**ethernet/IP 协议简介 pdf**

2018年08月01日 21:54:23 [AlexFL](https://me.csdn.net/weixin_42778398) 阅读数：153 标签： [ethernet/ip](http://so.csdn.net/so/search/s.do?q=ethernet/ip&t=blog)

目 录

1．现场总线控制技术与工业以太网

1. 工业以太网实时性问题

3．Ethernet／IP协议简介

4．Ethernet／I P通信适配器硬件设计与实现

5．EtherNet/IP 工业以太网优缺点及发展前景

Ethernet／IP协议简介

1 现场总线控制技术与工业以太网   
20世纪90年代以后随着现场总线控制技术的逐渐成熟，智能化与功能自治性的现场设备的广泛应用，嵌入式控制器、智能现场测控仪表和传感器等方便地接入了现场总线。   
现场总线控制系统(FCS)是顺应智能现场仪表而发展起来的。它的初衷是用数字通讯代替4–20mA模拟传输技术，但随着现场总线技术与智能仪表管控一体化(仪表调校、控制组态、诊断、报警、记录)的发展，在控制领域内引起了一场前所未有的革命。   
控制专家们纷纷预言：FCS将成为21世纪控制系统的主流。然而在控制界对FCS进行概念炒作的时候，却注意到它的发展在某些方面的不协调，其主要表现在迄今为止现场总线的通讯标准尚未统一：8种现场总线经过14年的纷争，最后IEC的现场总线标准化组织经投票，通过以下这8种现场总线成为IEC61158现场总线标准，即：FF H1，Control Net，ProfiBus，InterBus，P．Net，World FIP，Swift Net，FF之高速EtherNet即HSE。这8种现场总线互不兼容，这也使得各厂商的仪表设备难以在不同的FCS中兼容。此外，FCS的传输速率也不尽人意，以基金会现场总线(FF)正在制定的国际标准为例，它采用了ISO的参考模型中的3层(物理层、数据链路层和应用层)和极具特色的用户层，其低速总线H1的传输速度为31．25kbps，高速总线H2的传输速度为1 Mbps或2．5Mbps，这在有些场合下仍无法满足实时控制的要求。又如广泛用于汽车行业的Can总线   
系统，其最高的传输速率为1 Mbps／40米；这些现场总线受通讯距离制约较大。   
由于上述原因，使FCS在工业控制中的推广应用受到了一定的限制。   
以太网具有传输速度高、低耗、易于安装和兼容性好等方面的优势，由于它   
支持几乎所有流行的网络协议，所以在商业系统中被广泛采用。但是传统以太网   
采用总线式拓朴结构和多路存取载波侦听碰撞检测(CSMA／CD)通讯方式，在实时性要求较高的场合下，重要数据的传输过程会产生传输延滞，这被称为以太网的“不确定性”。研究表明：商业以太网在工业应用中的传输延滞在2～30ms之间，这是影响以太网长期无法进入过程控制领域的重要原因之一。因此对以太网的研究具有工程实用价值，从而产生了一种新型的针对工业控制领域的以太网一工业以太网。   
由于以太网具有应用广泛、价格低廉、通信速率高、软硬件产品丰富、应用   
支持技术成熟等优点，目前它已经在工业企业综合自动化系统中的信息层与控制   
层得到了广泛应用，并呈现向下延伸直接应用于工业控制现场的趋势。从目前国   
际、国内工业以太网技术的发展来看，目前工业以太网在控制层已得到广泛应用，   
并成为事实上的标准。未来工业以太网将在工业企业综合自动化系统中的现场设备之间的互连和信息集成中发挥越来越重要的作用。   
工业以太网技术作为后起之秀，迅速抢占着其它总线形式的市场，推动其发   
展的两大动力是：光纤环网的应用、分布智能装置仪表。   
光纤环网解决了两大问题：第一，轻松解决了在化工、矿业等极端条件的本   
质防爆问题，这一下子将以太交换设备向前推动了一个层次，使以太网可以到达   
工业现场层，第一次成为真正的FieldBus；第二，通过环网的冗余提高以太交换   
的可靠性，从而使工业以太网第一次可以应用对可靠性要求较高的应用环境中。   
而分布智能的装置仪表，解决了所谓以太传输时滞不确定性的诟病。首先，   
光纤环网的千兆交换速度，已经使绝大部分工业控制数据在可接受的时间内交换，对于大部分的工业生产信息，在100ms的时滞都是可以接受的。而如果所有的控制均需要通过集中的方式进行，显然这个时滞又太大了。可喜的是，工业控制装置和智能仪表正在向分布式发展。这种发展趋势，导致大量的本地控制指令不需要通过冗长的总线来传输，而是由仪表或装置的本地计算完成，这就不需要通过数据交换的方式苛刻地要求工业以太网的确定时延。   
2 工业以太网实时性问题   
工业以太网有着许多令人所信服的优点。但是传统商业以太网技术应用到工业现场仍然有着或多或少的不足和缺陷，经过许多研究机构和工程技术人员的不懈努力和对关键技术的研究，使传统以太网技术不断改进来满足工业现场控制要求。这些关键技术包括通信确定性和实时性技术、系统稳定性技术、系统互操作性技术、网络安全性技术、总线供电及本质安全与安全防爆技术等。下面就确定性和实时性做一些介绍。   
2.1 通讯确定性和实时性技术   
传统以太网采用总线式的拓扑结构和多路存取载波侦听／碰撞(CSMA／C通讯方式，即网络上的每个节点都通过竞争的方式来获取发送信息报文的权利，节点通过监听信道，当发现信道空闲时则把待发的信息报文发送出去，如果信道忙则处于等待状态。在发送信息后检测是否发生了碰撞，如果出现则退出信道等待重发。不难想象当网络负荷比较重的时候大量节点都在尝试重发进而导致网络堵塞，使一些节点的信息长时间得不到发送，这种特性称为以太网的不确定性。研究表明：传统以太网在工业控制中的传输延迟，对数据传送要求很高的场合是不能够应用的，这也影响了以太网技术在工业底层控制网络中的应用。   
随着以太网技术的不断发展，工业以太网在确定性和实时性方面已经基本达到了工业现场实时控制的要求。   
首先，在网络拓扑结构上采用了星形连接代替总线型连接。图1示意了两种不同的网络拓扑结构。其中的星形连接用网桥或路由器等设备将网络分割成多个网段(Segment)，在每个网段上以一个多口集线器为中心，将若干个设备或节点连接起来，这样挂接在同一网段上的所有设备形成一个冲突域(Collision)。每个冲突域均采用CSMA／CD机制来管理网络冲突。这种分段方法可以使每个冲突域的网络负荷减轻、碰撞几率减小。   
图1 以太网网络拓扑结构的比较   
3 Ethernet／IP协议简介   
现场总线国际标准IEC 61158经过十几年的争论和斗争后，放弃了其制定单   
一现场总线标准的初衷，最终发布了包括8种(第3版修订后增加了两种类型，而   
成为10种类型)类型总线的国际标准。这说明各大总线各具特点、不可互相替代   
的局面得到世界工控界的认可。   
目前有Modbus-IDA工业以太网，Ethernet／lP工业以太网，FF HSE工业   
以太网，ProfitNet工业以太网等几种协议。下来我们就Ethernet／IP工业以太网进行介绍。   
EtherNet／IP(EtherNet Industry Protoco1)是适合工业环境应用的协议体系。它是由两大工业组织ODVA(OpenDeviceNet Vendors Association)ControlNet International所推出的最新的成员。和DeviceNet以及ControlNet一样，它们都是基于CIP(Control and Informal／on Protoco1)协议的网络。它是一种是面向对象的协议，能够保证网络上隐式的实时I／0信息和显式信息(包括用于组态参数设置、诊断等)的有效传输。   
EtherNet／IP采用和DevieNet以及ControlNet相同的应用层协CIP(Control and Information Protoco1)，因此，它们使用相同的对象库和一致的行业规范，具有较好的一致性。EtherNet／IP采用标准的EtherNet和TCP／IP技术来传送CIP通信包，这样，通用且开放的应用层协议CIP加上已经被广泛使用的EtherNet和TCP／IP协议，就构成EtherNet／IP协议的体系结构。协议的各层结构如图2所示。

