Practical Troubleshooting and Problem Solving of Industrial Data Communications

Revision 5.1
Deon Reynders, Pr Eng - B Sc Eng Hons; MBA

Website: www.idc-online.com
E-mail: idc@idc-online.com
Copyright
All rights to this publication, associated software and workshop are reserved. No part of this publication or associated software may be copied, reproduced, transmitted or stored in any form or by any means (including electronic, mechanical, photocopying, recording or otherwise) without prior written permission of IDC Technologies.

Disclaimer
Whilst all reasonable care has been taken to ensure that the descriptions, opinions, programs, listings, software and diagrams are accurate and workable, IDC Technologies do not accept any legal responsibility or liability to any person, organization or other entity for any direct loss, consequential loss or damage, however caused, that may be suffered as a result of the use of this publication or the associated workshop and software.

In case of any uncertainty, we recommend that you contact IDC Technologies for clarification or assistance.

Trademarks
All terms noted in this publication that are believed to be registered trademarks or trademarks are listed below:

IBM, XT and AT are registered trademarks of International Business Machines Corporation. Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corporation.

Acknowledgements
IDC Technologies expresses its sincere thanks to all those engineers and technicians on our training workshops who freely made available their expertise in preparing this manual.
Who is IDC Technologies?
IDC Technologies is a specialist in the field of industrial communications, telecommunications, automation and control and has been providing high quality training for more than six years on an international basis from offices around the world.

IDC consists of an enthusiastic team of professional engineers and support staff who are committed to providing the highest quality in their consulting and training services.

The Benefits to you of Technical Training Today
The technological world today presents tremendous challenges to engineers, scientists and technicians in keeping up to date and taking advantage of the latest developments in the key technology areas.

- The immediate benefits of attending IDC workshops are:
  - Gain practical hands-on experience
  - Enhance your expertise and credibility
  - Save $$$s for your company
  - Obtain state of the art knowledge for your company
  - Learn new approaches to troubleshooting
  - Improve your future career prospects

The IDC Approach to Training
All workshops have been carefully structured to ensure that attendees gain maximum benefits. A combination of carefully designed training software, hardware and well written documentation, together with multimedia techniques ensure that the workshops are presented in an interesting, stimulating and logical fashion.

IDC has structured a number of workshops to cover the major areas of technology. These courses are presented by instructors who are experts in their fields, and have been attended by thousands of engineers, technicians and scientists world-wide (over 11,000 in the past two years), who have given excellent reviews. The IDC team of professional engineers is constantly reviewing the courses and talking to industry leaders in these fields, thus keeping the workshops topical and up to date.
Technical Training Workshops

IDC is continually developing high quality state of the art workshops aimed at assisting engineers, technicians and scientists. Current workshops include:

Instrumentation & Control
- Practical Automation and Process Control using PLC’s
- Practical Data Acquisition using Personal Computers and Standalone Systems
- Practical On-line Analytical Instrumentation for Engineers and Technicians
- Practical Flow Measurement for Engineers and Technicians
- Practical Intrinsic Safety for Engineers and Technicians
- Practical Safety Instrumentation and Shut-down Systems for Industry
- Practical Process Control for Engineers and Technicians
- Practical Programming for Industrial Control – using (IEC 1131-3; OPC)
- Practical SCADA Systems for Industry
- Practical Boiler Control and Instrumentation for Engineers and Technicians
- Practical Process Instrumentation for Engineers and Technicians
- Practical Motion Control for Engineers and Technicians
- Practical Communications, SCADA & PLC’s for Managers

Communications
- Practical Data Communications for Engineers and Technicians
- Practical Essentials of SNMP Network Management
- Practical Field Bus and Device Networks for Engineers and Technicians
- Practical Industrial Communication Protocols
- Practical Fibre Optics for Engineers and Technicians
- Practical Industrial Networking for Engineers and Technicians
- Practical TCP/IP & Ethernet Networking for Industry
- Practical Telecommunications for Engineers and Technicians
- Practical Radio & Telemetry Systems for Industry
- Practical Local Area Networks for Engineers and Technicians
- Practical Mobile Radio Systems for Industry
Electrical
- Practical Power Systems Protection for Engineers and Technicians
- Practical High Voltage Safety Operating Procedures for Engineers & Technicians
- Practical Solutions to Power Quality Problems for Engineers and Technicians
- Practical Communications and Automation for Electrical Networks
- Practical Power Distribution
- Practical Variable Speed Drives for Instrumentation and Control Systems

