Practical Modern SCADA Protocols

DNP3, IEC 60870.5 and Related Systems

Gordon Clarke
Deon Reynders

ELSEVIER
Newnes

Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems

Titles in the series

Practical Cleanrooms: Technologies and Facilities (David Conway)

Practical Data Acquisition for Instrumentation and Control Systems (John Park, Steve Mackay)

Practical Data Communications for Instrumentation and Control (John Park, Steve Mackay, Edwin Wright)

Practical Digital Signal Processing for Engineers and Technicians (Edmund Lai)

Practical Electrical Network Automation and Communication Systems (Cobus Strauss)

Practical Embedded Controllers (John Park)

Practical Fiber Optics (David Bailey, Edwin Wright)

Practical Industrial Data Networks: Design, Installation and Troubleshooting (Steve Mackay, Edwin Wright, John Park, Deon Reynders)

Practical Industrial Safety, Risk Assessment and Shutdown Systems for Instrumentation and Control (Dave Macdonald)

Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems (Gordon Clarke, Deon Reynders)

Practical Radio Engineering and Telemetry for Industry (David Bailey)

Practical SCADA for Industry (David Bailey, Edwin Wright)

Practical TCP/IP and Ethernet Networking (Deon Reynders, Edwin Wright)

Practical Variable Speed Drives and Power Electronics (Malcolm Barnes)

Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems

Gordon Clarke CP Eng, BEng, MBA, Western Technical Services, Hobart, Australia

Deon Reynders Pr.Eng, BSc(ElecEng)(Hons), MBA, IDC Technologies, Perth, Australia

Edwin Wright BSc, BE(Hons)(Elec), MIPENZ, IDC Technologies, Perth, Australia

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Newnes is an imprint of Elsevier

Newnes
An imprint of Elsevier
Linacre House, Jordan Hill, Oxford OX2 8DP
200 Wheeler Road, Burlington, MA 01803

First published 2004

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 07506 7995

For information on all Newnes Publications, visit our website at www.newnespress.com

Typeset and Edited by Vivek Mehra, Mumbai, India
(vivekmehra@tatanova.com)

Printed and bound in Great Britain

Contents

Preface

This is a comprehensive book covering the essentials of SCADA communication systems focusing on DNP3 and the other new developments in this area. It commences with a brief review of the fundamentals of SCADA systems hardware, software and the typical communications systems (such as RS-232, RS-485, Ethernet and TCP/IP) that connect the SCADA operator stations together.

A solid review is then done on the DNP3 and IEC 60870-5 protocol where the features, message structure, practical benefits and applications are discussed. The book is intended to be product independent but examples will be taken from existing products to ensure that all aspects of the protocols are covered.

DNP3 is an open protocol developed by Harris Controls Division, Distributed Automation Products in the early 1990s and released to the industry based DNP3 Users Group in November 1993. Much of the material on DNP3 contained within this text is based substantially on the documentation available from the DNP3 Users Group, with interpretation and presentation by the author. The author has tried to identify cases in the text where material has been reproduced directly from user group standards or other sources, and apology is offered if there are any inadvertent oversights in doing this.

This book provides you with the tools to design your next SCADA system more effectively using open protocols and to draw on the latest technologies.

After reading this you should be able to:

- Explain the fundamentals of DNP3 and associated SCADA protocols
- Demonstrate knowledge of the 'nuts and bolts' about selecting DNP3 based systems
- Apply the best current practice for data communications for SCADA systems
- Have a good working knowledge of the DNP3 and IEC 60870-5 protocols
- Troubleshoot simple problems with the DNP3
- Explain how UCA is structured and works
- Provide a working explanation of SCADA protocols and how they should be structured and applied
- Apply 'best practice' decisions on the best and most cost effective use of SCADA open protocols for your company

A basic working knowledge of SCADA and data communications is useful but not essential.

The structure of the book is as follows.

Chapter 1: *Introduction.* An introduction to DNP3 and IEC 60870-5 and other various SCADA protocols that are in use.

Chapter 2: *Fundamentals of SCADA communications.* The structure of SCADA systems and discussion of RTUs, communication architectures, basic standards such as RS-232 and the OSI model with a few remarks on typical SCADA protocols used.

Chapter 3: *Open SCADA protocols DNP3 and IEC 60870*. An introduction to open SCADA protocols.

Chapter 4: *Preview of DNP3*. A preview of DNP3 with the reasons for its remarkable success in the SCADA business.

Chapter 5: *Fundamentals of distributed network protocol.* The fundamentals of DNP3 with a detailed discussion of its underlying structure.

Chapter 6: *Advanced considerations of DNP3.* DNP3 subset definitions and conformance testing, interoperability and polling and communications options.

Chapter 7: *Preview of IEC 60870-5*. Describing how the protocol is referred by the standards and presenting its structure.

Chapter 8: *Fundamentals of IEC 60870-5*. A detailed presentation of the standards, structure and operation.

Chapter 9: *Advanced considerations of IEC 60870-5*. Presents application level functions, interoperability, provisions and network operations.

Chapter 10: *Differences between DNP3 and IEC 60870*. A discussion on the main differences between the DNP3 and the IEC 60870 standard.

Chapter 11: *Intelligent electronic devices (IEDs)*. A description of what an IED is and some issues on installation and commissioning.

Chapter 12: *Ethernet and TCP/IP networks*. The basics of networking, Ethernet and the TCP/IP protocol and their relevance to DNP3.

Chapter 13: *Fieldbus and SCADA communications systems*. The essentials of Fieldbus (such as Profibus and Foundation Fieldbus) and their relevance to DNP3.

