Investigation into Remote Monitoring of Power Transformers using SCADA

Solomon Nunoo[#1], Edward Kofi Mahama[#2]

[#] Department of Electrical and Electronic Engineering, University of Mines and Technology
Post Office Box 237, Tarkwa, Ghana

[1]snunoo@umat.edu.gh

***Abstract*- This paper investigates the use of internet-based Supervisory Control and Data Acquisition (SCADA) system to monitor power transformer parameters remotely and to investigate into how personnel can have access to their system regardless of their location. There are several parameters that can be monitored for efficient operation of a power transformer, although temperature, voltage, load and bushing condition are considered in this work because they are the major cause of transformer failure. In carrying out this work, the software and hardware components required to carry out the remote monitoring function was considered. Means of preventing hackers from getting access to the network have been considered. The implementation of the monitoring system will help to save running cost by optimising maintenance schedule and reduce risk of failure to the power transformer.**

Keywords*— *Internet-based SCADA, Automation, Power Transformers, Remote Monitoring, Maintenance Optimisation, SCADA Security

I. INTRODUCTION

The utility companies in Ghana responsible for generation, transmission and distribution of electrical power are Volta River Authority (VRA), Ghana Grid Company (GRIDCo), and Electricity Company of Ghana (ECG) and Northern Electrification Department (NED) respectively.

The power transformer is regarded as the heart of any electrical transmission and distribution system. At the output of the generator, they are used for stepping up voltage for transmission. In addition, at certain sections of the transmission system, they are used to either step-up or step-down the system voltage. Distribution utility companies require power transformers to step-down voltage to the required level for utilization by consumers.

There are several challenges that confront power transformers. Some of these include overheating, overloading and overvoltage. Non-monitoring and control of these parameters can lead to flashover between terminals, deterioration of insulation of transformer oil, burning of winding insulation, shortening of transformer life span and total breakdown of the power transformer. These can cause interruptions in the supply of power to consumers and subsequently an unreliable power system.

Unfortunately, some of these parameters are not adequately monitored due to the remoteness of some of the power transformers coupled with the fact that personnel have to travel long distances to transformer sites in order to monitor them. There is therefore the need for a novel technique to monitor these remote transformers. One such technique is to monitor critical power transformer parameters using an internet-based SCADA system in order to avoid or reduce disruptions that arise due to sudden or unexpected failure.

One of the main purposes of a SCADA application is to provide an operator with the graphical interface needed to monitor and control the production processes in an industrial plant [1]. Currently, most SCADA systems are based on bitmap graphics or proprietary vector formats to build the operator's interface.

An internet-based SCADA system may consist of intelligent RTUs, each of which has modularized hardware architecture and supports HTTP protocol, and a distributed master station, which has a web server/browser structure and decomposes the SCADA functions into multiple sets of Web site components [2]. Both the hardware design and software development for such a web-based SCADA system have been carried out in accordance with well-proven architecture modules, allowing the system to benefit from numerous available technologies and giving it added flexibility and scalability.

An internet-based SCADA display system designed using an object-oriented design approach and client/server module was proposed by [3] to allow the user great flexibility to dynamically interact with the SCADA system. Reference [4] has also proposed a concept for a TCP Java overall structure to implement an interaction between the SCADA systems and Web servers.

In an internet-based SCADA system, security is paramount and [5] has also discussed the aspect of security of SCADA systems and how the security enforcement in the system affects the overall performance and the real-time requirements.

Reference [6] has also compared protocols of the "traditional" SCADA networks to an "internet" based network. The authors also described and explained XML, JAVA and HTML and how it can play in the industrial/automation systems.

This research differs from the research published to date in that; it presents a remote monitoring system for power transformers using SCADA. This research also attempts to address associated problems that may arise in connection with the security of the system.