Project & Financial Management
- Practical Project Management for Engineers and Technicians
- Practical Financial Management and Project Investment Analysis
- How to Manage Consultants

Mechanical Engineering
- Practical Boiler Plant Operation and Management for Engineers and Technicians
- Practical Centrifugal Pumps – Efficient use for Safety & Reliability

Electronics
- Practical Digital Signal Processing Systems for Engineers and Technicians
- Practical Industrial Electronics Workshop
- Practical Image Processing and Applications
- Practical EMC and EMI Control for Engineers and Technicians

Information Technology
- Personal Computer & Network Security (Protect from Hackers, Crackers & Viruses)
- Practical Guide to MCSE Certification
- Practical Application Development for Web Based SCADA
Comprehensive Training Materials

Workshop Documentation
All IDC workshops are fully documented with complete reference materials including comprehensive manuals and practical reference guides.

Software
Relevant software is supplied with most workshops. The software consists of demonstration programs which illustrate the basic theory as well as the more difficult concepts of the workshop.

Hands-On Approach to Training
The IDC engineers have developed the workshops based on the practical consulting expertise that has been built up over the years in various specialist areas. The objective of training today is to gain knowledge and experience in the latest developments in technology through cost effective methods. The investment in training made by companies and individuals is growing each year as the need to keep topical and up to date in the industry which they are operating is recognized. As a result, the IDC instructors place particular emphasis on the practical hands-on aspect of the workshops presented.

On-Site Workshops
In addition to the quality of workshops which IDC presents on a world-wide basis, all IDC courses are also available for on-site (in-house) presentation at our clients’ premises. On-site training is a cost effective method of training for companies with many delegates to train in a particular area. Organizations can save valuable training $$$’s by holding courses on-site, where costs are significantly less. Other benefits are IDC’s ability to focus on particular systems and equipment so that attendees obtain only the greatest benefits from the training.

All on-site workshops are tailored to meet with clients training requirements and courses can be presented at beginners, intermediate or advanced levels based on the knowledge and experience of delegates in attendance. Specific areas of interest to the client can also be covered in more detail. Our external workshops are planned well in advance and you should contact us as early as possible if you require on-site/customized training. While we will always endeavor to meet your timetable preferences, two to three month’s notice is preferable in order to successfully fulfil your requirements. Please don’t hesitate to contact us if you would like to discuss your training needs.
Customized Training

In addition to standard on-site training, IDC specializes in customized courses to meet client training specifications. IDC has the necessary engineering and training expertise and resources to work closely with clients in preparing and presenting specialized courses.

These courses may comprise a combination of all IDC courses along with additional topics and subjects that are required. The benefits to companies in using training are reflected in the increased efficiency of their operations and equipment.

Training Contracts

IDC also specializes in establishing training contracts with companies who require ongoing training for their employees. These contracts can be established over a given period of time and special fees are negotiated with clients based on their requirements. Where possible, IDC will also adapt courses to satisfy your training budget.

References from various international companies to whom IDC is contracted to provide on-going technical training are available on request.

Some of the thousands of Companies worldwide that have supported and benefited from IDC workshops are:

## Contents

Preface xiii

1 Introduction 1
   1.1 Introduction 1
   1.2 Modern instrumentation and control systems 2
   1.3 Open systems interconnection (OSI) model 5
   1.4 Protocols 6
   1.5 Standards 7

2 Overall methodology 15
   2.1 Introduction 15
   2.2 Common problems and solutions 15
   2.3 General comments on troubleshooting 16
   2.4 A specific methodology 16
   2.5 Grounding/shielding and noise 17

3 EIA-232 overview 29
   3.1 EIA-232 interface standard (CCITT V.24 Interface standard) 29
   3.2 Half duplex operation of the EIA-232 interface 35
   3.3 Limitations 37
   3.4 Troubleshooting 38

4 EIA-485 overview 47
   4.1 The EIA-485 interface standard 47
   4.2 Troubleshooting 51

5 Current loop and EIA-485 converters overview 61
   5.1 The 20 mA current loop 61
   5.2 Serial interface converters 62
   5.3 Troubleshooting 63

