage of the control ethernet protocols are inevitable development trend.

Key words: Ethernet control network; CSMA/CD; real-time performance; EPA

0 引 言

随着计算机、通信、网络等信息技术的发展,信息交换的领域已经覆盖了工厂、企业乃至世界各地的市场,因此,需要建立包含从工业现场设备层到控制层、管理层等各个层次的综合自动化网络平台,建立以工业控制网络技术为基础的企业信息化系统。

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一线测量与控制信息传输的特殊任务,并产生或引发物质或能量的运动和转换,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。

收稿日期:2009-03-27;**修回日期**:2009-06-20
基金项目:2009年安徽省自然科学基金重大项目(ZD200905);中华全国供销合作总社研究项目(GXZS0812);安徽财经大学教研项目(ACJYYB200942)
作者简介:庄晓燕(1968-),女,实验师,研究方向为计算机控制;周森鑫,副教授,硕士生导师,博士,研究方向为计算机网络、计算机控制。

20世纪80年代产生和发展起来的现场总线技术,以全数字的通信代替4~20mA电流的模拟传输方式,使得控制系统与现场仪表之间不仅能传输生产过程测量与控制信息,而且能够传输现场仪表的大量非控制信息,使得工业企业的管理控制一体化成为可能。并且促使目前的自动化仪表,DCS和可编程控制器(PLC)等产品所面临的体系结构和功能结构产生重大变革。

现场总线技术在其发展过程中存在不足:

(1)现有的现场总线标准过多,仅国际标准IEC61158就包含了8个类型,未能统一到单一标准上来;

(2)不同总线之间不能兼容,不能真正实现透明信息互访,无法实现信息的无缝集成;

(3)由于现场总线是专用实时通信网络,成本较高;

(4)现场总线的速度较低,支持的应用有限,不便于和Internet信息集成。

工业以太网在技术上与商用以太网(即 IEEE802.3 标准)兼容,但在产品设计时,在材质的选用、产品的强度和适用性方面能满足工业现场的需要。工业以太网技术直接应用于工业现场设备间的通信已成大势所趋,随着以太网通信速率的提高、全双工通信、交换技术的发展,为以太网的通信确定性的解决提供了技术基础,从而消除了以太网直接应用于工业现场设备间通信的主要障碍,为以太网直接应用于工业现场设备间通信提供了技术可能。据美国权威调查机构 ARC (Automation Research Company)报告指出,今后 Ethernet 不仅继续垄断商业计算机网络通信和工业控制系统的上层网络通信市场,也必将领导未来现场总线的发展,Ethernet 和 TCP/IP 将成为器件总线和现场总线的基础协议[1~4]。

1 工业控制以太网的工作原理和性能分析

工业以太网的通讯模型如图 1 所示:

<table>
<tr><th colspan="2">ISO/OSI模型</th><th colspan="2">网络控制系统
通讯协议模型</th></tr>
<tr><td colspan="2"></td><td colspan="2">用 户 层</td></tr>
<tr><td>应 用 层</td><td></td><td colspan="2">应 用 层</td></tr>
<tr><td>表 示 层</td><td rowspan="2"></td><td colspan="2" rowspan="2">省略</td></tr>
<tr><td>会 话 层</td></tr>
<tr><td>传 输 层</td><td></td><td colspan="2">传 输 层</td></tr>
<tr><td>网 络 层</td><td></td><td colspan="2">网 络 层</td></tr>
<tr><td rowspan="2">数据链路层</td><td rowspan="2"></td><td colspan="2">L L C 层</td></tr>
<tr><td colspan="2">M A C 层</td></tr>
<tr><td>物 理 层</td><td></td><td colspan="2">物 理 层</td></tr>
</table>

图 1 工业以太网通讯模型图

通讯协议模型可参考 ISO/OSI 模型并进行简化,协议划分为高层的应用层和用户层,低层的数据链路层和物理层。高层的功能主要是完成各种控制算法,通过相关软件实现。低层的功能是完成通信介质访问控制,通过网络芯片实现。而中间屋网络的功能数据的交换和路由选择,通过交换和路由设备实现。在交换以太网中主要是通过交换机来实现。

