SUBJECT: POWER SYSTEM OPERATION AND CONTROL

SUBJECT CODE: EE 403

SEMESTER: VII

Module-1 **Computer Control of Power System:**

Introduction: Operating States of Power System, Objectives of Control, Key Concepts of Reliable Operation, Preventive and Emergency Controls, Energy Management Centres.

Supervisory Control and Data acquisition (SCADA): Introduction to SCADA and its Components, Standard SCADA Configurations, Users of Power Systems SCADA, Remote Terminal Unit for Power System SCADA, Common Communication Channels for SCADA in Power Systems, Challenges for Implementation of SCADA.

Introduction:

Operating states of a power system

The Power System needs to be operationally secure, i.e. with minimal probability of blackout and equipment damage. An important component of power system security is the system's ability to withstand the effects of contingencies. A contingency is basically an outage of a generator, transformer and or line, and its effects are monitored with specified security limits. The power system operation is said to be normal when the

power flows and the bus voltages are within acceptable limits despite changes in load or available generation. From this perspective, security is the probability of a power system's operating point remaining in a viable state of operation. System security can be broken down into TWO major functions that are carried out in an operations control centre:

Security assessment and (ii) security control.

The former gives the security level of the system operating state. The latter determines the appropriate security constrained scheduling required to optimally attaining the target security

level. Before going into the static security level of a power system, let us analyze the different operating states of a power system. The states of power system are classified into FIVE states:

1. Normal
2. Alert
3. Emergency
4. Extreme Emergency and
5. Restorative

COPY

Fig.1.1 below depicts these states and the ways in which transitions can occur from one state to another.

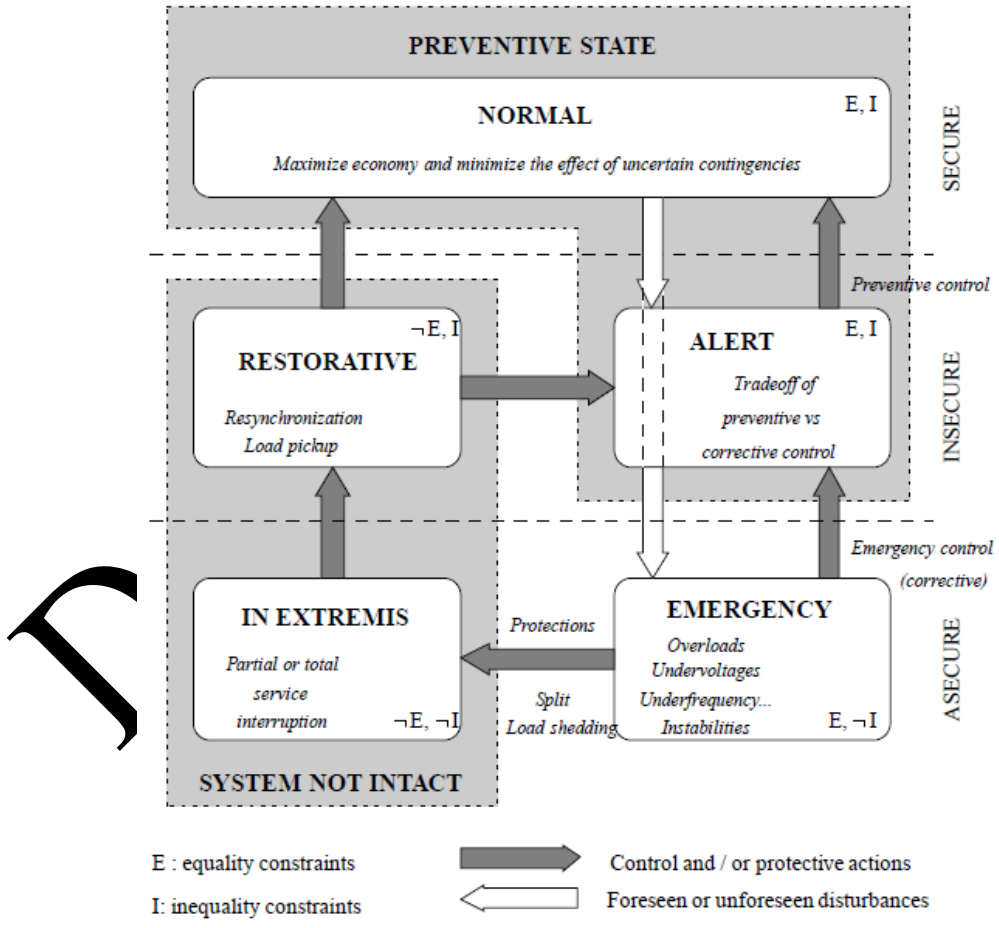

Fig.1.1 Power system operating states

The operation of a power system is usually in a normal state. Voltages and the frequency of the system are within the normal range and no equipment is overloaded in this state. The system can also maintain stability during disturbances considered in the power system planning. The security of the power system is described by Thermal, voltage and stability limits. The system can also withstand any single contingency without violating any of the limits. The system transits into the emergency state if a disturbance occurs when the system is in the alert state. Many system variables are out of normal range or equipment loading exceeds short-term ratings in this state. The system is still complete. Emergency control actions, more powerful than the control actions related to alert state, can restore the system to alert state. The emergency control actions include fault clearing,