6 Fiber optics overview 67
   6.1 Introduction 67
   6.2 Fiber-optic cable components 68
   6.3 Fiber optic cable parameters 69
   6.4 Types of optical fiber 70
## 12 DeviceNet overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1 Introduction</td>
<td>141</td>
</tr>
<tr>
<td>12.2 Physical layer</td>
<td>142</td>
</tr>
<tr>
<td>12.3 Connectors</td>
<td>143</td>
</tr>
<tr>
<td>12.4 Cable budgets</td>
<td>145</td>
</tr>
<tr>
<td>12.5 Device taps</td>
<td>146</td>
</tr>
<tr>
<td>12.6 Cable description</td>
<td>148</td>
</tr>
<tr>
<td>12.7 Network power</td>
<td>150</td>
</tr>
<tr>
<td>12.8 System grounding</td>
<td>152</td>
</tr>
<tr>
<td>12.9 Signaling</td>
<td>153</td>
</tr>
<tr>
<td>12.10 Data link layer</td>
<td>153</td>
</tr>
<tr>
<td>12.11 Troubleshooting</td>
<td>156</td>
</tr>
</tbody>
</table>

## 13 Profibus overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1 Introduction</td>
<td>163</td>
</tr>
<tr>
<td>13.2 ProfiBus protocol stack</td>
<td>164</td>
</tr>
<tr>
<td>13.3 System Operation</td>
<td>169</td>
</tr>
<tr>
<td>13.4 Troubleshooting</td>
<td>171</td>
</tr>
</tbody>
</table>

## 14 Foundation Fieldbus overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1 Introduction</td>
<td>175</td>
</tr>
<tr>
<td>14.2 The physical layer and wiring rules</td>
<td>176</td>
</tr>
<tr>
<td>14.3 The data link layer</td>
<td>180</td>
</tr>
<tr>
<td>14.4 The application layer</td>
<td>180</td>
</tr>
<tr>
<td>14.5 The user layer</td>
<td>181</td>
</tr>
<tr>
<td>14.6 Error detection and diagnostics</td>
<td>182</td>
</tr>
<tr>
<td>14.7 High-speed Ethernet (HSE)</td>
<td>182</td>
</tr>
<tr>
<td>14.8 Good wiring and installation practice with FieldBus</td>
<td>183</td>
</tr>
<tr>
<td>14.9 Troubleshooting</td>
<td>184</td>
</tr>
</tbody>
</table>

## 15 Industrial Ethernet overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1 Introduction</td>
<td>189</td>
</tr>
<tr>
<td>15.2 10 Mbps Ethernet</td>
<td>190</td>
</tr>
<tr>
<td>15.3 100 Mbps Ethernet</td>
<td>197</td>
</tr>
<tr>
<td>15.4 Gigabit Ethernet</td>
<td>198</td>
</tr>
<tr>
<td>15.5 Industrial Ethernet</td>
<td>198</td>
</tr>
<tr>
<td>15.6 Troubleshooting</td>
<td>201</td>
</tr>
<tr>
<td></td>
<td>TCP/IP overview</td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
</tr>
<tr>
<td>16</td>
<td>Introduction</td>
</tr>
<tr>
<td>16.1</td>
<td></td>
</tr>
<tr>
<td>16.2</td>
<td>Internet layer protocols (packet transport)</td>
</tr>
<tr>
<td>16.3</td>
<td>Host-to-host layer: End to end reliability</td>
</tr>
<tr>
<td>16.4</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>Radio and wireless communications overview</td>
</tr>
<tr>
<td>17</td>
<td>Introduction</td>
</tr>
<tr>
<td>17.1</td>
<td></td>
</tr>
<tr>
<td>17.2</td>
<td>Components of a radio link</td>
</tr>
<tr>
<td>17.3</td>
<td>The radio spectrum and frequency allocation</td>
</tr>
<tr>
<td>17.4</td>
<td>Summary of radio characteristics of VHF/UHF</td>
</tr>
<tr>
<td>17.5</td>
<td>Radio modems</td>
</tr>
<tr>
<td>17.6</td>
<td>Intermodulation and how to prevent it</td>
</tr>
<tr>
<td>17.7</td>
<td>Implementing a radio link</td>
</tr>
<tr>
<td>17.8</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>Appendix A Glossary</td>
</tr>
<tr>
<td></td>
<td>Appendix B Basic Terminology</td>
</tr>
<tr>
<td></td>
<td>Appendix C Practical Exercises</td>
</tr>
<tr>
<td></td>
<td>Appendix D Local services, regulations and standards</td>
</tr>
</tbody>
</table>
Preface