Chapter 14: *UCA protocol*. A review of the UCA protocol and its relevance to DNP3.

Chapter 15: *Applications of DNP3 and SCADA protocols*. Discussion of a water industry application.

Chapter 16: *Future developments*. The future developments of DNP3.

Acknowledgements

We would like to acknowledge Mr Ian Wiese, ‘SCADA architect extraordinaire’ and owner of the valuable SCADA website: www.iinet.net.au/~Ianw, and Mr Andrew West, Chair of the DNP Users Group Technical Committee for their valuable advice, encouragement and assistance in preparing this book. They obviously take no responsibility for the contents.

If you have any further interest in these topics we would like to recommend that you subscribe to:

www.lists.iinet.net.au/cgi-bin/mailman/listsinfo/scada
www.dnp.org

1

Introduction

Objectives

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

- Describe the essentials of SCADA systems
- Describe why open systems are important
- List the main advantages of using DNP3 and IEC 60870-5
- Describe the essentials of the layered communications architecture

1.1 Overview

This chapter serves to introduce the different topics that will be covered in the manual and gives an overall flavor of the associated training course. Note that this chapter is in many cases an extract from the material in later chapters where the various issues are covered in far greater detail.

It will be broken down into:

- SCADA systems
- Open systems and communication standards
- DNP3
- Local area networks, Ethernet and TCP/IP
- The UCA protocol

1.2 SCADA systems

SCADA (supervisory control and data acquisition system) refers to the combination of telemetry and data acquisition. SCADA encompasses the collecting of the information via a RTU (remote terminal unit), transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. The required control actions are then conveyed back to the process.

In the early days of data acquisition relay logic was used to control production and plant systems. With the advent of the CPU (as part of the microprocessor) and other electronic

devices, manufacturers incorporated digital electronics into relay logic equipment, creating the PLC or programmable logic controller, which is still one of the most widely used control systems in industry. As needs grew to monitor and control more devices in the plant, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs and/or DCS (distributed control systems) are used as shown below. Although initially RTU was often a dedicated device, PLCs are often used as RTUs these days.

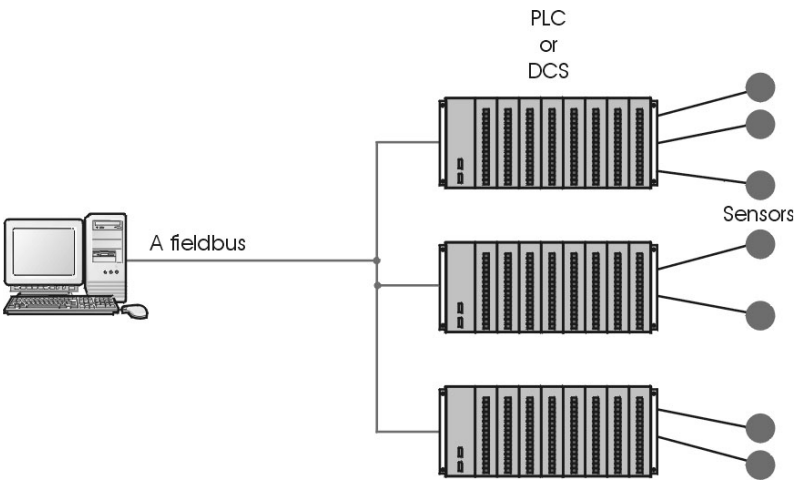

Figure 1.1
PC to PLC or DCS with a fieldbus and sensors

The advantages of the PLC/DCS/SCADA system are:

- The computer can record and store a very large amount of data
- The data can be displayed in any way the user requires
- Thousands of sensors over a wide area can be connected to the system
- The operator can incorporate real data simulations into the system
- Many types of data can be collected from the RTUs
- The data can be viewed from anywhere, not just on site

The disadvantages are:

- The system is more complicated than the sensor to panel type
- Different operating skills are required, such as system analysts and programmer
- With thousands of sensors there is still a lot of wire to deal with
- The operator can see only as far as the PLC

As the requirement for smaller and smarter systems grew, sensors were designed with the intelligence of PLCs and DCSs. These devices are known as IEDs (intelligent electronic devices). The IEDs are connected on a fieldbus such as Profibus, DeviceNet or Foundation Fieldbus to the PC. They include enough intelligence to acquire data, communicate to other devices and hold their part of the overall program. Each of these super smart sensors can have more than one sensor on board. Typically an IED could combine an analog input sensor, analog output, PID control, communication system and program memory in the one device.

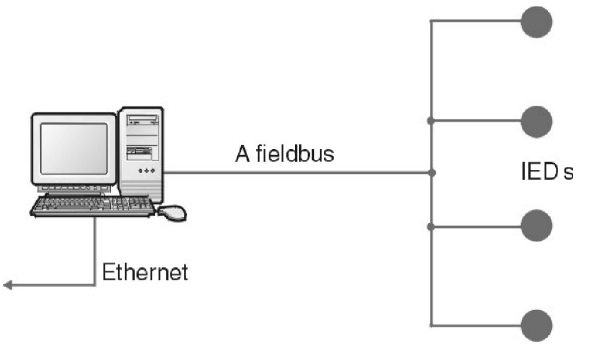

Figure 1.2
PC to IED using a fieldbus

The advantages of the PC to IED fieldbus system are:

- Minimal wiring is needed
- The operator can see down to the sensor level
- The data received from the device can include information such as serial numbers, model numbers, when it was installed and by whom
- All devices are plug and play; so installation and replacement are easy
- Smaller devices mean less physical space for the data acquisition system

The disadvantages of a PC to IED system are:

- The more sophisticated system requires better trained employees
- Sensor prices are higher (but this is offset somewhat by the lack of PLCs)
- The IEDs rely more on the communication system

1.2.1 SCADA hardware

A SCADA system consists of a number of remote terminal units (or RTUs) collecting field data and sending that data back to a master station via a communications system. The master station displays the acquired data and also allows the operator to perform remote control tasks.

