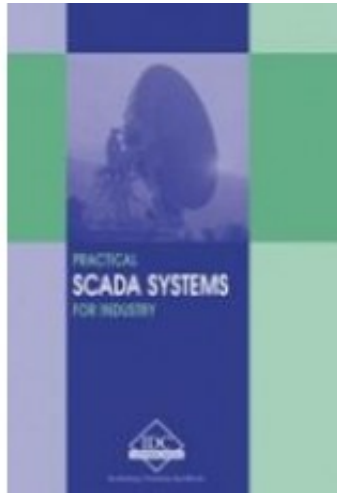


# SX-E - SCADA Systems for Industry



**Price: \$139.94**

**Ex Tax: \$127.22**

## **Short Description**

This manual covers the fundamentals of SCADA systems hardware, software and the communications systems (such as Ethernet and TCP/IP) that connect the SCADA operator stations together. It provides you with the tools to design your next SCADA system more effectively and to draw on the latest technologies.

## **Description**

This manual covers the fundamentals of SCADA systems hardware, software and the communications systems (such as Ethernet and TCP/IP) that connect the SCADA operator stations together. It provides you with the tools to design your next SCADA system more effectively and to draw on the latest technologies.

## **Table of Contents**

Download Chapter List

[Table of Contents](#)

## **First Chapter**

**Chapter 1: Introduction to Wide Area SCADA Systems**

# Introduction to Wide Area SCADA Systems

## 1.1 Brief History of Wide Area SCADA Systems

This Part of the SCADA manual introduces the fundamental concepts and the practical issues needed for wide area SCADA systems. These systems are used by Utilities for monitoring and controlling remote facilities such as pumping stations or electricity substations located across large geographical areas. Particular emphasis has been placed on the practical aspects of SCADA systems with a view to the future. Formulae and details that can be found in specialised manufacturer manuals have been purposely omitted in favour of concepts and definitions.

Part 2 of this SCADA manual addresses the application of SCADA systems for the monitoring and control of manufacturing facilities within a single site. Part 3 of this SCADA manual covers the additional elements that are common to all SCADA systems. These include Alarm Management, Human Management Interface (HMI), Network Security, SCADA Historians, Troubleshooting, Maintenance and Specification issues.

This chapter provides an introduction to the fundamental principles and terminology used in provision of SCADA networks for monitoring and controlling facilities over wide areas.

## 1.2 Fundamental Principles of SCADA Systems

In mining industries, public and private utilities, leisure and security industries there is a need to connect equipment and systems separated by large distances. This can range from tens of meters to thousands of kilometers. Control and monitoring equipment is used to send commands, programs and receive monitoring information from these remote locations.

Telemetry systems are used to measure the status of equipment at a distance. SCADA is an abbreviation of **S**upervisory **C**ontrol and **D**ata **A**cquisition. The *data acquisition* component provides for the collecting of information and transferring it back to the central site, that is the telemetry function. At the central site the data is stored, any necessary analysis is undertaken and the equipment status can be displayed on a number of operator screens. The *supervisory control* allows any

required control actions to be sent back to the remote equipment.

### **1.2.1 SCADA system**

A SCADA (or Supervisory Control and Data Acquisition) System means a system consisting of a number of Remote Terminal Units (or RTUs) collecting field data connected back to a master station via a communications system. The RTU acquires the data from the field devices and undertakes any required local control functions. This enables the RTU to do the local real-time control functions autonomously and it passes the supervisory information to the central control station. The master station displays the acquired data and also allows the operator to perform remote control tasks.

The accurate and timely data (normally real-time) allows for optimization of the operation of the plant 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.

There is a fair degree of confusion between the definition of SCADA systems and process control system. SCADA has the connotation of remote or distant operation. The inevitable question is how far "remote" is - typically this means over a distance such that the distance between the controlling location and the controlled location is such that direct-wire control is impractical (i.e. a communication link is a critical component of the system).

A successful SCADA installation depends on utilizing proven and reliable technology, with adequate and comprehensive training of all personnel in the operation of the system.