This is a comprehensive book covering the essentials of troubleshooting and problem solving of industrial data communications systems including areas such as RS–232, RS–485, industrial protocols such as Modbus, fiber optics, industrial Ethernet, TCP/IP, DeviceNet and Fieldbus protocols such as Profibus and Foundation Fieldbus. It can be used very beneficially in conjunction with the IDC Technologies two–day workshop on the topic.

We have taken all the key troubleshooting and problem-solving skills from experienced engineers and distilled these into one hard-hitting course to enable the user to solve real industrial communications problems.

The overall objective of the book is to help identify, prevent and fix common industrial communications problems. The focus is ‘outside the box.’ The emphasis is practical and on material that goes beyond typical communications issues. Also, on theory and focuses on providing with the necessary toolkit of skills in solving industrial communications problems whether it be RS–232/RS–485, Modbus, Fieldbus and DeviceNet or a local area network such as Ethernet. industrial communications systems are being installed throughout the plant today from connecting simple instruments to programmable logic controllers to PCs throughout the business part of the enterprise. Communications problems range from simple wiring problems to intermittent transfer of protocol messages.

The communications system on the plant underpins the entire operation. It is critical that there should be the knowledge and tools to quickly identify and fix problems as they occur, to ensure that there is a secure and reliable system. No compromise is possible here. This book distills all the tips and tricks learnt with the benefit of many years of experience. It offers a common approach covering all of the sections listed below with each standard/protocol having the following structure:

- Quick overview of the standard
- Common problems and faults that can occur
- Description of tools used
- Each of the faults and ways of fixing them are then discussed in detail

The aim is to provide enough knowledge to troubleshoot and fix problems, as quickly as possible.

At the conclusion of this book, you will be able to:

- Identify, prevent and troubleshoot industrial communications problems
- Fix over 60 of the most common problems that occur in RS–232/RS–485, Industrial Protocols (incl. Modbus/ Data Highway Plus), Industrial Ethernet, TCP/IP, DeviceNet and Fieldbus (such as Profibus and Foundation Fieldbus)
- Gain a practical toolkit of skills to troubleshoot industrial communications systems from RS–232, RS–485, Fiber Optics, Fieldbus to Ethernet
- Analyze most industrial communications problems and fix them
- Fault find your Ethernet and TCP/IP network problems

This book is intended for engineers and technicians who are:

- Instrumentation and control engineers/technicians
- Process control engineers
- Electrical engineers
- System integrators
- Designers
- Design engineers
- Systems engineers
- Network planners
- Test engineers
- Electronic technicians
- Consulting engineers
- Plant managers
- Shift electricians
A basic knowledge of data communications is useful but not essential.
The structure of the book is listed below. Each chapter is broken down into:

- Fundamentals of the standard or protocol
- Troubleshooting
Objectives

When you have completed study of this chapter you will be able to:

- Describe the modern instrumentation and control systems
- List the main industrial communications systems
- Describe the essential components of industrial communications systems

1.1 Introduction

Data communications involves the transfer of information from one point to another. In this book we are specifically concerned with digital data communication. In this context, 'data' refers to information that is represented by a sequence of zeros and ones, the same sort of data handled by computers. Many communications systems handle analog data; examples are telephone systems, radio and television. Modern instrumentation is almost wholly concerned with the transfer of digital data.

Any communications system requires a transmitter to send information, a receiver to accept it, and a link between the two. Types of link include copper wire, optical fiber, radio and microwave.

Some short-distance links use parallel connections, meaning that several wires are required to carry a signal. This type of connection was, before the advent of USB, mostly confined to devices such as local printers. Virtually all modern data communications use serial links in which the data is transmitted in sequence over a single circuit.

Digital data is sometimes transferred using a system that is primarily designed for analog communication. A modem, for example, works by using a digital data stream to modulate an analog signal that is sent over a telephone line. Another modem demodulates the signal to reproduce the original digital data at the receiving end. The word 'modem' is derived from modulator and demodulator.