II. OVERVIEW OF SCADA SYSTEMS

SCADA is a process control system that enables a site operator to monitor and control processes that are distributed among various remote sites [7]. SCADA system is often referred to as telemetry. A properly designed SCADA system saves time and money by eliminating the need for service personnel to visit each site for inspection, data collection/logging or make adjustments.

SCADA systems are computers, controllers, instruments, actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection. They are used in all types of industries; from electrical distribution systems, to food processing, to facility security alarms. Traditionally, SCADA systems have made use of the Public Switched Network (PSN) for monitoring purposes. Today many systems are monitored using the infrastructure of the corporate Local Area Network (LAN)/Wide Area Network (WAN).

Another common term used to describe a SCADA system is Human Machine Interface (HMI). It is used to describe any system that provides an interface between a person and a piece of machinery. The Industrial SCADA System falls into this category. It provides an HMI by displaying process variables to the operator and allowing control of the plan.

A. Functions of the SCADA System

A SCADA system has two basic functions [8], the first of which is to display information about the current operating conditions of a plant in an informative and graphical interface and the second is to allow supervisory control of the plant by personnel. Larger commercial systems may also have other features, such as historical trending of data to allow the past operation of the plant to be recorded for future reference and for faultfinding. These other features are secondary to the main purpose of the SCADA.

B. Components of SCADA System

The components of SCADA can be broadly divided into hardware and software [9].

1) Hardware Components: It refers to the physical components that make up the SCADA. These are the filed data interface devices (IEDs), remote terminal units (RTUs), communications medium, master station (central host computer) and operator workstations.

Field Data Interface Devices (IEDs): Digital or analogue intelligent electronic devices and control relays that directly interface with the managed system.

Remote Terminal Unit (RTUs): Gathers information from their remote site from various intelligent electronic devices. They are primarily used to convert electronic signals received from field interface devices into the language used to transmit the data over a communication channel.

Communications Medium: The devices used to connect the SCADA master unit to the RTUs in the field.

The Master Station: Initiates all communication, gathers data, stores information, sends information to other systems, and interfaces with operators. The major difference between the master station and RTU is that the master station initiates virtually all communication between the two.

Operator Workstations: Operator workstations are most often computer terminals that are networked with the SCADA central host computer.

2) Software Components: SCADA software is divided into two types; proprietary or open [10]. Companies develop proprietary software to communicate to their hardware. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems have gained popularity because of the interoperability they bring to the system. Key features of SCADA software include user interfaces, graphics displays, alarms, trends, RTU (and PLC) interface, scalability, access to data, database, networking, fault tolerance and redundancy, and client/server distributed processing.

C. SCADA Protocols

SCADA Communications protocols define the method by which data is transmitted along a communication link [11]. The data representations in a SCADA network are identified not in any fashion other than by unique addressing. The addressing is designed to correlate with the SCADA master station database.

Each protocol consists of two message sets. One set forms the master protocol, containing the valid statements for master station initiation or response, and the other set is the RTU protocol, containing the valid statements an RTU can initiate and

respond to. In most but not all cases, these pairs can be considered a poll or request for information or action and a confirming response.

D. SCADA System in Ghana

The components of the SCADA system combine to provide auto-remote control and switching capabilities into GRIDCo network and ECG's Primary network. The system provides the operators monitoring the HMI with sufficient information to operate the network. Furthermore, it gives warning and alarms for unexpected or critical events; allow remote control and post-fault analysis.

The section of the power system in Ghana that has benefited from SCADA is from the generation section through to the high voltage transmission network and sub-transmission network of the distribution utilities [12]. There is however no remote means of monitoring the condition of power transformers in the distribution utility companies which is a vital component of the power system. As such personnel have to travel long distances to remote site to take readings manually.

III. DESIGN METHODOLOGY

Power transformers are utilized in power transmission and distribution systems to modify the voltage of the power being provided. The ability to monitor and analyze various parameters about the transformer is critical for maintenance and troubleshooting as well as for proper and/or optimum loading. Various parameters are monitored using various techniques.

