1

Background to SCADA

1.1 Introduction and brief history of SCADA

This manual is designed to provide a thorough understanding of the fundamental concepts and the practical issues of SCADA systems. 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 specialized manufacturer manuals have been purposely omitted in favor of concepts and definitions.

This chapter provides an introduction to the fundamental principles and terminology used in the field of SCADA. It is a summary of the main subjects to be covered throughout the manual.

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. The operator manually operating various control knobs exercised supervisory control. These devices were and still are used to do supervisory control and data acquisition on plants, factories and power generating facilities. The following figure shows a sensor to panel system.

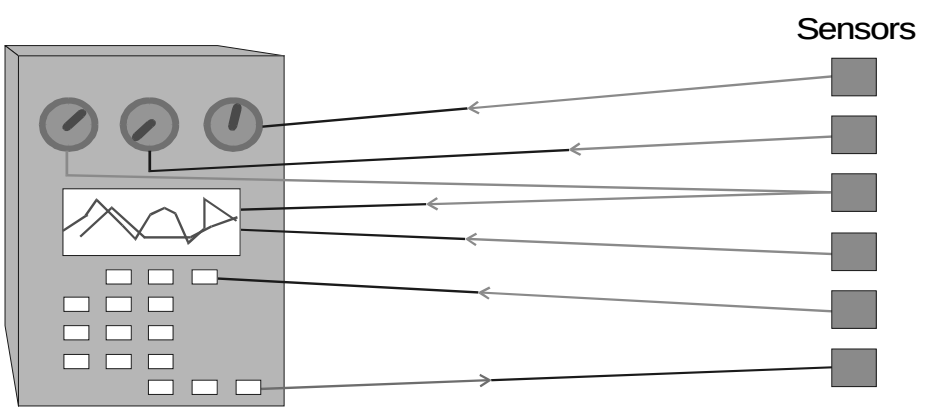

Figure 1.1
Sensors to panel using 4–20 mA or voltage

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

The disadvantages of a direct panel to sensor system are:

- The amount of wire becomes unmanageable after the installation of hundreds of sensors
- The quantity and type of data are 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

1.2 Fundamental principles of 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 receives 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 need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs and DCS (distributed control systems) are used as shown below.

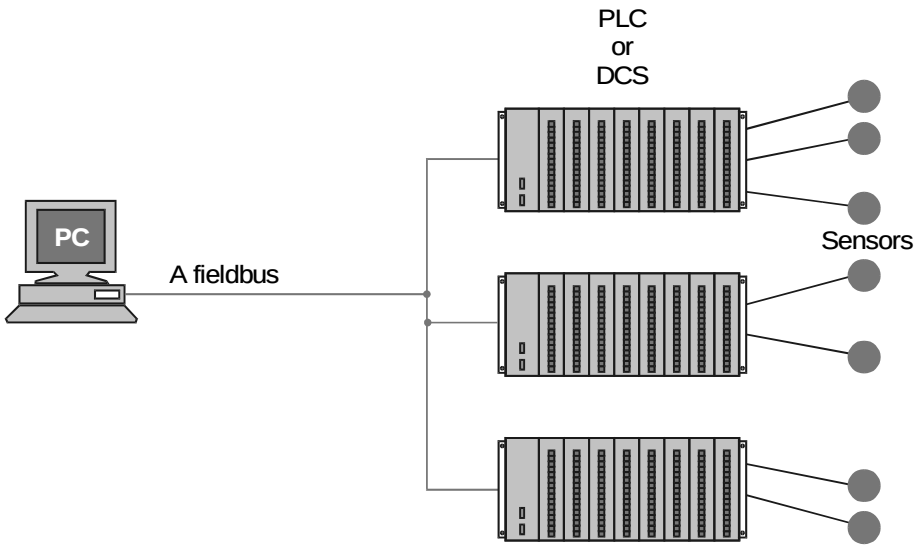

Figure 1.2
PC to PLC or DCS with a fieldbus and sensor

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 one device.