There must be mutual agreement on how data is to be encoded, i.e. the receiver must be able to understand what the transmitter is sending. The structure in which devices communicate is known as a protocol.

Over the past decade many standards and protocols have been established, which allow data communications technology to be used more effectively in industry. Designers and users are beginning to realize the tremendous economic and productivity gains possible with the integration of systems that are already in operation.

Protocols are the structure used within a communications system so that, for example, a computer can talk to a printer. Traditionally, developers of software and hardware platforms have developed protocols that only their own products could use. In order to develop more integrated instrumentation and control systems, standardization of these communication protocols was required.
Standards may evolve from the wide use of one manufacturer's protocol (a *de facto* standard) or may be specifically developed by bodies that represent specific industries. Standards allow manufacturers to develop products that will communicate with equipment already in use. For the customer this simplifies the integration of products from different sources.

The industrial communications market is characterized by a lack of standardization. There are, however, a few dominant standards. Modbus has been a *de facto* standard for many years and the tried and tested physical standards such as RS-232 and RS-485 have been widely used. The area that has caused a considerable amount of angst (and dare we say - irritation) amongst vendors and users is the choice of an acceptable Fieldbus, which would tie together instruments to programmable logic controllers and personal computers. This effort has resulted in a few dominant but competing standards such as Profibus, AS-i, DeviceNet and Foundation Fieldbus being used in various areas of industry.

The standard that has created an enormous amount of interest in the past few years is Ethernet. After initially being rejected as being non-deterministic, which means there cannot be guarantee that a critical message being delivered within a defined time, this thorny problem has been solved with the latest standards in Ethernet and the use of switching technology. The other protocol, which fits onto Ethernet extremely well, is TCP/IP. Being derived from the Internet, it is very popular and widely used.

### 1.2 Modern instrumentation and control systems

In an instrumentation and control system, data is acquired by measuring instruments and transmitted to a controller, typically a computer. The controller then transmits data (control signals) to control devices, which act upon a given process.

The integration of systems with each other enables data to be transferred quickly and effectively between different systems in a plant along a data communications link. This eliminates the need for expensive and unwieldy wiring looms and termination points.

Productivity and quality are the principal objectives in the good management of any production activity. Management can be substantially improved by the availability of accurate and timely data. From this, we can surmise that a good instrumentation and control system can facilitate both quality and productivity.

The main purpose of an instrumentation and control system, in an industrial environment, is to provide the following:

**Control of the processes and alarms**

Traditionally, control of processes such as temperature and flow was provided by analog controllers operating on standard 4-20 mA loops. The 4-20 mA standard is used by equipment from a wide variety of suppliers and it is common for equipment from various sources to be mixed in the same control system. Stand-alone controllers and instruments have largely been replaced by integrated systems such as Distributed Control Systems (DCSs), described below.

**Control of sequencing, interlocking and alarms**

Typically, this was provided by relays, timers and other components hardwired into control panels and motor control centers. The sequence control, interlocking and alarm requirements have largely been replaced by PLCs.

**An operator interface for display and control**

Traditionally, process and manufacturing plants were operated from local control panels by several operators, each responsible for a portion of the overall process. Modern control systems tend to use a central control room to monitor the entire plant. The control room is equipped with computer based operator workstations, which gather data from the field instrumentation and use it for graphical display to control processes, monitor alarms, control sequencing, and for interlocking.

**Management information**

Management information was traditionally provided by taking readings from meters, chart recorders, counters and transducers and from samples taken from the production process. This data
is required to monitor the overall performance of a plant or process and to provide the data necessary to manage the process. Data acquisition is now integrated into the overall control system. This eliminates the gathering of information and reduces the time required to correlate and use the information to remove bottlenecks. Good management can achieve substantial productivity gains.

The ability of control equipment to fulfill these requirements has depended on the major advances that have taken place in the fields of integrated electronics, microprocessors and data communications. The four devices that have made the most significant impact on how plants are controlled are:

- Distributed Control Systems (DCSs)
- Programmable Logic Controllers (PLCs)
- SCADA (Supervisory Control and Data Acquisition) systems
- Smart instruments

Distributed Control Systems (DCSs)

A DCS is hardware and software based (digital) process control and data acquisition system. The DCS is based on a data highway and has a modular, distributed, but integrated architecture. Each module performs a specific dedicated task such as the operator interface/analog or loop control/digital control. There is normally an interface unit situated on the data highway allowing easy connection to other devices such as PLCs and supervisory computer devices.