There is a history of unsuccessful SCADA systems - contributing factors to these systems including inadequate integration of the various components of the system, unnecessary complexity in the system, unreliable hardware and unproven software. Today hardware reliability is less of a problem; but the increasing software complexity is producing new challenges. It should be noted that many operators judge a SCADA system not only by the smooth performance of the RTUs, communication links and the master station (all falling under the umbrella of SCADA system) but also the field devices (both transducers and control devices). The field devices however fall outside the scope of SCADA in this manual and will not be discussed further. A diagram of a typical SCADA system is given below in Figure 1.1.

## **Figure 1.1**

### *Diagram of a typical SCADA system*

The communications system provides the pathway for communications between the master station and the remote sites. This communication system can be radio, telephone line, microwave and possibly even satellite.

The master station (and submasters) 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, submaster sites gather information from remote sites and act as concentrators relaying back to the master control station.

On a more complex SCADA system there are essentially five levels or hierarchies as illustrated in Figure 1.2:

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

## **Figure 1.2**

### *SCADA System Hierarchies*

## **1.3 Considerations of SCADA system**

Typical considerations when putting a SCADA system together are:

- Overall control requirements
  - Sequence logic
  - Analog loop control
  - Ratio and number of analog to digital points
  - Speed of control and data acquisition
- Master/Operator control stations
  - Type of displays required
  - Historical archiving requirements
- System consideration
  - Reliability/availability
  - Speed of communications/update time/system scan rates
  - System redundancy
  - Expansion capability
  - Application software and modeling

## **1.4 Benefits of SCADA systems**

Obviously a SCADA system's initial cost has to be justified. A few typical reasons for implementing a SCADA system are:

- Improved operation of the plant or process resulting in savings due to optimization of the system.
- Increased productivity of the personnel.
- Improved safety of the system due to better information and improved control.
- Protection of the plant equipment.
- Safeguarding the environment from a failure of the system.
- Improved energy savings due to optimization of the plant.
- Improved and quicker receipt of data so that clients can be invoiced more quickly and accurately.
- Government regulations for safety and metering of gas (for royalties & tax etc).

## **1.5 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 optimisation 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, fibre 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.

## **1.6 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.

### **Figure 1.3**

#### *Typical SCADA system*

*Citect and WonderWare are just two of the many 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 above diagram.*

#### Key Features of SCADA Software

- User Interface
- Graphics Displays
- Alarms
- Trends
- RTU (and PLC) Interface
- Scalability
- Access to Data
- Database
- Networking
- Fault Tolerance and Redundancy
- Client/Server Distributed Processing

## **1.7 Communications Protocols**

An efficient data communications network is an essential component of a SCADA system. The SCADA hardware usually has a serial data interface port such as RS-232, RS-485, etc. for configuration and exchanging data over slower serial links between different sites. Configuration issues for serial links will be discussed in Chapter 5. Alternatively they will use wide area networks (WAN) for data transfer, connected by means of a local area network (LAN) interface – usually Ethernet. LAN and WAN protocols are discussed in Chapter 6.

A communications system uses both hardware and software. The transmission medium connects to a physical interface then software protocols exchange the messages.

The physical interface provides the path for exchanging the data bits. An interface standard defines the electrical and mechanical details of the interface hardware that allow communications equipment from different manufacturers to be interconnected and exchange data bits. The RS-232 and RS-485 serial interface standards will be discussed.

The Protocols describe the rules used by the software to communicate. These define the format of the messages and the rules within which the data is exchanged. The sender and recipient communication.

The MODBUS and Distributed Network Protocol 3.0 (DNP3) protocols will be then be discussed in this part of the manual. MODBUS is a universal protocol typically used between sensors and actuators and the local controller, typically a PLC or RTU. DNP3 is a specialised SCADA protocol widely used by utilities in the electricity, water, wastewater, oil and gas industries. It is able to support report by exception, time-stamping of messages and transfer messages in numerous data formats.