The accurate and timely data allows for optimization of the plant operation and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier non-automated systems.

On a more complex SCADA system there are essentially five levels or hierarchies:

- Field level instrumentation and control devices
- Marshalling terminals and RTUs
- Communications system
- The master station(s)
- The commercial information technology (IT) or data processing department computer system

The RTU provides an interface to the field analog and digital sensors situated at each remote site.

The communications system provides the pathway for communications between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station.

1.2.2 SCADA software

SCADA software can be divided into two types, proprietary or open. Companies develop proprietary software to communicate to their hardware. These systems are sold as 'turn key' solutions. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability is the ability to mix different manufacturers' equipment on the same system.

Citect and WonderWare are just two of the open software packages available on the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system. The typical components of a SCADA system are indicated in the diagram below.

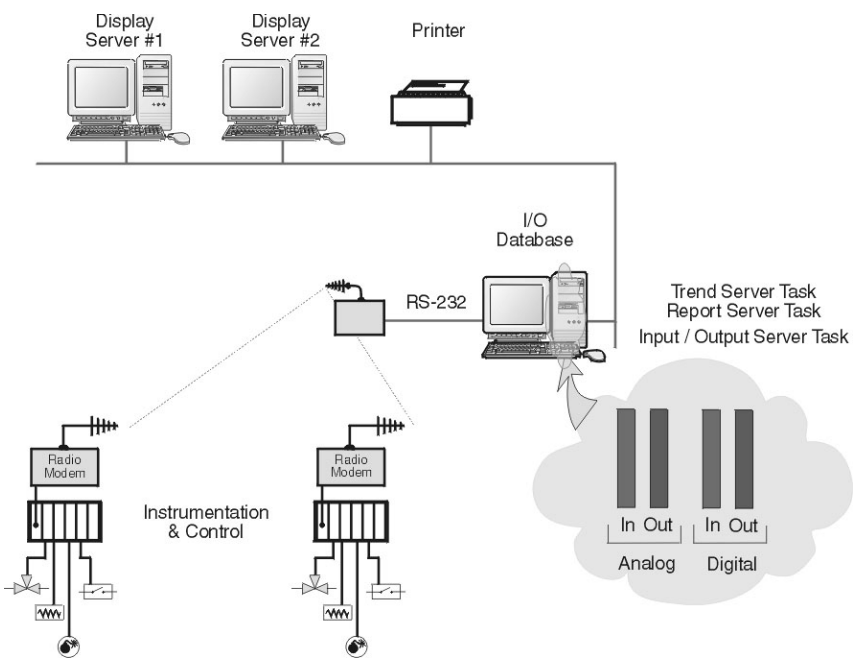

Figure 1.3
Typical SCADA system

1.3 Open systems and communications standards

A communication framework that has had a tremendous impact on the design of communications systems is the open systems interconnection (OSI) model developed by the International Standards Organization (ISO). The objective of the model is to provide a framework for the coordination of standards development and allows both existing and evolving standards activities to be set within that common framework.

The interconnection of two or more devices with digital communication is the first step towards establishing a network. In addition to the hardware requirements, the software problems of communication must also be overcome. Where all the devices on a network are from the same manufacturer, the hardware and software problems are usually easily solved because the system is usually designed within the same guidelines and specifications.

Open systems are those that conform to specifications and guidelines, which are 'open' to all. This allows equipment from any manufacturer, who complies with that standard, to be used interchangeably on the network. The benefits of open systems include multiple vendors and hence wider availability of equipment, lower prices and easier integration with other components.

In 1978 the ISO, faced with the proliferation of closed systems, defined a 'Reference Model for Communication between Open Systems' (ISO 7498), which has become known as the open systems interconnection model, or simply as the OSI model. OSI is essentially a data communications management structure, which breaks data communications down into a manageable hierarchy of seven layers. Each layer has a defined purpose and interfaces with the layers above it and below it. By laying down standards for each layer, some flexibility is allowed so that the system designers can develop protocols for each layer independent of each other. By conforming to the OSI standards, a system is able to communicate with any other compliant system, anywhere in the world.

It should be realized at the outset that the OSI reference model is not a protocol or set of rules for how a protocol should be written but rather an overall framework in which to define protocols. The OSI model framework specifically and clearly defines the functions or services that have to be provided at each of the seven layers (or levels).

The diagram below shows the seven layers of the OSI model.