Programmable Logic Controllers (PLCs)

PLCs were developed in the late sixties to replace collections of electromagnetic relays, particularly in the automobile manufacturing industry. They were primarily used for sequence control and interlocking with racks of on/off inputs and outputs, called digital I/O. They are controlled by a central processor using easily written 'ladder logic' type programs. Modern PLCs now include analog and digital I/O modules as well as sophisticated programming capabilities similar to a DCS, e.g. PID loop programming. High speed inter-PLC links are also available, such as 10/100/1000 Mbps Ethernet. A diagram of a typical PLC system is given in Figure 1.1.

---

**Figure 1.1**

*A typical PLC system*
Supervisory Control and Data Acquisition (SCADA) system

This refers to a system comprising a number of Remote Terminal Units (RTUs) collecting field data and connected back to a master station via a communications system. A diagram below gives an example of this.

![Diagram of a typical SCADA system](image)

**Figure 1.2**
*Diagram of a typical SCADA system*

Smart instrumentation systems

In the 1960s, the 4-20 mA analog interface was established as the *de facto* standard for instrumentation technology. As a result, the manufacturers of instrumentation equipment had a standard communication interface on which to base their products. Users had a choice of instruments and sensors from a wide range of suppliers, which could be integrated into their control systems.

With the advent of microprocessors and the development of digital technology, the situation has changed. Most users appreciate the many advantages of digital instruments. These include more information being displayed on a single instrument, local and remote display, reliability, economy, self-tuning and diagnostic capability. There is a gradual shift from analog to digital technology.

There are a number of intelligent digital sensors with digital communications capability for most traditional applications. These include sensors for measuring temperature, pressure, levels, flow,
mass (weight), density and power system parameters. These new intelligent digital sensors are known as 'smart' instruments.

The main features that define a 'smart' instrument are:

- Intelligent, digital sensors
- Digital data communications capability
- Ability to be multi-dropped with other devices

There is also an emerging range of intelligent, communicating, digital devices that could be called 'smart' actuators. Examples of these are devices such as variable speed drives, soft starters, protection relays and switchgear control with digital communication facilities.

Figure 1.3
Graphical representation of data communication

1.3 Open Systems Interconnection (OSI) model

The OSI model, developed by the International Organization for Standardization, has gained widespread industry support. The OSI model reduces every design and communication problem into a number of layers as shown in figure 1.4. A physical interface standard such as RS-232 would fit into the layer 1, while the other layers relate to the protocol software.
Messages or data are generally sent in frames (packets), which are simply a sequence of bytes. The protocol defines the length of the frame. Each frame requires a source address and a destination address so that the system knows where to send it, and the receiver knows where it came from. A packet starts at the top of the protocol stack, the Application layer, and passes down through the other software layers until it reaches the Physical layer. It is then sent over the link. When traveling down the stack, the packet acquires additional header information at each layer. This tells the corresponding layers at the next stack what to do with the packet. At the receiving end, the packet travels up the stack with each piece of header information being stripped off on the way. The Application layer at the receiver only receives the data sent by the Application layer at the transmitter.

The arrows between layers indicate that each layer reads the packet as coming from, or going to, the corresponding layer at the opposite end. This is known as peer-to-peer communication, although the actual packet is transported via Physical link. The middle stack in Fig. 1.4 (representing a router) has only the three lower layers, which is all that is required for the correct transmission of a packet between two devices in this particular case.

The OSI model is useful in providing a universal framework for all communication systems. However, it does not define the actual protocol to be used at each layer. It is anticipated that groups of manufacturers in different areas of industry will collaborate to define software and hardware standards appropriate to their particular industry. Those seeking an overall framework for their specific communications requirements have enthusiastically embraced this OSI model and used it as a basis for their industry specific standards.

