

SCADA

(Supervisory Control and Data Acquisition)

I. SCADA Overview

A. General Characteristics/Descriptions of a SCADA System

1. Monitors and controls a plant or equipment in industries
Example of industries: telecommunications, water and waste control, energy, oil and gas refining, and transportation
2. Encompasses the transfer of data between parts
Between:
 - a. SCADA central host computer and a number of RTUs and/or PLCs
 - b. Central host and operator terminals

RTU – Remote Terminal Unit, also known as Remote Telemetry Units

PLC – Programmable Logic Controller, a device used, traditionally, to automate monitoring and control of industrial facilities
3. Gathers information, transfers the information back to a central site, alerts the home station of the event related to the information, carrying out analysis and control and displaying the information in a logical and organized fashion.
For example, the information could be the location of a fault in a transmission line
4. Can be relatively simple or very complex
Simple: A SCADA system that monitors environmental conditions of a small office building.
Complex: A SCADA system that monitors all the activity in a nuclear power plant
A SCADA system that monitors all the activity of a municipal water system
5. SCADA Systems traditionally use PSN. Today many systems use LAN or WAN.
Wireless technologies are now being widely used in these systems.

PSN – Public Switched Network

LAN – Local Area Network

WAN – Wide Area Network

B. Components of SCADA Systems

1. Field data interface devices
 - one or more, usually RTUs or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators
2. Communication system
 - transfers data between field data interface devices and control units and the computers in the SCADA central host
 - can be radio, telephone, cable, satellite, etc., or any combination of these
3. Central host computer server or servers

- sometimes called a SCADA center, master station, or Master Terminal Unit (MTU)
- 4. Software systems
 - A collection of standard and/or custom software
 - sometimes called Human Machine Interface (HMI) or Man Machine Interface (MMI) software systems
 - used to:
 - a. provide the SCADA central host and operator terminal application
 - b. support the communication system
 - c. monitor and control remotely located field interface devices