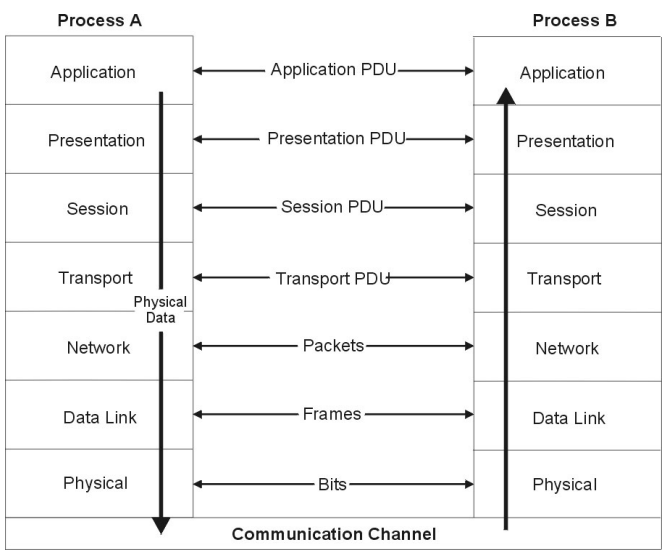

Figure 1.4
Full architecture of OSI model

A brief summary of the seven layers is as follows:

- **Application**
  The provision of network services to the user's application programs. Note: the actual application programs do NOT reside here
- **Presentation**
  Primarily takes care of data representation (including encryption)
- **Session**
  Control of the communications (sessions) between the users
- **Transport**
  The management of the communications between the two end systems
- **Network**
  Primarily responsible for the routing of messages
- **Data link**
  Responsible for assembling and sending a frame of data from one system to another
- **Physical**
  Defines the electrical signals and mechanical connections at the physical level

The figure below gives an idea on how transmission of a message is effected by each layer being encapsulated within the layer below it, before it is sent out on the physical data highway. Similarly once the packet (or more strictly speaking – the frame) is received each layer is then stripped off as the packet is pushed to the top where the message is then extracted.

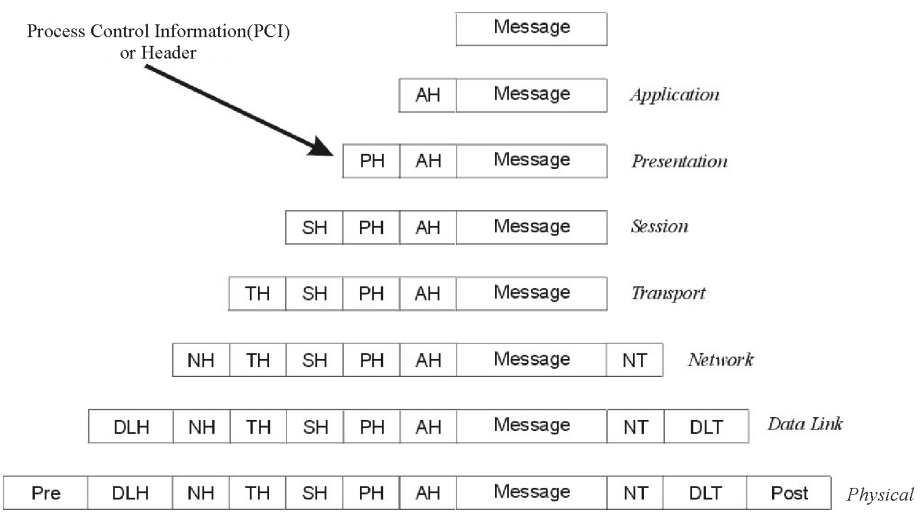

Figure 1.5
OSI message passing

1.4 IEC 60870.5 and DNP3.0

In 1988 the International Electrotechnical Commission (IEC) began publishing a standard entitled 'IEC 870 Telecontrol equipment and systems', of which one part was 'Part 5 Transmission Protocols'. This was developed in a hierarchical manner and published in

a number of sub-paths taking from 1990 to 1995 to completely define an open protocol for SCADA communications. The protocol was defined in terms of the open systems interconnection model (OSI) using a minimum sub-set of the layers; the physical, data link, and application layers. This included detailed definition of message structure at the data link level, and a set of application level data structures so that manufacturers could use the protocol to create systems that would be capable of interoperation.

The IEC standard was subsequently renumbered with the prefix 60 and so the IEC standard for transmission protocols is now IEC 60870.5.

The IEC 60870.5 protocol was defined primarily for the telecommunication of electrical system and control information, and accordingly has data structures that are specifically related to this application. Although it includes general data types that could be used in any SCADA application, the use of IEC 60870 has largely been confined to the electricity industry.

During the same period, which IEC 870 was progressively released, the DNP3 protocol was developed and released in North America.

DNP3 is an open protocol developed by Harris Controls Division, Distributed Automation Products in the early 1990s and released to the industry based DNP3 Users Group in November 1993.

Although the protocol is generally referred to as DNP3 or Distributed Network Protocol Version 3.0, it is the telecommunications standard that defines communications between master stations, remote telemetry units (RTUs) and other intelligent electronic devices (IEDs). It was developed to achieve interoperability among systems in the electric utility, oil & gas, water/waste water and security industries.

From its creation for the electrical distribution industry in America, DNP3 has gained significant acceptance in both geographic and industry terms. DNP3 is supported by a large number of vendors and users in electrical, water infrastructure, and other industries in North America, South America, South Africa, Asia, Australia and New Zealand. In Europe DNP3 competes with IEC 60870-5, which is widely used in that region. However, the IEC protocol is confined to the electrical distribution industry, whereas DNP3 has found wider industry applications in the oil & gas, water/waste water and security industries.

A key feature of the DNP3 protocol is that it is an open protocol standard and it is one that has been adopted by a significant number of equipment manufacturers.

DNP3 has been recognized as having a particularly strong compliance system. In addition to having a comprehensive specification of data objects, DNP3 has a detailed compliance certification system. This is based on having defined implementation sub-sets to which devices must be certified. This provides a means for manufacturers to implement reduced function systems that still provide defined levels of functionality.