excitation control, fast valving, generation tripping, generation run back-up, HVDC modulation, load curtailment, blocking of on-load tap changer of distribution system transformers and rescheduling of line flows at critical lines. The extreme emergency state is a result of the occurrence of an extreme disturbance or action of incorrect of ineffective

emergency control actions. The power system is in a state where cascading outages and shutdown of a major part of power system might happen. The system is in unstable state.

The control actions needed in this state must be really powerful. Usually load shedding of the most unimportant loads and separation of the system into small independent parts are required.

DO NOT COPY

Objective of the control

The objective of the control strategy is to generate and distribute power in an interconnected system as economically and reliably as possible while maintaining the frequency and voltage within permissible limits.

Changes in real power mainly affect the system frequency. Reactive Power however, is immune to changes in frequency and mainly depends on voltage changes. Thus real and reactive power is

controlled separately. The Load Frequency Loop (LFC) controls the real power and frequency and the automatic voltage regulator (AVR) controls the reactive power and voltage magnitude.

Today, in modern energy control centers the methods developed for control of individual generations, and eventually control of large interconnections are of critical importance. Modern Energy Control Centers (ECC) are equipped with on-line computers performing all signal processing through the remote acquisition systems known as supervisory control and data acquisition (SCADA) systems.

Key Concepts of Reliable Operation

There are a number of reasons why reliability is an important product attribute, including:

Reputation: A company's reputation is very closely related to the reliability of its products. The more reliable a product is, the more likely the company is to have a favourable reputation.

Customer satisfaction: While a reliable product may not dramatically affect customer satisfaction in a positive manner, an unreliable product will negatively affect customer satisfaction severely. Thus high reliability is a mandatory requirement for customer satisfaction.

Warranty costs: If a product fails to perform its function within the warranty period, not only the replacement and repair costs will negatively affect profits, there may be an unwanted negative publicity. Introducing reliability analysis is an important step in taking corrective action, ultimately leading to a product that is more reliable.

Repeat business: A concerted effort towards improved reliability shows existing customers that a manufacturer is serious about its product and committed to customer satisfaction. This type of attitude has a positive impact on future business.

Cost analysis: Manufacturers may take reliability data and combine it with other cost information to illustrate the cost-effectiveness of their products. This life cycle cost analysis can prove that although the initial cost of a product might be higher, the overall lifetime cost is lower than that of a competitor's because their product requires fewer repairs or less maintenance.

DO NOT COPY

Customer requirements: Many customers in today's market demand that their suppliers have an effective reliability program. These customers are conscious of the benefits of reliability analysis from their own experiences.

Competitive advantage: Many companies will publish their predicted reliability numbers to help gain an advantage over their competitors who either do not publish their numbers or have lower numbers.

Preventive and Emergency Controls

Power system security is more and more in conflict with economic and environmental requirements. Security control aims at making decisions in different time horizons so as to prevent the system from undesired situations, and in particular to avoid large catastrophic outages. Traditionally, security control has been divided in two main categories: preventive and emergency control. In preventive security control, the objective is to prepare the system when it is still in normal operation, so as to make it able to face future (uncertain) events in a satisfactory way. In emergency control, the disturbing events have already occurred, and thus the objective becomes to control the dynamics of the system in such a way that consequences are minimized. Preventive and emergency controls differ in many respects, among which we list the following

types of control actions: generation rescheduling, network switching reactive compensation, sometimes load curtailment for preventive control; direct or indirect load shedding, generation shedding, shunt capacitor or reactor switching, network splitting for emergency control.

Uncertainty: in preventive control, the state of the system is well known but disturbances are uncertain; in emergency control, the disturbance is certain, but the state of the system is often only partially known; in both cases, dynamic behavior is uncertain.

Open versus closed loop: preventive control is generally of the open loop feed-forward type; emergency control may be closed loop, and hence more robust with respect to uncertainties.