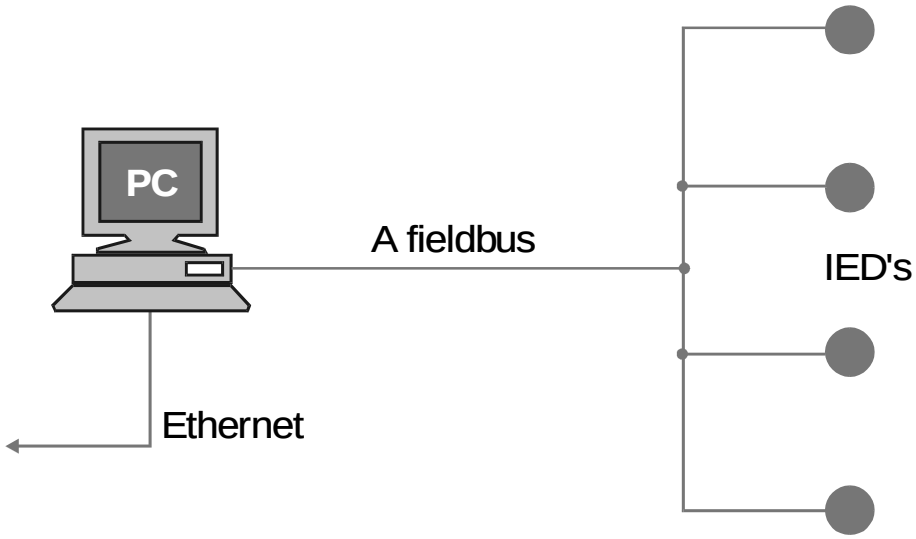

Figure 1.3
PC to IED using a fieldbus

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 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:

- 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

1.3 SCADA hardware

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

The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. This 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 communication 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.

1.4 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 this system 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 in 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.

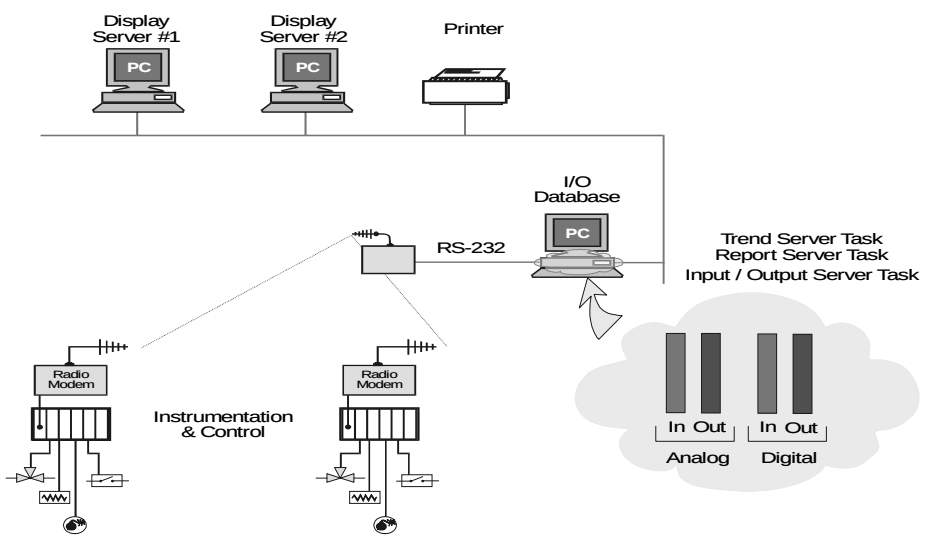

Figure 1.4
Typical SCADA system

Key features of SCADA software are:

- User interface
- Graphics displays
- Alarms
- Trends
- RTU (and PLC) interface
- Scalability

- Access to data
- Database
- Networking
- Fault tolerance and redundancy
- Client/server distributed processing

1.5 Landlines for SCADA

Even with the reduced amount of wire when using a PC to IED system, there is usually a lot of wire in the typical SCADA system. This wire brings its own problems, with the main problem being electrical noise and interference.

Interference and noise are important factors to consider when designing and installing a data communication system, with particular considerations required to avoid electrical interference. 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 voltage they are inherently susceptible to noise.