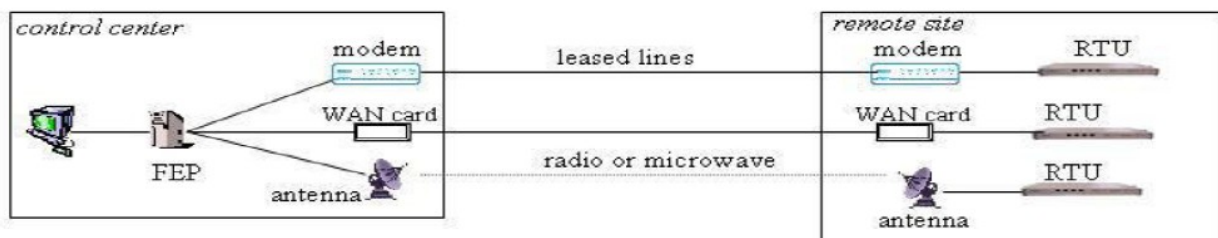


Figure 1. A Simple SCADA System

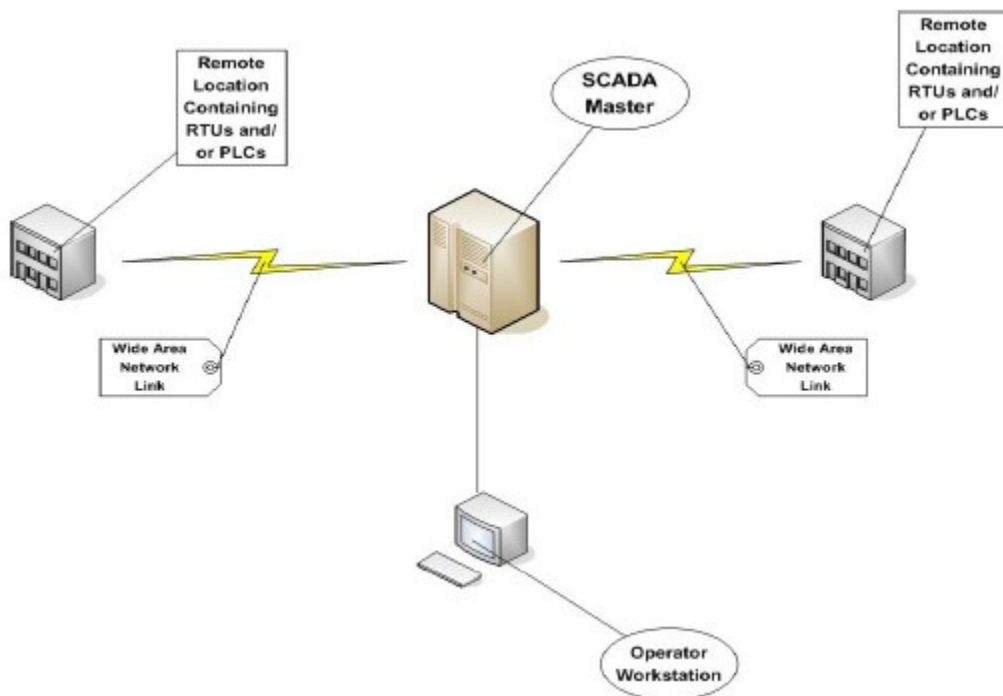


Figure 2. Typical SCADA System

Field Data Interface Devices

Sensors:

- Field devices such as reservoir level meters, water flow meters, valve position transmitters, temperature transmitters, power consumption meters, and pressure meters all **provide information** that can tell an experienced operator how well a system is performing.
- They form the "eyes and ears" of a SCADA system.

Actuators:

- Field devices or equipment such as electric valve actuators, motor control switchboards, and electronic chemical dosing facilities can be used to form the "hands" of the SCADA system and **assist in automating a process** of a particular system.
- RTUs are primarily used to convert electronic signals received from field devices into the language (known as the communication protocol) used to transmit the data over a communication channel.
 - PLCs, which have in the past been physically separate from RTUs, traditionally held the instructions for the automation of field devices. They connect directly to field devices and incorporate programmed intelligence in the form of logical procedures that will be executed in the event of certain field conditions.
 - Over time, RTUs also performed control function in addition to its traditional function. At the same time, traditional PLCs included communications modules that would allow PLCs to report the state of the control program to a computer plugged into the PLC or to a remote computer via a telephone line, thus enabling them to also perform the original basic function of RTUs.
 - As a result of these developments, the line between PLCs and RTUs has blurred and the terminology is virtually interchangeable. For the sake of simplicity, the term RTU will be used to refer to a remote field data interface device; however, such a device could include automation programming that traditionally would have been classified as a PLC.

Communication Networks

- Refers to the equipment needed to provide the means by which data can be transferred between the central host computer servers and the field-based RTUs.
- The medium used can either be cable, telephone or radio.
- Cable: usually implemented in a factory, not practical for systems covering large geographical areas (expensive: high cost of the cables, conduits and the extensive labor in installing them)
- Telephone lines: more economical solution for systems with large coverage.
 - Leased lines: used for systems requiring on-line connection with the remote stations, expensive since one telephone line per site needed

Dial-up lines: used on systems requiring updates at regular intervals (e.g., hourly updates), ordinary telephone lines can be used, host can dial a particular number of a remote site to get the readings and send commands.

- Radio: an economical solution for remote sites not accessible by telephone lines, radio modems are used to connect the remote sites to the host, an on-line operation can also be implemented on the radio system, a radio repeater is used to link sites where a direct radio link cannot be established.

Central Host Computer

- Most often a single computer or a network of computer servers that provide a man-machine operator interface to the SCADA system, 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 so that the viewing screens and associated data can be displayed for the operators using high resolution computer graphics to display a graphical user interface or mimic screen of the site or water supply network in question.
- Historically, SCADA vendors offered proprietary hardware, operating systems, and software that was largely incompatible with other vendors' SCADA systems. Expanding the system required a further contract with the original SCADA vendor.
- Host computer platforms characteristically employed UNIX-based architecture, and the host computer network was physically removed from any office-computing domain. Now, SCADA systems are available that can network with office-based personal computers, opening a range of possibilities for the linking of SCADA systems to office-based applications such as GIS systems, hydraulic modeling software, drawing management systems, work scheduling systems, and information databases.

Operator Workstations

- They 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
- Clients request and send information to the server based on the request and action of the operators.

Software Components

- Software of some form pervades all levels of a SCADA system; Man Machine Interface/ Human Machine Interface (MMI/HMI) package is the most obvious software component
- Software can be a significant cost item when developing, maintaining, and expanding a SCADA system, depending on the size and nature of the SCADA application
- A successful SCADA system depends on a well defined, designed, written, checked, and tested software; poor performances in any of these project phases will very easily cause a SCADA project to fail.
- It is important to ensure that adequate planning is undertaken to select the software systems appropriate to any new SCADA system.