In the past, many utilities have relied on preventive control in order to maintain system security at an acceptable level. In other words, while there are many emergency control schemes installed

DO NOT COPY

in reality, the objective has been to prevent these schemes as much as possible from operating, by imposing rather high objectives to preventive security control. As to any rule, there are exceptions: for example, controlled generation shedding has been used extensively in Northern America to handle transient stability problems; in the same way, corrective control has been used in many systems as an alternative to preventive control in the context of thermal overload mitigation. Nowadays, where the pressure is to increase trading and competition in the power system field, preventive security control is being considered as an impediment to competition; in turn, this breeds strong incentives to resort less on preventive control and more often on emergency control. The objective of this paper is essentially twofold: first, to concentrate on transient stability control, both preventive and emergency, and describe a general methodology able to realize convenient tradeoffs between these two aspects; second, to suggest means of integrated security control, coordinating various types of security (steady-state, voltage and transient stability).

The general methodology used to design transient stability control techniques relies on the transient stability method called SIME. In what follows, we first describe the fundamentals of SIME, and then concentrate on the advocated control techniques.

Energy Management Centres

The energy control center (ECC) has traditionally been the decision-center for the electric transmission and generation interconnected system. The ECC provides the functions necessary for monitoring and coordinating the minute-by-minute physical and economic operation of the power system. Maintaining integrity and economy of an interconnected power system requires significant coordinated decision-making. So one of the primary functions of the ECC is to monitor and regulate the physical operation of the interconnected grid. Most areas today have a two-level hierarchy of ECCs with the Independent System Operator (ISO) performing the high-level decision making and the transmission owner ECC performing the lower-level decision-making.

ECC Components

DO NOT COPY

The system control function traditionally used in electric utility operation consists of three main integrated subsystems: the energy management system (EMS), the supervisory control and data acquisition (SCADA), and the communications interconnecting the EMS and the SCADA (which is often thought of as part of the SCADA itself). The rest of the figure indicates the EMS. We will describe each one in the following subsections We distinguish EMS from distribution management systems (DMS). Both utilize their own SCADA, but for different functions. Whereas EMS/SCADA serves the high voltage bulk transmission system from the ECC, the DMS/SCADA serves the low voltage, distribution system from a distribution dispatch center. We are addressing in these notes the
EMS/SCADA

Supervisory Control and Data acquisition (SCADA):

Introduction

One of key processes of SCADA is the ability to monitor an entire system in real time. This is facilitated by data acquisitions including meter reading, checking statuses of sensors, etc that are communicated at regular intervals depending on the system.

A well planned and implemented SCADA system not only helps utilities deliver power reliably and safely to their customers but it also helps to lower the costs and achieve higher customer satisfaction and retention.

SCADA – Why do we need it?

If we did not have SCADA, we would have very inefficient use of human resources and this would cost us. In today's restructured environment SCADA is critical in handling the volume of data needed in a timely fashion Service restoration would involve travel time and would be significantly higher.

Basic Components of SCADA System

DO NOT COPY

Fig.1.2 shows the basic Components of SCADA System.A basic SCADA system consists of following components:

1. Human Machine Interface
2. Supervisory System
3. Remote Terminal Units
4. Programmable Logic Controllers (PLCs)
5. Communication Infrastructure
6. SCADA Programming

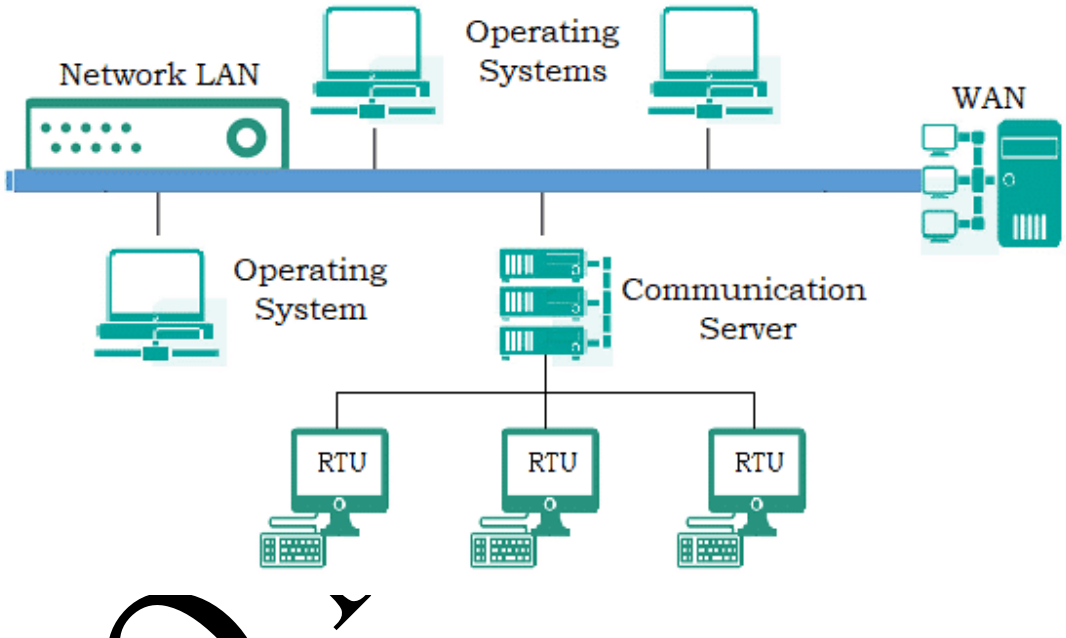

Fig.1.2 Basic Components of SCADA System

1. Human Machine Interface

It is an I/O device that allows a human operator to control the process data. This is achieved by linking SCADA's databases and software programs for providing management information like detailed schematics, scheduled maintenance, data diagnostics and logistic information. The operating personnel can also see the graphical representation of data.