1.4 Protocols

As previously mentioned, the OSI model provides a framework within which a specific protocol may be defined. A protocol, in turn, defines a frame format that might be made up of various fields as follows. The first field could be a string of ones and zeros to synchronize the receiver and to indicate the start of the frame (for use by the receiver). The second field could contain the destination address detailing where the message is going. The third field could contain the source address indicating where the message originated. The field in the middle of the message could be the actual data that has to be sent from transmitter to receiver. The final field contains end-of-frame indicators, which can be error detection codes and/or ending flags.
Protocols vary from the very simple (such as ASCII-based protocols) to the very sophisticated (such as TCP/IP), which operate at high speeds transferring megabits of data per second. There is no right or wrong protocol, the choice depends on a particular application.

1.5 Standards

A brief discussion is given below on the most important approaches that are covered in this book. These are the following:

- RS-232 (TIA-232)
- RS-485 (TIA-485)
- Fiber optics
- Modbus
- Modbus Plus
- Data Highway Plus /DH485
- HART
- AS-i
- DeviceNet
- Profibus
- Foundation Fieldbus
- Industrial Ethernet
- TCP/IP
- Radio and wireless communications

RS-232 interface standard

The RS-232 interface standard (officially called TIA-232) was issued in the USA in 1969 to define the electrical and mechanical details of the interface between Data Terminal Equipment (DTE) and Data Communications Equipment (DCE), which employ serial binary data interchange. The current version of the standard refers to DCE as Data Circuit-terminating Equipment.

In serial data communications, the communications system might consist of:

- The DTE, a data sending terminal such as a computer, which is the source of the data (usually a series of characters coded into a suitable digital form)
- The DCE, which acts as a data converter (such as a modem) to convert the signal into a form suitable for the communications link e.g. analog signals for the telephone system
- The communications link itself, for example, a telephone system
- A suitable receiver, such as a modem, also a DCE, which converts the analog signal back to a form suitable for the receiving terminal
- A data receiving terminal, such as a printer, also a DTE, which receives the digital pulses for decoding back into a series of characters

Figure 1.6 illustrates the signal flows across a simple serial data communications link.
The TIA-232 interface standard describes the interface between a terminal (DTE) and a modem (DCE) specifically for the transfer of serial binary digits. It leaves a lot of flexibility to the designers of the hardware and software protocol. With the passage of time, this interface standard has been adapted for use with numerous other types of equipment such as Personal Computers (PCs), printers, programmable controllers, Programmable Logic Controllers (PLCs), instruments and so on.

RS-232 has a number of inherent weaknesses that make it unsuitable for data communications for instrumentation and control in an industrial environment. Consequently, other TIA interface standards have been developed to overcome some of these limitations. The most commonly used among them for instrumentation and control systems are RS-422 (TIA-422) and RS-485 (TIA-485).

**RS-485 interface standard**

RS-485 is a balanced system with the same range as RS-422, but with increased data rates and up to 32 ‘standard’ transmitters and receivers per line. It is very useful for instrumentation and control systems, where several instruments or controllers may be interconnected on the same multipoint network.

A simple diagram of a typical RS–485 system is indicated in figure 1.7.

**Fiber optics**

There are two main approaches possible with fiber optic cables:

- Single mode (monomode) cabling
• Multimode cabling

Figure 1.8  
*Single mode and multimode optic fibers.*

This is widely used throughout industrial communications systems for two main reasons, namely immunity to electrical noise and optical isolation from surges and transients. As a result, fiber is tending to dominate in all new installations that require reasonable levels of traffic.

**Modbus**

This protocol was developed by Modicon (now part of Schneider Electric) for process control systems. This standard only refers to the Data Link and Application layers; any physical transport method can be used. It is a very popular standard with some estimates indicating that over 40% of industrial communications systems use Modbus. It operates as a master-slave protocol with up to 255 slaves.

![Modbus Message Frame](image)

**Figure 1.9**  
*Format of Modbus message frame*

The address field refers to the number of the specific slave device being accessed. The function field indicates the operation that is being performed, for example, read or write of an analog or digital point in the slave device. The data field is the data that is being transferred from the slave device back to the master or from the master to the slave device (a write operation). Finally, the error check field is to ensure that the receiver can confirm the integrity of the message; it could almost be considered to be a unique fingerprint.

