ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# SCADA (SUPERVISORY CONTROL & DATA ACQUISITION) FOR ISOLATED INDUSTRIALIZED FRAMEWORKS APPLICATIONS

**Aruna Rai Vadde*, Radhakrishna Bokka**

* Department of Electrical and Compter Engineering, College of Engineering and Technology, Wollega University, Ethiopia

Department of Electrical and Computer Engineering, College of Engineering and Technology, Hawassa University, Ethiopia

## ABSTRACT

SCADA frameworks are generally utilized as a part of industry for Supervisory Control and Data Acquisition of mechanical methodologies. Organizations that are individuals from institutionalization boards of trustees (e.g. OPC, OLE for Process Control) and are hence setting the patterns in matters of IT advances by and large add to these frameworks. In actuality, they are currently likewise infiltrating the test material science research facilities for the controls of auxiliary frameworks, for example, cooling, ventilation, power dispersion, and so forth. All the more as of late they were likewise requisitioned the controls of littler size molecule identifiers, for example, the L3 mount identifier and the NA48 test, to name only two illustrations at CERN.SCADA frameworks have made significant advance over the late years as far as usefulness, adaptability, execution and openness such that they are an option to in house improvement actually for exceptionally requesting and complex control frameworks as those of material science tests. This paper portrays SCADA frameworks regarding their construction modeling, their interface to the procedure equipment, the usefulness and application improvement offices they give. Some consideration is paid to the modern guidelines to which they withstand their arranged advancement and also the potential advantages of their utilization

**KEYWORDS**: SCADA, NA48test, Process control, and SCADA Frameworks.

## INTRODUCTION

Using powerful technologies, based on experience of qualified personal, SCADA (Supervisory Control and Data Acquisition) applications are created as a main tool for performing management, required by technical reengineering of an industrial company [1]. In modern manufacturing and industrial processes, mining industries, public and private utilities, leisure and security industries, control systems are often needed to connect equipment and systems separated by large distances. These systems are used to send commands, programs and receive monitoring information from these remote locations [2]. SCADA refers to the combination of control systems and data acquisition. In the early days of data acquisition, relay logic was used to control production and plant systems. With the advent of the CPU (Central Process Unit) and other intelligent electronic devices, manufacturers incorporated digital electronics into relay logic equipment [3]. The PLC (Programmable Logic Controller) is still one of the most widely used control systems in industry [4].

### WHY SCADA?

SCADA provides several unique features that make it a particularly good choice these features are as follows:

- ✓ The computer control primary equipments, record an store a very large amount of data from process
- ✓ The operator can incorporate real data simulations into the system
- ✓ The operator is assist by computer that recommend actions to keep the system safety
- ✓ Many types of data can be collected from the RTUs (Remote Terminal Unit), this creates online the image of the system.

### Network Architecture

Effective network design which provides the appropriate amount of segmentation between the Internet, the company's corporate network, and the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

SCADA network is critical to risk management in modern SCADA systems [5]. Network architecture weakness can increase the risk from Internet and other sources of intrusion.

**Hardware of SCADA**

SCADA solutions often have Distributed Control System (DCS) components. Use of "smart" RTUs or PLCs, which are capable of autonomously executing simple logic processes without involving the master computer, is increasing [6]. A standardized control programming language, IEC 61131-3 (a suite of 5 programming languages including Function Block, Ladder, Structured Text, Sequence Function Charts and Instruction List), is frequently used to create programs which run on these RTUs and PLCs. Unlike a procedural language such as the C programming language or FORTRAN, IEC 61131-3 has minimal training requirements by virtue of resembling historic physical control arrays. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC[7]. A Programmable Automation Controller (PAC) is a compact controller that combines the features and capabilities of a PC-based control system with that of a typical PLC. PACs are deployed in SCADA systems to provide RTU and PLC functions [8]. In many electrical substation SCADA applications, "distributed RTUs" use information processors or station computers to communicate with digital protective relays, PACs, and other devices for I/O, and communicate with the SCADA master in lieu of a traditional RTU [9].