Both DNP3 and IEC 60870-5 were designed specifically for SCADA (supervisory control and data acquisition) applications. These involve acquisition of information and sending of control commands between physically separate computer devices. They are designed to transmit relatively small packets of data in a reliable manner with the messages involved arriving in a deterministic sequence. In this respect they are different from more general purpose protocols, such as FTP which is part of TCP/IP, which can send quite large files, but in a way that is generally not as suitable for SCADA control.

Key features of these protocols:

- Open protocols, available for use by any manufacturer or user
- Designed for reliable communication of data and control
- Widely supported by manufacturers of SCADA master systems and software, and of RTUs and IEDs

1.5 Local area networks, Ethernet and TCP/IP

Linking computers and other devices together to share information is nothing new. The technology for local area networks (LANs) was developed in the 1970s by minicomputer manufacturers to link widely separated user terminals to computers. This allowed the sharing of expensive peripheral equipment as well as data that may have previously existed in only one physical location.

SCADA master stations and RTUs are increasingly using components of local area networks (such as Ethernet) and TCP/IP in the communications of the real time data. Although the OSI model is generally preferred, a simplified model called the TCP/IP reference model is used and which consists of the following four layers:

- **Layer 1**
  Network interface layer
  Provides the physical link between devices. Also known as the local network or network access layer
- **Layer 2**
  Internet layer
  Isolates the host from specific networking requirements. The Internet protocol (IP) exists here, but does not guarantee delivery
- **Layer 3**
  Service layer
  Supplies the host service requirements. The transmission control protocol (TCP) resides here, providing reliable end-to-end service
- **Layer 4**
  Application layer
  Provides user-to-host and host-to-user processing and applications

LANs (layer 1) are characterized by high-speed transmission over a restricted geographical area. Thick Ethernet (10Base5), for example, operates at 10 Mb/s over a maximum distance of 500 m before the signals need to be boosted.

While LANs operate where distances are relatively small, wide area networks (WANs) are used to link LANs that are separated by large distances that range from a few tens of meters to thousands of kilometers. WANs normally use the public telecommunication system to provide cost-effective connection between LANs.

The way the nodes are connected to form a network is known as its topology. A logical topology defines how the elements in the network communicate with each other, and how information is transmitted through a network. A physical topology defines the wiring layout for a network. This specifies how the elements in the network are connected to each other electrically.

The concept of internetworking allows one to interconnect many different physical networks and make them function as a coordinated unit. Each network may have its own underlying hardware technology – but these are hidden from the user by the Internet technology. The TCP/IP protocol is used to communicate across any two interconnected networks.

The Internet protocol (IP) is at the core of the TCP/IP suite that resides at the Internet layer. It is primarily responsible for routing packets towards their destination, from router to router. This routing is performed on the basis of the IP addresses, embedded in the header attached to each packet forwarded by IP.

The host-to-host communications layer (also referred to as the service layer, or as the transport layer in terms of the OSI model) is primarily responsible for ensuring end-to-end delivery of packets transmitted by the Internet protocol (IP). This additional reliability is needed to compensate for the lack of reliability in IP.

There are only two relevant protocols residing in the host-to-host communications layer, namely TCP (transmission control protocol) and UDP (user datagram protocol). In addition to this, the host-to-host layer includes the APIs (application programming interfaces) used by programmers to gain access to these protocols from the process/application layer.

TCP is a connection-oriented protocol (discussed later) and is therefore reliable. TCP establishes a connection between two hosts before any data is transmitted. It is therefore possible to verify that all packets are received on the other end and to arrange re-transmission in the case of lost packets. Since TCP provides all of these built-in functions, it involves significant additional overhead in terms of processing time and header size.

UDP is a ‘connectionless’ or non-connection-oriented protocol and does not require a connection to be established between two machines prior to data transmission. It is therefore said to be an ‘unreliable’ protocol – the word ‘unreliable’ is used here as opposed to ‘reliable’ in the case of TCP. As in the case of TCP, it makes use of the underlying IP protocol to deliver its datagrams.

There are a variety of application protocols available with the TCP/IP protocol suite. These are:

- **TELNET**
  This allows a user at one terminal to communicate interactively with an application process on another terminal
- **FTP**
  This allows a user to interact with a remote file system
- **SMTP**
  A network wide mail transfer service
- **SNMP**
  A user can obtain data on the network performance and control a gateway/bridge

To obtain an overall perspective, the following diagram illustrates the interrelation of the various TCP/IP protocol layers with reference to the original four layer ARPA net and the modern OSI-RM.