C. SCADA In Power Systems

- SCADA allows control operators to monitor, control, and dispatch generation, and obtain written reports of all parameters about the power system
- When problems occur in telecommunications equipment or control center equipment, system operators must occupy back-up control centers in order to resume monitoring and control functions of the power system
- Control centers and back-up control centers normally have emergency generators and uninterruptible power supply (UPS) systems.

D. SCADA Control Center Functions

- SCADA system is to remotely control all essential equipment in each substation from a single control center or backup control centers
 - Control/operate substation equipment
 - Close breakers
 - Control motors
 - Start Emergency generators
- The functions in the substation that are communicated to the control center are to measure, monitor, and control the substation equipment
- Control center basic functions:
 - to display the informationExamples of analog data acquisition information include:
 - Bus volts
 - Transformer watts
 - Feeder amps

- System VARs
- Regulator position
- Entry/security alarms
- Generator Data
- store the information
- generate alarms if anything abnormal is detected
- enable remote control operation of equipment
- initiate changes in the effort to regain normal operation
- SCADA systems have the capability of providing graphical representation of the generation stations, transmission lines, substations, and distribution lines
- SCADA alerts a control operator that a change of state occurred
- Operator actions provide feedback and displays to verify actions

II. SCADA Architectures

SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology.

Three generations of SCADA systems

1. First Generation – Monolithic
2. Second Generation – Distributed
3. Third Generation – Networked

1 Monolithic SCADA Systems

- These were standalone systems with virtually no connectivity to other systems; the concept of computing in general centered on “mainframe” systems; networks were generally non-existent, and each centralized system stood alone.
- The Wide Area Networks (WANs) that were implemented to communicate with remote terminal units (RTUs) were designed with a single purpose in mind—that of communicating with RTUs in the field and nothing else. (WAN protocols in use today were largely unknown at the time)
- The communication protocols in use were developed by vendors of RTU equipment and were often proprietary; were generally very “lean”, supporting virtually no functionality beyond that required scanning and controlling points within the remote device. It was generally not feasible to intermingle with RTU communications on the network other types of data traffic.
- Connectivity to the SCADA master station itself was very limited by the system vendor. Connections to the master typically were done at the bus level via a proprietary adapter or controller plugged into the Central Processing Unit (CPU) backplane.

- Redundancy was accomplished by the use of two identically equipped mainframe systems, a primary and a backup, connected at the bus level. The standby system's primary function was to monitor the primary and take over in the event of a detected failure; thus, little or no processing was done on the standby system.