2. Supervisory System

This system acts as a communication server between the HMI software in control room workstations and its equipment like PLCs, RTUs, sensors etc.

Smaller Supervisory Control and Data Acquisition systems have only a single PC that serves as a supervisory or master system. Larger Supervisory Control and Data Acquisition systems have multiple servers, sites for disaster recovery and distributed software applications. The servers are configured as dual-redundant or hot-standby formation for continuously monitoring server failure.

3. **Remote Terminal Units**

This system contains physical objects that are interfaced with Remote Terminal Units (RTUs). These electronic devices are controlled by microprocessors and are used for transmitting recorded data to the supervisory systems. They also receive data from the master system in order to control the connected objects.

They are also called as Remote Telemetry Units.

4. **Programmable Logic Controllers**

PLCs find their use in the Supervisory Control and Data Acquisition system through sensors. They are attached to the sensors in order to convert the sensor output signal into digital data.

They are preferred over RTUs because of their configuration, flexibility, affordability and versatility.

5. **Communication Infrastructure**

Generally, a combination of direct wired connection and radio is used in Supervisory Control and Data Acquisition systems. However, SDH/ SONET can also be used for larger systems like railways and power stations.

Among the compact SCADA protocols, few recognized and standardized protocols deliver information only when the RTUs are polled by the supervisory station.

6. **SCADA Programming**

DO NOT COPY

SCADA programming in HMI or master station is used for creating diagrams and maps that provide vital information during process or event failure. Most of the commercial Supervisory Control and Data Acquisition systems use standardized interfaces in programming. C language or derived programming language is generally used for such programming.

User of SCADA in Power System

As the power system deals with power generation, transmission and distribution sectors, monitoring is the main aspect in all these areas. Thus the SCADA implementation of power system improves the overall efficiency of the system for optimizing, supervising and controlling the generation and transmission systems. SCADA function in the power system network provides greater system reliability and stability for integrated grid operation.

SCADA for Power Generating Stations

With the use of Programmable Logic Controllers (PLC) hardware and powerful bus communication links along with SCADA software and hardware's in power generating stations, delivering an optimal solution for each and every process operation is flexible with advanced control structures. The below figure shows the SCADA structure in power generation where it supervises several operations including protection, controlling and monitoring. The functions of SCADA in power generation include

- Continuous monitoring of Speed and Frequency
- Geographical monitoring of coal delivery and water treatment processes
- Supervising the status of circuit breakers, protective relays and other safety related operations
- Generation operations planning
- Active and reactive power control
- Turbine protection
- Load scheduling
- Historical data processing of all generation related parameters

DO NOT COPY

SCADA for Power Distribution System

Fig.1.3 shows the SCADA for Power Distribution SystemPower distribution system deals with transmission of electric power from generating station to the loads with the use of transmission and distribution substations. Most of the power distribution or utility companies rely on manual labor to perform the distribution tasks like interrupting the power to loads, all the parameter hourly checking, fault diagnosis, etc. The implementing SCADA to the power distribution not only reduces the manual labor operation and its cost but facilitates automatic smooth operations with minimizing disruptions.

SCADA Application for Remote Industrial Plant

The main goal of this project is to process and control the working of industrial machinery by using SCADA.

