Supervisory Control and Data Acquisition

Aditya Bagri
Thadomal Shahani Engineering College, Mumbai University
Maharashtra, India

Richa Netto
Thadomal Shahani Engineering College, Mumbai University
Maharashtra, India

Dhruvil Jhaveri
Thadomal Shahani Engineering College, Mumbai University
Maharashtra, India

ABSTRACT
Since the advent of control systems, SCADA has played an important role in the field of automation. SCADA systems offer a means of controlling remotely located devices in an industrial process. Supervisory control can be combined with data acquisition wherein the data is obtained from the devices and it is processed further according to the user's needs. This paper offers an insight into the functioning of a typical SCADA system and its applications in the real world. The types of architecture of such control systems have been studied, along with an overview of the security concerns pertaining to them.

General Terms
Control Systems

Keywords
Data Acquisition, Human Machine Interface, Network Protocol, Process Control, Programmable Logic Controllers, Remote Terminal Unit, Sensors

1. INTRODUCTION
Industrial processes existing in the physical world are monitored and regulated by computer-controlled systems called Industrial Control Systems (ICS). SCADA (Supervisory Control and Data Acquisition) falls under the category of Industrial Control Systems.

Complexes of systems, or entire sites are monitored and controlled by integrated systems, more commonly denoted by SCADA.[1] It is a technology that offers users the potency to send control directives to and collect information from one or more distant facilities. SCADA eliminates the need of human presence at the remote facilities where standard operations take place.[2] Industrial processes worldwide are controlled by SCADA. It facilitates reduction of costs and increased efficacy along with an upsurge in the profitability of operations.

Over the last few years, considerable progress has been observed in terms of scalability, functionality, openness and performance of SCADA systems. They have even been considered as alternatives to in house development for extremely complicated and demanding control systems like the ones that are a part of physics experiments.[3]

2. WHAT IS SCADA?
A SCADA (supervisory control and data acquisition) has been present ever since there have been control systems. Data acquisition in the first SCADA systems was done using panels of meters, lights and strip chart recorders. Supervisory control was carried out by the operator who manually operated various control knobs. Such systems are still being used in factories, plants and power generating facilities.[4]

SCADA systems are a type of Industrial Control System. They are used to gather information and exercise control from remote locations. In situations where integrated data procurement is as significant as control, SCADA systems are employed to monitor remote units. These systems find applications in distribution processes such as water supply and wastewater collection systems, oil and gas pipelines, electrical utility transmission, and rail and other public transportation systems.

SCADA applications are comprised of two elements, namely, the process/machinery/system that needs to be controlled and an interconnection of devices which form an interface with the process under consideration via sensors and control outputs. This interconnection that allows the user to measure and monitor explicit elements of the said process, is the SCADA system.

SCADA systems perform consolidated control for various process inputs and outputs by integrating Human Machine Interface (HMI) software and data transmission systems with data acquisition systems.[5] The transfer of data between operator terminals, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), and the central host computer is included in SCADA systems.

A SCADA system collects relevant data, transfers the data back to a central site, then notifies the home station about the event, implementing the required analysis and control, and then displays the data in a logical and systematic manner using graphs or text, thus enabling the operator to control a whole process in real time. Public Switched Network (PSN) was used for control purposes in conventional SCADA systems. At present, the infrastructure provided by corporate Local Area Network (LAN) or Wide Area Network (WAN) is used to control a variety of systems. Monitoring is also carried out by extensively deploying wireless technologies.[6]

The two types of components that form a part of SCADA systems are:

i. Hardware: This usually comprises of a Master Terminal Unit (MTU) located at a control center, communications equipment such as cable, satellite, radio, etc. and one or more geographically dispersed field sites constituting of a RTU or a PLC that controls actuators and/or sensors.

ii. Software: Programming of the software is carried out to instruct the system about the parameters that need to be considered, their

permissible ranges and the response to be generated upon occurrence of an anomaly.[5]

client and collects time stamped data as well as other information about events and alarms. This helps in creating graphical trends and a database