图2 应用CIP的EtherNet/IP   
3.1 Ethernet／IP协议模型及协议内容   
1. 物理层和数据链路层   
EtherNet／IP在物理层和数据链路层采用以太网。其主要由以太网控制器芯片来实现。从图2可看出，不久的将来会出现更合适的物理层和数据链路层协议，   
会出现相应的芯片。但是上面的协议无须改变。   
2 .网络层和传输层   
EtherNet／IP在网络层和传输层采用标准的TCP／IP技术。对于面向控制的实时I／0数据，采用UDP／IP协议来传送，而对于显式信息(如组态、参数设置和诊断等)则采用TCP／IP来传送过程监控层流通的数据基本是显式信息，采用TCP／IP来传送，其优先级较低。而将来采用工业以太网EtherNet／IP协议的现场设备层，流通的数据基本是实时I／O数据，采用UDP／IP胁议来传送，其优先级较高。   
3. 控制及信息协议(ClP)   
控制及信息协议(CIP)是一种为工业应用开发的应用层协议，被DeviceNet、ControlNet、EtherNet／IP等3种网络所采用，因此这3种网络相应地统称为CIP网络.   
（1）CIP的特点有以下几点   
①报文   
CIP协议最重要的特点是可以传输多种类型的数据。工业应用中所需要传输的数据类型有I／O、互锁、配置、故障诊断、程序上载或下载等。这些不同类型的数据对传输服务质量的要求是不同的。重要的传输服务质量评价指标有确定性、单位时间内有通信行为的节点所占的比例、响应时间等。   
CIP根据所传输的数据对传输服务质量要求的不同，把报文分为两种：显   
式报文和隐式报文。显式报文用于传输对时间没有苛求的数据，比如程序的上载   
下载、系统维护、故障诊断、设备配置等。由于这种报文包含解读该报文所需要   
的信息，所以称为显式报文。隐式报文用于传输对时间有苛求的数据，如I／O、实时互锁等。由于这种报文不包含解读该报文所需要的信息，其含义是在网络配置时就确定的，所以称为隐式报文。由于隐式报文通常用于传输I／O数据，隐式报文又称为I／O报文或隐式I／O报文。   
在网络底层协议的支持下，CIP用不同的方式传输不同类型的报文，以满足它们对传输服务质量的不同要求。DeviceNet给予不同类型的报文不同的优先级，   
隐式报文使用优先级高的报头，显式报文使用优先级低的报头。ControlNet在预定时问段发送隐式报文，在非预定时问段发送显式报文。而Ethemet／IP用TCP来发送显式报文，用UDP来发送隐式报文。   
②面向连接   
CIP还有一个重要特点是面向连接，即在通信开始之前必须建立起连接，获取惟一的连接标识符(connection ID)。如果连接涉及到双向的数据传输，就   
需要两个CID。CID的定义及格式是与具体网络有关的，比如，DeviceNet的CID   
定义是基于CAN标识符的。通过获取CD，连接报文就不必包含与连接有关的所   
有信息，只需要包含CID即可，从而提高了通信效率。不过，建立连接需要用到   
未连接报文。未连接报文需要包括完整的目的地节点地址、内部数据描述符等信   
息，如果需要应答，还要给出完整的源节点地址。   
对应于两种CIP报文传输，CIP连接也有两种，即显式连接和隐式连接。建立连接需要用到末连接报文管理器(unconnected Message Manager—UCMM)，它是CIP设备中专门用于处理未连接报文的一个部件。如果节点A试图与节点B建立显式连接，它就以广播的方式发出一个要求建立显式连接的未连接请求报文，网络上所有的节点都接收到该请求，并判断是否发给自己的，节点B发现是发给自己的，其UCMM就做出反应，也以广播的方式发出一个包含CID的未连接响应报文，节点A接收到后，得知CID，显式连接就建立了。隐式连接的建立更为复杂，它是在网络配置时建立的，在这一过程中，需要用到多种显式报文传输服务。CIP把连接分为多个层次，从上往下依次是应用连接、传输连接和网络连接。一个传输连接是在一个或两个网络连接的基础上建立的，而一个应用连接是在一个或两个传输连接的基础上建立的。   
③生产者／消费者模型   
在传统的源／目的通信模式下，源端每次只能和一个目的地址通信，源端提供的实时数据必须保证每一个目的端的实时性要求，同时一些目的端可能不需要这些数据，因此浪费了时间，而且实时数据的传送时间会随着目的端数目的多少而改变。而在EtherNeL／IP所采用生产者／消费者通信模式下，数据之间的关联不是由具体的源、目的地址联系起来，而是以生产者和消费者的形式提供，允许网络上所有节点同时从一个数据源存取同一数据，因此使数据的传输达到了最优化，每个数据源只需要一次性的把数据传输到网络上，其它节点就可以选择性地接收这些数据，避免了浪费带宽，提高了系统的通信效率，能够很好地支持系统的控制、组态和数据采集。   
（2） CIP 协议功能及特征   
EtherNet/IP 其特色就是被称作控制和信息协议的CIP 部分。CIP 一方面提供实时I/O 通信，一方面实现信息的对等传输。其控制部分通过隐形报文来实现实时I/O 通信，信息部分则通过显性报文来实现非实时的信息交换。CIP 协议的一个重要的特性，是其介质无关性。即CIP 作为应用层协议的实施与底层介质无关。这就是人们可以在控制系统和I/O 设备上灵活实施这一开放协议的原因。同样，当未来新型的通讯手段出现时，人们一样可以方便地将其移植到更高性能的网络上实施，并且提供全部的网络功能，保证与原有现场总线或者以太网技术的透明性和一致性。   
3.2 EtherNet/IP 的通信机制   
1. 通信模式   
不同于源/目的通信模式，EtherNet/IP 采用生产/消费模式，它允许网络上的节点同时存取同一个源的数据。在生产/消费模式中，数据被分配一个唯一的标识，每一个数据源一次性的将数据发送到网络上，其他节点选择性的读取这   
些数据，从而提高了系统的通信效率。   
2. CIP 报文通信   
CIP 报文定义了显式报文和隐式报文两种报文类型, 隐式报文是对时间有苛刻要求的I/O信息(时间触发、控制器互锁等等)，此时数据量不大但需要高的速度或需要较长的源节点和其他节点连接时间，所以这部分采用的是速度较快的UDP 协议；显式报文数据量较大但不需要一直连接所以这部分采用TCP 协议。   
CIP 报文的通信分为无连接的通信和基于连接的通信。无连接的报文通信是CIP 定义的最基本的通信方式。设备的无连接通信资源由无连接报文管理器UCMM 管   
理。无连接通信不需要任何设置或任何机制保持连接激活状态; 基于连接的报文通信是CIP 网路传递报文的另一种方式,可用来传递I/O数据和显式报文。这种通信方式支持生产者/消费者模式的多点传输关系, 一次向多个目的节点进行高效的数据传输。   
4 Ethernet／I P通信适配器硬件设计与实现   
EtherNet／IP硬件设备开发主要有2种方式：一种是基于单板计算机系统；另外一种是开发嵌入式系统。嵌入式系统应用广泛，有非常多资源可供设计者使用，同时嵌入式系统硬件制作成本低，硬件设备可以设计的更为紧凑，有利于系统的小型化。下来介绍采用嵌入式系统设计Ethernet／IP通信适配器。   
4．1 硬件系统总体架构   
Ethernet／IP通信适配器作为工业控制中的网络设备，对数据处理能力、数据收发的实时性、可靠性上较商用以太网有着更严格的规范和要求，硬件必须能够满足这些功能及要求。而微处理器是系统的控制核心，其性能的好坏直接决定了系统性能的优劣；因此，本通信适配器选用三星公司的ARM9 S3C2410为CPU，其有丰富的外围接口功能，强大的处理能力。本系统硬件设计以S3C2410为核心，外围扩展了64MbitsSRAM、64Mbits NAND FLASH、以太网控制其CS8900、RS232串口、I/O接口、JTAG程序实时仿真接口等。系统总体硬件如图3