DO NOT COPY

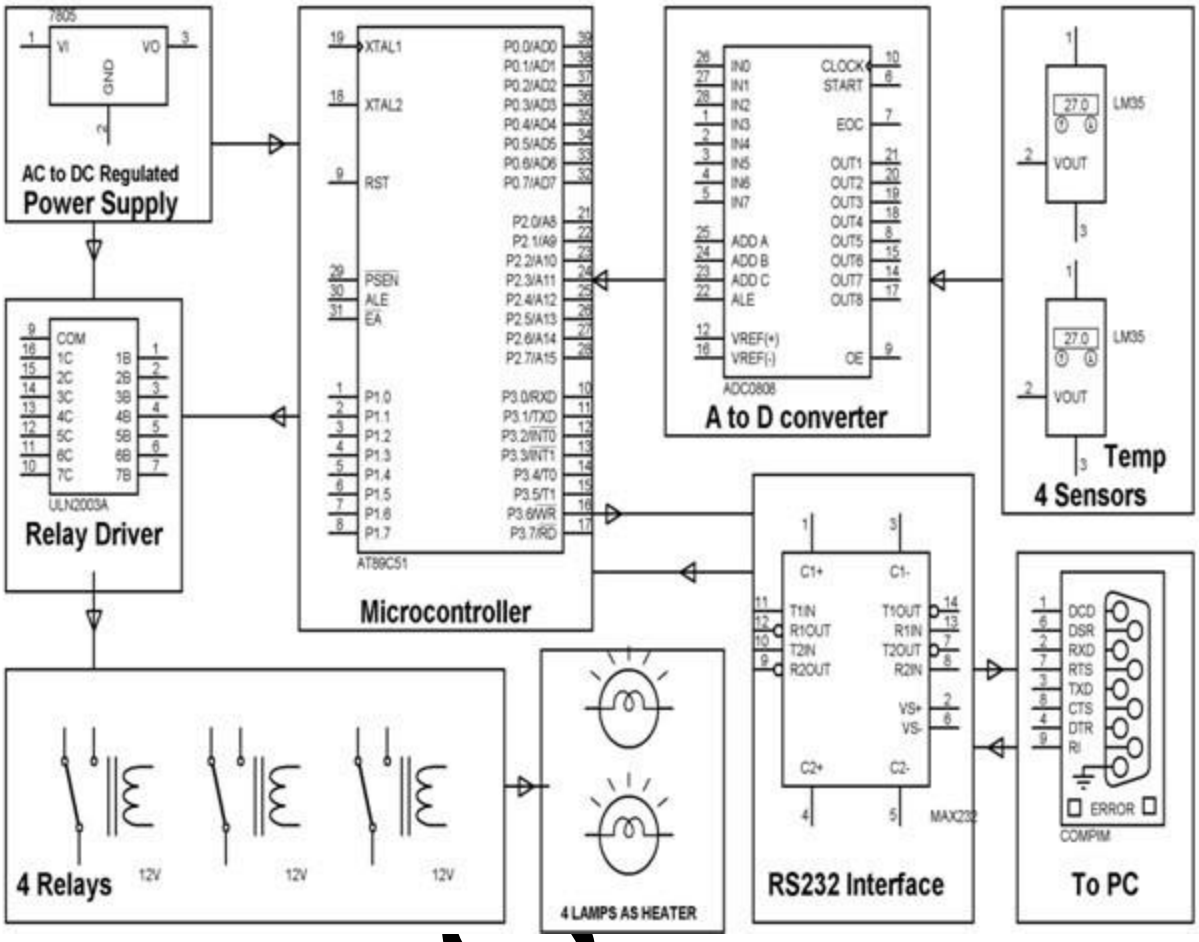

Fig.1.3 SCADA for Power Distribution System

DO NOT

SCADA Application Diagram for Remote Industrial Plant

The multiple mechanisms in the industries are unable to control manually. So, for controlling these mechanisms efficiently, it is necessary to adopt a technology namely SCADA

In this project, temperature sensors are used to collect temperature constantly and to send it to the microcontroller which is interfaced with the PC.If the temperature exceeds the predefined temperature limits, then the microcontroller sends a signal to the relay driver which in turn activates the relay to turn the lamps on or off. If this system fails, then an AV alarm generates from the PC using high-limit and low-limit features.

Hence, the mechanisms of industries can be controlled more efficiently and safely by using SCADA, which is more economical and time saving technology.

Wireless SCADA

The main intention of this project is to process and control the working of industrial machinery by using SCADA wirelessly.

