ijecs open access www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 3 Issue 1 Jan, 2014 Page No. 3743-3751*

# SCADA: *SUPERVISORY CONTROL AND DATA ACQUISITION*

**Kirti**
*Computer Science and Engineering*
*(Network Security)*
*India*

***Abstract— This paper presents a survey on SCADA: Supervisory Control And Data Acquisition. This discussion is centered on overview of SCADA, History of SCADA, security issues, security in SCADA, application of SCADA, operation of SCADA .SCADA systems perform data collection and control at the supervisory level. Some SCADA systems only monitor without performing controlling functions, but these systems are still referred to as SCADA systems.***

*Keywords— RTU, HMI, PLA, IED,*

## I. INTRODUCTION

SCADA stands for Supervisory Control And Data Acquisition. While North Americans use this term to refer to distributed measurement and control systems that are larger in scale, the rest of the world applies this term to any application that performs Supervisory Control And Data Acquisition functions.SCADA systems perform data collection and control at the supervisory level. Some SCADA systems only monitor without performing controlling functions, but these systems are still referred to as SCADA systems. SCADA systems are widely used for monitoring and controlling industrial systems including power plants, water and sewage systems, traffic control, and manufacturing industries. The security of SCADA networks is an important topic today due to the vital role that SCADA systems play in our national lives in providing essential utility services. Pervasive Internet accessibility at industrial work places increases the vulnerabilities of SCADA systems because this makes it possible for a remote attacker to gain control of, or cause disruption to the critical functions of the network. SCADA Systems SCADA (Supervisory Control and Data Acquisition) systems are computer based tools to control and monitor industrial and critical

infrastructure functions, such as the generation, transmission and distribution of electricity, gas, water, waste, railway and traffic control in real time. The primary function of a SCADA system is to efficiently connect and transfer information from a wide range of sources, and at the same time maintaining data integrity and security. SCADA systems have been around since the 1960s, when the direct human involvement in monitoring and control of utility plants was gradually replaced by remote operation of valves and switches through the use of modern telecommunication devices such as phones lines and dedicated circuits. The emergence of powerful personal computers and servers and the need to connect to the Internet have added a new dimension to the operation of SCADA systems. For example, the operator can remotely login to the SCADA systems without the need to be physically present at the remote control sites. Unfortunately, this has also led to an opportunity for intruders and attackers to compromise the system by posing as a legitimate operator or by taking control of the operator's computer. Figure illustrates how a modern SCADA system is connected. The field devices consist of Remote Terminal Units (RTU), Programmable Logic Devices (PLC), and Intelligent Electronic Devices (IED). A number of RTUs in remote locations collect data from devices and send log data and alarms to a SCADA terminal using various communication links including traditional telephone and computer network, wireless network, and fiber optic cables. Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Some industrial systems use PLCs to control end devices like sensors and actuators. Data from the RTUs and PLCs is compiled and formatted in such a way that a control room operator using a Human Machine Interface (HMI) can make supervisory decisions to adjust or override normal RTU (or PLC) controls. This data may also be collected and stored in a Historian, a type of Database Management System, to allow auditing, and the analysis of trends and anomalies.

