IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 3, June-July, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Scada Automation In Energy Management Systems

Ramleela Khare[1], Filipe Rodrigues E Melo[2]

[1]Director Research, The MRPC Company, Hyderabad, India

[2]Assoc. Professor Commerce, St. Xavier's College Of Arts, Science & Commerce, Goa

ABSTRACT

The paper outlines information about the SCADA techniques used by the author in the hardware models of a dynamic system developed by him. This includes the construction of a master unit for data acquisition and software to view the data of the Multi Function Meters from AC Network Analyzer—a dynamic model developed by him for the practical training to the engineers from the industry and engineering institutions for their laboratory. A critical literature review has been also presented covering a period of more than 15 years. The review indicates current application of SCADA to energy management systems, security and other aspects including the SCADA models as teaching aid.

Keywords*: SCADA, Energy Management System, Automation.*

1. INTRODUCTION

An outline is given here about Power Industry to highlight current scenario of Automation in generation, transmission and utilization of electrical power: The generation of power is achieved from various methods, the well known are: atomic / thermal / hydro / wind and solar. The various sources of electrical power have different economics and breakeven. The capital investment and running cost of each generation method varies. Almost all commercial electrical generation is achieved by using electromagnetic induction, in which mechanical energy forces an electrical generator to rotate. There are many different methods of developing the mechanical energy, including heat engines, hydro, wind and tidal power.

1.1 Power Generation

The direct conversion of nuclear potential energy to electricity by beta decay is used only on a small scale. In a full-size nuclear power plant, the heat of a nuclear reaction is used to run a heat engine. This drives a generator, which converts mechanical energy into electricity by magnetic induction. Most electric generator is driven by heat engines. The combustion of fuels supplies most of the heat to these engines, with a significant fraction from nuclear fission and some from renewable sources. The modern steam turbine currently generates about 80 percent of the electric power in the world using a variety of heat sources.

Large dams such as Three Georges Dam in China figure no. 1 can provide large amounts of hydroelectric power up to 22.5 GW.

Photo Figure no. 1

Reference: http://en.wikipedia.org/wiki/File:Dreischluchtendamm_hauptwall_2006.jpg

All turbines are driven by a fluid acting as an intermediate energy carrier. Many of the heat engines just mentioned are turbines. Other types of turbines can be driven by wind or falling water sources and includes:

I STEAM - Water is boiled to produce steam by:

* NUCLEAR FISSION

* FOSSIL FUELS (coal, natural gas, or petroleum): In hot gas (gas turbine), turbines are driven directly by gases produced by the combustion of natural gas or oil. Combined Cycle gas turbine plants are driven by both steam and natural gas. They generate power by burning natural gas in a gas turbine and use residual heat to generate additional electricity from steam. These plants offer efficiencies of up to 60%.

* RENEWABLE. The steam generated by:

a. Biomass

b. Solar Thermal Energy (the sun as the heat source) solar parabolic trough and solar power towers concentrate sunlight to heat a heat transfer fluid, which is then used to produce steam.

c. Geothermal power: Either steam under pressure emerges from the ground and drives a turbine or water evaporates to create vapor to drive a turbine.

d. Ocean Thermal Energy Conversion (OTEC)

Photo Figure no. 2
(Reference:http://en.wikipedia.org/wiki/File:Hoover_dam_from_air.jpg)

Large dams such as Hoover Dam (figure no 2) can provide large amounts of hydroelectric power up to 2.07 GW

II. WATER (hydroelectric): Turbine blades are acted upon by flowing water, produced by hydroelectric dams or tidal forces.

III.WIND AND SOLAR: Most of the wind turbines generate electricity from naturally occurring wind. Solar updraft tower use wind that is artificially produced inside the chimney by heating it with sunlight, and are more properly seen as forms of solar thermal energy.