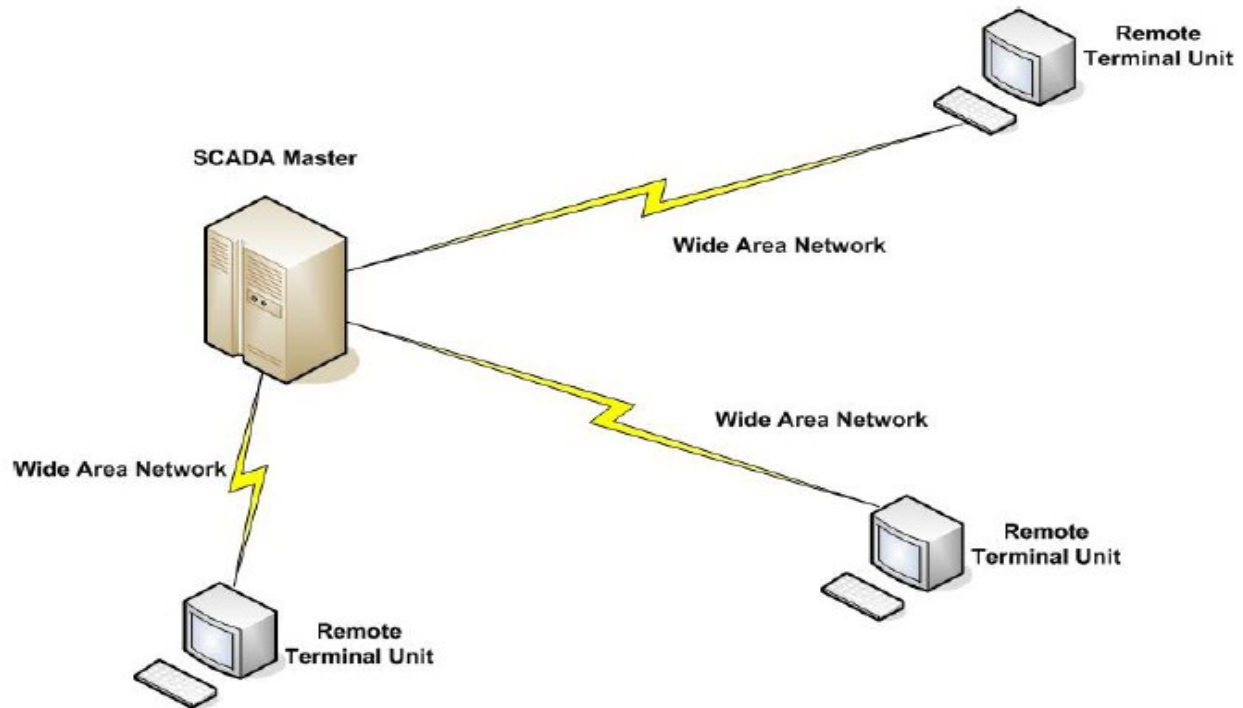


Figure 3. Typical First Generation SCADA Architecture

2 Distributed SCADA Systems

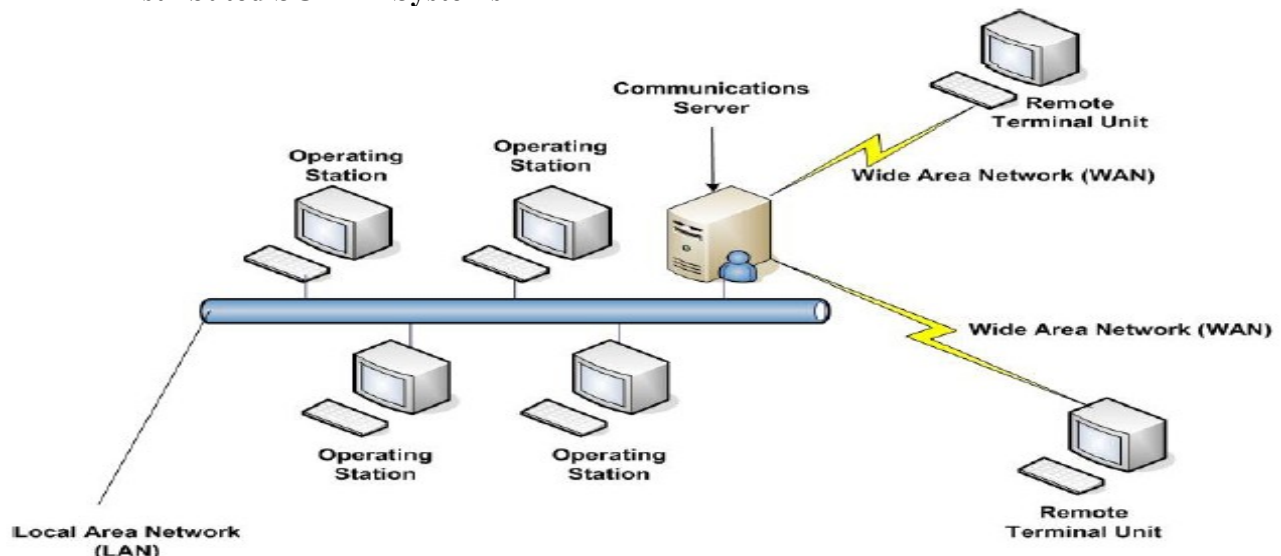


Figure 4. Second Generation SCADA Architecture

- These systems took advantage of developments and improvement in system miniaturization and Local Area Networking (LAN) technology to distribute the processing across multiple systems.

