An Analysis and Study on SCADA

Er. K. B. MOHD. UMAR ANSARI

BE(EEE), M.Tech (Electrical Power & Energy Systems), Ex-Engineer, PROTEQ, Gurgaon, India

ABSTRACT: SCADA stands for Supervisory Control and Data acquisition which is a process control system that enables a site operator to monitor and control process that is distributed among various remote sites. As such, it is a purely software package that is Positioned on top of hardware to which it is interfaced, in general via Programmable Logic Controllers (PLCs), or other commercial hardware modules. SCADA systems are combination of computers, controllers, instruments; actuators, networks and interfaces that manage the control of automated and allow analysis of those system by data collection and processing. They are used in most industrial processes: e.g. steel making, power generation (conventional and nuclear) and distribution, chemistry, but also in some experimental facilities such as nuclear fusion. The size of such plants ranges from a few 1000 to several 10 thousands input/output (I/O) channels. However, SCADA systems evolve rapidly and are now penetrating the market of plants with a number of I/O channels of several 100 K.

KEYWORDS: API, ERP, HMI, LAN, OPC, PLC, RTU, SCADA, SQL.

I.INTRODUCTION

A.SCADA EXPLAINED

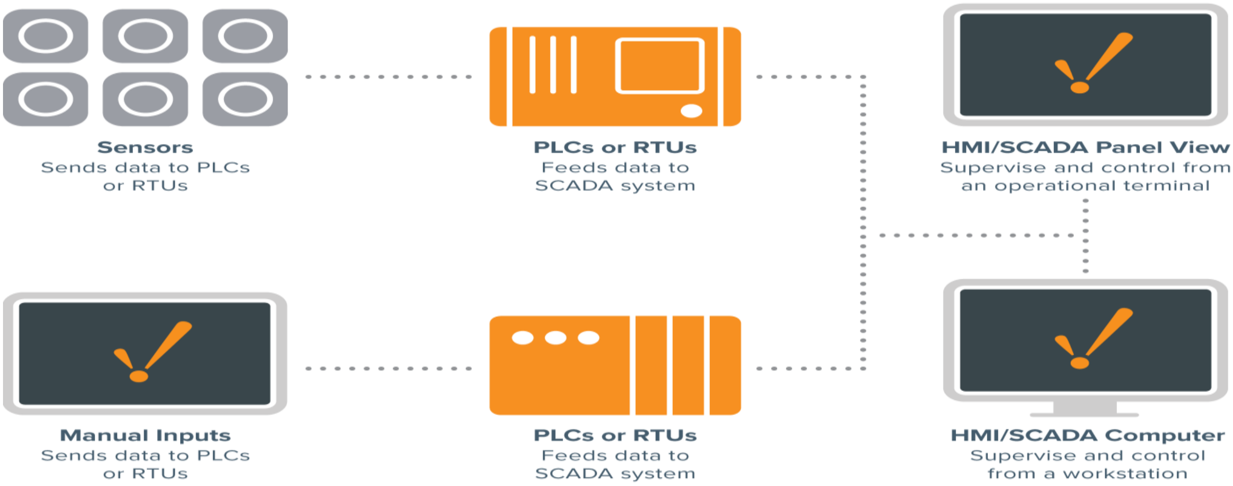
Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations
- Monitor, gather, and process real-time data
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
- Record events into a log file

SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.

The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software. The SCADA software processes, distributes, and displays the data, helping operators and other employees analyze the data and make important decisions.

For example, the SCADA system quickly notifies an operator that a batch of product is showing a high incidence of errors. The operator pauses the operation and views the SCADA system data via an HMI to determine the cause of the issue. The operator reviews the data and discovers that Machine 4 was malfunctioning. The SCADA system’s ability to notify the operator of an issue helps him to resolve it and prevent further loss of product.


Sensors
Sends data to PLCs or RTUs
PLCs or RTUs
Feeds data to SCADA system
HMI/SCADA Panel View
Supervise and control from an operational terminal
Manual Inputs
Sends data to PLCs or RTUs
PLCs or RTUs
Feeds data to SCADA system
HMI/SCADA Computer
Supervise and control from a workstation

B.WHO USES SCADA?

