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

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

MB-E - Practical Troubleshooting and Problem Solving of Modbus Protocols

Price: $139.94

Ex Tax: $127.22

Short Description

This manual focuses on the main issues of troubleshooting the industrial data communications network of today, enabling you to walk onto your plant or facility to troubleshoot and fix problems as quickly as possible. The focus is on the Modbus suite of protocols and their associated standards.

Description

This manual focuses on the main issues of troubleshooting the industrial data communications network of today, enabling you to walk onto your plant or facility to troubleshoot and fix problems as quickly as possible. The focus is on the Modbus suite of protocols and their associated standards.

Table of Contents

Download Chapter List

First Chapter

Chapter 1: Introduction

1

Introduction

Objectives

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

- Describe the modern instrumentation and control system
- 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 communication systems handle analog data; examples being 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 (the medium) 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 is confined to devices such as local printers. Virtually all modern data communications systems 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 should be mutual agreement on how data is to be encoded, that is, the receiver must be able to understand what the transmitter is sending. The rules governing the communication are known as *protocols.*

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

Historically, developers of software and hardware platforms have developed protocols that can only be used on their own products. In order to develop more integrated instrumentation and control systems, standardization of these communication protocols was required.

Standards may evolve from the widespread use of one manufacturer’s protocol (a *de facto*standard) or may be specifically developed by bodies that represent certain industries. Standards allow manufacturers to develop products that 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 PLCs and PCs. This effort has resulted in a few dominant, but competing standards such as PROFIBUS, DeviceNet and FOUNDATION Fieldbus being used in various areas of the industry.

The standard that has created an enormous amount of interest in the past few years is Ethernet. Initially it was rejected as being non-deterministic, which means there is no guarantee that a critical message is delivered within a defined time. This problem has been solved with the latest standards in Ethernet and the use of switching technology. The other protocol suite that fits onto Ethernet extremely well is TCP/IP. Being developed specifically for 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 the control devices, which act upon a given process.

The integration of systems in a plant allows data to be transferred quickly and effectively between different systems 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, analog controllers operating on standard 4-20 mA loops provide control of parameters such as temperature and flow. 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 (DCS), described below

- **Control of sequencing, interlocking and alarms**

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

- **An operator interface for display and control**

Traditionally, several operators are responsible for a portion of the overall process, operating process and manufacturing plants from various local control panels. 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 that gather data from the field instrumentation and use it for controlling the processes, monitoring alarms, control sequencing and 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 equipments to fulfill these requirements has depended on 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

1.2.5 DCSs

A DCS is a hardware- and software-based (digital) process control and data acquisition system. The DCS is based on a ‘data highway’ (bus) 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.

1.2.6 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 were controlled with 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 Mbps Ethernet. A diagram of a typical PLC system is given in Figure 1.1.

Figure 1.1

A typical PLC system

1.2.7 SCADA

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. Figure 1.2 below gives an example of this.

Figure 1.2

Diagram of a typical SCADA system

1.2.8 Smart Instrumentation systems

During 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, and 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’ Instrumentation (see Figure 1.3).

The main features that define a Smart Instrument (SI) 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 drive, 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 Layer 1, while the other layers relate to the protocol software.

Figure 1.4

Representation of the OSI model

Messages or data are generally sent in packets, which are simply a sequence of bytes. The protocol defines the length of the packet. Each packet 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. The user of the stack, e.g. the Client (residing on, say, a controller) passes the message to the Application layer at the top of the stack. It then proceeds down through the other protocol 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 receiver (e.g. the Server, residing on, say, an RTU) only receives the data sent by the Client.

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 communications medium. The middle stack in Figure 1.4 (representing a router) has only the three lower layers, which is all that is required for the routing of a packet between the 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 the 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 as follows. The first byte(s) can be a string of ones and zeros to synchronize the receiver, or flags and to indicate the start of the frame (for use by the receiver). The second byte could contain the destination address detailing where the message is going. The third byte could contain the source address noting where the message originated. The bytes in the middle of the message could be the actual data that has to be sent from the transmitter to receiver. The final byte(s) are the end-of-frame indicators, which can be error detection codes and/or ending flags (see Figure 1.5).

Figure 1.5

Basic structure of an information frame defined by a protocol

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
- RS-485
- Modbus
- Modbus Plus
- Ethernet, IEEE 802.3
- TCP/IP
- Wireless, IEEE 802.11 and IEEE 802.15

1.5.1 RS-232 interface standard

The RS-232C interface standard was issued by the EIA in 1969 to define the electrical and mechanical details of the interface between Data Terminal Equipment (DTE) and Data Communications Equipment (DCE), which employed serial binary data interchange.

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 (e.g. a modem), which acts as a data converter 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 such a simple serial data communications link.

Figure 1.6

A typical serial data communications link

The original RS-232 interface standard describes the interface between a terminal (DTE) and a modem (DCE) specifically for the transfer of serial binary digits. It left a lot of flexibility to the designers of the hardware and software. With time, the standard has been adapted for use with numerous other types of

equipment such as PCs, printers, programmable controllers, PLCs, instruments and so on. To recognize these additional applications, a subsequent version of the standard, (TIA/EIA-232E) expanded the meaning of the acronym DCE from ‘Data Communications Equipment’ to the more general ‘Data Circuit-terminating Equipment.’ The latest version of the standard is TIA-232F.

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-423, RS-422 and RS-485.

1.5.2 RS-485

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 shown in Figure 1.7.

Figure 1.7

Typical two-wire multi-dropRS-485 network

1.5.4 Modbus

This protocol developed by Modicon (now part of Schneider Electric) is used for process control systems. This standard only refers to the Data Link and Application layers so that any Physical layer implementation can be used. It is a

very popular standard, with some estimates indicating that over 40% of industrial communications systems use Modbus. Modbus Serial operates on a master-slave basis with up to 247 slaves (see Figure 1.9).

Figure 1.9

Format of Modbus Serial message frame

The Unit Identifier field refers to the number of the specific slave device being accessed. The Function Code field indicates the operation that is being requested, for example, read or write of an analog or digital point in the slave device. The Data field is an elaboration on the requested Function Code (for a request from the master) or the actual data being transferred from the slave device back to the master (a write operation). Finally, the Error Check field is to ensure that the receiver can confirm the integrity of the protocol; it could almost be considered to be a unique fingerprint.

1.5.5 Modbus Plus

Unlike Modbus, this is an actual turnkey system based on Modbus, and includes hardware as well. Unlike Modbus, which uses a master/slave Medium Access Control mechanism, Modbus Plus uses Token Passing.

1.5.12 Ethernet

Ethernet (especially the Industrial versions thereof) is rapidly growing in importance after initially being dismissed as not being reliable enough. 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 The IEEE 802.1p standard allows switch ports to be prioritized, resulting in very deterministic behavior.

1.5.13 TCP/IP

Since it forms the basis of the Internet, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite is also becoming popular for industrial applications, especially in conjunction with Ethernet. The suite covers three layers:

- The Process/Application layer

(equivalent to upper three layers in the OSI model)

- The Services or 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 use on the Internet. Arguably it is an overkill for some industrial communications applications. However, its low cost and wide support makes it very attractive.

1.5.14 Radio (or wireless) communications

The use of wireless in the industrial context commenced with the use of radio modems as indicated in Figure 1.15 where, for example, Modbus could be used over the specific radio modem as Physical layer. The use of the latest Wireless LAN standards such as IEEE 802.11b/a/g and IEEE 802.15 ‘Bluetooth’ is making this a reliable and a low-cost form of communication.

Figure 1.15

Radio modem configuration