图3 系统总体硬件   
4．2电源设计   
本通信适配器可以接现场I／O模块(现场I／O模块分为数字I／O及模拟I／O)，因此，设计电源时需充分考虑电源的驱动能力。电源不仅要给通信适配器供电，而且，需要给I／O模块的数字电路部分供电。本设计采用高效的开关电源设计，可满足8个扩展I／O模块的驱动能力。通信适配器中，不同的芯片采用的所要求的供电电压是不一样的。S3C2410需要的供电电压有：3．3V的数字电压及模拟电压、1．8V的数字电压及模拟电压、1．8V的PLL源电压；SRAM、NAND FLASH、I／O采用3．3V电压；JTAG、以太网控制其采用5V电压供电。工业以太网现场提供24VDC电源，因此，设计的电源模块必须提供把24VDC转换成5V、3．3V及1．8V的能力。   
4．3复位电路设计   
由于ARM芯片的高速、低电压供电和低功耗导致其噪声容限较低，对电源的纹波、瞬时响应性能、时钟源的稳定性和电源监控的可靠性等诸多方面提出了更高的要求。为了保证系统在上电启动及电压不稳定时能够正确工作，系统设计中采用了专门的微处理器电源监控芯片MAX708TESA。电路如图4所示。

图4 电源监控及复位电路   
在图4中，信号RESET连接到以太网控制器CS8900的复位引脚，因为CS8900的复位信号为高有效；信号RESET连接到S3C2410的复位引脚／RESET以及芯片内部JTAG接口电路的复位脚TRST。当复位按键Sl按下时，MAX708T立即输出复位信号，其引脚RESET输出高电平复位信号，引脚RESET输出低电平复位信号；此时S3C2410及以太网控制器CS8900都将复位。   
ARM微处理器必须保证在稳定的复位状态下启动，当微处理器在未知状态时，必须使它保持复位状态。MAX708TESA保证低电压的时候处理器处于复位状态，避免系统在上电、掉电及电源状态不稳定的时候代码执行出错。当上电的时候，如果电源达到1V，／RESET引脚输出逻辑低电平，RESET引脚输出逻辑高电平。当电源超出了复位的门栏电压，MAX708TESA的内部定时器保证／RESET和RESET引脚保持200ms的复位信号，这就保证了系统在电源不稳定或者电源过低的情况下始终维持在复位状态，降低系统运行出错的可能性。   
4．4以太网通讯接口设计   
4．4．1以太网电路原理   
以太网控制器是Ethernet／IP通信适配器中一个非常重要的物理部件，它实现以太网的数据链路层协议。为了保证设备能够很好地满足工业应用的要求，所选用的以太网控制器需具备以下一些特点：能在工业环境中运行，对高温低温、噪声、震动等有一定的抵抗能力；支持全双工通讯；支持10Mbit／s或100Mbit／s传输速率等。S3C2410A没有内置的以太网控制器，本文采用Cirrus Logic公司开发的CS8900A—IQ3作为Ethernet／IP通信适配器的以太网控制CS8900A-IQ3主要特点是：lOMbit／s的传输速率、支持全双工运作模式、内建缓冲区提供传送接收讯框(Frames)、可对错误的封包自动排除等；此外，其特有的PacketPagel”结构可以自动调适网络交通的模式以及系统可用的资源。以太网通讯接口设计中还需使用隔离变压器，其主要作用是把设备的有源部分和其网络接口隔离开，以避免干挠网络的运行。隔离变压器应该提供尽可能高的共模抑制比，ODVA／CI推荐采用在30HZ时共模抑制比在59dB以上的隔离变压器。   
4．4．2以太网芯片CS8900A-IQ3功能描述

