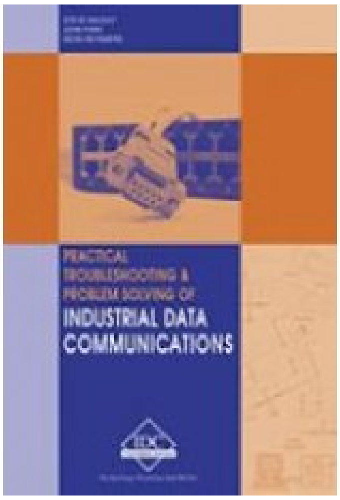
IDC Technologies - Books - 1031 Wellington Street West Perth WA 6005

Phone: +61 8 9321 1702 - Email: books@idc-online.com

ID-E - Practical Troubleshooting & Problem Solving of Industrial Data Communications



Price: $139.94

Ex Tax: $127.22

Short Description

Communications problems range from simple wiring problems to intermittent transfer of protocol messages. The communications system on your plant underpins your entire operation. It is critical that you have the knowledge and tools to quickly identify and fix problems as they occur, to ensure you have a secure system. No compromise is possible here. This manual 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 with each standard/protocol having the following structure: o Quick overview of the standard o Common problems and faults with this standard o Description of tools used Each of the typical faults are then discussed in depth with details on fixing them.

Description

Communications problems range from simple wiring problems to intermittent transfer of protocol messages. The communications system on your plant underpins your entire operation. It is critical that you have the knowledge and tools to quickly identify and fix problems as they occur, to ensure you have a secure system. No compromise is possible here. This manual 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 with each standard/protocol having the following structure: o Quick overview of the standard o Common problems and faults with this standard o Description of tools used Each of the typical faults are then discussed in depth with details on fixing them.

Table of Contents
Download Chapter List

Table of Contents

First Chapter
Practical Troubleshooting and Problem Solving of Industrial Data Communications - Introduction

1

Introduction

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.

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.

Figure 1.4

OSI model representation: two hosts interconnected via a router

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.

Figure 1.5

Basic structure of an information frame

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.

Figure 1.6

A typical 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.

Figure 1.7

Typical two-wire multidrop network for RS-485

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.

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.

Figure 1.10

Data Highway Plus protocol structure

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.

Figure 1.11

HART point-to-point communication.

AS-i

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.

Figure 1.12

DeviceNet and the OSI model

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.

Figure 1.13

Typical architecture of a Profibus system

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 8^{th}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 8^{th} 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

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.

Figure 1.15

Radio modem configuration