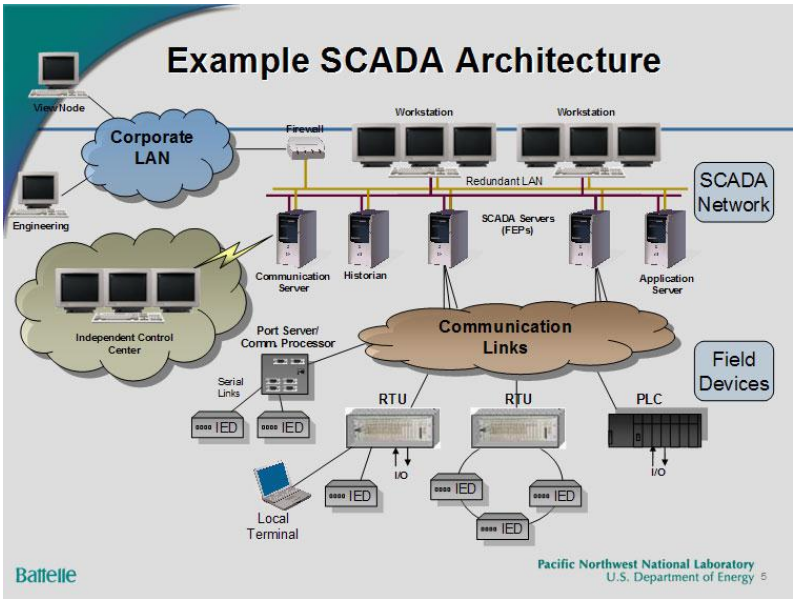


*Fig: An illustration of a SCADA system showing how the SCADA servers are connected to both the field devices and the corporate LAN.*

## HISTORY OF SCADA

SCADA systems became popular in the 1960's as the need to monitor and control remote equipment grew. Early SCADA systems used mainframe technology and required human operators to make action decisions and maintain the information systems. Because this increased the human labor cost, early SCADA systems were very expensive to maintain. Today, SCADA is generally much more automated, and consequently more cost-efficient.

## APPLICATION OF SCADA

### The 2 Basic Components of SCADA

Any SCADA scenario involves 2 basic components

1. Things you want to monitor and control
2. Devices you will use to perform monitoring and controlling functions

To monitor and control these elements using a SCADA system, you will need devices to collect

.

data from them and issue commands. This network of monitoring and control devices makes up your SCADA system. Using sensors (discrete or analog) and control relays, the system can collect information about processes and control individual pieces of equipment. The system is governed by a SCADA master, which collects data from monitoring devices and issues controls in response (either automatically or at the request of human operators).

### Where You Can Use SCADA

While SCADA can be used to manage any kind of equipment, SCADA systems are typically for the automation of industrial processes where humans are unable to manage complex or rapid operations. These are often fast-paced processes dealing with extremely delicate and tiny parts and equipment that are simply too difficult for human operators to monitor with any consistent level of accuracy

**SCADA systems are often used by:**

- **Power companies:** SCADA systems can be used to maximize the efficiency of power generation and distribution processes. More specifically, SCADA systems can monitor the power flow, power line voltage, circuit breaker status, and other electrical processes. SCADA systems can even be used to control individual sections of the power grid.
- **Major Utility Companies:** Both government and private utility companies use SCADA for water and sewage services. This includes collecting water use and distribution information, gauging supply levels, monitoring pressure readings, and other similar applications.
- **Physical sites:** SCADA systems can be used to control environmental factors at an organization's physical sites. SCADA data collection functions can be used at facilities and buildings to monitor variables such as temperate, lighting, and entry systems. The control functions of SCADA systems can be used to maintain specific environmental elements at these sites, keeping refrigeration units online, maintaining specific heating levels, and more.
- **Manufacturing companies:** Production managers can use SCADA to monitor their inventory. They can use their SCADA system to regulate production machinery and implement quality control tests. SCADA can be very beneficial for just-in-time manufacturers by automating production so that demand is met exactly, which reduces inventory costs.
- **Providers of mass transportation:** SCADA can be used to regulate critical transportation processes, like providing power for all types of public transportation, as well as automating related equipment, including traffic lights and railroad crossing gates. SCADA systems can even be used to track the progress of individual vehicles within a transportation network, including individual buses on city streets, or cars on a specific subway line.