SCADA will be used to help in sending the gathered data from the remote station to the control room to enable the necessary action to be taken. The internet is used as the medium of communication between the remote site and master station due to the numerous advantages it possesses. Though there are security risks that come with the internet-based SCADA system, necessary measures to check these challenges are also discussed.

A. Selection of Parameters to Monitor

There are a number of parameters that can be monitored for reliable operation of a power transformer. Some of the parameters are, bushing condition, input voltage, output voltage, operating frequency, temperature, tap changer position, transformer oil level, insulation level of transformer oil, and load.

A study by Electrical Power Research Institute (EPRI) showed that the cause of transformer failure due to bushing and insulation failure is about 30 % and 45 % respectively. Another study conducted by [13] resulted in the values given in the Table 1.

TABLE 1 TRANSFORMER FAILURE STATISTICS

Causes of Transformer Failure	**Percentage (%)**
Insulation Failure	52
Design	23
Unknown	10
Oil Contamination	4
Overloading	3

Though temperature is not found in the research results, it is seen as the greatest threat to the transformer winding and oil insulation failure in hot climates. As the transformer load increases, the current flowing through the secondary windings also increases, thus causing the temperature of the windings to increase. This causes the insulation of the windings to deteriorate and making short circuits faults imminent. Thus in selecting the parameters to monitor, priority was given to the parameters that mostly cause the transformer to failure. In this paper, temperature, load, bushing condition and line voltage are the parameters that are monitored.

B. The Designed Power Transformer Monitoring System

The power transformer monitoring system consists of the integration of the hardware components. This includes the master station, remote terminal unit, internet modem and the communication infrastructure. A database is included to store the acquired parameters from the RTU.

1) Master Station: The master stations establishes communication, which involves configuring RTU, initializing each RTU with input/output parameters as well as downloading control and data acquisition programs into RTU. It also controls operation of the communication link which involves polling each RTU for data and writing to the RTU, logging alarms and events to memory and operator display, as well as linking inputs and output at different RTUs automatically. In addition, it

diagnoses the RTUs, which involves accurate diagnostic information on failure of RTU and possible problems as well as predicting potential overloads, such as data overloads. Fig. 1 shows the architecture of the master station.

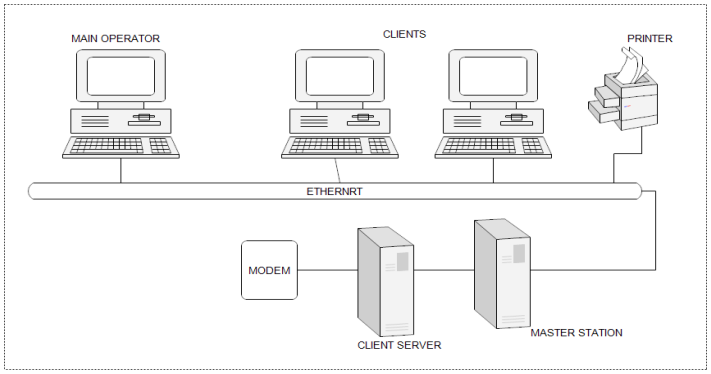

Fig. 1 Master Station Architecture

2) Remote Site Connection: At the remote site, current transformer, thermistor or thermocouple, bushing monitor and voltage transformer are used for sensing the concerned parameters. Fig. 2 shows the connection of the sensing devices to the power transformer and the RTU. Most power transformers has all of these sensing devices built in them with the exception of bushing monitor which is found in modern power transformers only. Therefore there is no need of building new circuit to sense these parameters. Usually there are terminals that are wired from these sensing devices to the mimic or display unit on the transformer.