SCADA systems are used by industrial organizations and companies in the public and private sectors to control and maintain efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime. SCADA systems work well in many different types of enterprises because they can range from simple configurations to large, complex installations. SCADA systems are the backbone of many modern industries, including:

➢ Energy	➢ Oil and Gas	➢ Transportation
➢ Food and beverage	➢ Power	➢ Water and waste water
➢ Manufacturing	➢ Recycling	➢ And many more

Virtually anywhere you look in today's world; there is some type of SCADA system running behind the scenes: maintaining the refrigeration systems at the local supermarket, ensuring production and safety at a refinery, achieving quality standards at a waste water treatment plant, or even tracking your energy use at home, to give a few examples.

Effective SCADA systems can result in significant savings of time and money. Numerous case studies have been published highlighting the benefits and savings of using a modern SCADA software solution such as Ignition.

C.THE BIRTH OF SCADA

To understand the origins of SCADA, we must understand the problems industrial organizations are trying to solve. Before the concept of SCADA was introduced in the mid-20th century, many manufacturing floors, industrial plants, and remote sites relied on personnel to manually control and monitor equipment via push buttons and analog dials.

As industrial floors and remotes site began to scale out in size, solutions were needed to control equipment over long distances. Industrial organizations started to utilize relays and timers to provide some level of supervisory control without having to send people to remote locations to interact with each device.

While relays and timers solved many problems by providing limited automation functionality, more issues began to arise as organizations continued to scale out. Relays and timers were difficult to reconfigure, fault-find and the control panels took up racks upon racks of space. A more efficient and fully automated system of control and monitoring was needed.

In the early 1950s, computers were first developed and used for industrial control purposes. Supervisory control began to become popular among the major utilities, oil and gas pipelines, and other industrial markets at that time. In the 1960s, telemetry was established for monitoring, which allowed for automated communications to transmit measurements and other data from remotes sites to monitoring equipment. The term “SCADA” was coined in the early

1970s, and the rise of microprocessors and PLCs during that decade increased enterprises' ability to monitor and control automated processes more than ever before.

D.THE EVOLUTION OF SCADA

The first iteration of SCADA started off with mainframe computers. Networks as we know them today were not available and each SCADA system stood on its own. These systems were what would now be referred to as monolithic SCADA systems.

In the 80s and 90s, SCADA continued to evolve thanks to smaller computer systems, Local Area Networking (LAN) technology, and PC-based HMI software. SCADA systems soon were able to be connected to other similar systems. Many of the LAN protocols used in these systems were proprietary, which gave vendors control of how to optimize data transfer. Unfortunately, these systems were incapable of communicating with systems from other vendors. These systems were called distributed SCADA systems.

In the 1990s and early 2000s, building upon the distributed system model, SCADA adopted an incremental change by embracing an open system architecture and communications protocols that were not vendor-specific. This iteration of SCADA, called a networked SCADA system, took advantage of communications technologies such as Ethernet. Networked SCADA systems allowed systems from other vendors to communicate with each other, alleviating the limitations imposed by older SCADA systems, and allowed organizations to connect more devices to the network.

While SCADA systems have undergone substantial evolutionary changes, many industrial organizations continued to struggle with industrial data access from the enterprise level. By the late 1990s to the early 2000s, a technological boom occurred and personal computing and IT technologies accelerated in development. Structured query language (SQL) databases became the standard for IT databases but were not adopted by SCADA developers. This resulted in a rift between the fields of controls and IT, and SCADA technology became antiquated over time.

Traditional SCADA systems still use proprietary technology to handle data. Whether it is a data historian, a data connector, or other means of data transfer, the solution is messy and incredibly expensive. Modern SCADA systems aim to solve this problem by leveraging the best of controls and IT technology.

E.MODERN SCADA SYSTEMS

Modern SCADA systems allow real-time data from the plant floor to be accessed from anywhere in the world. This access to real-time information allows governments, businesses, and individuals to make data-driven decisions about how to improve their processes. Without SCADA software, it would be extremely difficult if not impossible to gather sufficient data for consistently well-informed decisions.

Also, most modern SCADA designer applications have rapid application development (RAD) capabilities that allow users to design applications relatively easily, even if they don't have extensive knowledge of software development.