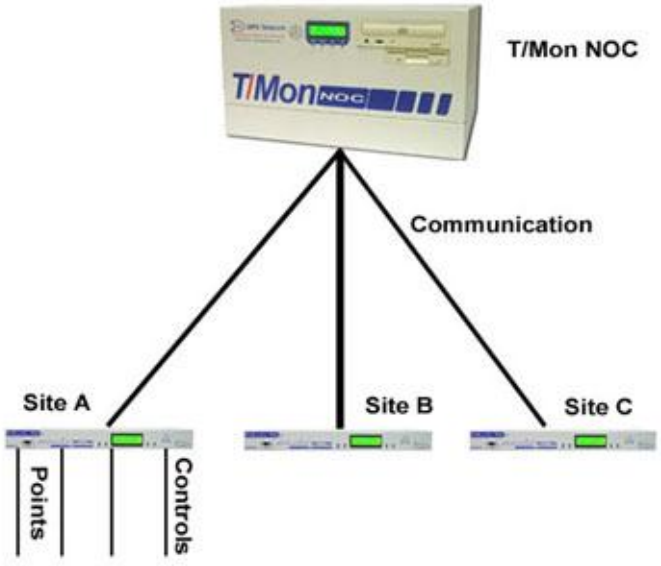
# IV. OPERATIONS & TASK OF SCADA

**SCADA System Operation:** There are four parts common to every SCADA system:

1. **Sensors (either digital or analog) and control relays** - These are input/output devices that monitor and control the managed processes and equipment.
2. **Remote telemetry units (RTU's)**- These are devices deployed in the field at specific sites and locations. RTU's gather information locally from the sensors to report back to the SCADA master unit. RTU's can also issue control commands to the control relays it communicates with.
3. **SCADA master units**- SCADA master units are the main, user-end component of the entire SCADA monitoring system.

They are also sometimes referred to as the SCADA HMI (Human-Machine Interface). The master provides the central processing capability for the SCADA system. Master units connect the human operators to the system with a browser interface that allows the system operator to respond to data gathered from all parts of the network.

4. **The communications network**- The communication network provides the connection between the SCADA master unit and the RTU's in the field. It is the all-important link between the far-flung elements of a geo-diverse operation.




These parts enable a SCADA system to perform four types of tasks:

1. **Data collection**- A SCADA system is composed of large numbers of sensors that collect inputs into a system, or measure the output levels of a system or process. The information collected by these sensors is collected by the **RTU**'s locally, and then forwarded to the SCADA master, where reports and alarms are presented to the network operator.

   Sensors can be classified as two types, either discrete or analog. Discrete sensors collect information about simple events, whereas analog sensors can provide more detailed information that can fall within a range of values, rather than a present/not present type of situation. Analog sensors are particularly useful in measuring environmental factors, such as temperature and humidity, battery levels, fuel levels, and more.

2. **Communication of data across the network**- To monitor geo-diverse operational systems from a centralized location, you need a communications network. This network provides you with a means to transport all information collected across the system. SCADA communications generally take place on

Ethernet and IP over SONET. To alleviate security concerns when transporting sensitive data, communication of data should be done over internal LAN/WANs, not the public Internet.

SCADA uses protocol communication methods, so input and output devices cannot interpret or create SCADA communications on their own. RTU's interpret information from attached sensors and transmit it to the SCADA master (HMI). In turn, the RTU receives control commands in protocol format from the SCADA master, and forwards these commands to the appropriate control relays. This allows the SCADA master to control individual operational processes throughout the network from a single location

3. **Information reporting**- A SCADA system presents data to operators via the SCADA HMI (Human-Machine Interface). Along with presenting this data, the SCADA master station also performs many other tasks for network operators. The master continuously monitors all sensors and alerts the operator when there is a Change-of-State (COS) event within the managed system. The master presents a comprehensive view of the entire network of devices, and presents more specific information about the managed equipment and processes when the system operator requests it. The master also presents reports and summarizes historical trends of data gathered by the system.
4. **System control functions**- A SCADA solution with control functions can respond to COS events anywhere in the system by automatically issuing related, user-specified commands. If you have an advanced SCADA master, this can be done without any human intervention at all, resulting in instantaneous response to dynamic problems and threats. Advanced systems also allow overriding of automatic controls as the need occurs.

