LECTURE 2: SCADA HARDWARE

2.1 Introduction:
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.

SCADA system essentially has five levels or hierarchies, as listed below
1. Field level instrumentation and control devices: These analog and digital sensors situated at each remote site
2. Marshalling terminals and RTUs: These provides an interface to the field devices
3. Communications system: Communications systems form the backbone of SCADA. The widely used systems are wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection techniques are used for efficient and optimum transfer of data pathway for communications between the master station and the remote sites
4. The master station(s): The master stations gather data from the various RTUs provide an operator interface for display of information and control of the remote sites
5. Information Technology (IT) Applications: The commercial information technology (IT) or data processing department computer system.

2.2 SCADA Hardware Functions
There are many functions of SCADA; some of them are listed below.
   a. Data Collection: collecting of the information via a RTU (remote terminal unit)
   b. Data Transfer: transferring it to the central site
   c. Data Processing: Carrying out any necessary analysis and control
   d. Information Display: Displaying that information on operator screens or displays
   e. Control Actions: Required control actions are then conveyed back to the process

2.3 Remote Terminal Units (RTU)
An RTU (sometimes referred to as a remote telemetry unit) as the title implies, is a standalone data acquisition and control unit, generally microprocessor based, which monitors and controls equipment at some remote location from the central station. Its primary task is to control and acquire data from process equipment at the remote location and to transfer this data back to a central station. It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station.

There is also a facility to be configured locally by some RTU programming unit. Although traditionally the RTU communicates back to some central station, it is also possible to communicate on a peer-to-peer basis with other RTUs. The RTU can also act as a relay station (sometimes referred to as a store and forward station) to another RTU, which may not be accessible from the central station. 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. Small sized RTUs generally have less than 10 to 20 analog and digital signals, medium sized RTUs have 100 digital and 30 to 40 analog inputs. RTUs, having a capacity greater than this can be classified as large.

**RTU Hardware:**
The RTU Hardware consists of a set on inputs, outputs, memory and communications. There are further classified as following

Inputs
- Analog inputs (AI)
- Counter inputs (CI)
- Digital inputs (DI)

Outputs
- Analog outputs (AO)
- Digital outputs (DO)

Memory
- Static and Dynamic Memory
- Control processor and associated memory

Communications and Other equipment
- Communication interface(s)
- Power supply
- RTU rack and enclosure

### 2.3 SCADA RTU

The SCADA RTU is a small rugged computer which provides intelligence in the field, and allows the central SCADA master to communicate with the field instruments. It is a stand alone data acquisition and control unit. Its function is to control process equipment at the remote site, acquire data from the equipment, and transfer the data back to the central SCADA system. There are two basic types of RTU - the "single board RTU" which is compact, and contains all I/O on a single board, and the "modular RTU" which has a separate CPU module, and can have other modules added, normally by plugging into a common "backplane" (a bit like a PC motherboard and plug in peripheral cards).

### 2.4 A typical single board RTU.
The single board RTU normally has fixed I/O eg 16 digital inputs, 8 digital outputs, 8 analogue inputs, and say 4 analogue outputs. It is normally not possible to expand its capability. The modular RTU is designed to be expanded by adding additional modules. Typical modules may be an 8 analog in
module, a 8 digital out module. Some specialised modules such as a GPS time stamp module may be available.

**Hardware functionality in an RTU**
The SCADA RTU is a small ruggedized computer. It has the following hardware features:

**Memory**
- CPU and volatile memory.
- Non volatile memory for storing programs and data.

**Interface**
- I/O interfaces to DI/DO/AI/AO's.
- Real time clock.

**Communications**
- Communications capability either through serial port(s) or sometimes with an on board modem.

**Power Equipment**
- Secure Power supply with battery backup.
- Watchdog timer to ensure the RTU restarts if something fails.