由于工业自动化网络控制系统不单单是一个完成数据传输的通信系统,而且还是一个借助网络完成控制功能的自控系统。它除了完成数据传输之外,往往还需要依靠所传输的数据和指令,执行某些控制计算与操作功能,由多个网络节点协调完成自控任务。因而它需要在应用、用户等高层协议与规范上满足开放系统的要求,满足互操作条件。对应于 ISO/OSI 七层通信模型,以太网技术规范只映射为其中的物理层和数据链路层;而在其之上的网络层和传输层协议,目前以 TCP/IP 协议为主(已成为以太网之上传输层和网络层"事实上的"标准)。而对较高的层次如会话层、表示层、应用层等没有作技术规定。目前商用计算机设备之间是通过 FTP(文件传送协议),Telnet(远程登录协议),SMTP(简单邮件传送协议),HTTP(WWW 协议),SNMP(简单网络管理协议)等应用层协议进行信息透明访问的,它们如今在互联网上发挥了非常重要的作用。但这些协议所定义的数据结构等特性不适合应用于工业过程控制领域现场设备之间的实时通信。为满足工业现场控制系统的应用要求,必须在 Ethernet + TCP/IP 协议之上,建立完整的、有效的通信服务模型,制定有效的实时通信服务机制,协调好工业现场控制系统中实时和非实时信息的传输服务,形成为广大工控生产厂商和用户所接收的应用层、用户层协议,进而形成开放的标准。为此,各现场总线组织纷纷将以太网引入其现场总线体系中的高速部分,利用以太网和 TCP/IP 技术,以及原有的低速现场总线应用层协议,从而构成了所谓的工业以太网协议,如 HSE. PROFInet, Ethernet/IP 等。

工业以太网在技术上与商用以太网(即 IEEE802.3 标准)兼容,但在产品设计、材质的选用、产品的强度和适用性方面能满足工业现场的需要。即满足以下要求:

(1) 环境适应性。

包括机械环境适应性(如耐振动、耐冲击)、气候环境适应性(工作温度要求为 -40℃ ~ +85℃,至少为 -20℃ ~ +70℃,并要耐腐蚀、防尘、防水)、电磁环境适应性或电磁兼容性 EMC 应符合 EN 50081 - 2, EN 50082 - 2 标准。

(2) 可靠性。

工业以太网产品要适应工业控制现场的恶劣环境,同时还包括数据传输的准确可靠。

(3) 安全性。

在易爆或可燃的场合,工业以太网产品还需要具有防爆要求,包括隔爆、本质安全两种方式。在商业应用中,对实时性的要求基本不涉及安全,而过程控制对实时性的要求是硬性的,常常涉及生产设备和人员安全。

(4) 安装方便,适应工业环境的安装要求。

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地工作的问题,一些公司专门开发和生产了导轨式收发器、集线器和交换机系列产品,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。另外一些公司还专门开发和产生了用于工业控制现场的加固型连接件(如加固的

RJ45 接头、具有加固 RJ45 接头的工业以太网交换机、加固型光纤转换器/中继器等),可以用于工业以太网变送器、执行机构等。工业以太网设备与商用以太网设备之间的区别如表 1 所示。

表 1　工业以太网与商用以太网设备的区别

	工业以太网	商用以太网
元器件	工业级	商用级
接插件	耐腐蚀、防尘、防水,如加固型 RJ45,DB-9,航空接头等	一般 RJ45
工作电压	24VDC	220VAC
电源冗余	双电源	一般没有
安装方式	采用 DIN 导轨或其它方式固定安装	桌面、机架
工作温度	-40℃~85℃或-20℃~70℃	5℃~40℃
电磁兼容性标准	EN50081-2 或 EN50082-2(工业级 EMC)	EN50081-2 或 EN50082-2(办公室用 EMC)
MTBF 值	至少 10 年	3~5 年

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,即信号传输要足够的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 碰撞检测方式,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,因此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。然而,快速以太网与交换式以太网技术的发展,给解决以太网的非确定性问题带来了新的契机,使这一应用成为可能。首先,Ethernet 的通信速率从 10M,100M 增大到如今的 1000M,10G,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。其次,采用星型网络拓扑结构,交换机将网络划分为若干个网段。Ethernet 交换机由于具有数据存储、转发的功能,使各端口之间输入和输出的数据帧能够得到缓冲,不再发生碰撞;同时交换机还可对网络上传输的数据进行过滤,使每个网段内节点间数据的传输只限在本地网段内进行,而不需经过主干网,也不占用其它网段的带宽,从而降低了所有网段和主干网的网络负荷。再次,全双工通信又使得端口间两对双绞线(或两根光纤)上分别同时接收和发送报文帧,也不会发生冲突。因此,采用交换式集线器和全双工通信,可使网络上的冲突域不复存在(全双工通信),或碰撞机率大大降低(半双工),因此使 Ethernet 通信确定性和实时性大大提高。