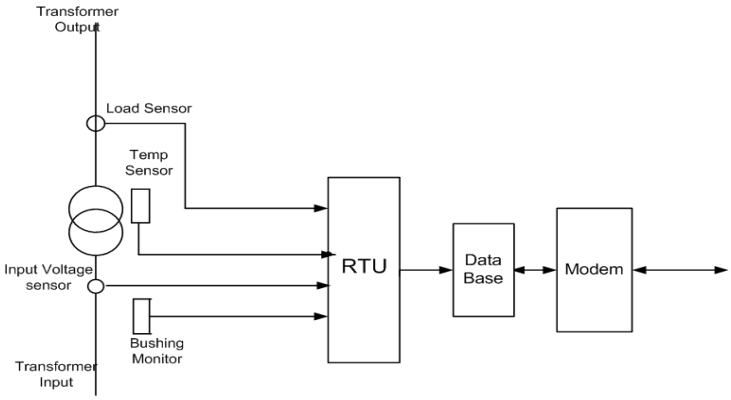

Fig. 2 Remote Site Architecture

Modern power transformers are usually provided with auxiliary terminals but the old ones in the system lack these terminals. In order to monitor temperature, load, bushing condition and voltage remotely making use of the SCADA system, the auxiliary terminal will be tapped and connected to the RTUs. Thus, the RTUs will signal the operator via the internet to the master station for appropriate action to be taken.

3) Design Flow Chart: The RTU polls the sensed parameters from the output of the sensors. The read values are then compared with the set point of the parameters based on the configuration of the RTU. If the readings are above the preset values, a signal is sent via the internet to the master station. Fig. 3 shows the design flow chart for the monitoring system.

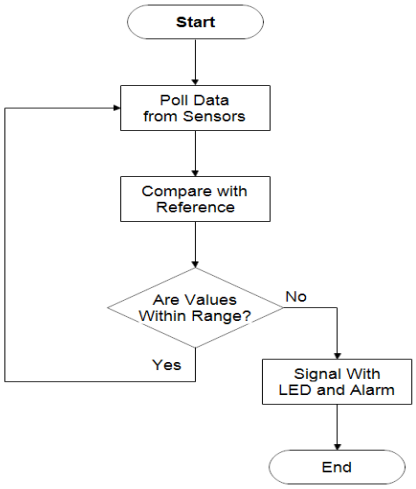

Fig. 3 Monitoring Flow Chart

In the case of temperature exceeding its safe limit, a standby cooling system is activated in addition to signalling at the master station. This standby cooling re-enforce the transformer cooling system, thus helping to quicken the cooling rate of the transformer. The detailed flow chart with the standby cooling system activation is shown in Fig. 4. X, Y, and Z are the reference/set point values for voltage, current and temperature respectively.

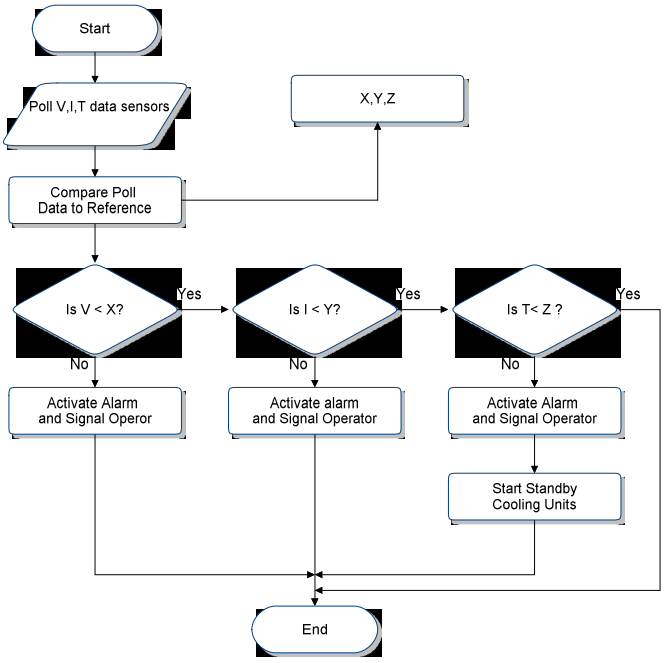

Fig. 4 Detailed Monitoring Flow Chart

4) Communication Medium: Since the beginning of mainstream networked computing and the internet, there has been substantial evolution in the communications methods used to connect computers. Over the past decade, the focus of web applications has shifted from connectivity, using such protocols as TCP/IP, to presentation focused applications using HTML. The most recent shift in focus has been towards programmability using XML [14]. These technologies are implemented with the goal of making interoperability easier amongst different platforms and programming languages. For this work, XML is examined because it is the appropriate method used for communicating data which should be machine readable.