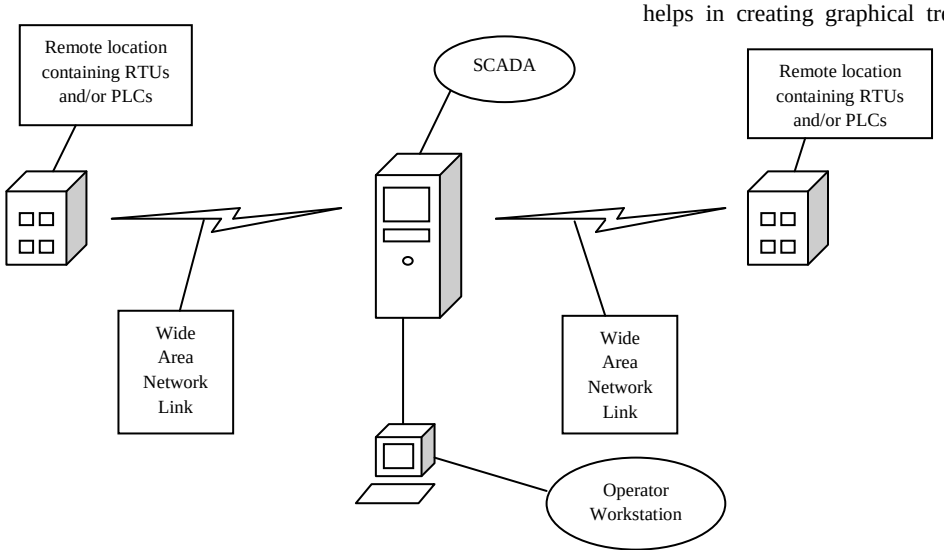

Fig 1: A typical SCADA system

When a process is widely distributed, SCADA allows an operator to be present at a central location and make set point changes on distant process controllers. The changes may comprise of opening or closing of valves and switches, gathering measurement information, and monitoring alarms. As they reduce the number of routine visits by the operator, the benefits of SCADA systems in terms of cost reduction are especially observed when the dimensions of the process become very large.[2]

3. COMPONENTS

A typical SCADA system consists of the following subsystems:

- Remote Terminal Units (RTUs): RTUs are small, computerized electronic devices controlled by a microcontroller. They are deployed in the field at specific sites and locations and connected to the sensors.[7] RTUs are points where information is gathered from sensors and commands are delivered to control relays. They also convert sensor signals to digital data.
- Programmable Logic Controllers (PLCs): They are similar to RTUs in functionality. PLCs are sometimes used as a replacement for RTUs owing to their lesser cost, diversity and flexibility.
- A Telemetry System: PLCs and RTUs are connected with the various other components in the process. This is done using a telemetry system.
- Data Acquisition Server: It connects the software to field devices so that clients can obtain information from them.
- Sensors and Control Relays: These directly interface with the system.
- Human Machine Interface (HMI): The HMI device is like an interface between the client and the SCADA system. Through it, the operator can control and manage the process while at the same time requesting data from the server.
- A Historian: It requests data from the server like a that can be queried.
- SCADA Master Unit: These are large computers that acquire data and control the system. Master Units are like central processors that regulate the managed system on the basis of sensor inputs.
- A Communication Networks: It connects the SCADA Master Unit to the RTUs.

4. WORKING

SCADA systems comprise of telemetry and data acquisition. SCADA incorporates gathering of data, conveying it back to the central unit, performing any required examination and control followed by presenting the data on numerous operator displays. The necessary control tasks are then communicated back to the process.

The SCADA working principle encompasses the following four functions:

i. Data acquisition
ii. Networked data communication
iii. Data presentation
iv. Control [7]

These functions are elaborated as follows:

Various types of sensors such as those of pressure, temperature, Hall Effect etc are set at assorted locations in the industrial installations where perpetual monitoring is necessary. The various parameters are continuously measured by these sensors and their observations are conveyed to the microcontroller for further processing. Accurate working of the plant and frequent assessment is crucial to these places but human involvement presents severe accidental threats and also causes operational losses. To solve this, sensors are placed at critical sites rather than human monitoring.