## **1.8 Serial Communications for SCADA Systems**

SCADA systems were developed to monitor and control equipment which could be separated by considerable distances. The communication links between the RTUs and the Master stations were originally provided only by relatively low speed serial systems operating over a pair of wires or a low speed VHF radio system. These communication links are connected to the RS-232 or RS-485 interfaces of the RTU. These systems can provide a cost effective solution where short messages are sent and adequate response times can be achieved using lower data rates. In this chapter we will consider these communications options using data rates up to 115kbps.

Interference and noise are important factors to consider when designing and installing a data communication system with particular considerations required to avoid electrical interference. These issues are discussed in Part 3 of this Manual. Noise can be defined as the random generated undesired signal that corrupts (or interferes with) the original (or desired) signal. This noise can get into the cable or wire in many ways. It is up to the designer to develop a system that will have a minimum of noise from the beginning. Because SCADA systems typically use small signal voltages they are inherently susceptible to noise. The use of twisted pair shielded Cat5E cables is a requirement on most systems. Using good quality cable with correct installation techniques ensures the system



will be as noise free as possible.

Fibre Optic cable is gaining popularity because of its noise immunity and electrical isolation

## **1.9 LAN/WAN Communication for SCADA Systems**

### **Figure 1.4**

*Plant SCADA System using LAN*

When higher speed communication is required for SCADA systems then Local Area Networks are often used, generally using Industrial Ethernet which is described in detail in Part 2, Chapter 5. A typical SCADA system using a Local Area Network within a plant network is shown in Figure 1.4. Communication in the Control Room between the SCADA server(s) and the Operators is most commonly done by Ethernet as shown. Connection between the local controllers (PLC or RTU) within a site can be done with Ethernet, and fiber optic cables are often used for these connections. Fiber optic systems have tremendous advantages for this purpose, including high noise immunity, long distances, lightning immunity and electrical isolation.

Where the local controllers are separated by large distances then the communication may be done over a Wide Area Network (WAN) as illustrated in Figure 1.5 .

### **Figure 1.5**

*Wide Area Networks used to transfer data on a SCADA system*

## **1.10 Communication architectures**

### **1.10.1 Point to point**

This is the simplest configuration where data is exchanged between two stations. One station can be set up as the master and one as the slave. It is possible for both stations to communicate in full duplex mode (transmitting and receiving on two separate frequencies) or simplex with only one frequency (see Figure 1.6).

## **Figure 1.6**

*Point to point (two station)*

### **1.10.2 Multipoint (or multiple stations)**

In this configuration there is generally one master and multiple slaves. Generally data points are efficiently passed between the master and each of the slaves. If two slaves need to transfer data between each other they would do so through the master which would act as arbitrator or moderator.

Alternatively it is possible for all the stations to act in a peer to peer communications manner with each other. This is a more complex arrangement requiring sophisticated protocols to handle collisions between two different stations wanting to transmit at the same time (see Figure 1.7).

## **Figure 1.7**

*Multiple stations*

### **1.10.3 Store and Forward Relay Stations**

This can be a component of the other approaches discussed above where one station retransmits messages onto another station out of the range of the master station.

There is no simultaneous transmission of the message by the store and forward station. It retransmits the message at the same frequency as it received it after the message has been received from the master station (see Figure 1.8).

This approach is slower than a talk through repeater as each message has to be sent twice. The advantages are a considerable savings in mast heights and costs.

## **Figure 1.8**

*Store and forward station*

### **1.10.4 Talk through repeaters**

This is the generally preferred way of increasing the radio systems range. This retransmits a radio signal received simultaneously on another frequency. It is normally situated on a geographically high point.

The repeater receives on one frequency and retransmits on another frequency simultaneously. This means that all the stations it is repeating the signal to must receive and transmit on the opposite frequencies.

It is important that all stations communicate through the talk through repeater. It must be a common link for all stations and thus have a radio mast high enough to access all RTU sites. It is a strategic link in the communication system; failure would wreak havoc with the entire system.

The antenna must receive on one frequency and transmit on a different frequency. This means that the system must be specifically designed for this application with special filters attached to the antennas.

There is still a slight time delay in transmission of data with a repeater. The protocol must be designed with this in mind with sufficient lead time for the repeater's receiver and transmitter to commence operation (see Figure 1.9).