5) XML Web Services: Extensible Markup Language (XML) is a set of rules for encoding documents in machine-readable form. An XML Web Service is a technology, implemented in the Microsoft .NET framework that allows access to software components on different machines across a network using standard web protocols and the XML data format [14].

XML Web Service was chosen for a number of reasons. The major reason is that, the Web Service uses HTTP and therefore port 80 to communicate. This port is left open on firewalls, which therefore means that implementation is easier as ports do not have to be individually configured by the network administrator. Another important reason is that the system is easily scalable. The amount of data transmitted at any time can be easily increased without much additional programming. This

ease of implementation also extends to easy implementation of security measures such as HTTPS. Finally, and importantly, XML Web Services are also platform independent. All of these things add up to make an XML Web Service a good base for an internet-based SCADA system.

6) Communication Protocol: In order for a SCADA system to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850, IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. DNP3 will be used in this work.

DNP3 Protocol: The DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in automation systems. It is usually used in utilities such as water and electric companies. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It is primarily used for communications between a master station and IEDs or RTUs. DNP3 supports multiple-slave, peer-to-peer and multiple-master communications.

C. Security of the Designed SCADA Network

Security is the greatest issue of concern to users of internet-based SCADA systems. The potential exists for unauthorized users to gain access to sensitive information from the SCADA system or indeed gain access to control of the factory plant. The risk of this occurring can be reduced by implementing appropriate security measures such as firewalls, cryptography, digital certificates and public key infrastructure [3].

1) Internet Protocol Security Virtual Private Network: Internet Protocol Security (IPSec) Virtual Private Network (VPN) is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit [15].

IPSec Security Features: IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- *Authentication*: Verifies that the packet received is actually from the claimed sender.
- *Integrity*: Ensures that the contents of the packet did not change in transit.
- *Confidentiality*: Conceals the message content through encryption.

IPSec VPNs provide access to entire subnets of the corporate network. A user who has the remote VPN client software installed comes through the Internet to the firewall or VPN gateway and initiates a key exchange (IKE). Once the user is properly authenticated, a VPN pipe/tunnel is created and the VPN then has the option to run in two modes; tunnel and transport [16].

In transport mode, the transport layer segment of the packet is encrypted while in tunnel mode the entire packet is encrypted, making tunnel the preferred method. The strength of IPSec VPNs lies in the fact that it encrypts packets of information, significantly increasing its ability to provide data confidentiality and integrity [17]. It uses universally accepted cryptography standards such as 3DES, MD5 SHA for encrypting data and authenticating packets. It can use IKE with digital certificates or pre-shared secrets for two-way authentication to ensure that the user is who they say they are [18]. It is for these reasons that IPSec is still the primary choice for site-to-site VPNs.

IV. CONCLUSIONS

Remote monitoring system using Supervisory Control and Data Acquisition (SCADA) has been discussed. The parameters to monitor were selected based partly on a research by [13] which showed that the major causes of power transformer failure are overvoltage, overload, excessive temperature and bushing failure. The software components, hardware components and means of communication over the internet have also been discussed. In addition, a means of securing the SCADA network has been considered.

Remote monitoring of power transformer will help to save running costs of transmission and distribution systems by optimizing maintenance schedules. It will also help increase safety for personnel and reduce the risk of catastrophic failure to the power transformer.