The use of twisted pair shielded cat5 wire is a requirement on most systems. Using good wire coupled with correct installation techniques ensures the system will be as noise free as possible.

Fiber optic cable is gaining popularity because of its noise immunity. At the moment most installations use glass fibers, but in some industrial areas plastic fibers are increasingly used.

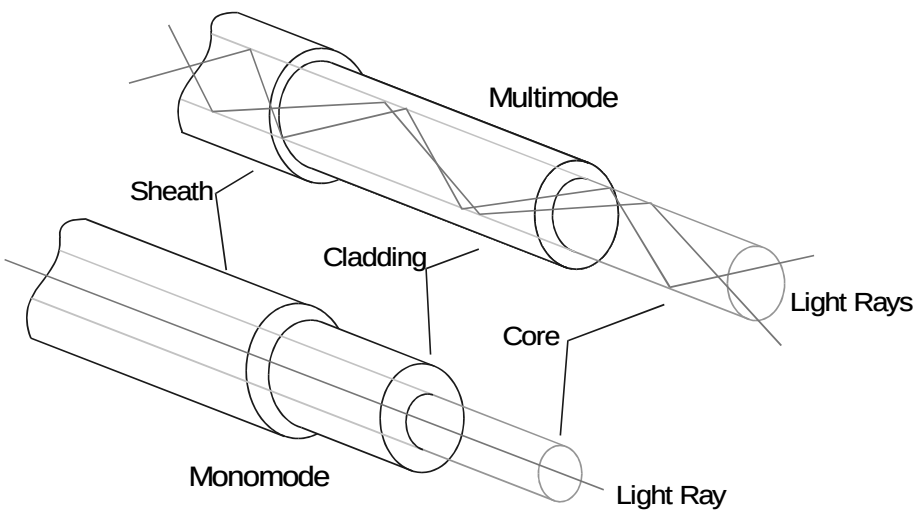

Figure 1.5
Glass fiber optic cables

Future data communications will be divided up between radio, fiber optic and some infrared systems. Wire will be relegated to supplying power and as power requirements of electronics become minimal, even the need for power will be reduced.

1.6 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 communication path between computers, file-servers, terminals, workstations, and various other intelligent peripheral equipments, which are generally referred to as devices or hosts. A LAN allows access for 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 use 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.

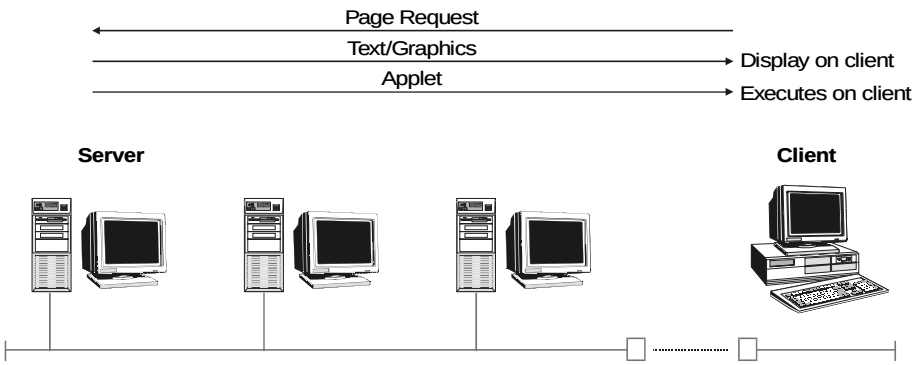

Figure 1.6
Ethernet used to transfer data on a SCADA system

1.7 Modem use in SCADA systems

Figure 1.7
PC to RTU using a modem

Often in SCADA systems the RTU (remote terminal unit (PLC, DCS or IED)) is located at a remote location. This distance can vary from tens of meters to thousands of kilometers. One of the most cost-effective ways of communicating with the RTU over long distances can be by dialup telephone connection. With this system the devices needed are a PC, two dialup modems and the RTU (assuming that the RTU has a built in COM port). The modems are put in the auto-answer mode and the RTU can dial into the PC or the PC can dial the RTU. The software to do this is readily available from RTU manufacturers. The modems can be bought off the shelf at the local computer store.