## **Figure 1.9**

*Talk through repeaters*

## 1.11 Communication philosophies

There are two main communication philosophies possible. These are:

- Polled (or Master-slave)
- Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

The one notable method for reducing the amount of data that needs to be transferred from one point to another (and to improve the overall system response times) is to use exception reporting which is discussed later. With radio systems exception reporting is normally associated with the CSMA/CD philosophy but there is no theoretical reason why it cannot be applied to RTUs where there is a significant amount of data to be transferred to the master station.

This discussion concentrates on the radio communications aspects. It is difficult to use token bus or CSMA/CD on cable systems other than in a LAN context (with consequent short distances). For longer distances, cable systems would use a polled philosophy.

### 1.11.1 Polled (or Master-Slave)

This can be used in a point to point or multipoint configuration and is probably the simplest philosophy to use. The master is in total control of the communication system and makes regular (repetitive) requests for data and to transfer data to and from each one of a number of slaves. The slaves do not initiate the transaction but rely on the master. It is essentially a half duplex approach where the slave only responds on a request from the master. If a slave does not respond in a defined time, the master then retries (typically up to three times) and then marks the slave as unserviceable and then tries the next slave node in the sequence. It is possible to retry the unserviceable slave again on the next cycle of polling.

The advantages of this approach are:

- Software is easily written and is reliable due to the simplicity of the philosophy.
- Link failure between the master and a slave node is detected fairly quickly.
- No collisions can occur on the network; hence the data throughput is predictable and constant.

- For heavily loaded systems with each node having constant data transfer requirements this gives a predictable and efficient system.

The disadvantages are:

- Variations in the data transfer requirements of each slave cannot be handled.
- Interrupt type requests from a slave requesting urgent action cannot be handled (as the master may be processing some other slave).
- Systems which are lightly loaded with minimum data changes from a slave are quite inefficient and unnecessarily slow.
- Slaves needing to communicate with each other have to do so through the master with added complexity in the design of the master station.

Two applications of the polled (or master slave) approach are given in the following two implementations.

This is possibly the most commonly used technique and is illustrated in Figure 1.10 below.

## **Figure 1.10**

*Illustration of polling techniques for master station and RTUs*

There are certain considerations to refine the polling scheme beyond that indicated in the diagram above. These are:

If there is no response from a given RTU during a poll, a timeout timer has to be set and three retries (in total) initiated before flagging this station as inactive.

If an RTU is to be treated as a priority station it will be polled at a greater rate than a normal priority station. It is important not to put too many RTUs on the priority list, otherwise the differentiation between high and normal priority becomes meaningless.

An example of a high and normal priority arrangement is given in Figure 1.11.

## **Figure 1.11**

## *High and normal priority arrangement*

A priority message sent from the master station can override the standard polling sequence. In this case the master station complete the poll request for a specific station and then sends out the priority request to a specific station (which was not necessarily next in the polling sequence). It can then wait a predefined time for a response from this RTU or continue with polling a few more stations in the polling sequencer, before requesting a reply from this specific station.

Care should be taken in defining the optimum values for the timers - e.g. a satellite link may have significant develop compared to a leased line communications system.

### **1.11.2 CSMA/CD system (peer to peer)**

*RTU to RTU Communication*—In the situation where on RTU wants to communicate with another, a technique to do this to respond to a poll by the master station with a message with a destination address other than that of the master stations.

The master station will then examine the destination address field of the message received from the RTU and if does not mark its own, retransmit onto the appropriate remote station.

This approach can be used in a master slave network or a group of stations all with equal status. It is similar to the operation of Ethernet discussed in section XXX.

The only attempt to avoid collisions is to listen to the medium before transmitting. The systems rely on recovery methods to handle collision problems. Typically these systems are very effective at low capacity rates; as soon as the traffic rises to over 30% of the channel capacity there is an avalanche collapse of the system and communications becomes unreliable and erratic. The initial experiments with radio transmission between multiple stations (on a peer to peer basis) used CSMA/CD.

This technique is used solely on networks where all nodes have access to the same media (within radio range or on a common cable link). All data is transmitted by the transmitting node first encapsulating the data in a frame with the required destination node address at the head of the frame. All nodes will

read this frame and the node which identifies its address at the head of the frame will then continue reading the data and respond appropriately.