Ethernet 进入工业控制领域的另一个主要问题是,它所用的接插件、集线器、交换机和电缆等均是为商用领域设计的,而未针对较恶劣的工业现场环境来设计(如冗余直流电源输入、高温、低温、防尘等),故商用网络产品不能应用在有较高可靠性要求的恶劣工业现场环境中。随着网络技术的发展,上述问题正在迅速得到解决。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。台湾四零四科技(Moxa Technologies)在 2002 年 6 月推出工业以太网产品 - MOXA EtherDevice Server(工业以太网设备服务器),特别设计用于连接工业应用中具有以太网络接口的工业设备(如 PLC,HMI,DCS 系统等)。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[5,6]。

2　工业以太网协议简介

目前现场总线体系中,基于以太网的通信协议除了现场总线应用行规国际标准 IEC 61784-1 中包含的 HSE, Ethernet/IP, Profinet 之外,还包括 EPA, EtherCAT, Ethernet PowerLink, Vnet/IP, TCnet, Modbus/IDA 等 6 个新的提案。

HSE 是现场总线基金会在据弃了原有高速总线 H2 之后的新作。HSE 在低四层直接采用以太网 + TCP/IP,在应用层和用户层直接采用 FF H1 的应用层服务和功能块应用进程规范,并通过链接设备(Linking Device)将 FF H1 网络连接到 HSE 网段上,HSE 链接设备同时也具有网桥和网关的功能,它的网桥功能能够用来连接多个 H1 总线网段,使不同 H1 网段上面的 H1 设备之间能够进行对等通信而无需主机系统的干预。HSE 主机可以与所有的链接设备和链接设备上挂接的 H1 设备进行通信,使操作数据能传送到远程的现场设备,并接收来自现场设备的数据信息,实现监控和报表功能。监视和控制参数可直接映射到标准功能块或者"柔性功能块"(FFB)中。

Profinet 由 Siemens 开发并由 Profibus International 支持,目前它有 3 个版本,第一个版本定义了基于 TCP/UDP/IP 的自动化组件。采用标准 TCP/IP + 以太网作为连接介质,采用标准 TCP/IP 协议加上应用层的 RPC/DCOM 来完成节点之间的通信和网络寻址。它可以同时挂接传统 Profibus 系统和新型的智能现场设备。现有的 Profibus 网段可以通过一个代理设备(proxy)连接到 Profinet 网络当中,使整套 Profibus 设备和协议能够原封不动地在 Profinet 中使用。传统的 Profibus 设备可通过代理与 Profinet 上面的 COM 对象

进行通信,并通过 OLE 自动化接口实现 COM 对象之间的调用。它将以太网应用于非时间关键的通信,用于高层设备和 Profibus－DP 现场设备技术之间,以便将实时控制域通过代理集成到一个高层的水平上。第二个版本中,Profinet 在以太网上开辟了两个通道:标准的使用 TCP/IP 协议的非实时通信通道,另一个是实时通道,旁路第三层和第四层,提供精确通信能力。该协议减少了数据长度,以减小通信栈的吞吐量。为优化通信功能,Profinet 根据 IEEE 802.p 定义了报文的优先级,最多可用 7 级。Profinet 第三版采用了硬件方案以缩小基于软件的通道,以进一步缩短通信栈软件的处理时间。为连接到集成的以太网交换机,Profinet 第三版还开始解决基于 IEEE 1588 同步数据传输的运动控制解决方案。

Ethernet/IP(Ethernet/Industrial Protocol,以太网工业协议)由 ROCKWELL 定义,并由 ODVA 和 ControlNet International 支持。Ethernet/IP 网络采用商业以太网通信芯片、物理介质和星形拓扑结构,采用以太网交换机实现各设备间的点对点连接,能同时支持 10Mbps 和 100Mbps 以太网商业产品,Ethernet/IP 协议由 IEEE 802.3 物理层和数据链路层标准、TCP/IP 协议组和控制与信息协议 CIP(Control Information Protocol)等三个部分组成,前面两部分为标准以太网技术,其特色就是被称作控制和信息协议的 CIP 部分。Ethernet/IP 为了提高设备间的互操作性,采用了 ControlNet 和 Devicenet 控制网络中相同的 CIP,CIP 一方面提供实时 I/O 通信,一方面实现信息的对等传输,其控制部分用来实现实时 I/O 通信,信息部分则用来实现非实时的信息交换。