Line modems are used to connect RTUs to a network over a pair of wires. These systems are usually fairly short (up to 1 kilometer) and use FSK (frequency shift keying) to communicate. Line modems are used to communicate to RTUs when RS-232 or RS-485 communication systems are not practical. The bit rates used in this type of system are usually slow, 1200 to 9600 bps.

1.8 Computer sites and troubleshooting

Computers and RTUs usually run without problems for a long time if left to themselves. Maintenance tasks could include daily, weekly, monthly or annual checks. When maintenance is necessary, the technician or engineer may need to check the following equipment on a regular basis:

- The RTU and component modules
- Analog input modules
- Digital input module
- Interface from RTU to PLC (RS-232/RS-485)
- Privately owned cable
- Switched telephone line
- Analog or digital data links
- The master sites
- The central site
- The operator station and software

Two main rules that are always followed in repair and maintenance of electronic systems are:

- If it is not broken, don’t fix it
- Do no harm

Technicians and engineers have caused more problems, than they started with, by doing stupid things like cleaning the equipment because it was slightly dusty. Or trying to get that one more .01 dB of power out of a radio and blown the amplifier in the process.

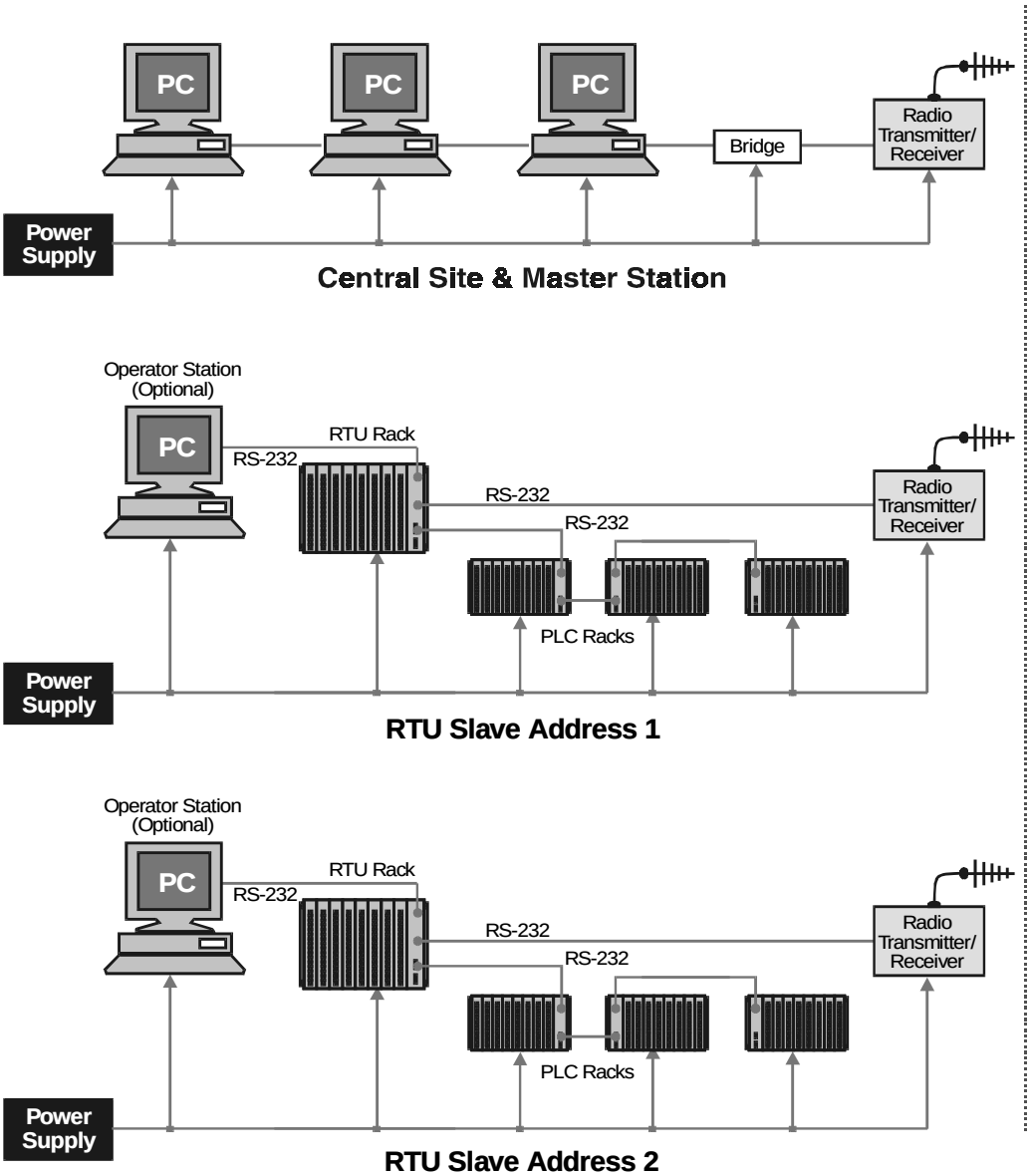

Figure 1.8
Components that could need maintenance in a SCADA system

1.9 System implementation