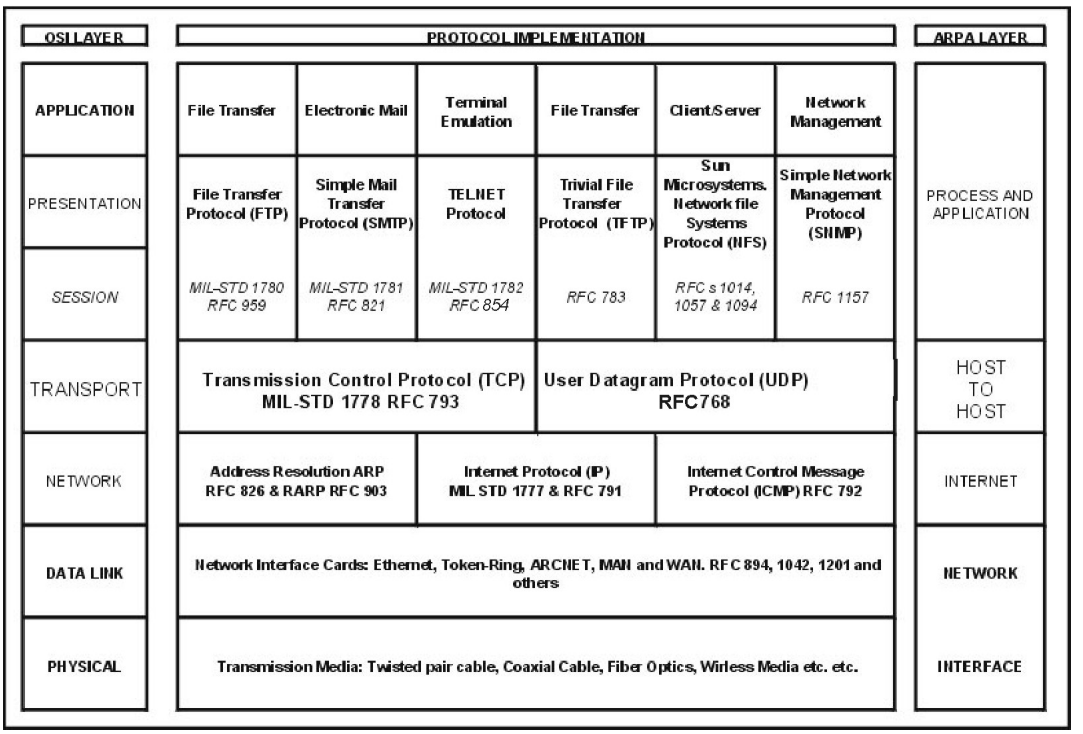

Figure 1.6
TCP/IP and OSI model layers

1.6 UCA protocol

The electric industry, through the Electric Power Research Institute (EPRI) began developing the Utility Communications Architecture (UCATM) in 1988. The result is a complete set of standards allowing UCA compliant monitoring and control devices to inter-operate with utility applications (not just SCADA) in a multi-vendor environment. This protocol is sometimes (incorrectly) regarded as a replacement for DNP3. This is unlikely to happen but both will likely complement each other.

UCA is more than a communications protocol. It is a comprehensive system intended to allow utilities to purchase 'off-the-shelf' UCA compliant devices (such as pole top reclosers, transformers, pumps, valves, flow meters etc) and to have these devices automatically integrated into the SCADA and information technology systems. The industry agreed data relevant to that device will be automatically transferred to SCADA and IT systems identifying themselves as requiring it.

The 'plug and play' concepts, ease of configuration and integration, and predefined data models mean UCA will reduce the costs within the various utility industries, and ensure the success of UCA. UCA is already a fact of life for the electricity industry with many vendors offering UCA compliant products and a large installed base of systems, particularly in the US. Within the water and gas industries it will take a number of years before the data models are agreed and trialled.

Outside the utilities there is little push for UCA, although the concepts are likely to become routine in the SCADA industry.

In 1999, the Institute of Electrical and Electronic Engineers (IEEE) published the UCA Version 2 as an IEEE standard.

EPRI began a successful campaign to have the IEEE oversee UCAs continued development. As a result, the IEEE published UCA Version 2 as an IEEE standard in 1999. UCA-2 addressed the issues that were identified in field testing of the original specification, and it embraced the Internet suite of protocols, which had become widely accepted since the early days of UCA-1.

It is envisaged that DNP3 and UCA will complement each other in the near future.

2

Fundamentals of SCADA communications

Objectives

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

- Describe the essentials of the SCADA hardware and software
- Describe the key components of an RTU
- List the different communication philosophies used
- Describe the RS-232 and RS-485 standards
- List the key components of the Modbus protocol
- Explain the seven different layers of the OSI model

2.1 SCADA systems

2.1.1 Introduction and brief history of SCADA

SCADA (supervisory control and data acquisition) has been around as long as there have been control systems. The first 'SCADA' systems utilized data acquisition by means of panels of meters, lights and strip chart recorders. Supervisory control was exercised by the operator, who manually operated various control knobs. These devices were and still are used to do supervisory control and data acquisition on plants, factories and power generating facilities. The Figure 2.1 shows a sensor to panel system.

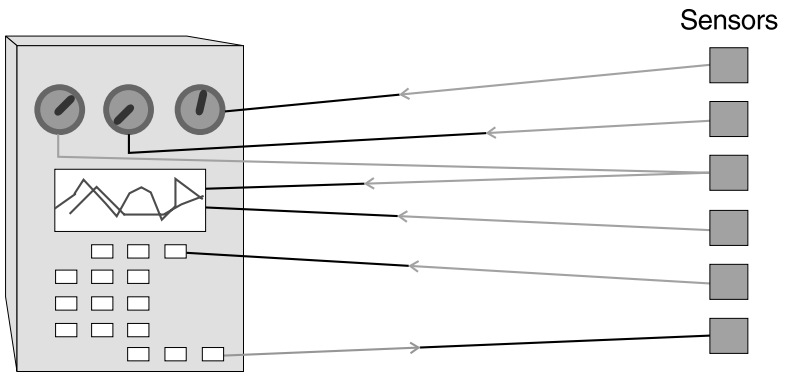

Figure 2.1
Sensors to panel using 4–20 mA or voltage

The sensor to panel type of SCADA system has the following advantages:

- It is simple, no CPUs, RAM, ROM or software programming needed
- The sensors are connected directly to the meters, switches and lights on the panel
- It could be (in most circumstances) easy and cheap to add a simple device like a switch or indicator

This approach has, however, several disadvantages:

- The amount of wire becomes unmanageable after the installation of hundreds of sensors
- The quantity and type of data is minimal and rudimentary
- Installation of additional sensors becomes progressively harder as the system grows
- Re-configuration of the system becomes extremely difficult
- Simulation using real data is not possible
- Storage of data is minimal and difficult to manage
- No off-site monitoring of data or alarms
- Someone has to watch the dials and meters 24 hours a day

2.1.2 Modern SCADA systems

In modern manufacturing and industrial processes, mining industries, public and private utilities, leisure and security industries telemetry is often needed to connect equipment and systems separated by large distances. This can range from a few meters to thousands of kilometers. Telemetry is used to send commands, programs and receive monitoring information from these remote locations.

