# SCADA

# scada

- SCADA is an acronym for Supervisory Control and Data Acquisition.
- SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

# Overview

- These systems encompass the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs) and/or Programmable Logic Controllers (PLCs), and the central host and the operator terminals.
- A SCADA system gathers information (such as where a leak on a pipeline has occurred), transfers the information back to a central site, then alerts the home station that a leak has occurred, carrying out necessary analysis and control, such as determining if the leak is critical, and displaying the information in a logical and organized fashion.
- Traditionally, SCADA systems have made use of the Public Switched Network (PSN) for monitoring purposes.
- Today many systems are monitored using the infrastructure of the corporate Local Area Network (LAN)/Wide Area Network (WAN).
- Wireless technologies are now being widely deployed for purposes of monitoring

# SCADA systems consist of:

- A **Human-Machine Interface** or **HMI**.
- **Remote Terminal Units** (RTUs)
- **Programmable Logic Controller** (PLCs)
- **Communication** infrastructure connecting the supervisory system to the **Remote Terminal Units.**

# Human-Machine Interface

- **HMI** is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram.

# Remote Terminal Units

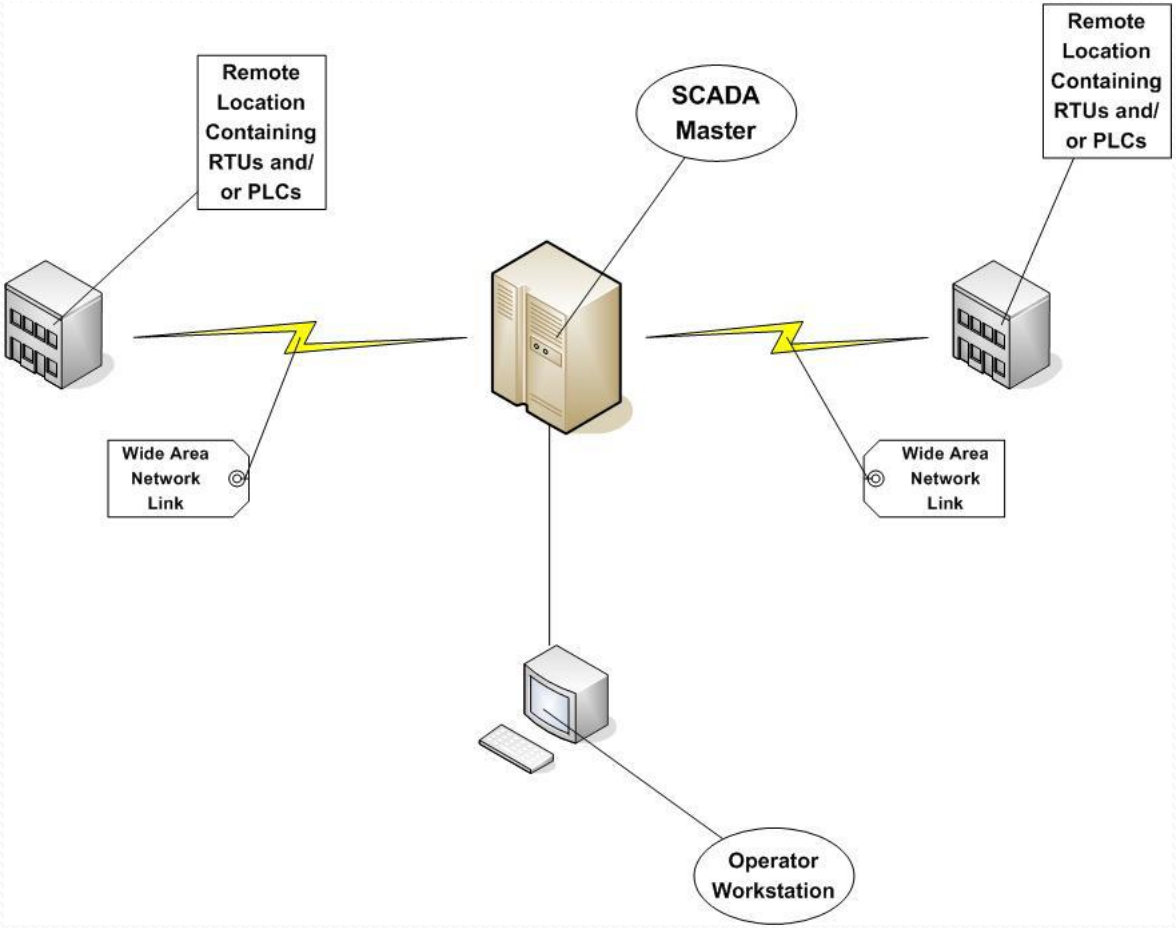
- They are primarily used to convert electronic signals received from field interface devices into the digital data and they are sent to supervisory system.