When first planning and designing a SCADA system, consideration should be given to integrating new SCADA systems into existing communication networks in order to avoid the substantial cost of setting up new infrastructure and communications facilities. This may be carried out through existing LANs, private telephone systems or existing radio systems used for mobile vehicle communications. Careful engineering must be carried out to ensure that overlaying of the SCADA system on to an existing communication network does not degrade or interfere with the existing facilities.

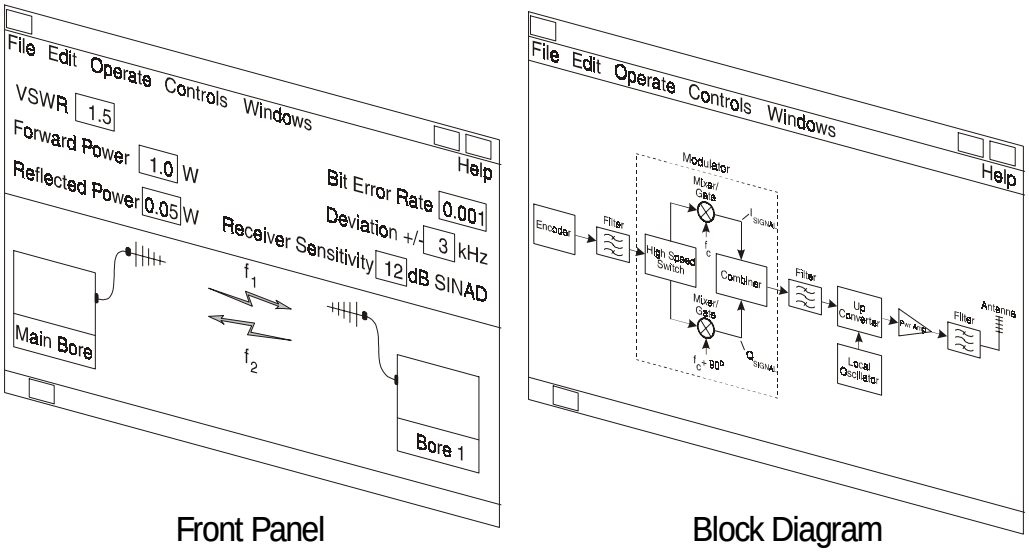

Figure 1.9
Front panel display of SCADA software and its block diagram

If a new system is to be implemented, consideration must be given to the quality of the system to be installed. No company has an endless budget. Weighing up economic considerations against performance and integrity requirements is vital in ensuring a satisfactorily working system at the end of the project. The availability of the communications links and the reliability of the equipment are important considerations when planning performance expectations of systems.

All the aforementioned factors will be discussed in detail in the book. They will then be tied together in a systematic approach to allow the reader to design, specify, install and maintain an effective telemetry and data acquisition system that is suitable for the industrial environment into which it is to be installed.