**SECURITY ISSUE IN SCADA**

**We Apply Network Traffic Monitoring Techniques For SCADA System Security:**

Traffic monitoring is used in configuration management for tasks such as estimating the traffic demands between different points in the net- work, so that network capacity can be allocated to these demands. In performance management, traffic monitoring can be used to determine whether the measured traffic levels exceed the allocated network capacity, thus causing congestion or delays. When a fault occurs in the network, traffic monitoring is used in fault management to help locate the source of the fault, based on changes in the traffic levels through the surrounding network elements. In accounting management, traffic monitoring is needed to measure the network usage by each customer, so that costs can be charged accordingly in terms of the volume and type of traffic generated. Finally, network traffic monitoring can be used in security

management to identify unusual traffic flows, which may be caused by a denial-of-service attack or other forms of misuse.

Today many of the SCADA systems are also connected to the corporate network where a manager or an engineer can view and change control settings. The data is transferred through a communication server that is protected by a firewall from the corporate network which is often connected to the wider Internet. The SCADA data is increasingly being transported using the TCP/IP protocol for increased efficiency, enhance interconnectivity, and because of the ease of using commercial-off the shelf hardware and software. Protocols such as Mod bus and DNP3 that had been traditionally used for interconnection within SCADA network are increasingly being transported over TCP/IP as the field devices are also providing IP support. This leads to a standardized and transparent communication model both within and outside the SCADA network. As TCP/IP is becoming the predominant carrier protocol in modern SCADA networks, it introduces the potential for innovative attacks targeting the SCADA system, which had been previously isolated from the corporate information technology and communications infrastructure. Since most SCADA protocols were not designed with security issues in mind, therefore, an attack on the TCP/IP carrier could expose the unprotected SCADA data. In addition, traditional attacks from the Internet could be transported through the interconnected corporate network into the SCADA network and disrupt the industrial processes

**PROTECTING SCADA SYSTEMS** :

By Using Network Traffic Monitoring As shown in Fig., SCADA system is different from normal TCP/IP network. In addition to the normal TCP/IP network, a SCADA system has its own industrial process which is normally involving industrial specific networking protocols. No literature report has been found on how to use network traffic c monitoring management for the protection of the SCADA systems. In this chapter, an architecture of network traffic monitoring management is suggested as shown in Fig. for the protection of the SCADA systems.