Remote terminal unit

# Programmable Logic Controller

- PLCs are used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- PLCs have their origins in the automation industry and therefore are often used in manufacturing and process plant applications.
- As PLCs were used more often to replace relay switching logic control systems, telemetry was used more and more with PLCs at the remote sites

# Typical SCADA System



# SCADA control room

# Field Data Interface Devices

- Field data interface devices form the "eyes and ears" of a SCADA
- Before any automation or remote monitoring can be achieved, the information that is passed to and from the field data interface devices must be converted to a form that is compatible with the language of the SCADA system.
- To achieve this, some form of electronic field data interface is required.

# Communications Network

- The communications network is intended to provide the means by which data can be transferred between the central host computer servers and the field-based RTUs .
- The Communication Network refers to the equipment needed to transfer data to and from different sites.
- The medium used can either be cable, telephone or radio.

# Central Host Computer

- The central host computer or master station is most often a single computer or a network of computer servers that provide a man-machine operator interface to the SCADA system.
- The computers process the information received from and sent to the RTU sites and present it to human operators in a form that the operators can work with.
- Operator terminals are connected to the central host computer by a LAN/WAN.
- Host computer platforms characteristically employed UNIX-based architecture.

# Operator Workstations and Software Components

- Operator workstations are most often computer terminals that are networked with the SCADA central host computer.
- The central host computer acts as a server for the SCADA application, and the operator terminals are clients that request and send information to the central host computer based on the request and action of the operators.
- An important aspect of every SCADA system is the computer software used within the system.
- The most obvious software component is the operator interface or Man Machine Interface/Human Machine Interface (MMI/HMI).