- Multiple stations, each with a specific function, were connected to a LAN and shared information with each other in real-time. These stations were typically of the mini-computer class, smaller and less expensive than their first generation processors.
- Some of these distributed stations served as
 - Communications processors - primarily communicating with field devices such as RTUs.
 - Operator interfaces - providing the human-machine interface (HMI) for system operators.
 - Calculation processors or database servers.
- The distribution of individual SCADA system functions across multiple systems provided more processing power for the system as a whole than would have been available in a single processor.
- The networks that connected these individual systems were generally based on LAN protocols and were not capable of reaching beyond the limits of the local environment.
- Some of the LAN protocols that were used were of a proprietary nature
 - Vendor created its own network protocol or version thereof rather than pulling an existing one off the shelf.
 - Vendor was able to optimize its LAN protocol for real-time traffic, but it limited (or effectively eliminated) the connection of network from other vendors to the SCADA LAN.
- Distribution of system functionality across network-connected systems served also to improve the redundancy and reliability of the system as a whole.
 - The distributed architecture often kept all stations on the LAN in an online state all of the time.
 - If an HMI station were to fail, another HMI station could be used to operate the system, without waiting for failover from the primary system to the secondary.
- The WAN used to communicate with devices in the field were largely unchanged by the development of LAN connectivity between local stations at the SCADA master.
- The second generation of SCADA systems was also limited to hardware, software, and peripheral devices that were provided or at least selected by the vendor.

3 Networked SCADA Systems

- The current generation of SCADA master station architecture is closely related to that of the second generation.

- The primary difference and the major improvement: It is an open system architecture rather than a vendor controlled, proprietary environment.
 - There are still multiple networked systems, sharing master station functions.
 - There are still RTUs utilizing protocols that are vendor-proprietary.
- The major improvement comes from the use of WAN protocols such as the Internet Protocol (IP) for communication between the master station and communications equipment. This allows the portion of the master station that is responsible for communications with the field devices to be separated from the master station “proper” across a WAN. Vendors are now producing RTUs that can communicate with the master station using an Ethernet connection.
- Opening the system architecture makes it possible to utilize open standards and protocols and to distribute SCADA functionality across a WAN and not just a LAN.
- Open standards eliminate a number of the limitations of previous generations of SCADA systems. The utilization of off-the-shelf systems makes it easier for the user to connect third party peripheral devices (such as monitors, printers, disk drives, tape drives, etc.) to the system and/or the network.
- As vendors have moved to “open” or “off-the-shelf” systems, they have gradually gotten out of the hardware development business and concentrated their development in an area where they can add specific value to the system—that of SCADA master station software.
- The distribution of SCADA functionality over a WAN, that is, by distributing the processing across physically separate locations, it becomes possible to build a SCADA system that can survive a total loss of any one location.