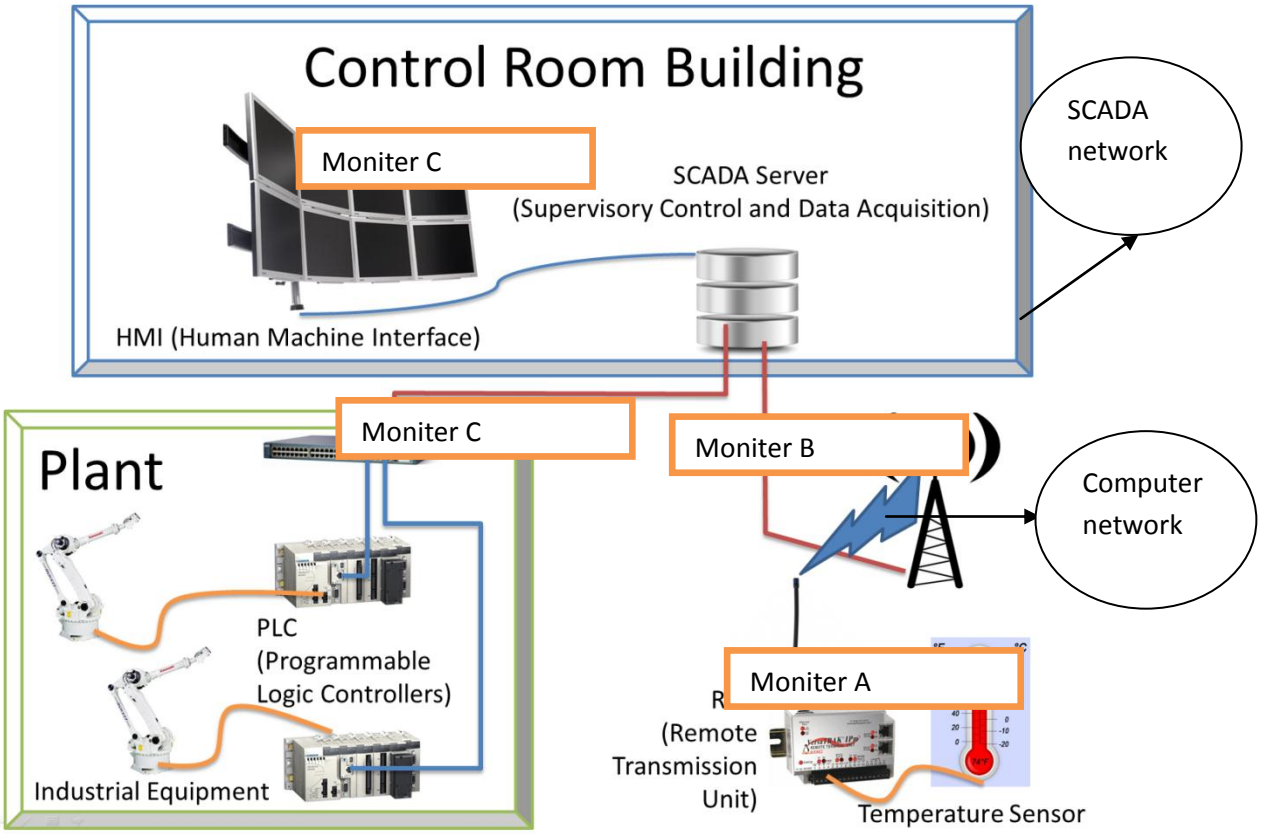



*Fig: Monitoring of SCADA server*

This is a distributed network traffic monitoring architecture. In this architecture, monitoring sensors A, B, C, and D are deployed in the system. Monitor A is deployed between the Corporate LAN and the firewall of the SCADA network .Monitor B is deployed immediately after the firewall of the SCADA network. This arrangement can monitor the network traffic attempting to access the SCADA system and network traffic that has eventually gone through the firewall. As new attack scan potentially penetrate the firewall, it is essential to monitor all traffic that has successfully passed the firewall. Monitor C is monitoring all traffic flowing with in the SCADA LAN.

**FUTURE ASPECTS FOR SECURITY IN SCADA**

**Cryptographic Protection of SCADA Communications**

Goal is to protect Master-Slave(RTU) communication links from a variety of active/passive attacks

• Develops standard "retrofit solution" for insecure communication links via "cryptographic modules" Dialup Frame Relay Microwave and other Serial Links

• Encryption and key management protocol developed specifically for low-latency applications

Low speed links

Short Messages

Request/Response

Polled Messages

## Addressing SCADA Control System Vulnerabilities

So what needs to be done?

Best Practices – policy, procedures, design and deployment of existing tools and technology

New Technology – identify limitations of existing products and technology, conduct mid-long term R&D to define requirements

Both require extensive testing and validation.

- Provides shared-key authentication
- Defines new SCADA Link Security (SLS) Protocol

**CONCLUSION**

Scada is the acronym for supervisory control and data acquisition which are industrial control systems. These systems are used to monitor various processes such as those involving the development of infrastructure and industrial processes. These systems however do not control processes in real time. The primary function of a SCADA system is to efficiently connect and transfer information from a wide range of sources, and at the same time maintaining data integrity and security. The security of SCADA networks is an important topic today due to the vital role that SCADA systems play in our national lives in providing essential utility services. Pervasive Internet accessibility at industrial work places increases the vulnerabilities of SCADA systems because this makes it possible for a remote attacker to gain control of, or cause disruption to the critical functions of the network.

## Refrences:


- Network monitoring tools,availableathttp://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html
- Technical white paper for NetStream, available at http://www.huawei.com/products/datacomm/pdf
- SandiaNational Laboratories, available at http://www.sandia.gov/scada/documents/pdf
- An engineering approach to computernetworking: ATM networks ,the internet, and the telephone network.
- Cisco: Introduction to CiscoIc OS NetFlow at technical overview.
- Shaw, T., "Energy Infrastructure Cyber Security: Pipelines—A Step-by-Step Guide for Keeping Pipeline Infrastructure Safe From All Cyber Attacks," Oil & Gas Journal Research Center, 2009.
- www .dpstele .com/training