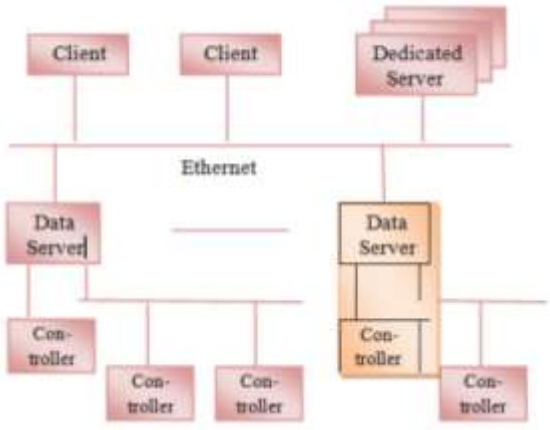


***Figure 1: Typical Hardware Architecture***

***Confidentiality:*** Generally, there are no mechanisms in SCADA to provide confidentiality of communications. If lower level protocols do not provide this confidentiality then SCADA transactions are communicated "in the clear" meaning that intercepted communications may be easily read.

***Authentication:*** Many SCADA systems give little regard to security, often lacking the memory and bandwidth for sophisticated password or authentication systems. As a result there is no mechanism to determine a system user's identity or what that user is authorized to access. This allows for the injection of false requests or replies into the SCADA system.

Lack of session structure: SCADA systems often lack a session structure which, when combined with the lack of authentication, allow the injection of erroneous or rogue requests or replies into the system without any prior knowledge of what has gone on before.

## CYBER SECURITY FOR SCADA

Cyber security for SCADA Systems provides a high-level overview of this unique technology, with an explanation of each market segment. Cyber security for SCADA Systems is suitable for the non-technical management level personnel as well as IT personnel without SCADA experience. The security issues with SCADA systems as follows:

Traditionally SCADA systems were designed around reliability and safety. Security was not a consideration. However, security of these systems is increasingly becoming an issue due to:

- ✓ Increasing reliance on public telecommunications networks to link previously separate SCADA systems is making them more accessible to electronic attacks;
- ✓ Increasing use of published open standards and protocols, in particular Internet technologies, expose SCADA systems to Internet vulnerabilities;
- ✓ The interconnection of SCADA systems to corporate networks may make them accessible to undesirable entities;
- ✓ Lack of mechanisms in many SCADA systems to provide confidentiality of

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

communications means that intercepted communications may be easily read;
- ✓ Lack of authentication in many SCADA systems may result in a system user's identity not being accurately confirmed.

**SCADA Security**

The majority of SCADA systems have useful lifetimes ranging from 15 to 30 years. In most instances the underlying protocols were designed without modern security

The rapid advance of technology and the changing business environment is driving change in SCADA network architecture, introducing new vulnerabilities to legacy systems.

The current push towards greater efficiency, consolidated production platforms and larger companies with smaller staffing levels is leading to changes in SCADA systems which are raising many questions about security.

- ✓ An increasing reliance on public telecommunications networks to link previously separate SCADA systems;
- ✓ Increasing use of published open standards and protocols, in particular Internet technologies; and
- ✓ The interconnection of SCADA systems to other business networks to enhance the amount, detail and timeliness of information available to management.

***Commodity Infrastructure:*** The changes in SCADA systems have exposed them to vulnerabilities that may not have existed before. For example, the switch from using leased telecommunications lines to public infrastructure i.e. Public CDMA and GSM networks, the use of commodity computers running commodity software and the change from proprietary to open standards have meant that vulnerabilities have been introduced into SCADA systems.

## 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.

For large collaborations, as using a SCADA system for their 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

## APPLICATIONS

Supervisory Control and Data Acquisition (SCADA) systems have been widely used in industry applications. Due to their application specific nature, most SCADA systems are heavily tailored to their specific applications. For example, a remote terminal unit (RTU) that monitors and controls a production well in an oilfield is only connected with a few sensors at the well it resides. The RTU usually collects sensor data at pre-defined intervals, and only sends data back when being polled by a central data server. A user can only access the data in one of the two ways: directly connecting to the RTU in the field or reading from the data server in the control room. A major drawback of typical SCADA systems is their inflexible, static, and often centralized architecture, which largely limits their interoperability with other systems. For example, in a SCADA system developed for oil and gas fields, the RTUs are usually places at production wells and injection wells. However, there are many other places, such as pipeline, tanks, etc., that have valuable data but are too expensive (e.g., cable requirement) to deploy more RTUs. In such cases, sensor networks are a perfect solution to extend the sensing capability of the SCADA system. However, it is difficult to integrate sensor networks with current SCADA systems due to their limited interoperability. We identify that enabling such interoperability is an important task for future SCADA systems.