**Modbus Plus**

This built on Modbus and incorporated the protocol within a token passing operation. This protocol was generally confined to Modicon PLCs and never really enjoyed support as an open protocol.
Data Highway Plus /DH485

This protocol formed the backbone of the Allen Bradley (now Rockwell Automation) range of programmable logic controllers. It is a protocol defining three layers of the OSI model viz. Physical layer, Data Link layer and Application layer. A diagram of how it is structured is shown here.

![Data Highway Plus protocol structure](image)

There are two addresses (DST and SRC) in this protocol message, indicating destination and source addresses. This is the result of using a token passing system where each station on the network has the ability to be the master for a short period of time.

HART

The Highway Addressable Remote Transducer (HART) protocol is a typical smart instrumentation Fieldbus that can operate in a hybrid 4-20 mA digital fashion. It has become popular as it is compatible with the 4-20mA standard. A typical diagram of how it operates is shown below.

![HART point-to-point communication](image)
This must be one of the most robust standards for simple digital control. It is almost idiot-proof from a wiring point of view with a very simple wiring philosophy. It is a master-slave network, which can achieve transfer rates of up to 167 Kbps where, for example, with 31 slaves and 124 I/O points connected, a 5 mS scan time can be achieved.

DeviceNet

DeviceNet, developed by Allen Bradley (now Rockwell Automation), is a low-level oriented network focusing on the transfer of digital points. It defines all seven OSI layers as indicated below and can support up to 64 nodes with as many as 2048 total devices. The cabling is straightforward and simple and allows power to be carried for the instruments as well.

![DeviceNet and the OSI model](image)

Profibus

Although initially spawned by the German standards association, this standard based on the RS-485 standard (Profibus DP) and the IEC 61158 standard (Profibus PA) for the Physical layer, has become a very popular international standard. A typical configuration is shown in the diagram below.

![Typical architecture of a Profibus system](image)
Profibus uses a combination strategy of token passing and master-slave operation to achieve its communications results. It defines three layers of the OSI model; namely the Physical layer, the Data Link layer and the Application layer. Like many other Field buses, it also has an added 8th layer, the so-called ‘user layer’.

Foundation Fieldbus

Foundation Fieldbus comes as a low-speed version called H1 and a high-speed version called HSE. Three layers of the OSI model (the Physical, Data Link and Application) and an additional 8th layer, the User layer are defined. It is eminently suitable for use with analog parameters where there is a minimum 100-msec update time required on the H1 standard (31.25 Kbps). For the high-speed version (HSE), Fast Ethernet (100 Mbps) is used. The HSE version, albeit different to the H1 version at OSI layers 1 and 2, is otherwise compatible with the H1 standard on the Application layer and the User layer.

Industrial Ethernet

Industrial Ethernet is rapidly growing in importance after initially being dismissed as not being deterministic. One of the main reasons for its success is its simplicity and low cost. Originally, Ethernet used only CSMA/CD (Carrier Sense Multiple Access with Collision Detection) as its media access control method. This is a non-deterministic method, not ideal for process control applications. Although all modern versions of Ethernet (100 Mbps and up) conform with CSMA/CD requirements for the sake of adherence to the IEEE 802.3 standard, they also allow full duplex operation. Most modern Industrial Ethernet systems are 100 Mbps full duplex systems and allow switch ports to be prioritized, resulting in very deterministic behavior. This is far simpler than the token passing method of communications. A typical example of the 100BaseTX topology is given below.

![Figure 1.14
100BaseTX star topology](image)

TCP/IP

Being a child of the Internet, the Transmission Control Protocol (TCP) /Internet Protocol (IP) suite has become very popular for use in conjunction with Ethernet. It defines three layers viz.:

- Process/Application layer
  (equivalent to upper three layers- Session, Presentation and application- in the OSI model)
- Service layer (Host-to-Host) layer
  (equivalent to the Transport layer in the OSI model)
- Internet layer
  (equivalent to the Network layer of the OSI model)

It is a very low cost protocol with wide support due its compatibility with the Internet. Arguably it is an over-kill for some industrial communications applications. However, its low cost and wide support makes it very attractive.

**Radio/microwave communications**

The use of wireless communications in an industrial context commenced with the use of radio modems as indicated in the diagram below where, for example, Modbus could be used over the specific radio modem Data Link layer. The use of the latest Wireless LAN standards such as IEEE 802.11 is making this a reliable and low cost form of communication.

![Radio modem configuration](image)