IV. RECIPROCATING ENGINES: Small electricity generators are often powered by reciprocating engines burning diesel, biogas or natural gas. Diesel engines are often used for back up generation, usually at low voltages. However most large power grids also use diesel generator originally provided as emergency back up for a specific facility such as a hospital, to feed power into the grid under certain circumstances. Biogas is often combusted where it is produced, such as a landfill or wastewater treatment plant, with a reciprocating engine or a micro turbine which is a small gas turbine. Generation sources like wind and hydro power use mechanical energy of moving masses of air or water to produce electric energy. Still other devices, such as fuel cells, use chemical reactions to generate electric energy. However, in all these cases, some of the input energy is lost in the process.

1.2 Transmission of Generated Power

The generated electrical power is then transmitted to the consumer destination located at various sites. Domestic and commercial establishments act as a load or consumers of the generated electric power. The function of transmission line is to carry or transfer the electric power to its destination points that is a sub-station. The transmission lines carry HVAC (High Voltage Alternating Current) power if medium distances or HVDC (High Voltage Direct Current) power for long distances. The transmission lines have natural characteristics which cause loss of power during transmission, HVDC is preferred due to less loss of power but the equipment used for HVDC lines are costly therefore it is only applied for long line transmission and HVAC is preferred for short and medium length transmission lines. The economics and efficiency is thus achieved.

Moving large amounts of power over very long distances is separate from distribution, which refers to the process of delivering electric energy from the High Voltage (HV) transmission grid to specific locations such as a residential street or commercial park. Distribution is usually considered to encompass the substations and feeder lines that take power from the high voltage grid and progressively step down the voltage eventually to the 230V level at which power enters our homes.

The transmission and distribution or “T&D” system includes everything between a generation plant and an end-use site. Along the way, some of the energy supplied by the generator is lost due to the resistance of the wires and equipment that the electricity passes through. Most of this energy is converted to heat. Just how much energy is taken up as losses in the T&D system depends on the physical characteristics of the system in question as well as how it is operated. Generally speaking, T&D losses between 6% and 8% are considered normal.

After receiving the electrical power from the generating station through transmission line to sub-station, the distribution takes place. The substations are located near domestic or commercial consumers, hence the substation have a very complex network of power distribution. The distribution point that is a substation has the entire details of what kind and characters of ‘load type’ of consumers are on their network.

The load comprises 3 parameters:

Resistance / Inductive Reactance / Capacitive Reactance (R, XL, XC) each kind of load has different effect on the entire network of power system. Now the generation, transmission line and distribution houses are a part of network which means any kind of disturbance caused in any part of power network system would cause disturbance to the entire network.

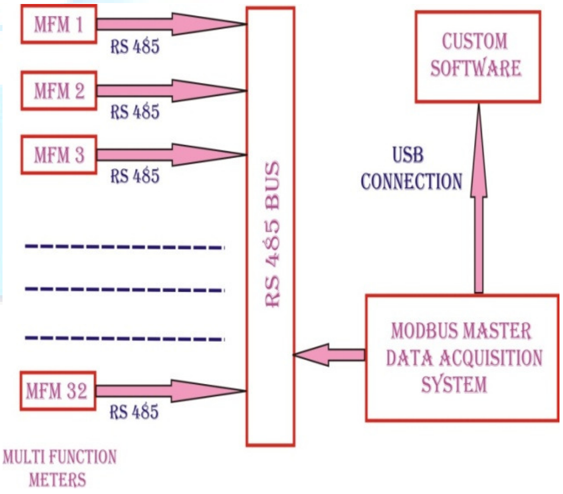
Most of the transmission lines that make up the transmission grid are high-voltage AC lines. HVDC transmission offers advantages over AC by reducing 25% lower line losses increasing two to five times the capacity of an AC line at similar voltage, plus the ability to precisely manage and control flow of power. However, the relatively high cost of HVDC terminal stations relegated the technology to being used only in long-haul applications.