Another drawback of the current SCADA systems is their limited extensibility to new applications. In the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

above oilfield monitoring example, a user in the field can only access a sensor's data by physically going to that well and connecting to its RTU. If the company wants to extend its SCADA system by adding a safety alarm system, it will be very difficult to add the new application.

The original application only monitors well production at predefined intervals or on demand. The new application requires real-time interaction between sensors and mobile users in the field. The RTUs that detect a safety problem need to proactively report the problem without waiting. The rigid design of current RTUs makes it hard to extend the SCADA from one application to another.

The Deploying a SCADA system in a large field is very expensive If the SCADA system is interoperable with new technologies, such as sensor networks, and extensible for new applications, it will be able to significantly improve the productivity at a minimal cost.

**Communication Architecture:** Current SCADA systems are essentially a centralized communication system, where the data server polls each remote terminal unit (RTU) to collect data. There is no data sharing and forwarding between different RTUs. Usually these RTUs only communicate with the data server. This communication architecture is not flexible to interact with other systems, such as the embedded sensor networks and mobile users in the field. Designing flexible communication architecture is one of the key factors to enable interoperability and extensibility.

**Open and Interoperable Protocols**: We suggest that SCADA systems should adopt the use of Internet technologies for networking, rather than proprietary or link-level approaches. Collect and manipulate different types of sensor data. It also includes how to discover and configure sensors. An open protocol should be extensible to support various types of sensors. These protocols should also address what types of data should be transmitted and to whom. For example, raw data are only sent to data server for archival. Status summaries will be sent to managers and engineers, while emergency safety alarms should be broadcast to all field operators.

**Smart remote terminal units**: Remote terminal units play an important role in the new communication architecture we described above. They serve as bridge points to sensor networks as well as access points to mobile users in the field. They respond to users queries and collect data from specific sensors. These RTUs should be smart enough to perform preliminary data processing. The first reason is to validate the data collected from different sensors. Sensors can give false values due to various reasons. It is important to validate them before use them to make important decisions. For example, in oilfield monitoring, a false sensor reading may result in a mistaken decision to shut in a well and lose production. The RTU is in a good position to validate sensor readings by cross checking from adjacent sensors.

Another reason of requiring smart RTUs is that they are important in changing the reactive operation to proactive operation. Current SCADA systems mainly operate in the reactive mode, where data are usually sent in response to the data server's polling.

In a new class of applications, detection needs to be done in real time, and events need to be reported immediately, such as pipeline leakage, or H2S detection. Intelligent algorithms will run on these smart RTUs to process data in real time.

Finally, these RTUs need to be smart enough to protect data from unauthorized access and altering. Access control and security measures need to be installed to protect the sensing system from attackers and ensure data integrity.

## CONCLUSION

SCADA can be an extraordinary instrument while working in a situation where operational obligations need to be checked through electronic correspondence rather than mainly. An administrator can position a valve to open or close through SCADA without leaving the control station or the PC. The SCADA framework likewise can switch a pump or engine on or off and has the capacity of putting engines on a Hand working status, Off, or Automatic. Hand alludes to working the supplies mainly, while Automatic has the gear work as per set focuses the administrator gives on a PC that can correspond with the supplies through SCADA.

## REFERENCES

1. "SCADA Systems April 2014".

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

2. How The "Internet Of Things" Is Turning Cities Into Living Organisms Retrieved September 16, 2013
3. Boyes, Walt (2011). Instrumentation Reference Book, 4th Edition. USA: Butterworth-Heinemann. p. 27. ISBN 0-7506-8308-2.
4. Slay, J.; Miller, M. (November 2007). "Chpt 6: Lessons Learned from the Maroochy Water Breach". Critical infrastructure protection (Online-August.). Springer Boston. pp. 73–82. ISBN 978-0-387-75461-1. Retrieved 2 May 2012.
5. "External SCADA Monitoring". Epiphany Case Studies. Epiphan Systems Inc. Retrieved 2 May 2012.
6. "Security for all". InTech. June 2008. Retrieved 2 May 2012."S4 2008 Agenda".
7. "Cyber threats, Vulnerabilities and Attacks on SCADA Networks". Rosa Tang, berkeley.edu. Retrieved 1 August 2012.
8. "Industrial Security Best Practices". Rockwell Automation. Retrieved 26 Mar 2013.