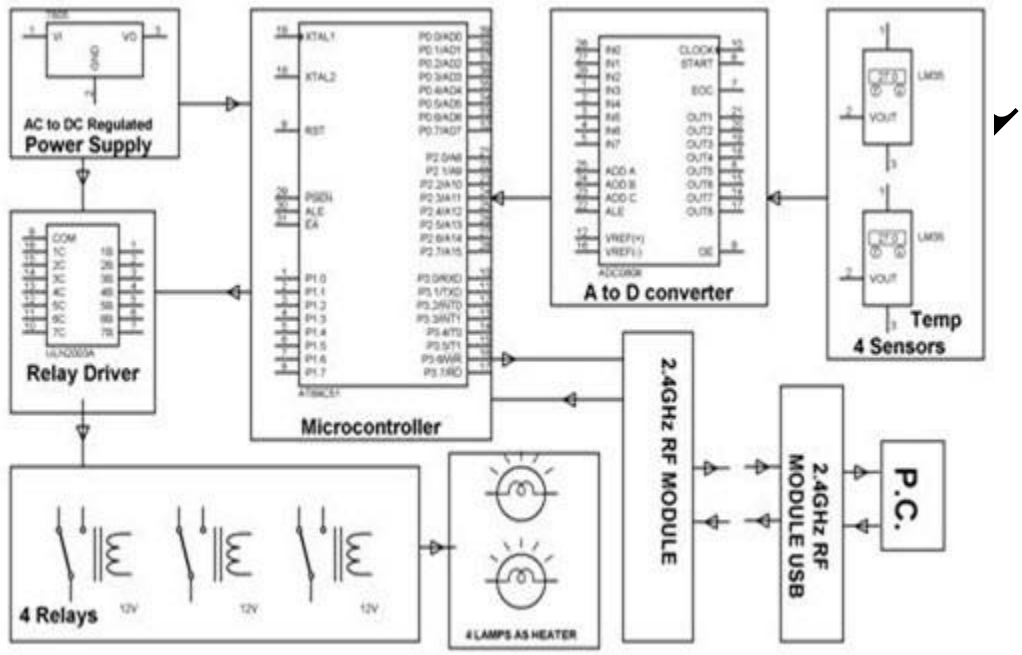

Fig.1.4 Wireless SCADA

Fig.1.4 shows the wireless SCADA system. The multiple mechanisms in the large-scale-remote industries are difficult to control manually. So, for controlling these mechanisms efficiently, a technology namely wireless SCADA (supervisory control and data acquisition) is required. In large-scale wireless industries, by using wireless SCADA, you can monitor all the processes and control the factors which are affecting them.

In this project, a remote plant operation is undertaken to operate the remote plant. Here, temperature sensors are interfaced properly to the 8051 microcontroller. The data which is received from the temperature sensors is continuously sent over 2.4GHz transmitter wirelessly to the microcontroller. Then, it is received by the 2.4GHz USB type receiver which is connected to a PC.

At the front end, a data-acquisition system is loaded on the computer which takes these values and displays them on its front panel and also logs them in the database. One can set parameters such as set point, a low and high limit on the computer screen. When the sensor's temperature goes away from set point, then the microcontroller sends command to the related relay. The lamps connected through the relay contacts are turned on or off. If this system fails, then an AV alarm will be generated on the PC using high limit and low limit features.

Hence, the mechanisms of large scale remote industries can be controlled more efficiently and safely using wireless SCADA, which is more economical and time-saving technology.

Thus, this is all about the SCADA applications in power systems. SCADA is used in the industry with the perfect "Man Machine Interface". It has solved many problems related to supervision, monitoring, controlling and data acquisition. It has manifold applications like Distribution Management, Energy Management, Power Plant Management, Oil and Gas Distribution System. SCADA has also enabled grid monitoring by virtue of which power can be bought & shared on a national basis. So the application of SCADA is beneficial to the Indian power sector as well. Leave your comments about this article in comment section.

A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects. Other terms that may be used for RTU are remote telemetry unit and remote telecontrol unit.

An RTU monitors the field digital and analog parameters and transmits data to the Central Monitoring Station. It contains setup software to connect data input streams to data output streams, define communication protocols, and troubleshoot installation problems.

DO NOT COPY

An RTU may consist of one complex circuit card consisting of various sections needed to do a custom-fitted function or may consist of many circuit cards including CPU or processing with communications interface(s), and one or more of the following: (AI) analog input, (DI) digital (status) input, (DO/CO) digital (or control relay) output, or (AO) analog output card(s).

An RTU might even be a small process control unit with a small Data Base for PID, Alarming, Filtering, Trending functions and so on complemented with some BASIC (programming language) tasks. As it is used in pipeline, grid guarding systems, or for example in the Biosphere II project. Key in such environments it can operate under harsh conditions for example from -50 to 70 degrees Celsius, switch its IO system only on when needed. For example, it communicates via RS485 or wireless communication links in a multi-drop configuration. In this type of configuration it is a remote unit that collects data and performs simple control tasks. It does not have moving parts and uses extremely low power and is often solar powered.

Power supply

A form of power supply will be included for operation from the AC mains for various CPU, status wetting voltages and other interface cards. This may consist of AC to DC converters where operated from a station battery system.

RTUs may include a battery and charger circuitry to continue operation in event of AC power failure for critical applications where a station battery is not available.

Digital (status) inputs

Most RTUs incorporate an input section or input status cards to acquire two state real-world information. This is usually accomplished by using an isolated voltage or current source to sense the position of a remote contact (open or closed) at the RTU site. This contact position may represent many different devices, including electrical breakers, liquid valve positions, alarm conditions, and mechanical positions of devices. Counter inputs are optional.

Analog inputs

A RTU can monitor analog inputs of different types including 0-1 mA, 4–20 mA current loop, 0–10 V., ±2.5 V, ±5.0 V etc. Many RTU inputs buffer larger quantities via transducers to convert

DO NOT COPY

and isolate real-world quantities from sensitive RTU input levels. An RTU can also receive analog data via a communication system from a master or IED (intelligent electronic device) sending data values to it.