The introduction of modern IT standards and practices such as SQL and web-based applications into SCADA software has greatly improved the efficiency, security, productivity, and reliability of SCADA systems.

SCADA software that utilizes the power of SQL databases provides huge advantages over antiquated SCADA software. One big advantage of using SQL databases with a SCADA system is that it makes it easier to integrate into existing MES and ERP systems, allowing data to flow seamlessly through an entire organization.

Historical data from a SCADA system can also be logged in a SQL database, which allows for easier data analysis through data trending.

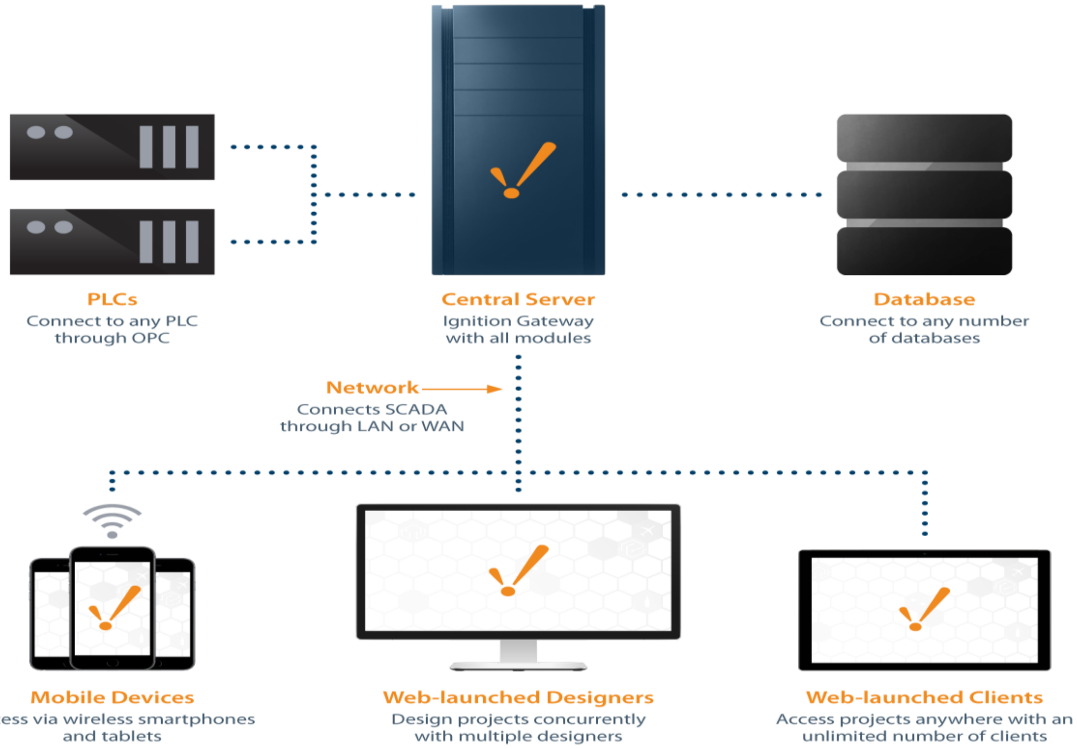
F.LEARN ABOUT IGNITION - THE NEW SCADA: IGNITION HMI/SCADA SOFTWARE

Ignition by Inductive Automation® is an industrial automation software platform that many businesses and organizations have switched to for their HMI/SCADA needs.

Ignition has been installed in thousands of locations in over 100 countries since 2010. Its powerful and robust nature allows SCADA system integrators to reach the demands of their customers while costing less than other SCADA software solutions. Here are a few reasons why more enterprises are choosing Ignition:

- Ignition uses modern IT practices that make it compatible with current SCADA system components.
- Its unique licensing model lets users pay a flat fee based on the number of servers. Other SCADA vendors typically charge per client or per tag, but Ignition offers unlimited clients and tags.
- Ignition is web-deployable: it can be downloaded and installed in a few minutes, and clients can be launched or updated instantly.

Inductive Automation's motto of "Dream It, Do It" is a perfect embodiment of what Ignition can do. While its bold claims may sound too good to be true, one demonstration of the software proves how powerful it really is. Once you see what's possible, you'll begin to imagine how the software can fit your SCADA needs and open up new possibilities.


