Chapter 5:
Industrial Control Busses

5.1 Introduction

A complex automated industrial system — say a manufacturing assembly line — usually needs an organized hierarchy of controller systems to function. In this hierarchy there is usually a Human Machine Interface (HMI) at the top, where an operator can monitor or operate the system. This is typically linked to a middle layer of programmable logic controllers (PLC) via a non time critical communications system (e.g. Ethernet). At the bottom of the control chain is the **fieldbus** which links the PLCs to the components which actually do the work such as sensors, actuators, electric motors, console lights, switches and contactors. A Fieldbus is an industrial network system for real-time distributed control.

Until recently, a PLC would communicate with a slave machine using one of several possible open or proprietary protocols, such as Modbus, Sinec H1, Profibus, CANopen, DeviceNet or FOUNDATION Fieldbus. However, there is now increasing interest in the use of Ethernet as the link-layer protocol, with one of the above protocols as the application-layer (see OSI model). As the following figure shows, Ethernet is now increasing in its popularity over other industrial bus protocols.

5.2 FieldBus

There are a wide variety of concurring fieldbus standards. Some of the most widely used ones include:

- AS-Interface
- CAN
- CANopen
- DeviceNet
- SERCOS_interface
- EtherCAT
- FOUNDATION fieldbus
- HART Protocol
- Industrial Ethernet
- Interbus
- LonWorks
- Modbus
- PROFIBUS
- BITBUS

Fieldbus devices are more flexible than older devices due to the inclusion of a CPU. For example, a pressure transducer can measure process pressure, atmospheric pressure, and also process temperature and supply all three via the fieldbus. Other major cost savings from using fieldbus are due to wiring and installation — the 4–20 mA analogue signal standard requires each device to have its own pair of wires and its own analog connection point at the controller level. Fieldbus eliminates this need by requiring one communication point at the controller level to connect to multiple (100's) of analog and digital points, while at the same time reducing the length of cable runs by connecting to the field devices in a daisy-chain, star, ring, branch, tree style network topology.

5.3 Industrial Ethernet

Industrial Ethernet is the name given to the use of the Ethernet protocol in an industrial environment, for automation and production machine control.

Until recently, a PLC would communicate with a slave machine using one of several possible open or proprietary protocols, such as Modbus, Sinec H1, Profibus, CANopen, DeviceNet or FOUNDATION Fieldbus. However, there is now increasing interest in the use of Ethernet as the link-layer protocol, with one of the above protocols as the application-layer (see OSI model).

During recent years a number of Ethernet based industrial communication system have been established, most of them with extensions for real-time communication. These have the potential to replace the traditional field busses in the long term. Currently the issue stopping most Ethernet fieldbus implementations is the availability of device power. Most industrial measurement & control devices need to be powered from the bus and Power-Over-Ethernet (PoE) does not deliver enough.

- EtherCAT
- Ethernet Powerlink
- SERCOS III
- PROFINET IO
- ETHERNET/IP
- VARAN
- SafetyNET p

A common property of all of these systems seems to be that they are supported by only one PLC/DCS manufacturer for their central logic, and hardly any are compatible with any other.

Some of the advantages are:

- Increased speed, up from 9.6 kbit/s with RS232 to 1 Gbit/s with IEEE 802 over Cat5e/Cat6 cables or optical fiber
- Increased overall performance
- Increased distance
- Ability to use standard access points, routers, switches, hubs, cables and optical fiber, which are immensely cheaper than the equivalent serial-port devices
- Ability to have more than two nodes on link, which was possible with RS485 but not with RS232
- Peer-to-peer architectures may replace master-slave ones
- Better interoperability
- The difficulties of using industrial Ethernet are:
- Migrating existing systems to a new protocol (however many adapters are available)
- Real-time uses may suffer for protocols using TCP (but some use UDP and layer 2 protocols for this reason)
- Managing a whole TCP/IP stack is more complex than just receiving serial data

Serial	Ethernet	Protocol	Network	Standards
Modbus-RTU	Modbus-TCP	TCP/IP		IEC 61158 and IEC 61784
Profibus	PROFINET IO	Isochronous real time protocol (IRT), Real time protocol (RT), Real time over UDP protocol (RTU)	Switches, router and wireless, from 100 Mbit/s up to 1 Gbit/s	IEC 61158 and IEC 61784
DeviceNet (CIP); ControlNet (CIP)	EtherNet/IP (CIP)	TCP/IP; UDP/IP	Switches, router and wireless, from 100 Mbit/s up to 1 Gbit/s	IEC 61158 and IEC 61784; ODVA EtherNet/IP standard
Foundation Fieldbus H1	Foundation Fieldbus High Speed Ethernet (HSE)			
CANopen	Ethernet Powerlink		Ethernet 100Mbit/s	by EPSG (Ethernet Powerlink Standardization Group)
CANopen	EtherCAT	EtherCAT, EtherCAT/UDP	Ethernet 100Mbit/s	IEC 61158, IEC/PAS 62407, IEC 61784-3, ISO 15745-4
	VARAN **V**ersatile **A**utomation **R**andom **A**ccess **N**etwork	VARAN, TCP/IP, Safety	Ethernet 100Mbit/s	VARAN-BUS USER GROUP - VNO