图5 CS8900A-CQ3功能图   
在电源开启或硬件复位后，CS8900A–IQ3要传送或接收封包时必须先芯片内部的组态、控制寄存器作参数的设置，比如说：存储器的基底位址、以太网络的物理位址、什么形态的讯框可以被接收和底层媒体介面是什么等等设置。这些参数的来源有两个地方：一个是由host透过ISA汇流排写入CS8900A-CQ3，另一个则是通过外部EEPROM自动载入进来。在所有寄存器设置完毕后CS8900A-CQ3便可进行相关动作.基本上CS8900A—CQ3的主要运作有两个部份：封包传送、封包接收。   
封包传送：   
在CS8900A-CQ3的封包传送过程中有两个阶段：   
(1)封包传送第一个阶段：   
主机将封包数据搬移至CS8900A—C03的缓冲存储器，这样子的搬移动作是在主机发出传送命令时所发生的。传送命令是要通知CS8900A-CQ3有封包数据需要被传送，并且何时要被传送(可在CS8900A-CQ3缓存器内设置成5，381，1021或是所有bytes被传送出去)，以及如何被传送出去(有无CRC、添加的位数据等等)。在传送命令发出后，传送的长度也要告知，这样CS8900A-CQ3需要多少的缓冲空间才可被配置出来。当足够的缓冲空间被配置出来后，主机便可透过I／O模式或是Memory的模式，将封包数据写入CS8900A-CQ3的内部存储器。   
(2)封包传送第二个阶段：   
CS8900A—CQ3将封包数据转换成以太网络讯框，之后送到网络CS8900A—CQ3会在传送缓冲空间累积到足够的数据(先前在CS8900A—CQ3缓存器内设置成5，381，1021或是所有bytes被传送出去等情形)，便马上传送出去。被传送出去的数据依照IEEE802．3以太网络讯框的格式(如下图所示)传送到网络上，以太网络讯框的最大数据酬载量(Payload)为1500 Bytes，最小为46 Bytes，如果上层封包数据量(包含CRC即Cyclic Redundancy Check，也就是FCS即Frame CheckSequence)小于46Bytes，那么CS8900A-CQ3会依照缓存器的设定来决定是否要填加位以补足讯框的最小量，最后再加上4 Bytes FCS送出。   
封包接收：   
(1)封包接收的第一个阶段：   
CS8900A-CQ3接收以太网络讯框后，将讯框存放在内部芯片的内存中，将前导的字节(preamble)以及Start of Frame启始字节移除掉，然后利用地址过滤器比对是否该接收的讯框目的地的地址与网络芯片所设置的地址相同，如果正确的话，便存放在CS8900A—CQ3内部存储器，然后CS8900A-CQ3检查CRC以及相关设定，   
以更进一步确认讯框之无误，然后通知微处理器讯框已被接收的事件。   
(2)封包接收的第二个阶段：   
主机利用ISA总线来传送已接收的讯框至主机上的内存存放。而这个传送的动作可以利用I／0模式、Memory模式或DMA模式达成。   
4．5串行通讯接口设计   
S3C2410A内置3通道UART控制器，可以基于DMA模式或中断模式工作，支持5bits、6bits、7bits或者8bits串行数据发送／接收。本文采用MAXIMG公司为嵌   
入式低功耗应用设计的MAX3232作为串口通讯收发器，MAX3232工作电压为3．3V，输出电平完全兼容RS232工业标准，最大收发速率为120kbps。本文设计Ethernet／IP通讯模块可通过串口直接与PC机连接，并使用串口为程序调试打印信息。串行通讯接口如图6所示：

图6 RS232接口电路图   
4．6 主从USB接口设计   
包括一个USB主机端口和一个USB设备端口。主机端口连接外围设备，如鼠标等，设备端口用于连接PC机。S3C2410A芯片内集成了USB主从控制器，因此，电路上只需加效应管驱动即可构成完整的USB电路，无需加任何USB芯片，这大大简化了电路设计。

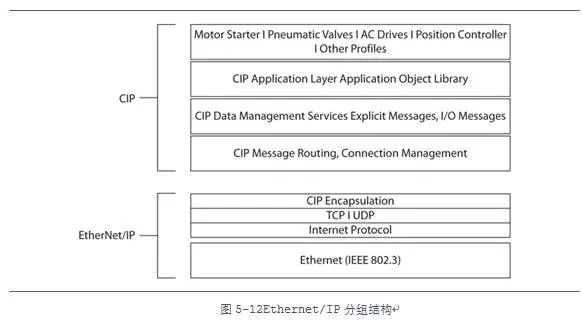
图7 USB接口   
4．7 外部I／0扩展接口设计   
Ethernet／IP通信适配器采用总线模式与多个数字I／O模块相连接，在通信适配器内部给每个I／O模块分配了一个的物理地址，S3C2410A通过具体的物理地址直接读写I／O模块的数据。在S3C2410A与I／O接口之间采用了总线驱动器件，一方面提高主控制器的总线驱动能；另一方面可以隔离S3C2410A系统总线与外部I／O模块直接连接。外部扩展I／O接口原理如图4．12所示。图8中／CER为外部I／O模块的片选信号，／RW输出型I／O的写信号，／OE为输入型I／O的读信号， T为I／O模块产生的中断信号。对于比较重要的I／O可以采用中断的方式进行读写，正常情况下，以查询方式读写I／O数据。

图8 外部扩展IO接口原理   
5 EtherNet/IP 工业以太网优缺点及发展前景   
EtherNet/IP 工业以太网具有许多优点,比如由其组成的系统兼容性和互操作性好,资源共享能力强,可以很容易的实现将控制现场的数据与信息系统上的资源共享; 数据的传输距离长、传输速率高;易与Internet 连接,低成本、易组网,与计算机、服务器的接口十分方便,受到了广泛的技术支持。基于商业以太网开发的各种以太网报文侦听和流量优化控制软件，甚至可以不加改变的应用到工业以太网控制系统中。   
但是，工业以太网也有瓶颈，主要是缺乏实时性和确定性、报文利用率低、回路供电、实时性环境适应等问题。以太网采用的CSMA/CD 协议，不支持优先级。报文头部比较大，载荷数据相对较少，相对现在广泛应用的一些现场总线协议而言，报文利用率较低。总线上无电源。这不但增加了重新购买电源和布置电源线的费用，而且现有以太网线比现场总线更容易受到电磁干扰。缺乏工业级的接插件。由于工业现场存在的腐蚀性气体，震动、维修和检测时的经常拔插等问题。因此需要一种通用工业级接插件。但是工业级接插件的引入势必增加设备的投资。所以，目前EtherNet/IP 工业以太网的应用主要是在自动化领域的信息层和控制层。在设备层则使用ODVA 支持的ControlNet DeviceNet现场总线，利用总线在设备层的抗干扰能力强等优点作为以太网的补充。   
随着网络交换技术、全双工通信、流量控制等技术的发展，EtherNET/IP 工业以太网有一网到底的美景，它可以一直延伸到企业现场设备控制层，所以被人们普遍认为是未来控制网络的最佳解决方案。