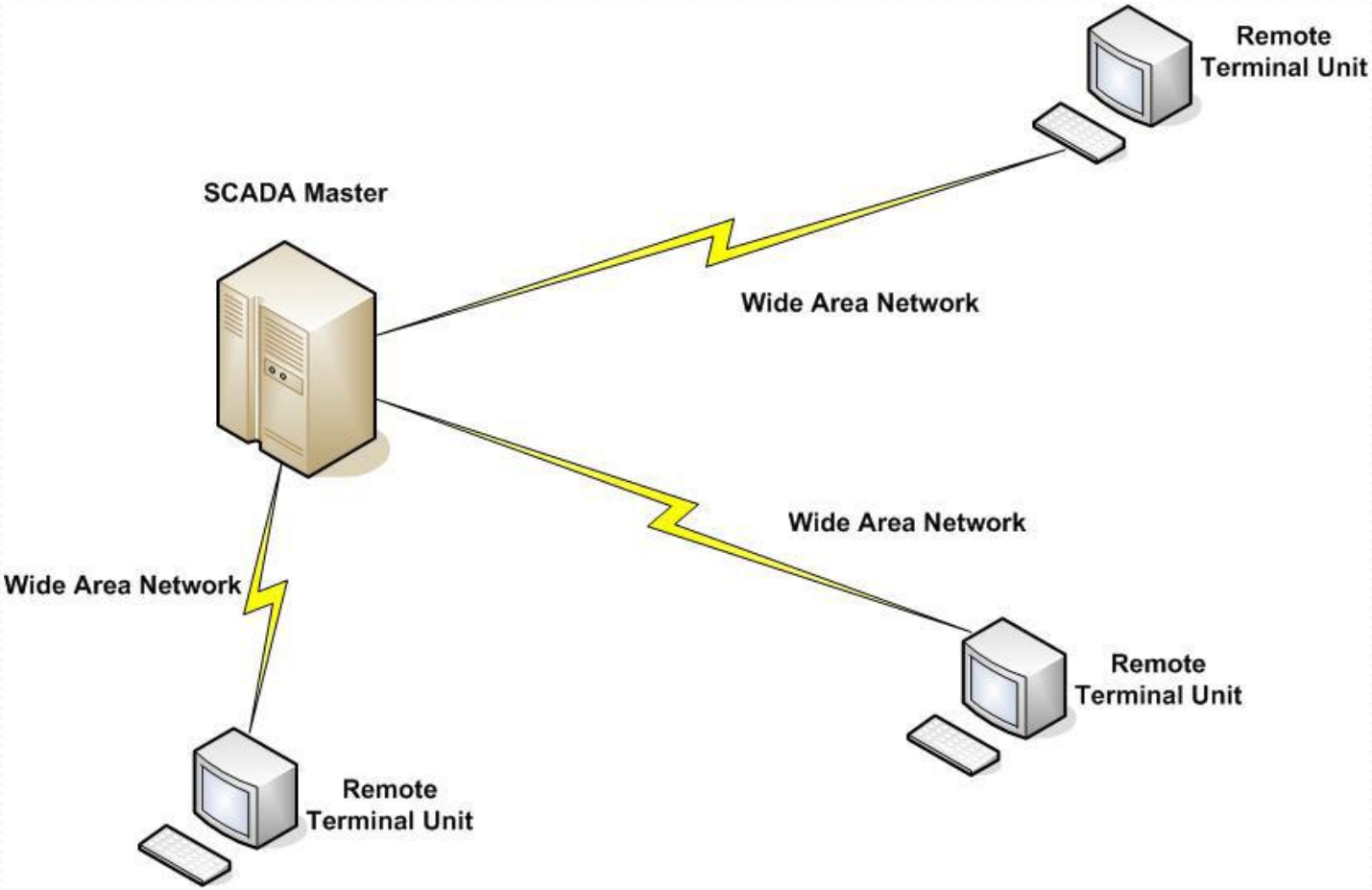
# SCADA Architectures

- SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology. The following sections will provide a description of the following three generations of SCADA systems:
    - First Generation – Monolithic
    - Second Generation – Distributed
    - Third Generation – Networked

# Monolithic SCADA Systems

- In the first generation, computing was done by Mainframe computers
- Networks did not exist at the time SCADA was developed. Thus SCADA systems were independent systems with no connectivity to other systems.
- Wide Area Networks were later designed by RTU vendors to communicate with the RTU.
- The communication protocols used were often proprietary at that time.
- The first-generation SCADA system was redundant since a back-up mainframe system was connected at the bus level and was used in the event of failure of the primary mainframe system.