The microcontroller is fixed on to the general-purpose microcontroller board. It implements an appropriate algorithm to convert readings, based on the inputs that it receives, into standard units. The microcontroller board is also connected to

a wireless network protocol such as GSM, Internet, Bluetooth, and ZigBee. These provide for smooth transmission of information from remote areas to the central control unit. At the receiver end, the data is presented on the computer screen where human supervision is applied and hence the distant sections of the industrial unit are controlled from one common site. The supervisor is immediately instructed by the system in the event of an anomaly and financial and operational losses are avoided.[1]

5. ARCHITECTURE

The expansion and augmentation of modern computing technology has paralleled the evolution of SCADA systems. The four classifications of the generations of SCADA systems are as follows:

i. First Generation – Monolithic: This period refers to the time when computing represented standalone 'Mainframe Computers'. Networks were nearly non-existent. There existed a line dedicated exclusively for the purpose of communication, linking the RTU and the central computer. The vendors developed protocols to agreeably match their own market and did not offer either inter-market compatibility or flexibility of functionality. Linking a similar mainframe at the bus level offered redundancy.

ii. Second Generation – Distributed: Computing load was distributed through numerous systems utilizing LAN networks to its advantage. Every system was assigned a particular operation such as communication processor, calculation processor, database server etc. This was geographically constrained and was not suitable for widely distributed systems. Communication between the RTUs and the main distributed network was made available by the use of WAN which remained unchanged.

iii. Third Generation – Networked: Following up on the second generation, it pursues open system architecture instead of vendor-controlled environment. Open standards allay many restrictions permitting cross vendor compatibility and the utilization of any off-the-shelf standard product. This paved the way for companies such as HP, Compaq and Sun Microsystems to pursue hardware manufacturing and made the vendors move out of it. An additional layer of security to the data and improved disaster survivability is implemented by the use of WAN networks like Internet Protocol for communication to separate the main master station from the network by using an intervening communications server.

iv. Fourth Generation - "Internet of Things": To facilitate a significant reduction in infrastructure costs and an increase in the ease of maintenance and integration, SCADA systems have progressively embraced the Internet of Things technology; a move that has been corroborated by the commercial availability of cloud computing. SCADA systems are now capable of reporting the status of a process in near real-time. They are now able to implement more complicated control algorithms than are pragmatically feasible to execute on conventional systems. Moreover, the use of open protocols for networking, like TLS, is inherent in the Internet of Things technology; thus providing a highly understandable and manageable security boundary.[6]

6. PROTOCOLS

The Internet provides us with open systems that are freely accessible by all, thus allowing rapid transmission of information to all stakeholders in an organization. This greatly helps in the reduction of costs.[4]

Hence, conventional SCADA systems are increasingly being built upon Internet-based protocols. With time, this will allow the suppliers to emphasize on delivering excellent application software. These systems will be developed with support from open Internet protocols that are used to connect the various elements of a network together.

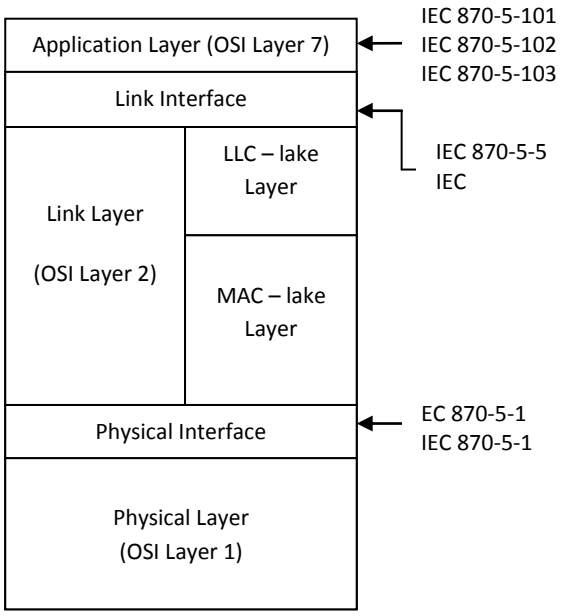

Fig 2 : Protocols and Layers

The Remote Terminal Unit (RTU) in a SCADA system usually has no information about what it is measuring; it follows orders given to it and sends back a report containing the results. The master station, on the other hand, needs to have complete information about what the data is and who needs to use it.