**RTU Software functions**
All RTU's require the following functionality. In many RTU's these may be intermingled and not necessarily identifiable as separate modules. Real time operating system, which can be a specific RTOS, or it may be code that started out life as one big loop scanning the inputs, and monitoring the communications ports. Driver for the communications system, which is the link to the SCADA Master. Device drivers for the I/O system connecting to the field devices. SCADA applications like scanning of inputs, processing and storing of data, responding to requests from the SCADA master over the communications network. Some method to allow the user applications to be configured in the RTU. This may be simple parameter setting, enabling or disabling specific I/O's or it may represent a complete user programming environment. Diagnostics. Some RTU's may have a file system with support for file downloads. This supports user programs, and configuration files.

**2.5 Basic operation**
The RTU will operate scanning its inputs, normally at a fairly fast rate. It may do some processing such as change of state processing, time stamping of changes, and storage of the data awaiting polling from the SCADA master. Some RTU's have the ability to initiate reporting to the SCADA master, although more common is the situation where the SCADA master polls the RTU's asking for changes. The RTU may do some alarm processing. When polled by the SCADA master, the RTU must respond to the request, which may be as simple as "give me all your data", to a complex control function to be executed. RTU's are specialty devices manufactured often by small suppliers in batches of as little as one hundred. They are made for niche markets, and at the smaller end can be subject to intense cost pressures. Therefore not all RTU's support all functionality. Larger RTU's may be capable of processing hundreds of inputs, and even controlling smaller "sub RTU's". These are obviously more expensive. The processing power of an RTU ranges from small 8 bit processors with minimal memory to larger sophisticated RTU's capable of time stamping data to millisecond accuracy.

**RTU Standards**
As indicated RTU's are specialty devices. There has been a lack of standards, especially in the communications area, and generally RTU's from one supplier cannot be mixed with RTU's from another supplier. An industry has grown up developing protocol converters and emulators. Recently
some standards have begun to emerge for RTU's. Some standards are i) DNP3 and IEC870 for communications and ii) IEC1131-3 for programming RTU's.

**Difference between PLC and RTU**
A PLC (programmable logic controller) is a small industrial computer which originally replaced relay logic. It had inputs and outputs similar to those an RTU has. It contained a program which executed a loop, scanning the inputs and taking actions based on these inputs. Originally the PLC had no communications capability, but they began to be used in situations where communications was a desirable feature. Communications modules were developed for PLC's, supporting ethernet (for use in distributed control systems) and the Modbus communications protocol for use over dedicated (wire) links. As time goes on we will see PLC's support more sophisticated communications protocols.

RTU's have always been used in situations where the communications are more difficult, and the RTU's strength was its ability to handle difficult communications. RTU's originally had poor programmability in comparison to PLC's. As time has gone on, the programmability of the RTU has increased.

### 2.6 Features of SCADA

The important features of SCADA are the following:

1. Alarm Handling
2. Trend Curves Patterns
3. Data Access and Retrieval
4. Computer Networking and Processing

**Alarms Handling**
Alarm handling consists essentially of time stamped alarms to 1 millisecond precision. Single network acknowledgment and control of alarms with Sharing and Displaying of Alarms to all clients in chronological order. It performs Dynamic allocation of alarm pages and keeps track of deviation and rate of change monitoring for analog alarms. It has the option of Historical alarm and event logging. It is capable of performing On-line alarm disable and threshold modification with the option of preparing Event-triggered alarms and Alarm-triggered reports

**Trends curves**
Trend curves and patterns consists of Trend zooming and display of data. It performs Export and Archiving of historical trend data with Event based trends for Short and long term trend display. It has the option of On-line change of time-base and retrieval of archived historical trend data.

**Real Time access and archiving and database Management.**
Real time access and data retrieval consists of Direct, real-time access to data by any network user as well as Third-party access to real-time data. It has Network DDE compatibility for read, write and exec with DDE to all I/O device points. ODBC driver support and Direct SQL commands or high level reporting

**Computer Networking and processing**
Computer Networking and processing aspect of supports all compatible networks and protocols. It has Centralized alarm, trend and report processing – data available from anywhere in the network and Dual networks for full LAN redundancy. Open architecture design with Real-time multitasking are important features with Client/server fully supported with Distributed project updates and Concurrent support of multiple display nodes