REFERENCES

[1] G. R. Garcia and E. Gelle, 2004. SVG for SCADA Applications: A Practical Approach. [Online]. Available: http://www.svgopen.org/2004/papers/SVGforSCADA/

[2] D. Li, Y. Serizawa, and M. Kiuchi, "Concept Design for a Web-based Supervisory Control and Data-Acquisition (SCADA) System," in *Proc. IEEE PES Transmission and Distribution Conference and Exhibition*, 2002, p.32-36.

[3] B. Qiu, and H. B. Gooi, "Web-based SCADA Display Systems (WSDS) for access via Internet," *IEEE Transactions on Power Systems*, Vol. 15, No. 2, 2000, p.681-686.

[4] M. Clayton and A. Juan, 2002. A SCADA-Web Interconnection with TCP in Java. [Online] Available: http://ess.web.cern.ch/ESS/GIFProject/PVSSJava/pvssweb.0.8.pdf.

[5] A.K. Wright, J.A. Kinast, and J. McCarty, "Low-Latency Cryptographic Protection for SCADA Communications", in *Proc. ACNS*, 2004, p.263-277.

[6] R. Fan, L. Cheded, and O. Toker, "Internet-based SCADA: A new approach using JAVA and XML," *IEE Computing & Control Engineering Journal*, Vol. 16, Issue 5, Oct.-Nov. 2005, p. 22-26.

[7] A. Goel and R. S. Mishra. "Remote Data Acquisition Using Wireless-SCADA System", *International Journal of Engineering (IJE)*, Vol. 3, Issue 1, 2009, p. 58-65.

[8] B. Berry, 2009. A Fast Introduction to SCADA Fundamentals and Implementation, DSP Telecom. Available: http://www.dpstelecom.com/w_p.

[9] Anon, 2006. SCADA Systems for Command, Control, Communications, Computer Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities. [Online] Available: http://armypubs.army.mil/eng/DR_pubs/DR_a/pdf/tm5_601.pdf.

[10] D. Reynders, G. Clarke and E. Wright, *Practical Modern SCADA Protocols, 60870.5 and Related Systems*, Newness and Elsevier Advance Technology Limited, United Kingdom, 2004.

[11] Anon, 2004, The Fundamentals of SCADA, Bentley Press, Incorporated, [Online]. Available: ftp://ftp2.bentley.com/dist/collateral/whitepaper/fundscada_whitepaper.pdf.

[12] S. Nunoo, and A. K. Ofei, "Distribution Automation (DA) Using Supervisory Control and Data Acquisition (SCADA) with Advanced Metering Infrastructure (AMI)", in *Proc. IEEE Conference on Innovative Technologies for an Efficient and Reliable Electricity Supply*, 2010, p. 454-458.

[13] W. H. Bartley, 2003, Investigation into Transformer Failures, [Online]. Available: http://www.bplglobal.net/eng/knowledge-center/download.aspx?id=191.

[14] J. M. Lynch, "An Internet Based SCADA System", BSc Project Report, University of Southern Queensland, Queensland, Oct. 2005.

[15] Anon, 2005, Virtual Private Networking Basics, NETGEAR, Incorporated, [Online] Available: http://documentation.netgear.com/reference/esp/vpn/pdfs/FullManual.pdf.

[16] S. Ferrigni, 2003, SSL Remote Access VPNs: Is this the end of IPSec?, SANS Institute, [Online]. Available: http://www.sans.org/reading_room/whitepapers/vpns/ssl-remote-access-vpns-ipsec_1285.

[17] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence, and M. Pozzuoli, 2008, Securing SCADA Communications following NERC CIP Requirements, RuggedCom, Inc., [Online]. Available: http://www.ruggedcom.com/pdfs/white_papers/security-scada-energy-week.pdf.

[18] F. Alsiherov, and T. Kim, 2010, "Research Trend on Secure SCADA Network Technology and Methods," *WSEAS Transactions on Systems and Control*, Vol. 5, No. 8, p. 635-645.