Table 5.1 Summary of different types of Industrial Ethernet busses.

5.4 Theoretical Background in Networking

ISO/OSI Reference Model:

Modern computer networks are designed in a highly structured way. To reduce their design complexity, most networks are organized as a series of layers, each one built upon its predecessor.

The OSI Reference Model is based on a proposal developed by the International Organization for Standardization (ISO). The model is called ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems - that is, systems that are open for communication with other systems.

The OSI model has seven layers which are:

Layer 1 - Physical

> Physical layer defines the cable or physical medium itself, e.g., thinnet, thicknet, unshielded twisted pairs (UTP). All media are functionally equivalent. The main difference is in convenience and cost of installation and maintenance. Converters from one media to another operate at this level.

Layer 2 - Data Link

> Data Link layer defines the format of data on the network. A network data frame, aka packet, includes checksum, source and destination address, and data. The largest packet that can be sent through a data link layer defines the Maximum Transmission Unit (MTU). The data link layer handles the physical and logical connections to the packet's destination, using a network interface. A host connected to an Ethernet would have an Ethernet interface to handle connections to the outside world, and a loopback interface to send packets to itself.

Layer 3 - Network

> NFS uses Internetwork Protocol (IP) as its network layer interface. IP is responsible for routing, directing datagrams from one network to another. The network layer may have to break large datagrams, larger than MTU, into smaller packets and host receiving the packet will have to reassemble the fragmented datagram. The Internetwork Protocol identifies each host with a 32-bit IP address.

Layer 4 - Transport

Transport layer subdivides user-buffer into network-buffer sized datagrams and enforces desired transmission control. Two transport protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), sits at the transport layer. Reliability and speed are the primary difference between these two protocols. TCP establishes connections between two hosts on the network through 'sockets' which are determined by the IP address and port number. TCP keeps track of the packet delivery order and the packets that must be resent. Maintaining this information for each connection makes TCP a stateful protocol. UDP on the other hand provides a low overhead transmission service, but with less error checking. NFS is built on top of UDP because of its speed and statelessness. Statelessness simplifies the crash recovery.

Layer 5 - Session

The session protocol defines the format of the data sent over the connections. The NFS uses the Remote Procedure Call (RPC) for its session protocol. RPC may be built on either TCP or UDP. Login sessions use TCP whereas NFS and broadcast use UDP.

Layer 6 - Presentation

External Data Representation (XDR) sits at the presentation level. It converts local representation of data to its canonical form and vice versa. The canonical uses a standard byte ordering and structure packing convention, independent of the host.

Layer 7 - Application

Provides network services to the end-users. Mail, ftp, telnet, DNS, NIS, NFS are examples of network applications.

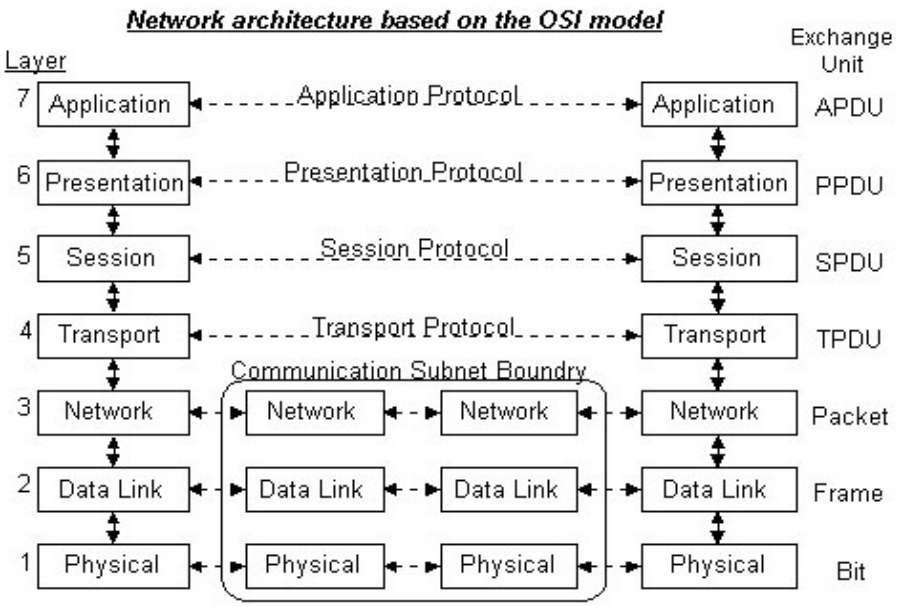

Figure 5.1 Network architecture based on the OSI model.