PLCs
Connect to any PLC through OPC
Central Server
Ignition Gateway with all modules
Database
Connect to any number of databases
Network
Connects SCADA through LAN or WAN
Mobile Devices
Access via wireless smartphones and tablets
Web-launched Designers
Design projects concurrently with multiple designers
Web-launched Clients
Access projects anywhere with an unlimited number of clients

II.ARCHITECTURE

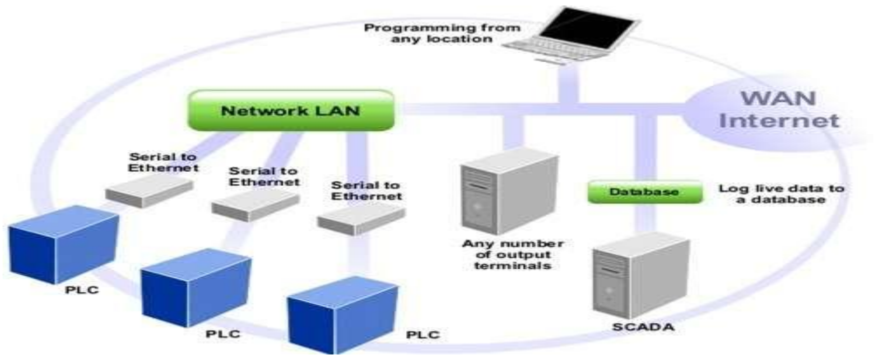
A SCADA System usually consists of the following subsystems:

- A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through this, the human operator monitors and controls the process.
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process.
- Remote Terminal Units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.
- Programmable Logic Controller (PLCs) used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- Communication infrastructure connecting the supervisory system to the Remote Terminal Units.

First generation: "Monolithic": 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.

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.

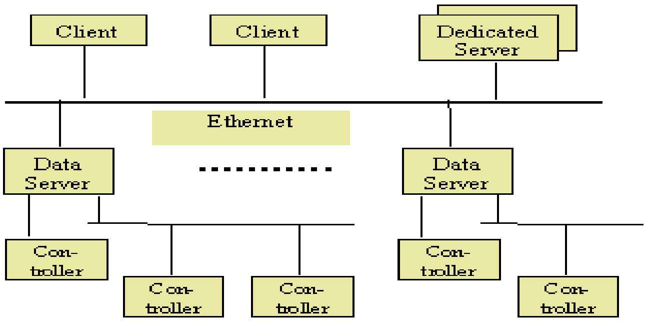
Third generation: "Networked": These are the current generation SCADA systems which use open system architecture rather than a vendor-controlled proprietary environment. The SCADA system utilizes open standards and protocols, thus distributing functionality across a WAN rather than a LAN. It is easier 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.



SCADA Architecture

A. HARDWARE ARCHITECTURE

Basic layers in a SCADA system can be classified in two parts generally: the "client layer" which caters for the man machine interaction and the "data server layer" which handles most of the process data control activities. The data servers communicate with devices in the field through process controllers.



Hardware Architecture Diagram

Process controllers, e.g. PLCs, are connected to the data servers either directly or via networks or field buses. Data servers are connected to each other and to client stations via an Ethernet LAN. The data servers and client stations are NT platforms but for many products the client stations may also be W95 machines.

Remote Terminal Unit (RTU): The RTU connects to physical equipment. Typically, an RTU converts the electrical signals from the equipment to digital values such as the open/closed status from a switch or a valve, or measurements such as pressure, flow, voltage or current. By converting and sending these electrical signals out to equipment the RTU can control equipment, such as opening or closing a switch or a valve, or setting the speed of a pump.

Supervisory Station: The term "Supervisory Station" refers to the servers and software responsible for communicating with the field equipment (RTUs, PLCs, etc), and then to the HMI software running on workstations in the control room, or elsewhere. In smaller SCADA systems, the master station may be composed of a single PC. In larger SCADA systems, the master station may include multiple servers, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server failure

B. SOFTWARE ARCHITECTURE

The products are multi-tasking and are based upon a real- time database (RTDB) located in one or more servers. Servers are responsible for data acquisition and handling. (E.g. polling controllers, alarm checking, calculations, logging and archiving) on a set of parameters, typically those they are connected to. However, it is possible to have dedicated servers for particular tasks, e.g. data logger a SCADA architecture that is generic for the products that were evaluated.