这一篇依然是协议层面的，协议层面会翻译三篇，下一篇是电力系统中用的比较多的DNP3。这一篇中大部分引用的资料都可以访问到，只有一篇reversemode.com上的writeup（http://reversemode.com/downloads/logix\_report\_basecamp.pdf）需要身份认证才能下载，如果有朋友能下载求分享。

## ****Ethernet/IP****

## 与Modbus相比，EtherNet/IP 是一个更现代化的标准协议。由工作组ControlNetInternational与ODVA在20世纪90年代合作设计。EtherNet/IP是基于通用工业协议（Common Industrial Protocol，CIP）的。CIP是一种由ODVA支持的开放工业协议，它被使用在诸如DeviceNet和ControlNet以及EtherNet/IP等串行通信协议中。美国的工控设备制造商Rockwell/Allen-Bradley已经围绕EtherNet/IP进行了标准化，其他厂商如Omron也在其设备上支持了EtherNet/IP。EtherNet/IP已经变得越来越受欢迎，特别是在美国。尽管EtherNet/IP比Modbus更现代化，但仍然存在协议层面的安全问题。EtherNet/IP通常通过TCP/UDP端口44818运行。此外，EtherNet/IP还有另一个端口TCP/UDP端口2222。使用这个端口的原因是EtherNet/IP实现了隐式和显示两种消息传递方式。显式消息被称为客户端/服务器消息，而隐式消息通常被称为I/O消息。



EtherNet/IP是为了在以太网中使用CIP协议而进行的封装。EtherNet/IP的CIP帧封装了命令、数据点和消息等信息。CIP帧包括CIP设备配置文件层、应用层、表示层和会话层四层。数据包的其余部分是EtherNet/IP帧，CIP帧通过它们在以太网上传输。EtherNet/IP分组结构如图5‑12所示。

CIP规范对数据包结构有很多的规定，这意味着每个使用EtherNet/IP的设备必须实现符合规范的命令。下面是EtherNet/IP首部中封装的CIP帧字段：

* Command

两字节整数，对应一个CIP命令。CPI标准要求，设备必须能接收无法识别的命令字段，并处理这种异常。

#### Length

两字节整数，代表数据包中数据部分的长度。对于没有数据部分的请求报文，该字段为0。

#### Session Handle

会话句柄（session handle）由目标设备生成，并返回给会话的发起者。该句柄将用于后续与目标设备的通信。

#### Status

Status字段存储了目标设备执行命令返回的状态码。状态码“0”代表命令执行成功。所有的请求报文中，状态码被置为“0”。其它的状态码还包括：

- 0x0001无效或不受支持的命令

- 0x0002目标设备资源不足，无法处理命令

- 0x0003数据格式不正确或数据不正确

- 0x0065接收到无效的数据长度

#### Sender Context

命令的发送者生成这六字节值，接收方将原封不动的返回该值。

#### Options

该值必须始终为0，如果不为零，数据包将被丢弃。

#### Command-specific data

该字段根据接收/发送的命令进行修改。

如果请求发送方是工程师站，大多数会话中执行的第一条命令是“List Identity”命令。如下所示的数据包，命令字段是0x63，代表“List Identity”命令，上下文是“0x00006a0ebe64”。这个命令与Modbus功能码43非常相似，可以查询设备信息，如供应商、产品、序列号、产品代码、设备类型和版本号等。使用在Github项目pyenip中找到的Python脚本ethernetip.py（https://github.com/paperwork/pyenip/blob/master/ethernetip.py），你可以查询Ethernrt/IP设备的信息。默认情况下，这个脚本不会解析一些响应，你需要取消脚本底部的testENIP()函数的注释后，它才会发送和接收“ListIdentity”命令。在执行脚本的。

同时，你可以使用Wireshark查看请求和响应的数据包。

我们在这个例子中没有提供脚本代码，因为它大约有1000行代码。你可以通过访问下面这个GitHub链接来获取脚本（https://github.com/paperwork/pyenip/blob/605ad6d026865e3378542d4428ec975e7c26d2e4/ethernetip.py）。

### ****设备信息泄露****

* 流行程度：10
* 利用难度：8
* 影响面：3
* 威胁评分：7

Digital Bond在项目Redpoint中实现了一个和pyenip很像的脚本，可以用来从远程设备中获取信息。Redpoint脚本使用了上一节提到的“ListIdentity”命令字，并使用NES脚本来解析请求。这个脚本有一个有意思的地方，它的“Conmmand Specific Data”部分包含了一个套接字地址（ip地址和端口号）。这是暴露的远程设备的真实ip地址和端口号，即使它位于NAT设备之后。

通过Shodan搜索（https://www.shodan.io/search?query=port%3A44818），我们发现大量的设备暴露的IP字段和实际扫描的IP地址不同。所以我们得出结论，大多数的Ethernet/IP设备部署在内部网络中，而不是直接暴露在互联网上。如下图5‑15所示的是使用nmap扫描CompactLogix控制系统的扫描结果，可以看到暴露的设备ip和扫描ip不匹配，说明目标系统位于路由器或防火墙之后。

上图显示了一些信息，包括设备的制造商“Rockwell”。设备的制造商在响应中是一个两字节的制造商ID，它映射了一组支持Ethernet/IP的厂商名单。但是，这个厂商名单不是公开的。我们在深入研究Wireshark捕获的数据包后，发现数据包被Wireshark解析后，制造商ID被替换成了制造商名称。这说明Wireshark拥有如何映射制造商ID和名称的信息。通过对Github上Wireshark源代码的一些搜索，我们发现了如下代码片段，它告诉我们该如何解析制造商ID。在解析工控协议的时候，Wireshark常常是一个强大而好用的资源。

使用像“List Identity”这样的命令，你可以简单的重放数据包，几乎不用修改数据包。会话句柄将被设置为0，意味着没有会话生成，因为该命令只是简单的发送命令和接收系统响应。为了进一步与设备进行通信，需要发送注册会话命令（0x65）。这个命令会设置会话句柄ID，这个ID将用于后续会话的通信。如下图5‑16所示，注册会话的请求使用标准ID“0x00000000”，目标设备返回了它生成的会话句柄“0x03A566BB”。