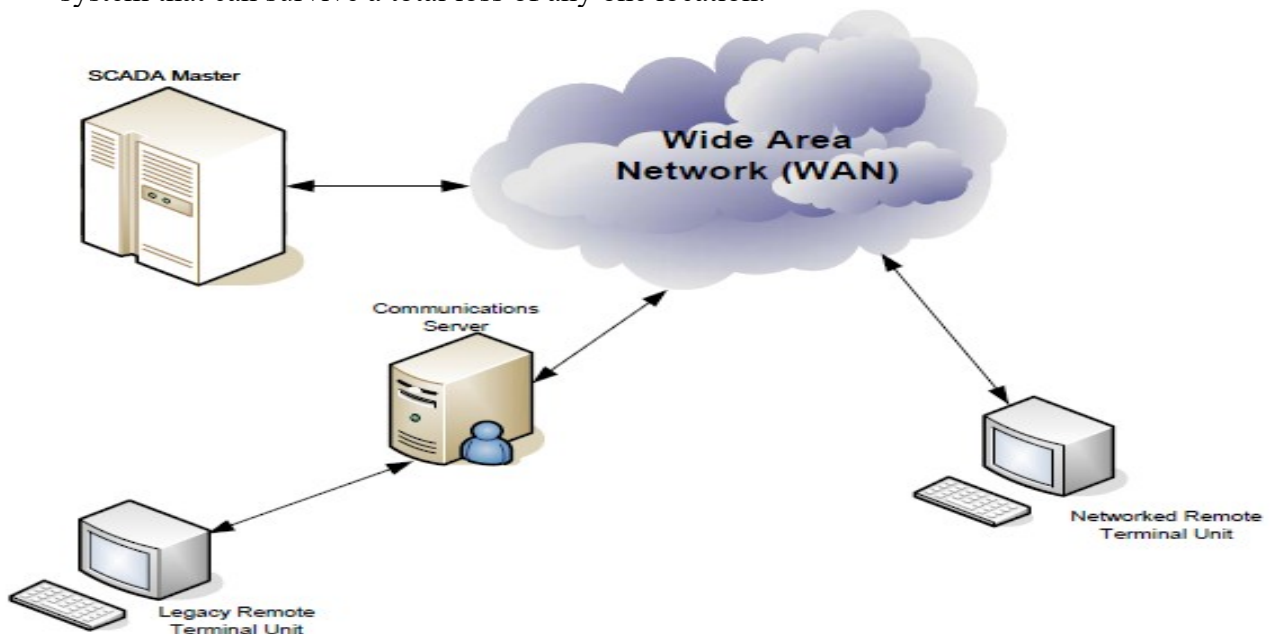


Figure 5 Third Generation SCADA System

III. SCADA Protocols

Technically, protocol refers to rules for networking computers, or a set of technical rules for the transmission and receipt of information between computers.

Some Of The Protocols Used In SCADA Communication

1. **IEC 60870.** IEC 60870 was defined basically for the telecommunications of electrical system, and control information and its data structures are geared to that application. It is the most popular standard in the United States of America for electrical power grid SCADA systems. (IEC - International Electrotechnical Commission)
2. **DNP3.** The second protocol specifically designed for SCADA communications is the Distributed Network Protocol Ver-sion 3 (DNP3). DNP3 was created for the electrical industry, but it has been adapted by other industry sectors and is the leading protocol for most SCADA applications in Europe.
3. **HDLC.** Primarily, High Level Data Link Control (HDLC) and Modbus were two of other SCADA standards existing. HDLC, defined by ISO for point-to-point and point-to-multipoint links, is also known as Synchronous Data Link Control (SDLC) and Advanced Data Communication control Procedure (ADCCP). It is a bit-based protocol, the precursor to Ethernet, and is quickly being replaced by DNP3, TCP/IP and Industrial Ethernet2.
4. **Modbus.** Modbus is a messaging structure developed by Modicon in 1979, used to establish master-slave/client-server communication between intelligent devices. Modbus is a comparatively slow protocol that does not define interfaces, thus permitting users to choose between EIA-232, EIA-422, EIA-485 or 20mA current loop. While slow, it is widely accepted and in reality has become standard--a new study indicated that 40% of industrial communication applications use Modbus.
5. **Profibus.** Profibus is a German standard that defines three types: Field Message Specification (FMS) for application in general data acquisition systems, Decentralized Peripherals (DP) for use when fast communication is needed, and Process Automation (PA) for use when highly reliable and safe communication is required.
6. **UCA.** The Utility Communications Architecture (UCA) is an enterprise from the Electric Power Research Institute (EPRI) designed for the electrical industry. It is more than only a protocol definition; it is a comprehensive set of standards designed to allow "plug and play" integration into systems, letting manufacturers to design off-the-shelf compliant devices. IEEE adopted the UCA standards process in 1999 and Electrical and Electronic Engineering 2012, 2(3): 158-163 161 has developed extensions for the water industry. Other industries are also examining UCA for suitability.

IV. Security and Vulnerability of SCADA Systems

SCADA systems have evolved in recent years and are now based on open standards and COTS products. Most SCADA software and hardware vendors have embraced Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet communications, and many have encapsulated their proprietary protocols in TCP/IP packets. While all of this evolution towards more open-based standards has made it easier for the industry to integrate various diverse systems together, it has also increased the risks of less technical personnel gaining access and control of these industrial networks.

- Increasing communications increased vulnerability to attack
- The Stunt worm, which attacked nuclear power plants in Iran- brought attention to grid security
- The systems used to control nuclear power plants are very similar to those which run the power grid
- Stuxnet was delivered as part of a Siemens industrial control system, an internal threat rather than an external one – not by a hacker
- The Government Accountability Office (GAO) report concluded that there are gaps in cybersecurity regulation and problems with jurisdiction and that even when regulation exists utilities are focused on regulatory compliance rather than comprehensive security
- Currently NERC (North American Electric Reliability corporation) defines national standards on cybersecurity for utilities
- Experts say the NERC standards are not sufficient to ensure robust security in the smart grid
- Making sure the standards are implemented correctly via testing and monitoring is also an area of concern

V. SCADA Standards Organizations

There are many organizations involved in the standardization of SCADA systems.

- 1. The Institute of Electrical and Electronics Engineers (IEEE)**
- 2. American National Standards Institute (ANSI)**
- 3. Electric Power Research Institute**
- 4. International Electrotechnical Commission**
- 5. DNP3 Users Group**