C. HUMAN-MACHINE INTERFACE (HUI)

A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through which the human operator controls the process. An HMI is usually linked to the SCADA system's databases and software programs, to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides. The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram. This means that the operator can see a schematic representation of the plant being controlled.

D. COMMUNICATIONS

Internal Communication: Server-client and server-server communication is in general on a publish-subscribe and event-driven basis and uses a TCP/IP protocol, i.e. a client application subscribes to a parameter which is owned by a particular server application and only changes to that parameter are then communicated to the client application.

E. INTERFACING

Application Interfaces / Openness The provision of OPC client functionality for SCADA to access devices in an open and standard manner is developing. There still seems to be a lack of devices/controllers, which provide OPC server software, but this improves rapidly as most of the producers of controllers are actively involved in the development of this standard. OPC is currently being evaluated by the CERN-IT-CO group [4]. The products also provide:

- an Open Data Base Connectivity (ODBC) interface to the data in the archive/logs, but not to the configuration database,
- an ASCII import/export facility for configuration data,
- a library of APIs supporting C, C++, and Visual Basic (VB) to access data in the RTDB, logs and archive.

The API often does not provide access to the products internal features such as alarm handling, reporting, trending, etc. The PC products provide support for the Microsoft standards such as Dynamic Data Exchange (DDE) which allows e.g. to visualize data dynamically in an EXCEL spreadsheet, Dynamic Link Library (DLL) and Object Linking and Embedding (OLE).

Database: The configuration data are stored in a database that is logically centralized but physically distributed and that is generally of a proprietary format. For performance reasons, the RTDB resides in the memory of the servers and is also of proprietary format. The archive and logging format is usually also proprietary for performance reasons, but some products do support logging to a Relational Data Base Management System (RDBMS) at a slower rate either directly or via an ODBC interface.

F. SCALABILITY

Scalability is understood as the possibility to extend the SCADA based control system by adding more process variables, more specialized servers (e.g. for alarm handling) or more clients. The products achieve scalability by having multiple data servers connected to multiple controllers. Each data server has its own configuration database and RTDB and is responsible for the handling of a sub-set of the process variables (acquisition, alarm handling, archiving.

G. REDUNDANCY

The products often have built in software redundancy at a server level, which is normally transparent to the user. Many of the products also provide more complete redundancy solutions if required.

Functions of SCADA

1. Data Acquisition

In SCADA systems, MTU performs the periodic acquisition of data from RTUs. As discussed above that the RTU can respond in either a request form the MTU or continuously transferring the data when changes of state of a parameter takes place or when limits of the parameter exceeded, even without a request from the MTU.
The data acquisition process includes internal scanning of RTU internal database, periodic RTU polling by MTU, transmission of data by RTU to MTU, scaling of data into engineering units and updating a previous value or state in the database.

2. Human Machine Interface (HMI)

SCADA products display the information on multiple screens, which combines both text and synoptic diagrams. It provides the provision for human operators to continuously monitor the operations and to intervene when necessary.
SCADA HMI software consists of library of graphical symbols to which tag names are associated for a particular device or parameter such as ON/OFF status of switch, level information on tank, etc.).
Display selection on HMI is organized mostly in a tree structure, where index pages allow human operator to select various displays using a cursor, keyboard, trackball, or touch-screen positioning techniques.

3. Supervisory Control

It is the process of controlling the equipment operations from remote locations. In SCADA systems, the MTU in the master station sends the control instructions such as set points and discrete control commands to the RTU at remote station. At the remote stations, RTU receives the commands and accordingly controls the appropriate actuator.
The supervisory control includes selection of the remote station, choosing the device to be controlled and executing the desired command such as close or trip. Most of the systems employ check-before-operate method for correct selection and operation of the equipment in the remote place.

4. Trending

All SCADA products provide trending facilities which display the gathered (real-time) or saved (historian) data on various charts. The parameters to be trended on a specific chart can be defined online or it can be predefined.
These charts are able to display one or more parameter using one or more plots. It provides the automatic scrolling of data with enhanced zoom features. Historian trending is possible with archived databases.