There are protocols to be followed for the same. Each protocol has two parts:

- The Master Protocol, comprising of the statements from the master RTU.
- The RTU Protocol, comprising of the instructions from RTU to the main computer.

The master and the RTU communicate, forming a model for RTU to Intelligent Electronic Device (IED) Communications. The most widely known model is the International Electrotechnical Commission (IEC) 60870-5 series and the Distributed Network Protocol version 3 (DPNP3).

7. SECURITY

SCADA systems have evolved over the years. Recently, they have been based on open standards. Suppliers of SCADA systems have started to adopt the Transmission Control Protocol/Internet Protocol (TCP/IP) and Ethernet communications. Several of them have encapsulated their registered protocols in TCP/IP packets.

Although the evolution towards more open-based standards has simplified the integration of various diverse systems together, it has also intensified the threat of less technical employees gaining access and control of these industrial networks. Examples of threats that open standards based SCADA systems can be exposed to are Denial of Service attacks, System Downtime, Trojans, keyloggers for password stealing, defamation, etc. Specific and specialized security layers are hence needed for SCADA systems.

In addition to the usual, steadily increasing cyber threats, several factors have contributed to the growth of risks in control systems. These include:

i. Implementation of standardized technologies with known vulnerabilities.
ii. Connectivity of control systems to other networks.
iii. Constraints on the use of existing security technologies and practices.
iv. Insecure remote connections.
v. Widespread availability of technical information about control systems. [6]

There are numerous tools and techniques that can be used to manage the threats to SCADA systems. A major design consideration is the flexibility that should be provided by the security configurations. Each industry must determine the goals of their organization and arrive at a cost effective solution to these issues.

Compromises to SCADA systems would impact multiple areas of the society; therefore the security of such systems is essential. For example, all customers receiving electricity from a source whose electrical SCADA system is compromised, thus causing a blackout would suffer monetary losses and inconvenience.

8. APPLICATIONS

The SCADA technology has a diverse range of potential applications. This is due to the fact that several industries need the comprehensive monitoring and control capabilities that SCADA systems offer. Physical processes are commonly managed by these control systems.

Some of the most common applications of SCADA systems are:

- Electric power generation, distribution and transmission: Electric utilities make use of SCADA systems to observe the flow of current and line voltage, to control the operation of circuit breakers and to switch on or off various sections of the power grid.
- Gas utilities: SCADA tools are required to monitor the flow of gas through the circulation chain and also maintain the supporting telecom infrastructure online.
- Water and sewage: Local government water utilities make use of these control systems to manage and regulate the movement of water, reservoir levels, pipe pressure and other aspects. Wastewater managing plants make use of flow rate and contaminant sensors.
- Buildings, facilities and environments: Facility managers use SCADA to monitor heating, ventilation and air conditioning systems, cooling units like refrigerators, entry and lighting systems.
- Manufacturing: Handling the records of parts, managing industrial automation and robots and monitoring process and quality control is done by SCADA systems to ensure that productivity targets are met.The systems track the number of units manufactured in a production line and their respective stages of completion.
- Mass transit: Transport authorities make use of SCADA systems to regulate electricity to trams and subways; to automate traffic signals for railways and roads and detect ones that are out-of-order; to track and find trains and buses; and to control traffic flow.

9. RESULT

SCADA systems are of great significance in process control. They can be used for a wide range of applications, both small, like climate control, and large, like monitoring a nuclear plant or mass transportation system. This has lead to proliferation in the use of SCADA systems across a multitude of industries. As demonstrated by the figure below, the importance of SCADA system benefits among its users includes an array of characteristics.