SCADA refers to the combination of telemetry and data acquisition. SCADA encompasses the collecting of the information, transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. The required control actions are then conveyed back to the process.

In the early days of data acquisition relay logic was used to control production and plant systems. With the advent of the CPU and other electronic devices, manufacturers

incorporated digital electronics into relay logic equipment. The PLC or programmable logic controller is still one of the most widely used control systems in industry. As needs grew to monitor and control more devices in the plant, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs and DCS or (distributed control systems) are used as shown below.

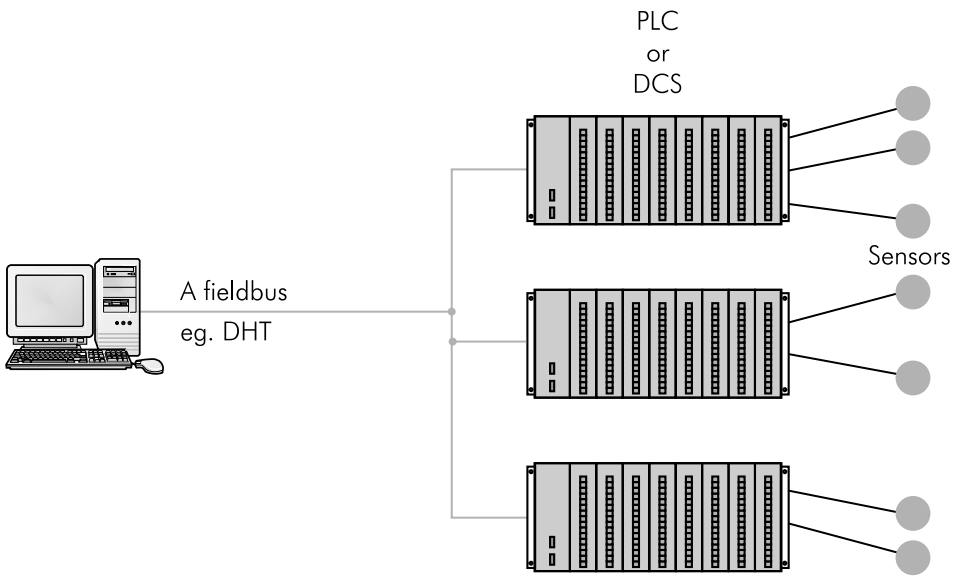

Figure 2.2
PC to PLC or DCS with a plant bus and sensors

The advantages of the PLC/DCS SCADA system are:

- The computer can record and store a very large amount of data
- The data can be displayed in any way the user requires
- Thousands of sensors over a wide area can be connected to the system
- The operator can incorporate real data simulations into the system
- Many types of data can be collected from the RTUs
- The data can be viewed from anywhere, not just on site

The disadvantages are:

- The system is more complicated than the sensor to panel type
- Different operating skills are required, such as system analysts and programmer
- With thousands of sensors there is still a lot of wire to deal with
- The operator can see only as far as the PLC

As the requirement for smaller and smarter systems grew, sensors were designed with the intelligence of PLCs and DCSs. These devices are known as IEDs (intelligent electronic devices). The IEDs are connected on a fieldbus such as Profibus, DeviceNet or Foundation Fieldbus to the PC. They include enough intelligence to acquire data, communicate to other devices and hold their part of the overall program. Each of these super smart sensors can have more than one sensor on board. Typically an IED could combine

an analog input sensor, analog output, PID control, communication system and program memory in the one device.

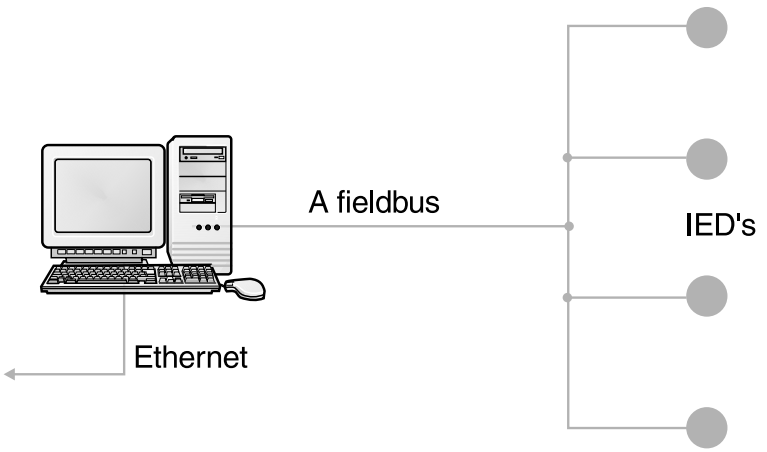

Figure 2.3
PC to IED using a fieldbus

The advantages of the PC to IED fieldbus system are:

- Minimal wiring is needed
- The operator can see down to the sensor level
- The data received from the device can include information like…serial numbers, model numbers, when it was installed and by whom
- All devices are plug and play, so installation and replacement are easy
- Smaller devices means less physical space for the data acquisition system

The disadvantages of a PC to IED system are:

- The more sophisticated system requires better trained employees
- Sensor prices are higher (but this is offset somewhat by the lack of PLCs)
- The IEDs rely more on the communication system.