### ****Ethernet/IP中间人攻击****

* 流行程度：5
* 利用难度：8
* 影响面：8
* 威胁评分：7

Ethernet/IP具有和大多数工控协议相似的问题。资讯和培训公司Kenexis发布了针对Ethernet/IP的中间人攻击示例演示。这些示例可以在它们的Github项目主页上找到（https://github.com/kenexis/PortableICS-MITM）。与Modbus不同，简单的数据包重放对Ethernet/IP的某些指令无效。这使得攻击变得稍微复杂了一些。然而，对于大多数攻击者而言，只要对Ethernet/IP的协议稍有了解，这点困难将是微不足道的。一旦会话句柄通过协商被确定，只要通过手动改变序列号，就可以实现像之前Modbus-vcr工具那样的中间人攻击。

### ****Ethernet/IP高危命令字****

* 流行程度：5
* 利用难度：8
* 影响面：8
* 威胁评分：7

就像Modicon利用功能码90来终止CPU，一些Ethernet/IP设备也支持类似的命令字。Digital Bind的Basecamp项目中，发布了一个Metasploit模块（https://www.rapid7.com/db/modules/auxiliary/admin/scada/multi\_cip\_command），可以被用来终止一个Allen-Bradley ControlLogix控制系统中的大量PLC，以及其它的一些坏坏的事情，比如使以太网卡崩溃。

Digital Bond的Ruben Santamarta在撰写Basecamp项目的Writeup“Attacking ControlLogix”（http://reversemode.com/downloads/logix\_report\_basecamp.pdf）时写道“我们发送的每个数据包必须包含会话句柄。这就是全部，然后我们Hack了控制器。在协议层面没有更多的安全机制了。”[译者注：reversemode.com上的文档我下载不下来，有能够下载的朋友求分享]。Ruben指出，只要了解Session Handle即可轻松攻击Ethernet/IP。是这个攻击奏效的另一个关键是Allen-Bradley实现的一个命令字。Allen-Bradley在NOP（0x00）命令中实现了终止CPU的功能。

这个命令在CPI或Ethernet/IP的规范中没有记录，是Allen-Bradley/Rockwell控制器的私有实现。通过对大量设备的测试，我们发现，在一些旧的固件中，不仅ControlLogix CPU被终止，而且设备崩溃，需要重新启动硬盘。对于当前的型号，PLC必须拔下并重新插入才能再次运行。极少数情况下，PLC需要重新编程。

我们还是坚持一贯的建议，如果你想测试你的Ethernet/ip设备，请只对非生产设备执行这些测试，并确保你已经被授予对设备执行exploit的许可，因为在设备上执行这些测试的后果是不可测的。

**各种工业以太网比较（EtherCAT,EtherNet/IP,ProfiNet,Modbus-TCP,Powerlink）**

2014年10月02日 23:53:51 [齐鸣飞](https://me.csdn.net/xqmoo8) 阅读数：33754更多

个人分类： [Communication basics](https://blog.csdn.net/xqmoo8/article/category/1236845)

EtherCAT（以太网控制自动化技术）是一个以以太网为基础的开放架构的现场总线系统，EterCAT名称中的CAT为ControlAutomation Technology（控制自动化技术）首字母的缩写。最初由德国倍福自动化有限公司(Beckhoff AutomationGmbH)研发。EtherCAT为系统的实时性能和拓扑的灵活性树立了新的标准，同时，它还符合甚至降低了[现场总线](http://baike.baidu.com/view/15180.htm)的使用成本。EtherCAT的特点还包括高精度设备同步，可选线缆冗余，和功能性安全协议(SIL3)。

**Ethernet/IP**是一个面向工业自动化应用的工业[应用层](http://baike.baidu.com/view/239619.htm)协议。它建立在标准UDP/IP与TCP/IP协议之上，利用固定的以太网硬件和软件，为配置、访问和控制工业自动化设备定义了一个[应用层](http://baike.baidu.com/view/239619.htm)协议西蒙公司开发

PROFINET由PROFIBUS国际组织（PROFIBUS International，PI）推出，是新一代基于工业以太网技术的自动化[总线标准](http://baike.baidu.com/view/672343.htm)。作为一项战略性的技术创新，[PROFINET](http://baike.baidu.com/view/835484.htm)为自动化通信领域提供了一个完整的网络解决方案，囊括了诸如实时以太网、[运动控制](http://baike.baidu.com/view/1501678.htm)、分布式自动化、故障安全以及网络安全等当前自动化领域的热点话题，并且，作为跨供应商的技术，可以完全兼容[工业以太网](http://baike.baidu.com/view/568270.htm)和现有的[现场总线](http://baike.baidu.com/view/15180.htm)（如[PROFIBUS](http://baike.baidu.com/view/14965.htm)）技术，保护现有投资。

PROFINET是适用于不同需求的完整解决方案，其功能包括8个主要的模块，依次为实时通信、分布式现场设备、[运动控制](http://baike.baidu.com/view/1501678.htm)、分布式自动化、网络安装、IT标准和信息安全、故障安全和[过程自动化](http://baike.baidu.com/view/5981041.htm)。

MODBUS/TCP是简单的、中立厂商的用于管理和控制自动化设备的MODBUS系列通讯协议的派生产品。显而易见，它覆盖了使用TCP/IP协议的 “Intranet”和“Internet”环境中MODBUS 报文的用途。协议的最通用用途是为诸如PLC’s，I/O模块，以及连接其它简单域总线或I/O模块的网关服务的。  
MODBUS/TCP协议是作为一种（实际的）自动化标准发行的。既然MODBUS已经广为人知，该规范只将别处没有收录的少量信息列入其中。然而，本规范力图阐明MODBUS中哪种功能对于普通自动化设备的互用性有价值，哪些部分是MODBUS作为可编程的协议交替用于PLC’s的“多余部分”。  
　　它通过将配套报文类型“一致性等级”，区别那些普遍适用的和可选的，特别是那些适用于特殊设备如PLC’s的报文。

[POWERLINK=CANopen+Ethernet](http://baike.baidu.com/view/5997651.htm?fr=aladdin#1_1)

鉴于[以太网](http://baike.baidu.com/view/848.htm)的蓬勃发展和CANopen在自动化领域里的广阔应用基础，EthernetPOWERLINK 融合了这两项技术的优点和缺点，即拥有了Ethernet的高速、开放性接口，以及CANopen在工业领域良好的SDO 和PDO 数据定义，在某种意义上说POWERLINK就是Ethernet 上的CANopen，[物理层](http://baike.baidu.com/view/239585.htm)、[数据链路层](http://baike.baidu.com/view/239592.htm)使用了Ethernet介质，而[应用层](http://baike.baidu.com/view/239619.htm)则保留了原有的SDO和PDO对象字典的结构