However with this style of operation it is possible for two nodes to try and transmit at the same time, with a resultant collision. In order to minimize the chance of a collision, the source node first listens for a carrier signal (indicating that a frame is being transmitted) before commencing transmission. Unfortunately this does not always work where certain stations (which cannot hear each other) try and transmit back to the station simultaneously.

There is a collision here which only the master can detect (and thus correct). However it is possible that two (or more) transmitting nodes may determine that there is no activity on the system and both start to transmit at the same time. Intuitively, this means that two bits of the same polarity will add together, and the resultant signal seen by the transceivers exceeds that which could come from a single station. A collision is said to occur. The two or more transmitting nodes that were involved in the collision, then wait for a further short random time interval before trying to retransmit again.

It is possible (especially on the standard cable type systems) for the transmitting nodes to see a collision when it occurs (with TTR radios) and to enforce the collision by sending a random bit pattern for a short period (called a jam sequence). This would occur before waiting the random time interval. It ensures that the master site sees the collision.

### **1.11.3 Reporting by Exception**

Exception Reporting (or event reporting) is a technique to reduce the unnecessary transfer of data is to use some form of exception reporting. This approach is popular with the CSMA/CD philosophy but it could also offer a solution for the polled approach where there is a considerable amount of data to transfer from each slave.

The remote station monitors its own inputs for a change of state or data. When there is a change of state, the remote station writes a block of data to the master station when the master station polls the remote.

Typical reasons for using polled report by exception include:

- The communications channel is operating at a low data rate (say 4800

- bps)
- There is substantial data being monitored at the remote stations (say 80 bits or more)
- There are more than 10 RTUs linked to one master station

Each analogue or digital point that has to be reported back to the central master station has a set of exception reporting parameters associated with it. The type of exception reporting depends on the particular environment but could be (see Figure 1.12):

- High and low alarm limits of analogue value
- Percent of change in the full span of the analogue signal
- Minimum and maximum reporting time intervals

## **Figure 1.12**

### *Exception reporting system*

When an analogue value changes in excess of a given parameter or an alarm occurs an exception report is generated.

A digital point generates an exception report when the point changes state (from a '0' to a '1' or vice versa).

The advantages of this approach are quite clearly to minimize unnecessary (repetitive) traffic from the communications system.

The disadvantages are essentially:

- The master station may only detect a link failure after a period of time due to the infrequency of communication.
- The data in the system is not always the latest and may be up to 30 minutes old for example.
- There is effectively a filtering action on analogue values by the master station as small variations do not get reported; only once the analogue values are outside the limits.
- The operator must manually institute a system update to gain the latest data from the RTUs.



#### 1.11.4 Polling Plus CSMA/CD with Exception Reporting

A practical and yet novel approach to combining all the approaches discussed previously is to use the concept of a slot time for each station.

Assume that the architecture is for a master and a number of slaves which need to communicate with the master station. There is no communication between slaves required (except possibly through the master).

The time each station is allowed to transmit is called a slot time. There are two types of slots:

- A slave (or a few slaves) transmitting to a master.
- A master transmitting to a slave.

A slot time is calculated as the sum of the maximums of modem up time (30 milliseconds) plus radio transmit time (100 milliseconds) plus time for protocol message (58.3 milliseconds) plus muting time (25 milliseconds) of transmitter. Typical times are given in brackets after the description.

The master commences operations by polling each slave in turn (and thereafter every 3600 seconds, say). Each slave will synchronize in on the master message and will transmit an acknowledged message. The time slots will alternate for the master transmitting and the master receiving. Hence, on a change in state of a slave node it will transmit the data on the first master receiver time slot. If two remote slaves try to transmit in the same time slot, the message will be corrupted and the slaves will not receive a response from the master. The slaves will then select a random master receiver time slot to attempt a retransmission of the message. If the master continues to get corrupted messages, it may elect to do a complete poll of all the remote slaves (as the CSMA/CD type mechanism is possibly breaking down due to excessive traffic).