TCP/IP Network Model

Although the OSI model is widely used and often cited as the standard, TCP/IP protocol has been used by most Unix workstation vendors. TCP/IP is designed around a simple four-layer scheme. It does omit some features found under the OSI model. Also it combines the features of some adjacent OSI layers and splits other layers apart. The four network layers defined by TCP/IP model are as follows.

Layer 1 - Link

This layer defines the network hardware and device drivers.

Layer 2 - Network

This layer is used for basic communication, addressing and routing. TCP/IP uses IP and ICMP protocols at the network layer.

Layer 3 - Transport

This layer handles communication among programs on a network. TCP and UDP fall within this layer.

Layer 4 - Application

End-user applications reside at this layer. Commonly used applications include NFS, DNS, ARP and FTP.

Data Flow within a Protocol Stack

As the reference model indicates, protocols (which compose the various layers) are like a pile of building blocks stacked one upon another. Because of this structure, groups of related protocols are often called *stacks* or *protocol stacks*.

Data is passed down the stack from one layer to the next, until it is transmitted over the network by the network access layer protocols. The four layers in this reference model are crafted to distinguish between the different ways that the data is handled as it passes down the protocol stack from the application layer to the underlying physical network.

At the remote end, the data is passed up the stack to the receiving application. The individual layers do not need to know how the layers above or below them function; they only need to know how to pass data to them.

Each layer in the stack adds control information (such as destination address, routing controls, and checksum) to ensure proper delivery. This control information is called a *header* and/or a *trailer* because it is placed in front of or behind the data to be transmitted. Each layer treats all of the information that it receives from the layer above it as data, and it places its own header and/or trailer around that information.

These wrapped messages are then passed into the layer below along with additional control information, some of which may be forwarded or derived from the higher layer. By the time a message exits the system on a physical link (such as a wire), the original message is enveloped in multiple, nested wrappers—one for each layer of protocol through which the data passed. When a protocol uses headers or trailers to package the data from another protocol, the process is called *encapsulation.*

TCP (Transmission Control Protocol)

- The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks.

- TCP is a connection-oriented transport protocol that sends data as an unstructured stream of bytes. By using sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to a destination node. Where data has been lost in transit from source to destination, TCP can retransmit the data until either a timeout condition is reached or until successful delivery has been achieved. TCP can also recognize duplicate messages and will discard them appropriately. If the sending computer is transmitting too fast for the receiving computer, TCP can employ flow control mechanisms to slow data transfer. TCP can also

communicate delivery information to the upper-layer protocols and applications it supports.

- Unlike TCP's traditional counterpart, UDP (User Datagram Protocol), which can immediately start sending packets on the account of reliability, TCP provides connections that need to be established before sending data. TCP connections have three phases:

    1. connection establishment,
    2. data transfer,
    3. connection termination,

- To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

    1. The active open is performed by the client sending a SYN to the server.
    2. In response, the server replies with a SYN-ACK.
    3. Finally the client sends an ACK (usually called SYN-ACK-ACK) back to the server.

    At this point, both the client and server have received an acknowledgement of the connection.

- TCP supports many of the Internet's most popular application protocols and resulting applications, including the World Wide Web, e-mail, File Transfer Protocol and Secure Shell.
- TCP has been optimized for wired networks. Any packet loss is considered to be the result of congestion and the window size is reduced dramatically as a precaution. However, wireless links are known to experience sporadic and usually temporary losses due to fading, shadowing, handoff, etc. that cannot be considered congestion. Erroneous back-off of the window size due to wireless packet loss is followed by a congestion avoidance phase with a conservative decrease in window size which causes the radio link to be underutilized. Extensive research has been done on this subject on how to combat these harmful effects. Suggested solutions can be categorized as end-to-end solutions (which require modifications at the client and/or server), link layer solutions (such as RLP in CDMA2000), or proxy based solutions (which require some changes in the network without modifying end nodes).
- For further details and information about TCP operation, the reader is encouraged to read the RFC793 document.