虽然这些工业以太网都是国际标准，但是指的是IEC 61784里的标准，但是这些工业以太网不都是标准的以太网。即这些工业以太网并不都是符合IEEE802.3U的标准，这当中只有Modbus-TCP和EtherNet/IP是符合IEEE802.3U的，只有符合IEEE802.3U标准的，才能与IT和以太网将来的发展相兼容。而不符合IEEE802.3U标准的，基本上可以讲不是以太网，它们都对以太网进行了修改，或者是硬件或者是软件，已经不是以太网了。

各种工业以太网的区别其实主要就是协议的区别，其中最主要的还是应用层协议的区别，我们知道，按照ISO的参考模型，网络被划分为7层。

a.     Modbus TCP和EtherNet/IP的区别主要是应用层不相同，ModbusTCP的应用层采用Modbus协议，而EtherNet/IP采用CIP协议，这两种工业以太网的数据链路层采用的是CSMA/CD，因此是标准的以太网，另外，这两种工业以太网的网络层和传输层采用TCP/IP协议族。还有一个区别是，Modbus协议中迄今没有协议来完成功能安全、高精度同步和运功控制等，而EtherNet/IP有CIPSafety、CIP Sync和CIP Motion来完成上述功能，所以才有Schneider加入ODVA，成为ODVA的核心成员来推广EtherNet/IP。由于这两种网络都是标准的TCP/IP以太网，所以所有标准以太网节点都可以接入这两种网络。

b.     b. 至于EthernetPowerLink(EPL), Ethernet PowerLink就是个怪胎，PowerLink虽然在物理层和数据链路层还是采用标准的以太网，但是它又添加了另一个数据链路层，此EPL数据链路层在结构上为于以太网数据链路层之上。我们知道数据链路层的一个子层的MAC(介质访问)层的作用是[color=#FF0000]决定哪一个节点可以占有总线，也即决定哪个节点一个发送数据[/color]。所以本来由以太网的数据链路层来决定哪一个节点占用总线，现在它被位于它之上的EPL数据链路层给架空了，由这个EPL数据链路层通过软件的方式来决定哪个节点发送数据。所有在这样的一个EPL工业以太网系统中，不能使用交换机，只能使用HUB，所以对100M的网络，EPL总的带宽是小于100m,一盘情况下只有40－50M，而如果采用交换机的工业以太网，它的带宽可以达到大几百M,另外在EPL网络上，所有的节点都要实现EPL数据链路。没有实现EPL数据链路层的节点不能接入此网络。

 c. PROFINET分为原来划分为v1,v2,v3，现在一般称为ProfiNetCBA、ProfiNet IO和ProfiNet IRT.也就是通过以太网来实现对等通讯、实时控制和运动控制。v1采用TCP/IP协议，采用标准的以太网，而V2和V3不采用tcp/ip协议，这两种都绕过tcp/ip协议，采用另外的网络层和传输层协议，开发ProfiNet采用开发人员人员认为tcp/ip协议增加了数据在网络中的传输延迟，其实这是一种误解，据美国密歇根大学的教授研究后认为数据在TCP/IP中的传输延迟很小，他们研究得出数据在经过TCP,IP栈时延迟只有不到100微秒，如果采用UDP/IP时就更小，同时他们研究也得出数据在不同应用层延时比较大，不同的协议延迟不一样，但是相差不是很大，从200us-800us不等，他们经过实验后认为以太网的基础设施(指交换机、网卡等）和TCP/IP协议并不是影响工业以太网实时性的主要原因，而认为应用层协议才是主要原因。所以密歇根大学的教授认为绕开TCP/IP协议没有丝毫的意义，反而由于缺少了TCP/IP协议，使得设备也就缺少了IT功能，与其它现场总线没有区别。 ProfiNet V3就更特别了，它不完全采用标准以太网的数据链路层，有一不时间采用以太网的数据链路层(CSMA/CD)，而另外一部分时间采用自己的数据链路层，通过一个高精度的时间来完成。所以ProfiNet V3也就不是标准的以太网了，也就给Profinet v3带来如下的问题：不能采用标准的交换机、不能采用标准的以太网芯片、与企业网相连可能会出现问题，与标准以太网相连还要特殊的网关、添加和删除一个节点都需要重新组态网络和重新启动网络、至今没有千兆网络，还有最重要的是，当标准以太网以后发展了后，它不能与标准以太网相兼容，不具有将来以太网所应具有的功能。

 d. EtherCat这种工业以太网也很奇怪，它们不使用标准的芯片，一般不使用交换机，软件也不是标准的，对以太网的数据帧进行了一些修改，我们知道一个数据帧只有一个源节点，但是对于EtherCat一个数据可能有多个源节点，即一个数据是由多个节点发送的数据组合而成的。所以对于这样的网络，标准的以太网设备也不能接入这样的网络。

我认为Ethernet/IP和ProfiNet这两种工业以太网都适合各个行业，并不象heidai讲的应用的行业不一样。首先这两种工业以太网都用于传输非实时数据，还可传输实时数据，即可以用于离散控制，也可用于过程控制(当然现在还不能用于本安应用)。其次，这两种工业以太网都可用于网络功能安全传输，Ethernet/IP有CIP Safety协议，而ProfiNet有Profisafe协议,还有在运动控制方面ProfiNet有 ProfiNet IRT，而EtherNet/IP则有CIP Safety,二者都可以用于中高端的运动控制。最后两者都有基于IEEE1588的高精度时钟同步。而Modbus TCP,EtherCat和PowerLink,都只能完成部分控制任务，如Modbus TCP一般只作常规IO实时和非实时数据。而EtherCat和PowerLink则更象是为运动控制而开发的，这二者好像没有功能安全、在PLC和DCS控制方面也没有得到大自动化公司的支持，况且这两者又对以太网进行修改，一个在软件，另一个在软件和硬件方面都进行了修改，都不能兼容标准的以太网设备，个人认为这样做得不偿失，为满足运动控制而不能兼容已有的标准的以太网设备而开发的工业以太网并不是以太网，与其说是工业以太网还不如说是另一种现场总线。  
   我认为工业以太网的竞争将会在Ethernet/IP和ProfiNet间进行，而其它工业以太网都是这两者的陪衬，将会逐渐退出市场。  
   EtherNet/IP以后将由罗克韦尔自动化、Omron、施耐德和思科公司来推动，而ProfiNet将由业界老大西门子公司带领一些小公司去奋斗，由国内PLC厂商中的老二、老三和老五对老大，不知谁将引导未来。

