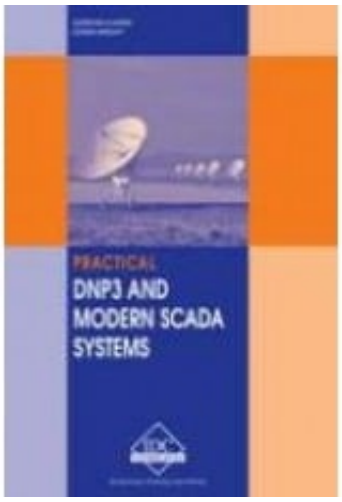
IDC Technologies - Books - 1031 Wellington Street West Perth WA 6005

Phone: +61 8 9321 1702 - Email: publishing@eit.edu.au

DN-E - Practical DNP3 and Modern SCADA Systems



Availability: In Stock

Price: $139.94

Ex Tax: $127.22

Short Description

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

A solid review is then done on the DNP3 protocol where its features, message structure, practical benefits and applications are discussed. The manual is intended to be product independent but examples will be taken from existing products to ensure that all aspects of the DNP3 protocol are covered. The manual provides you with the tools to design your next SCADA system more effectively using DNP3 and draw on the latest technologies.

Description

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

A solid review is then done on the DNP3 protocol where its features, message

structure, practical benefits and applications are discussed. The manual is intended to be product independent but examples will be taken from existing products to ensure that all aspects of the DNP3 protocol are covered. The manual provides you with the tools to design your next SCADA system more effectively using DNP3 and draw on the latest technologies.

Table of Contents
Download Chapter List

Table of Contents

First Chapter
Practical DNP3 and Modern SCADA Systems - Introduction

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 book and give an overall flavour 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 and IEC 61850 Protocols

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 in Figure 1.1. Although initially a RTU was often a dedicated device, PLCs are often used as RTUs these days.

Figure 1.1

PC to PLC or DCS with a field 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 field bus 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 field bus

The advantages of the PC to IED field bus 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 is 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

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 Figure 1.3.

Figure 1.3

Typical SCADA system

1.3 OSI reference model

Faced with the proliferation of closed network systems, the *International*

Organization for Standardization (ISO) defined a ‘Reference Model for Communication between Open Systems’ in 1978. This has become known as the Open Systems Interconnection Reference model, or simply as the OSI model (ISO7498). The OSI model 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.

At the outset it should be realized 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).

Since there must be at least two sites to communicate, each layer also appears to converse with its peer layer at the other end of the communication channel in a virtual (‘logical’) communication. These concepts of isolation of the process of each layer, together with standardized interfaces and peer-to-peer virtual communication, are fundamental to the concepts developed in a layered model such as the OSI model. The OSI layering concept is shown in Figure 1.4.

The actual functions within each layer are provided by entities that are abstract devices, such as programs, functions, or protocols that implement the services for a particular layer on a single machine. A layer may have more than one entity – for example a protocol entity and a management entity.

Entities in adjacent layers interact through the common upper and lower

boundaries by passing physical information through *Service Access Points* (SAPs). A SAP could be compared to a pre-defined ‘post-box’ where one layer would collect data from the previous layer. The relationship between layers, entities, functions and SAPs are shown in Figure 1.4.

Figure 1.4

OSI layering concept

Figure 1.5

Relationship between layers, entities, functions and SAPs

In the OSI model, the entity in the next higher layer is referred to as the N+1 entity and the entity in the next lower layer as N–1. The services available to the higher layers are the result of the services provided by all the lower layers.

The functions and capabilities expected at each layer are specified in the model. However, the model does not prescribe how this functionality should be implemented. The focus in the model is on the ‘interconnection’ and on the information that can be passed over this connection. The OSI model does not concern itself with the internal operations of the systems involved.