The RTU or host system translates and scales this raw data into the appropriate units such as the quantity of water left, temperature degrees, or Megawatts, before presenting the data to the user via the human–machine interface.

Digital (control relay) outputs

RTUs may drive high current capacity relays to a digital output (or "DO") board to switch power on and off to devices in the field. The DO board switches voltage to the coil in the relay, which closes the high current contacts, which completes the power circuit to the device.

RTU outputs may also consist of driving a sensitive logic input on an electronic PLC, or other electronic device using a sensitive 5 V input.

Analog outputs

While not as commonly used, analog outputs may be included to control devices that require varying quantities, such as graphic recording instruments (strip charts). Summed or processed data quantities may be generated in a master SCADA system and output for display locally or remotely, wherever needed.

Software and logic control

Modern RTUs are usually capable of executing simple programs autonomously without involving the host computers of the DCS or SCADA system to simplify deployment and to provide redundancy for safety reasons. An RTU in a modern water management system will typically have code to modify its behavior when physical override switches on the RTU are toggled during maintenance by maintenance personnel. This is done for safety reasons; a miscommunication between the system operators and the maintenance personnel could cause system operators to mistakenly enable power to a water pump when it is being replaced, for example.

DO NOT COPY

Maintenance personnel should have any equipment they are working on disconnected from power and locked to prevent damage and/or injury.

Communications

A RTU may be interfaced to multiple master stations and IEDs (Intelligent Electronic Device) with different communication media (usually serial (RS232, RS485, RS422) or Ethernet). An RTU may support standard protocols (Modbus, IEC 60870-5-101/103/104, DNP3, IEC 60870-6-ICCP, IEC 61850 etc.) to interface any third party software.

Data transfer may be initiated from either end using various techniques to insure synchronization with minimal data traffic. The master may poll its subordinate units (Master to RTU or the RTU poll an IED) for changes of data on a periodic basis. Analog value changes will usually only be reported only on changes outside a set limit from the last transmitted value. Digital (status) values observe a similar technique and only transmit groups (bytes) when one included point (bit) changes. Another method used is where a subordinate unit initiates an update of data upon a predetermined change in analog or digital data. Periodic complete data transmission must be used periodically, with either method, to insure full synchronization and eliminate stale data. Most communication protocols support both methods, programmable by the installer.

Multiple RTUs or multiple IEDs may share a communications line, in a multi-drop scheme, as units are addressed uniquely and only respond to their own polls and commands.

IED communications

IED communications transfer data between the RTU and an IED. This can eliminate the need for many hardware status inputs, analog inputs, and relay outputs in the RTU. Communications are accomplished by copper or fibre optics lines. Multiple units may share communication lines.

Master communications

Master communications are usually to a larger control system in a control room or a data collection system incorporated into a larger system. Data may be moved using a copper, fibre optic or radio frequency communication system. Multiple units may share communication lines.

SCADA communication channels

DO NOT COPY

In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols is now improved and contain extensions to operate over TCP/IP. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced. RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. This paper discusses and compares T101 and DNP3. These two open communication protocols that provide for interoperability between systems for telecontrol applications. Both are now competing within the world market. DNP is widely used in North America, South America, South Africa, Asia and Australia, while IEC 60870-5-101 or T101 is strongly supported in the Europe.

IEC 60870-5

IEC 60870-5 is the collection of standards produced by the IEC(International Electrotechnical Commission). It was created to provide an open standard for the transmission of SCADA telemetry control and information. It provides a detailed functional description for telecontrol equipment and systems for controlling geographically widespread processes specifically for SCADA systems. The standard is intended for application in the electrical industries, and has data objects that are specifically intended for such applications. It is also applicable to general SCADA applications in any industry. But IEC 60870-5 protocol is primarily used in the electrical industries of European countries. When the IEC 60870-5 was initially completed in 1995 with the publication of the IEC 870-5-101 profile, it covered only transmission over relatively low bandwidth bit-serial communication circuits. With the increasingly widespread use of network communications technology, IEC 60870-5 now also provides for communications over networks using the TCP/IP protocol suite. This same sequence of development occurred for DNP3.

DO NOT COPY

T101

T101 or IEC 60870-5-101 (IEC101) is an international standard prepared by TC57 for power system monitoring, control & associated communications. This is compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and uses standard asynchronous serial tele-control channel interface between DTE and DCE. The standard is suitable for multiple configurations like point-to-point, star, mutidropped etc.

T101 features 60870-5-101 or T101 have many features such as the following:

• Supports unbalanced (master initiated message) & balanced (master/slave initiated message) modes of data transfer. Link address and ASDU addresses are provided for classifying the end station and different sectors under the same. Data is classified into different information objects and each information object is provided with a specific address. Facility to classify the data into high priority (class-1) and low priority (class-2) and transfer the same using separate mechanisms.