EPA 系统中,将控制网络划分为若干个控制区域,每个控制区域即为一个微网段。每个微网段通过 EPA 网桥与其他网段进行分隔,该微网段内 EPA 设备间的通信被限制在本控制区域内进行,而不会占用其他网段的带宽资源。处于不同微网段内的 EPA 设备间的通信,需由相应的 EPA 网桥进行转发控制。EPA 网桥至少有 2 个 EPA 接口,当它需要转发报文时,首先检查报文中的源 IP 地址与目的 IP 地址、EPA 服务标识等信息,以确认是否需要转发,并确定报文转发路径。因此,任何广播报文的转发也将受到控制,而不会发生采用一般交换机所出现的广播风暴。而连接在每个微网段的 EPA 设备,通过其内置的通信栈软件,分时向网络上发送报文,以避免两个设备在同一时刻向网络上同时发送数据,避免报文碰撞,用户可以预知其发出的信息在可预知的时间内到达目的站点。EPA 系统中,支持 IEEE 1588 的时间同步,还支持标准以太网帧与 EPA 实时以太网帧的并行传输。

EtherCAT(Ethernet for Control Automation Technology)是由德国倍福 Beckhoff 公司开发,并由 EtherCAT 技术组(EtherCAT Technology Group,ETG)支持。它采用以太网帧,并以特定的环状拓扑发送数据。网络上的每一个站均从以太网帧上取走与该站有关的数据,或并插入该站本身特定的输入/输出数据。网络内的最后一个模块向第一个模块发送一个帧以形成和创建一个物理和逻辑环。EtherCAT 还通过内部优先级系统,使实时以太网帧比其他的数据(如组态或诊断数据等)具有较高的优先级。组态数据只在传输实时数据的间隙(如间隙时间足够传输的话)中传输,或者通过特定的通道传输。EtherCAT 还保留标准以太网功能,并与传统 IP 协议兼容。为了实现这样的装置,需要专用 ASIC 芯片,以集成至少两个以太网端口,并采用基于 IEEE 1588 的时间同步机制,以支持控制中的实时应用。

Powerlink 由贝加莱 B&R 公司开发,并由 Ethernet Powerlink 标准化组(Ethernet Powerlink Standardisation Group,EPSG)支持。Powerlink 协议对第三、四层的 TCP(UDP)/IP 栈进行了扩展。它在共享式以太网网段上采用槽时间通信网络管理(Slot Communication Network Management,SCNM)控制网络上的数据流量。SCNM 采用主从调度方式,每个站只有在收到主站请求的情况下,才能发送实时数据。因此,在一个特定的时间,只有一个站能够访问总线,所以没有冲突,从而确保了通信的实时性。为此,Powerlink 需采用基于 IEEE 1588 的时间同步。在其扩展的第二版中,包括了基于 CANopen 的通信与设备行规。

VNET/IP 由日本横河 Yokogawa 开发,该协议的实时扩展是实时可靠数据报协议(Real－time & Reliable Datagram Protocol,RTP),在传输层采用 UDP 协议,但在 IP 栈协议层进行了优化以实现冗余网络联结。

TCnet 是由日本东芝 Toshiba 开发的,它在 MAC 进行了实时扩展,并基于标准以太网开辟了两个冗余通道连接。

Modbus/TCP 由施耐德电气定义,并由 Modbus－IDA 支持,它在 TCP/IP 网络上应用 Modbus 协议。其实时扩展采用了在 UDP 上的实时发布者预订者(Real－time Publisher Subscriber,RTPS)。Modbus/TCP 是 Modbus 的延伸,它基于以太网和标准 TCP/IP 协议,直接应用第四层。它定义了一个结构简单的、开放和广泛应用的传输协议,用于主从式通信。IDA 结构可用于实时和非实时应用,其确定性通信可以通过 IDA

中间件来实现。中间件包含了标准的 Modbus/TCP 协议。IDA 还采用基于 Web 的通信应用,提供了水平和垂直的集成,并扩展了 Web 服务器的应用[7,8]。