5. Alarm Processing

It involves in alerting the operator to unscheduled events by informing place of occurrence, time of occurrence, device ID and nature of the event.

Alarms are logically programmed on the master control station by comparing the received data with appropriate limits. It is possible to handle alarms on multiple priority level. Alarms can be suppressed either by individual or as a complete group.

6. Information Storage and Reports

SCADA stores the gathered data on either disks or permanent storage devices. The logging of data is performed on a cyclic basis, which means the time span of a rotating historical file is limited (which can be 40 days or 12 months). Once the period is completed or the log is full, it archives the data to permanent storage device and then the information older than the file time span is discarded. This allows the user to retrieve and analyze the data whenever it is needed. SCADA provides the report generation using SQL type queries. The historical file provides the source of information for generating various reports. SCADA also facilitates to print and archive reports.

7. Automation

The majority of the products allow actions to be automatically triggered by events. A scripting language provided by the SCADA products allows these actions to be defined. In general, one can load a particular display, send an Email, run a user defined application or script and write to the RTDB.

The concept of recipes is supported, whereby a particular system configuration can be saved to a file and then re-loaded at a later date. Sequencing is also supported whereby, as the name indicates, it is possible to execute a more complex sequence of actions on one or more devices. Sequences may also react to external events. Some of the products do support an expert system but none has the concept of a Finite State Machine (FSM).

Applications of SCADA

The characteristics such as flexibility, reliability and scalability of SCADA have made its extensive use in automating complex systems.

There are numerous real-world applications where SCADA already been successful in delivering monitoring and control solutions over a wide range of industries, ranging from energy production to agricultural systems. Some of these applications are given below.

Waste Water Treatment

The waste water treatment involves in filtering the raw water from wells or surface and to discharge the clean water into the distribution system. The processing areas in the water treatment process include low lift or raw water station, pre-treatment, filtration, high lift or treated water station and chemical injection systems.

Here, each stage is employed with PLCs as RTUs along with sensors and actuators for field level monitoring and control of operations. SCADA system enables the central monitoring thorough HMI workstations by gathering data via communication network from various stages of water treatment.

Electrical Power Distribution System

SCADA system automates the electrical distribution tasks with the use of intelligent electronic devices (IEDs) as RTUs. SCADA supervises the entire distribution system so as to reduce the duration of outages and for an optimum operation. The functions of SCADA in power distribution system include substation control, feeder control and end user load control.

RTUs/ IEDs in a substation, feeder, or end use installations gather the field data, including status of switches, transformers, circuit breakers, fault information, energy consumption and billing.

At the central monitoring side, MTU receives the data from RTUs, displays it on HMIs, provides the data trending and logging. It also maintains the desired level of currents, voltages, and power factor and correspondingly generates the alarms and sends back control signals to remote stations.

Power Generating Stations

In thermal power plants, various equipments are distributed over plant area, which all are connected with SCADA systems. The SCADA enables monitoring and control of numerous boilers, turbines and pumps.

SCADA automates and supervises the operations of the plant, including pulverizing of coal, control of steam flow, turbine start/stop status, water control into the boiler, power distribution and control.

In case of wind power plants, SCADA provides the real time visibility of the remote plant and facilitates the control of plant remotely and centrally. In this, SCADA controls the wind turbines during start-up, power production, shutdown and stopped (faulty) cases. Also, it provides online data, histories, alarms and the HMI.

Industrial Control

SCADA usage is often found in many industrial applications including manufacturing industries (steel plants), process industries, oil and gas industries, food processing, and so on.

SCADA integration into the industries processes results higher production rates, increases quality of products and provides the cost-effective operation. In these industries PLCs plays a major role in dealing with field parameters and to transfer them to the central controlling station.