• Possibility of classifying the data into different groups (1-16) to get the data according to the group by issuing specific group interrogation commands from the master & obtaining data under all the groups by issuing a general interrogation.

• Cyclic & Spontaneous data updating schemes are provided. Facility for time synchronization Schemes for transfer of files

Remote Terminal Unit

• Single indication without / with 24 / with 56 bit timestamps.

• Double indication without / with 24 / with 56 bit timestamps.

• Step position information without / with 24 / with 56 bit timestamps.

• Measured value – normalized, scaled, short floating point without / with timestamps.

DO NOT COPY

• Bitstring of 32 bit without / with timestamps. • Integrated totals (counters) without / with timestamps. • Packed events (start & tripping) of protection equipments

• Single commands

• Double commands

• Regulating step command

• Set point commands of various data formats

• Bitstring commands

• Interrogation commands

• Clock synchronization & delay acquisition commands

• Test & reset commands

DO NOT COPY

DNP3 Protocol

The DNP3 or Distributed Network Protocol is a set of communications protocols used between components in process automation systems. It is usually used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA systems. It is used by SCADA Master Stations or Control Centers, Remote Terminal Units, and Intelligent Electronic Devices. It is primarily used for communications between a master station and IEDs or RTU's. DNP3 supports multiple-slave, peer-to-peer and multiple-master communications. It supports the operational modes of polled and quiescent operation. The latter is also referred to as reporting by exception.

Challenges for Implementation of SCADA

SCADA systems are rapidly being adopted for monitoring and industrial automation for outside-the-fence applications. The adoption has been particularly strong in the areas of water, wastewater, electric power, and natural gas. Naturally, there have been challenges during this period. Operators using outside-the-fence monitoring face challenges that inside-the-fence applications simply do not.

For example, power and communications are both significant limitations when connecting remote assets to SCADA systems. When implemented in a manufacturing plant, all inputs to a SCADA system have access to a fixed and reliable power supply. By contrast, a programmable logic controller (PLC) or remote telemetry unit (RTU) deployed in a remote location cannot easily be wired to a fixed source of power. Instead, they must usually rely on batteries, which deplete and require periodic replacement. Solar panels can offer redundant supply, but they require maintenance (they become less effective when covered with debris or dust and therefore need to be cleaned periodically). They are also vulnerable to vandalism and theft, particularly when they are installed at street level in urban environments.

Certain sensors are more energy-intensive than others, increasing the challenge posed by obtaining adequate power. More frequent wireless data transmission of larger packet sizes place significant demands on the battery powering the wireless modem of an RTU or PLC. Addressing these technological limitations requires higher energy-density or larger batteries, more frequent battery replacements, or using communication networks with lower energy requirements. All these approaches entail additional cost to the network operator.

Connectivity is another challenge. Telecommunications operators may have strong coverage in some areas, but limited signal in others. Obtaining SIM cards and data plans from multiple carriers to ensure reliable connectivity and verifying which carriers offer reliable network strength at each remote installation location is a difficult and costly undertaking. In addition, network strength can vary considerably based on unpredictable conditions such as weather.

Low-power wide area networks (LPWAN), such as those developed by Sigfox and the LoRA Alliance, show great promise. However, network coverage is still limited, and tight bandwidth

limitations dictate the type, amount, and transmission frequency of data over these networks. 2G, 3G, CDMA, LTE cellular, and satellite networks are currently too power intensive to enable fully-autonomous operations for longer durations with frequent data transmission. Future cellular networks (4G and 5G), including NarrowBand IoT (NB-IoT), will offer significantly more power-efficient communications when rolled out in the coming years, but it remains to be seen which specific variant will dominate the market.

An inside-the-fence operator has visibility and autonomy when a local area network (LAN) fails. As the administrator and owner of the network, a plant operator can work swiftly to resolve network issues to minimize downtime. The same cannot be said for outside-the-fence operators relying on third-party wireless networks. When connectivity on cellular and satellite networks fails, a SCADA operator has to rely on the network operator to remedy the situation. Given the much larger extent of their network under management, the response time is naturally slower than what could be offered by a proprietary network operator. In addition, when the downtime is due to defects with the communications infrastructure on the remote assets themselves, they must be repaired *in situ*, making rectifying the situation far costlier.

Despite the challenges of integrating SCADA systems with outside-the-fence applications, their benefits outweigh the challenges. Technologies to resolve the difficulties of integrating remote assets with SCADA systems exist and are being developed on an ongoing basis.

SCADA systems are invaluable tools for monitoring and automation of assets and processes, but challenges exist when attempting to integrate with remote equipment. Obtaining reliable power and communications are two major challenges that must be overcome.

****