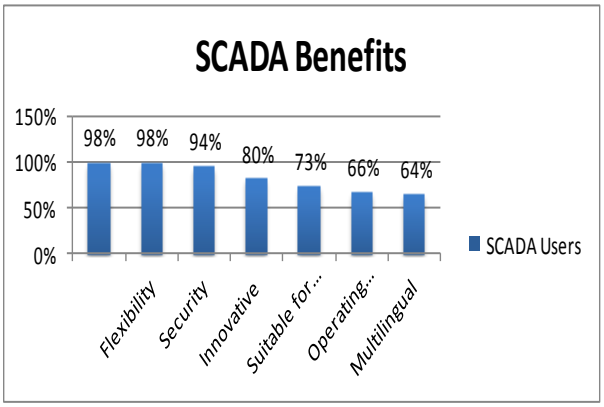

Fig 3 : Importance of SCADA system benefits according to users

SCADA systems are extremely cost efficient; fewer personnel are needed to control equipment at remote locations and manage maintenance problems thus resulting in a considerable reduction in operation, maintenance and training costs. Also, these systems can be configured for several applications, thereby obviating the need for tailored software development. Since they are primarily used in mission critical manufacturing processes, where reliability and productivity is of utmost importance, SCADA systems are designed to be robust. The ease of integration with existing business systems has lead to an increase in production and portability. Finally, SCADA systems aid in analysis and control of the quality of the manufactured product with the help of standard SCADA functionality.

10. CONCLUSION

SCADA has come a long way from the obscurity of research labs into the industrial environment and the everyday discussions of people. SCADA systems have grown roots everywhere, from power generation plants to automobile factories; from regulating and controlling the water we drink and air we breathe to monitoring transport systems. It greatly reduces operating costs of human resources as personnel no longer need to waste time wandering all over the site, while simultaneously improving the reliability and performance of the system. Since SCADA systems also indicate the level of risk and threat, the need for site visits can be converted into a far more judiciously prioritized decision.

Although technical merit is credited as a desirable attribute of any control system, the driving force in today's industries is the rapid reduction of costs.[4] As companies attempt to increase their profits out of plants and governments raise the capacities of municipal structures in plants, SCADA systems will proliferate and help deliver precise data and employ complete control over processes.

11. ACKNOWLEDGEMENT

The authors wish to thank Mr. Aashish Jha, lead trainer at the Hewlett Packard Educational Services-Summer Training Program, 2014, India.

12. REFERENCES

[1] Chandini A, Jaishree Sain J, Pande Appurv Prasad, Sayeda Banu and Rajeswari P, "SCADA: Data Acquisition and Industrial Automation through Smart Systems", International Conference on Electronics and Communication Engineering, Apr. 2013.

[2] Cornel Antal and Teodor Maghiar, "Automatic Control Data Acquisition (SCADA) for Geothermal Systems", International Summer School, 2001.

[3] A. Daneels and W. Salter, "What is SCADA?", International Conference on Accelerator and Large Experimental Pysics Control Systems, 1999.

[4] David Bailey and Edwin Wright, "Practical SCADA for Industry", IDC Technologies, pp. 1-36, 2003.

[5] Keith Stouffer, Joe Falco, and Karen Kent, "Guidelines to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security", National Institute of Standards and Technology Special Publication, pp. 3-7, Sept. 2006.

[6] "Supervisory Control and Data Acquisition (SCADA) Systems", Technical Information Bulletin, National Communications System, Oct. 2004.

[7] Rajeev Kumar Chauhan, M. L. Dewal, and Kalpana Chauhan, "Intelligent SCADA System", International Journal on Power System Optimization and Control, vol.2, no. 1, 2010.

[8] Boyer S., 2009 SCADA: Supervisory Control And Data Acquisition. Instrument Society of America.

[9] Benoit Rohee and Bernard Riera, "Advanced supervisory control for manufacturing systems: from concepts to a separated monitoring system", International Journal of Intelligent Systems Technologies and Applications, Volume-6, No.3/4 pp. 381 – 401, 2009.

[10] U. S. Patil, "Study of Wireless Sensor Network in SCADA System for Power Plant", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Volume-1, Issue-2, 2011.

[11] Sandip C.Patel and Pritimoy Sanyal, "Securing SCADA System", Information Management & Computer Security Journal, Volume-16, Issue-4, pp. 398 – 414, 2008.

[12] Stuart G. McGrady, 2013 Designing SCADA Application Software – A Practical Approach. Elsevier Inc.

[13] Frank Lamb, 2013 Industrial Automation Hands-On. McGraw Hill Education.

[14] Chikuni, E. and Dondo, M., "Investigating the security of electrical power systems SCADA," AFRICON 2007 - Inst vol., no., pp.1,7, 26-28, , Sept. 2007.