When the OSI model was being developed, a number of principles were used to determine exactly how many layers this communication model should encompass. These principles are:

- A layer should be created where a different level of abstraction is required
- Each layer should perform a well-defined function
- The function of each layer should be chosen with thought given to defining internationally standardized protocols
- The layer boundaries should be chosen to minimize the information flow across the boundaries
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy

The use of these principles led to seven layers being defined, each of which has been given a name in accordance with its process purpose. Figure 1.6 shows the seven layers of the OSI model.

Figure 1.6

T*he OSI reference model*

At the transmitter, the user invokes the system by passing data and control information (physically) to the highest layer of the protocol stack. The system then passes the data physically down through the seven layers, adding headers (and possibly trailers), and invoking functions in accordance with the rules of the protocol. At each level, this combined data and header ‘packet’ is termed a protocol data unit or PDU. At the receiving site, the opposite occurs with the headers being stripped from the data as it is passed up through the layers. These header and control messages invoke services and a peer-to-peer logical interaction of entities across the sites.

At this stage, it should be quite clear that there is NO connection or direct communication between the peer layers of the network. Rather, all communication is across the physical layer, or the lowest layer of the stack. Communication is down through the protocol stack on the transmitting stack and up through the stack on the receiving stack. Figure 1.7 shows the full architecture of the OSI model, whilst Figure 1.8 shows the effects of the addition of headers (protocol control information) to the respective PDUs at each layer. The net effect of this extra information is to reduce the overall bandwidth of the communications channel, since some of the available bandwidth is used to pass control information.

Figure 1.7

Full architecture of OSI model

Figure 1.8

OSI message passing

1.3.1 OSI layer services

Briefly, the services provided at each layer of the stack are:

Application (layer 7) – the provision of network services to the user's application programs (clients, servers, etc.). Note: the user's actual application programs do NOT reside here

Presentation (layer 6) – maps the data representations into an external data format that will enable correct interpretation of the information on receipt. The mapping can also possibly include encryption and/or compression of data

Session (layer 5) – control of the communications between the users. This includes the grouping together of messages and the coordination of data transfer between grouped layers. It also effects checkpoints for (transparent) recovery of aborted sessions

Transport (layer 4) – the management of the communications between the two end systems

Network (layer 3) – responsible for the control of the communications network. Functions include routing of data, network addressing, fragmentation of large packets, congestion and flow control

Data Link (layer 2) – responsible for sending a frame of data from one system to another. Attempts to ensure that errors in the received bit stream are not passed up into the rest of the protocol stack. Error correction and detection techniques are used here

Physical (layer 1) – Defines the electrical and mechanical connections at the physical level, or the communication channel itself. Functional responsibilities include modulation, multiplexing and signal generation. Note that the Physical layer defines, but does NOT include the medium. The medium is located below the physical layer and is sometimes referred to as layer 0

1.4 IEC 60870.5 and DNP 3.0

In 1988 the International Electrotechnical Commission (IEC) began publishing a standard entitled ‘IEC 870 Telecontrol equipment and systems’, Part 5 of which described the Transmission Protocols. This was developed in a hierarchical manner and published in a number of sub-parts 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 subset 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 published by Westronic (later renamed Harris Distributed Automation Products) in 1992 and released to the industry based DNP3 Users Group in November 1993.

Although the protocol is officially referred to as Distributed Network Protocol Version 3.0, this has been shortened to DNP3 within this text. DNP3 is a 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 recognised 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 subsets 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 are:

- 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 500m before the signals need to be boosted. Modern industrial LANs use either twisted pair or fiber optic media in a point-to-point architecture connecting the devices directly to an Ethernet switch at either 10 or 100 MBps.

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 use either the public telecommunication system or private networks 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 API's (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 1.9

OSI and ARPA model layers

1.6 UCA and IEC 61850 protocols

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 UCA’s 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.

IEC 61850 has been developed as a Substation Automation Protocol. As such it has essentially overtaken all of UCA 2.0 functionalities and has been extended to incorporate real-time communications protocols to enable Ethernet communication between protection IEDs and RTUs in a substation environment.

It is envisaged that DNP3 and IEC 61850 will complement each other in the near future.