2.1.3 SCADA hardware

A SCADA system consists of a number of remote terminal units (or RTUs) collecting field data and sending that data back to a master station via a communications system. The master station displays the acquired data and also allows the operator to perform remote control tasks.

The accurate and timely data allows for optimization of the plant operation and process. A further benefit is more efficient, reliable and most importantly, safer operations. This all results in a lower cost of operation compared to earlier non-automated systems.

On a more complex SCADA system there are essentially five levels or hierarchies:

- Field level instrumentation and control devices
- Marshalling terminals and RTUs
- Communications system
- The master station(s)
- The commercial data processing department computer system

The RTU provides an interface to the field analog and digital sensors situated at each remote site.

The communications system provides the pathway for communications between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station.

2.1.4 SCADA software

SCADA software can be divided into two types, proprietary or open. Companies develop proprietary software to communicate to their hardware. These systems are sold as 'turn key' solutions. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability is the ability to mix different manufacturers' equipment on the same system.

Citect and WonderWare are just two of the open software packages available on the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system. The typical components of a SCADA system are indicated in the next diagram.

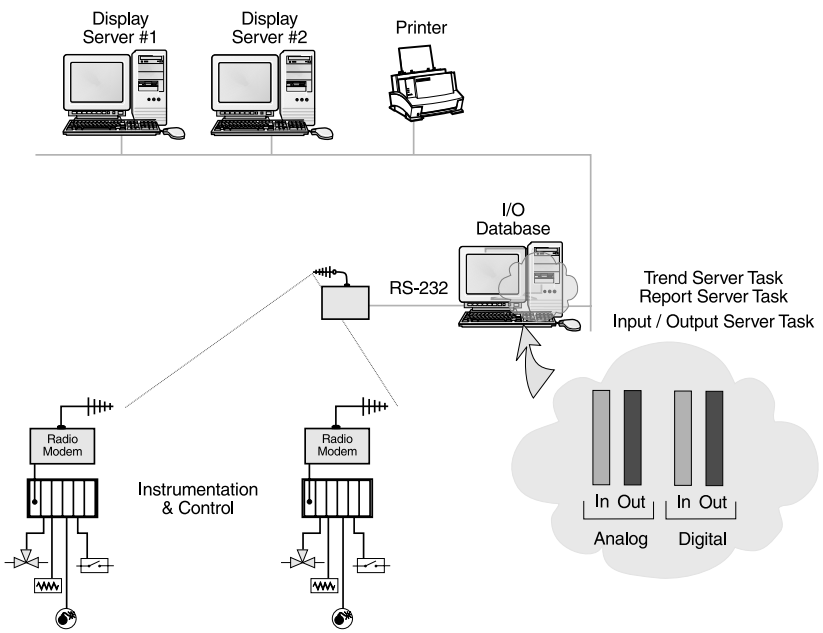

Figure 2.4
Typical SCADA system

Key features of SCADA software include:

- User interfaces
- Graphics displays
- Alarms
- Trends
- RTU (and PLC) interface
- Scalability
- Access to data
- Database
- Networking
- Fault tolerance and redundancy
- Client/server distributed processing

2.1.5 SCADA and local area networks

Local area networks (LAN) are all about sharing information and resources. To enable all the nodes on the SCADA network to share information, they must be connected by some transmission medium. The method of connection is known as the network topology.

Nodes need to share this transmission medium in such a way as to allow all nodes access to the medium without disrupting an established sender.

A LAN is a communications path between computers, file-servers, terminals, workstations and various other intelligent peripheral equipment, which are generally referred to as devices or hosts. A LAN allows access to devices to be shared by several users, with full connectivity between all stations on the network. A LAN is usually owned and administered by a private owner and is located within a localized group of buildings.

Ethernet is the most widely used LAN today because it is cheap and easy to use. Connection of the SCADA network to the LAN allows anyone within the company with the right software and permission, to access the system. Since the data is held in a database the user can be limited to reading the information. Security issues are obviously a concern, but can be addressed.

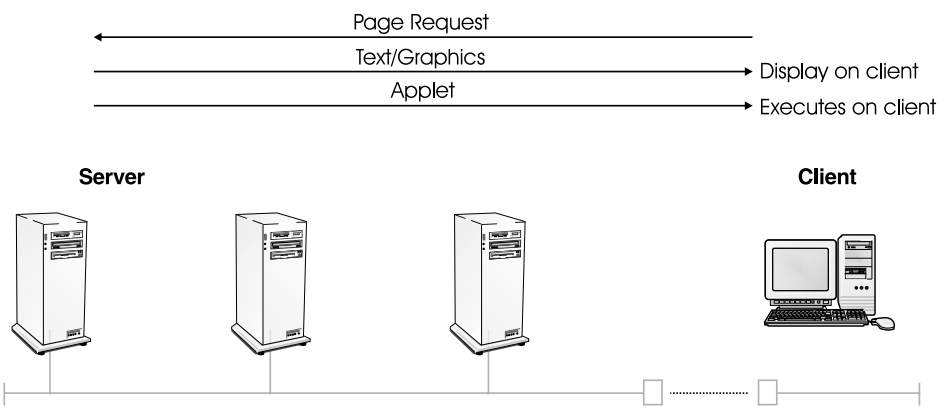

Figure 2.5
Ethernet used to transfer data on a SCADA system