3　工业以太网发展趋势与前景展望

工业控制系统是实现工业生产自动化的关键,是衡量一个国家工业水平的重要指标。从理论上说,工业控制系统将进入集网络化、软件控制、现代传感器技术为一体的复杂控制系统阶段。基于以太网的工业网络控制系统具有数据传输率高、可靠性好、易维护、可远程传输、互操作性好等优点。因此,基于以太网的工业控制网络是工业控制系统的发展趋势。据美国权威调查机构 ARC(Automation Research Company)报告指出,今后 Ethernet 不仅继续垄断商业计算机网络通信和工业控制系统的上层网络通信市场,也必将领导未来现场总线的发展,Ethernet 和 TCP/IP 将成为器件总线和现场总线的基础协议。美国 VDC(Venture Development Corp.)调查报告也指出,Ethernet 在工业控制领域中的应用将越来越广泛,市场占有率的增长也越来越快。为此,国际电工委员会 IEC 起草了实时以太网(Real - time Ethernet, RTE)标准,旨在推动以太网技术在工业控制领域的全面应用。

在国家"863"计划的支持下,我国开展了 EPA (Ethernet for Plant Automation)技术的研究,重点研究以太网技术应用于工业控制现场设备间通信的关键技术:

① 实时通信技术。其中采用以太网交换技术、全双工通信、流量控制等技术,以及确定性数据通信调度控制策略、简化通信栈软件层次、现场设备层网络微网段化等针对工业过程控制的通信实时性措施,解决了以太网通信的实时性。

② 总线供电技术。采用直流电源耦合、电源冗余管理等技术,设计了能实现网络供电或总线供电的以太网集线器,解决了以太网总线的供电问题。

③ 远距离传输技术。采用网络分层、控制区域微网段化、网络超小时滞中继以及光纤等技术解决以太网的远距离传输问题。

④ 网络安全技术。采用控制区域微网段化,各控制区域通过具有网络隔离和安全过滤的现场控制器与系统主干相连,实现各控制区域与其他区域之间的逻辑上的网络隔离。

⑤ 可靠性技术。采用分散结构化设计、EMC 设计、冗余、自诊断等可靠性设计技术等,提高基于以太网技术的现场设备可靠性。

科技部也发布了基于高速以太网技术的现场总线设备研究项目,其目标是:攻克应用于工业控制现场的高速以太网的关键技术,其中包括解决以太网通信的实时性、可互操作性、可靠性、抗干扰性和本质安全等问题,同时研究开发相关高速以太网技术的现场设备、网络化控制系统和系统软件等。

从工业以太网技术发展形势看,尽管各种工业以太网技术可能会像现场总线国际之争那样,出现多协议并存局面,但以太网协议的相融统一并以网到底是工业控制以太网发展的必然趋势,以太网在工业控制系统中的应用必将越来越广[8]。

参考文献:

[1] Hoang H, Jonsson M, Hagstrom U. Switched realtime ethernet with earliest deadline first scheduling protocols and traffic handling[C]//Proceedings of the International Parallel and Distributed Processing Symposium. [s.l.]: IEEE computer society, 2002: 94 - 99.

[2] Hoang H. Real - Time Communication for Industrial Embedded Systems Using Switched Ethernet[C]//Parallel and Distributed Processing Sysposium[s.l.]. IEEE computer society, 2004: 127 - 130.

[3] Seifert R. The Switch Book: The Complete Guide to LAN Switching Technology[M]. [s.l.]. Wiley, 2000: 587 - 647.

[4] Zhang Wei. Stability analysis of networked control systems [D]. Ohio, US: Case Western Reserve University, 2001.

[5] Nilsson J, Bernhardsson B, Wittenmark B. Stochastic analysis and control of real - time systems with random time delays [J]. Automatica, 1998, 34(1): 57 - 64.

[6] 李　杨,周　原,方潜生,等. 工业以太网及 OPC 在智能建筑中的应用[J]. 计算机技术与发展, 2007, 17(12): 22 - 26.

[7] 王天然,周　悦. FF 现场总线系统实时通信的分析及启发式调度[J]. 仪器仪表学报, 2003, 24(1): 1 - 6.

[8] 李　嘉,杨佃福. 引入以太网技术是现场总线技术发展的一个必然趋势[J]. 自动化仪表, 2001, 22(5): 1 - 4.

(上接第 242 页)

[J]. 微计算机信息, 2007, 23(8): 132 - 133.

[6] ARINC Specification 659 Backplane Data BuS[M]. [s.l.]: the Airlines Electronic Engineering Committee, 1993.

[7] 孙玉焕. 64 位 CPU 的 FPGA 原型验证[J]. 电子应用技术, 2007(21): 158 - 160.

[8] 王本有,苏守宝,汪德如. 一种基于 FPGA 的 CPU 设计[J]. 计算机技术与发展, 2008, 18(6): 221 - 224.