III.SECURITY ISSUES

The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems and office networks and the Internet has made them more vulnerable to attacks. Consequently, the security of SCADA-based systems has come into question as they are increasingly seen as extremely vulnerable to cyber warfare/cyber terrorism attacks. In particular, security researchers are concerned about:

- ➢ the lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks
- ➢ the belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
- ➢ the belief that SCADA networks are secure because they are physically secured
- ➢ the belief that SCADA networks are secure because they are disconnected from the Internet.
- ➢ a Driver Development Toolkit to develop drivers for hardware that is not supported by the SCADA product. Parameter values at the cursor position can be displayed.
- ➢ The trending feature is either provided as a separate module or as a graphical object (ActiveX), which can then be embedded into a synoptic display. XY and other statistical analysis plots are generally not provided.

EVOLUTION

SCADA vendors release one major version and one to two additional minor versions once per year. These products evolve thus very rapidly so as to take advantage of new market opportunities, to meet new requirements of their customers and to take advantage of new technologies. Most of the SCADA products that were evaluated decompose the process in “atomic” parameters to which a Tag-name is associated. This is impractical in the case of very large processes when very large sets of Tags need to be configured. As the industrial applications are increasing in size, new SCADA versions are now being designed to handle devices and even entire systems as full entities (classes) that encapsulate all their specific attributes and functionality. In addition, they will also support multi-team development. As far as new technologies are concerned, the SCADA products are now adopting:

- ➢ Web technology, ActiveX, Java, etc.

- OPC as a means for communicating internally between the client and server modules. It should thus be possible to connect OPC compliant third party modules to that SCADA product.

IV.ENGINEERING

One should rightly anticipate significant development and maintenance savings by adopting a SCADA product for the implementation of a control System. The need for proper engineering can’t be sufficiently emphasized to reduce development effort and to reach a system that complies with the requirements, that is economical in development and maintenance and that is reliable and cheap. Examples of engineering activities specific to the use of a SCADA system are the definition of:

- a library of objects (PLC, device, subsystem) complete with standard object behaviour (script, sequences, ...), graphical interface and associated scripts for animation,
- templates for different types of "panels", e.g. alarms, * instructions on how to control e.g. a device ...,
- a mechanism to prevent conflicting controls (if not provided with the SCADA),
- alarm levels, behaviour to be adopted in case of specific alarms, ...

V.CONCLUSION: POTENTIAL BENEFITS OF SCADA

The benefits one can expect from adopting a SCADA system for the control of experimental physics facilities can be summarized as follows:

- A rich functionality and extensive development facilities. The amount of effort invested in SCADA product amounts to 50 to 100 p-years!
- The amount of specific development that needs to be performed by the end-user is limited, especially with suitable engineering.
- Reliability and robustness. These systems are used for mission critical industrial processes where reliability and performance are paramount. In addition, specific development is performed within a well-established framework that enhances reliability and robustness.
- Technical support and maintenance by the vendor.
- Using a SCADA system for the controls ensures a common framework not only for the development of the specific applications but also for operating the detectors. Operators experience the same "look and feel" whatever part of the experiment they control. However, this aspect also depends to a significant extent on proper engineering.

VI.FUTURE SCOPE & TRENDS IN SCADA

North American Electric Reliability Corporation has specified that electrical system data should be time-tagged to the nearest millisecond. Electrical system SCADA systems provide this Sequence of events recorder function, using Radio clocks to synchronize the RTU or distributed RTU clocks.

SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Although certain characteristics of frame-based network communication technology (determinism, synchronization, protocol selection, environment suitability) have restricted the adoption of Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

A few vendors have begun offering application specific SCADA systems hosted on remote platforms over the Internet.

SCADA systems are becoming increasingly ubiquitous. Thin clients, web portals, and web based products are gaining popularity with most major vendors. The increased convenience of end users viewing their processes remotely introduces security considerations. While these considerations are already considered solved in other sectors of Internet services, not all entities responsible for deploying SCADA systems have understood the changes in accessibility and threat scope implicit in connecting a system to the Internet.

REFERENCES

1. IEEE Tutorial Course—Fundamentals of Supervisory Control Systems.

2. "ANSI/IEEE Standard C37.1-1979", Definition Specification and Analysis of Manual Automatic and Supervisory Station Control and Data Acquisition, 1987.

3. IEEE Recommended Practice for Master/Remote Communications, Jan. 1986.

4. IEEE Std C37.1TM-2007, "IEEE Standard for SCADA and Automation Systems" IEEE Power and Energy Society, IEEE, USA, 2008, pp. 19-21.