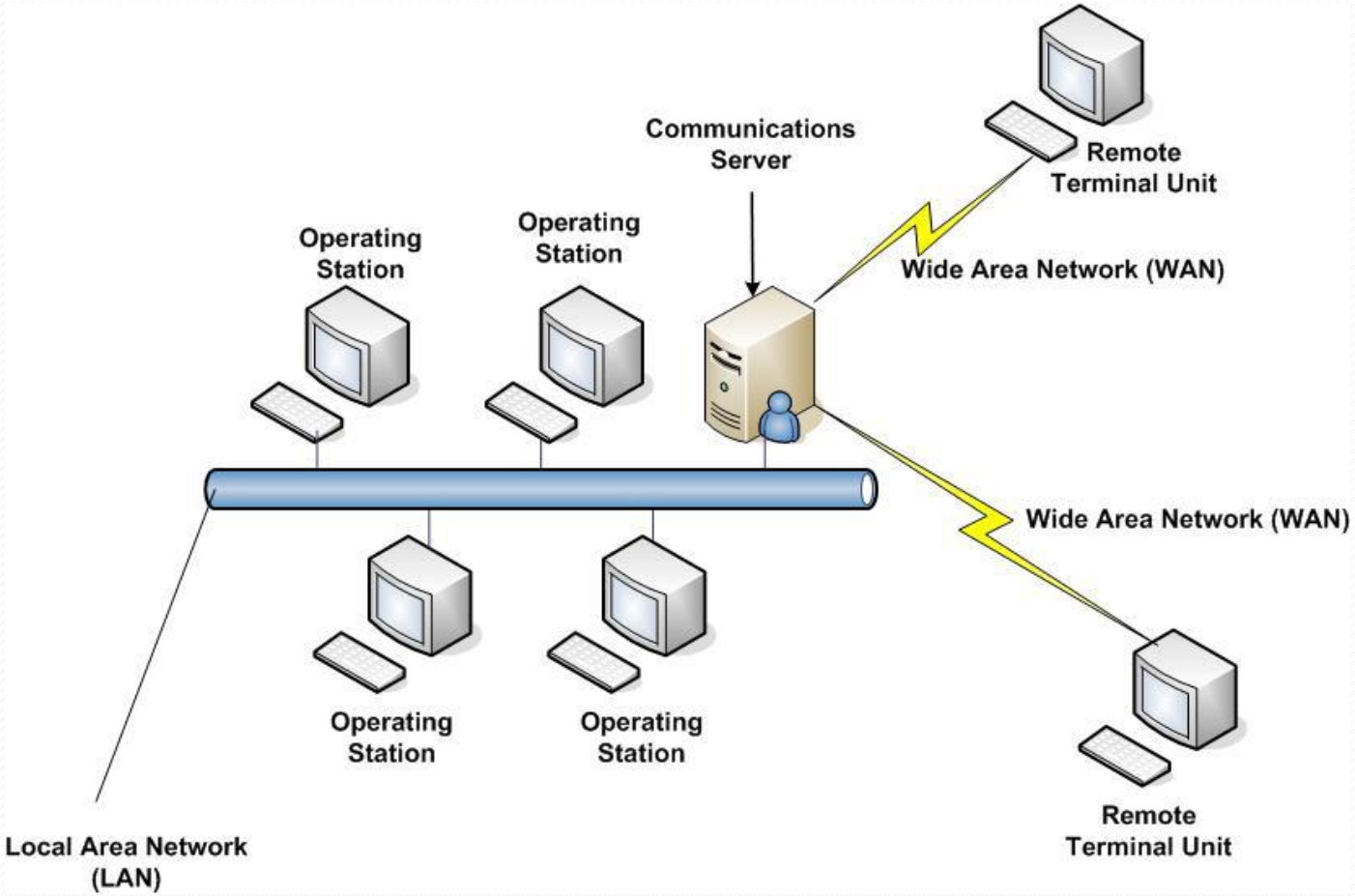
# First Generation SCADA Architecture



# Second generation: "Distributed"

- The processing was distributed across multiple stations which were connected through a LAN and they shared information in real time.
- Each station was responsible for a particular task thus making the size and cost of each station less than the one used in First Generation.
- The network protocols used were still mostly proprietary, which led to significant security problems for any SCADA system that received attention from a hacker.
- Since the protocols were proprietary, very few people beyond the developers and hackers knew enough to determine how secure a SCADA installation was. Since both parties had invested interests in keeping security issues quiet, the security of a SCADA installation was often badly overestimated, if it was considered at all.

# Second Generation SCADA Architecture



# Third generation: "Networked"

- These are the current generation SCADA systems which use open system architecture rather than a vendor-controlled proprietary environment.
- The SCADA system utilizes open standards and protocols, thus distributing functionality across a WAN rather than a LAN.
- It is easier to connect third party peripheral devices like printers, disk drives, and tape drives due to the use of open architecture.
- WAN protocols such as Internet Protocol (IP) are used for communication between the master station and communications equipment.
- Due to the usage of standard protocols and the fact that many networked SCADA systems are accessible from the Internet, the systems are potentially vulnerable to remote cyber-attacks.
- On the other hand, the usage of standard protocols and security techniques means that standard security improvements are applicable to the SCADA systems, assuming they receive timely maintenance and updates

# Security issues

**Threats**

- unauthorized access to the control software - human access or viral infection
- packet access to the network segments hosting SCADA devices.

# Why the security of scada is important……..

- SCADA systems are used to  control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society.

# conclusion

- SCADA systems have been used for years in the utilities industry with great success.
- Now more than ever, it is important that our critical infrastructures such as power grids, water processing systems, and the Public Switched Network (PSN), be monitored and protected by SCADA architectures.