 其实，工业以太网里还有几个怪胎，举两个例吧：  
  
SynqNet: 丹纳赫主导的，几乎只用在运动控制，而且据说只用在了半导体机械行业（奇怪的是，不才也搞半导体机械很久了，却从来没看到过SynqNet，孤陋寡闻啊）。只用了以太网的硬件，完全和我们平常说的以太网没有任何关系，连MAC层都没有。当然如此运用，速度性能当然好，但未来难说。  
  
Sercos III: 光纤SercosII的新一代以太网版本，背后推手是博世力士乐，只用在运动控制。也基本上是只用了以太网底层硬件，系统里竟然连switch都不允许用。速度当然快，但只比SercosII快了一倍。估计用了SercosII的用户，谁会去更新到一个没快了多少的新系统啊，还没问世，就已经不被业界看好了。  
  
我个人认为，最后一定是大西洋两岸的两大巨人之间的角力，就像以前的现场总线战争，最后还不是Profibus和DeviceNet，别的都只能当陪衬的角色？  
  
当然，现在大家都在看中国这个大西洋两岸以外的单一最大市场，中国把砝码放在谁这一边，可能会使天平倾斜一点。但最后，肯定两者都会存在的。我个人认为，咱们应该选Ethernet/IP这一边站

 中国用户和制造商应选择Ethernet/IP还是ProfiNet，各人的看法有所不同，不过我认为firstrazor所说的没错，有于ProfiNet采用了专门的芯片、网卡、交换机等以太网基础设施，虽然ProfiNet应用层协议是公开的，但这些芯片却是专用，国内的制造商要想开发符合ProfiNet标准的设备，确要依赖于这些芯片，受制于提供芯片的公司，也就是西门子公司，因此可以将ProfiNet并不是完全开放的。而相反，Ethernet/IP不论是在软件还是硬件上都是标准和开放的，国内的工业以太网制造商还是选择EtherNet/IP为好，至于最终用户的选择，当然是从可靠性、价格、兼容性和可替换性方面考虑，可靠性方面，二者没有明显区别，在其它方面Ethernet/IP具有明显的优势

Ethernet/IP、Profinet、Modbus TCP/IP三种协议的区别在协议层不同而已。取个例子，以太网就像高速公路，Ethernet/IP、Profinet、Modbus TCP/IP分别像高速公路上的宝马、奔驰、奥迪车，都可以从一个城市把物品运送到另一城市。但是每个车上安装的零件无法和另一车上的零件进行更换。  
Ethernt/IP属于ODVA组织，Rockwell只是其中一个推广力度比较大的公司而已。施耐德也是ODVA组织的成员，施耐德所有PLC都可以支持Ethernt/IP协议。Ethernt/IP协议是十大总线之一，和Controlnet、Devicenet一起称为CIP总线。可以实现协议间路由，但是需要Rslinx软件进行配置。通讯时需要设置RPI参数，没有任何客户端的反馈信息，因此不管现场客户端是否收到数据，数据一致由服务器不断的发，缺少相应的检测。  
Profinet也是十大总线之一，由西门子主推，Profinet在很多方面比Ethernet/IP、Modbus TCP/IP要强，比如同步，安全总线等方面，也是为了保证数据的可靠性和安全性，在开放性方面较差一些。  
Modbus TCP/IP由Modbus IDA组织提出，有施耐德旗下的Modicon公司主推，在目前施耐德所有PLC产品中都支持，同时也支持Ethernet/IP协议，Modbus TCP/IP是免费的、全开放协议，可以用VB等高级编程语言调用winsock控件即可实现与PLC的数据通讯，因此，很多产品都支持该协议。同时利用该协议进行通讯时，可以得到客户端的数据校验返回，因此可靠性和安全性较高，当然牺牲了数据量。  
1; 这几种协议有什么区别和优势。  
三种协议各有优缺点  
2：现实工程中是考虑性价比的，那一种性格比高。  
现实中楼主选择什么厂家的PLC，建议选择对应的以太网协议，除了施耐德和Rockwell的PLC都支持Ethernet和Modbus TCP/IP协议外（施耐德在两个协议支持上做的更好），目前都没有任何网关产品可以实现Profinet与其它协议的转换。即便有相应的网关，不论成本增加了多少，还牺牲了实时性。因此，建议选择什么PLC，选择相应的以太网即可。性能在目前的所有控制系统中差别不大。

我们知道通信网络的核心是OSI（Open System Interconnection开放式系统互联）参考模型，共分7层，如果对此有所了解，就很容易理解通信技术。IP（属于第三层网络层）定义设备间通过逻辑地址（Internal Protocol因特网协议地址）传输数据，连接位于不同广播域的设备；  
Ethernet IP网络就是通过以太网协议地址建立通信，即通过设定IP地址和相同的子网掩码进行访问，实现比较简单经济；  
TCP/IP（Transmission Control Protocol，传输控制协议）通过因特网协议地址进行允许数据进行可靠的传输，位于OSI模型的第四层（传输层），基于TCP/IP的发送和接收，使得设备在工业以太网上的通信非常容易，该协议支持大量数据的传输，数据可以通过以太网或TCP/IP网络（拨号网络或以太网）传输。它是IT领域关于通讯协议方面事实上的标准，其响应时间大约在100ms的量级，主要用于工厂控制级；  
PROFINET是PROFIBUS国际组织（PI）推出，是新一代基于工业以太网技术的自动化总线标准，它提供了一个自动化通信领域完整的网络解决方案，保证了通信的实时型，完全兼容工业以太网和现有的现场总线（PROFIBUS）技术。PROFINET根据响应时间分为三种通信方式：基于工业以太网技术、使用TDCP/IP和IT标准的TCP/IP标准通信；实时通信（RT）应用于传感器和执行器设备之间的数据交换，响应时间为3-10ms，相当于PROFIBUS总线响应时间; 等时同步实时（IRT）通讯，应用于要求最高的运动控制、伺服控制，响应时间小于1ms。  
可以看出Ethernet IP相当于常规的以太网通信，通讯响应时间长，而且数据传输不可靠；TCP/IP是IT领域关于通讯协议方面事实上的标准，数据传输可靠，应用于一般工业控制；PROFINET主要用于实时性要求高的运动控制中，响应时间小，但要求所有网络节点的同步性好，如果采用IRT通讯需要如西门子IRT同步实时ASIC芯片。  
除非要求实时性高的场合，工业控制的以太网解决方案一般采用TCP/IP通讯就足够了（西门子称为S5兼容通信协议。