Power electronics devices known as Flexible AC Transmission Systems, or FACTS, provides a variety of benefits for increasing transmission efficiency. It allows existing AC lines to be loaded more heavily without increasing the risk of disturbances on the system. Actual results vary with the characteristics of each installation. A FACTS device enhances transmission capacity by 20 to 40% and stabilizes voltage. FACTS devices offer a good example of how efficiency and reliability improvements often go hand in hand. Unlike shifting and constructing a new transmission line, FACTS devices can be implemented quickly (less than a year from purchase to completion in some cases). They immediately boost the transmission capacity of the given line while also providing voltage support and bolstering the local grid's ability to withstand disturbances.

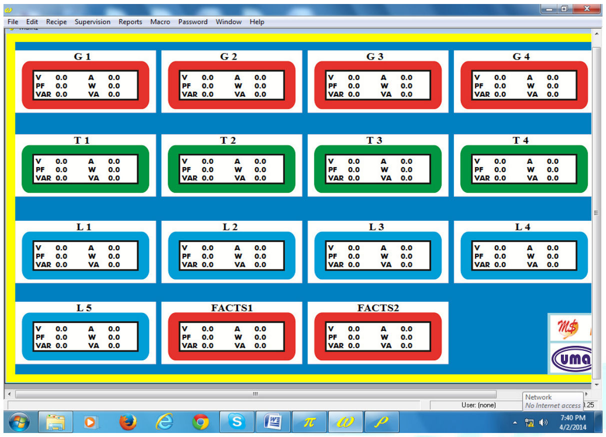
SCADA AUTOMATION

ACADA is essential in introducing efficiency in control of power flow and related operations of the machinery. This will eliminate the wastage of power and help in achieving the goal with economy. It also provides security to the power network and helps in maintaining the uninterrupted supply by introducing intelligent algorithms. A broad based review here covers various aspects of SCADA components, machinery and applications.

Computer Interface for Data Logging (data acquisition) to the Computer from MFM by providing RS485 port with each Multi-function Meter (MFM), RS485 Bus and Mod bus Master Data acquisition system see figure 3 and 5 with USB connection for 20 nos. MFM with software see Figure. 4. Figure 3. Gives the layout of the Master Hardware for Data Acquisition for single phase Multifunction Meter



Modbus Master Data Acquisition System figure 3



```
G 1                 G 2                 G 3                 G 4
V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0
PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0
VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0

T 1                 T 2                 T 3                 T 4
V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0
PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0
VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0

L 1                 L 2                 L 3                 L 4
V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0
PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0
VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0

L 5                 FACTS1              FACTS2
V    0.0  A   0.0   V    0.0  A   0.0   V    0.0  A   0.0
PF   0.0  W   0.0   PF   0.0  W   0.0   PF   0.0  W   0.0
VAR  0.0  VA  0.0   VAR  0.0  VA  0.0   VAR  0.0  VA  0.0
```

Figure 4 Software on the computer displays data acquisition from various MFM. The software shown in figure 4 displays layout of along with a FACTS device these are marked G1 to G4 for generators, TL1 to TL4 for transmission line, L1 to L5 for loads and for FACTS device as FACTS 1 & FACTS 2

Figure 5. SCADA ARCHITECTURE FOR THE POWER SYSTEM MONITOR

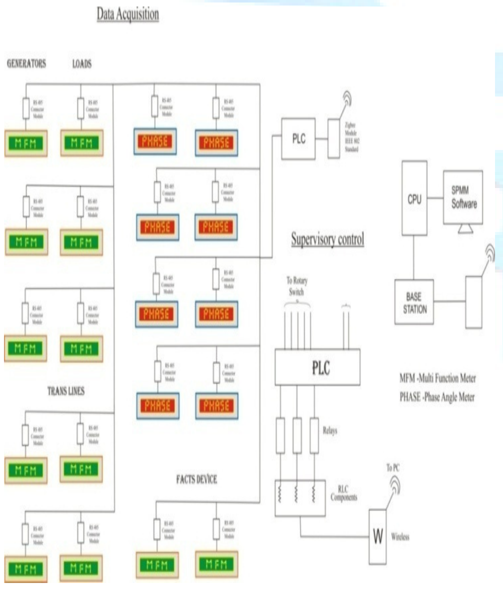


Figure 5 gives the SCADA architecture of the scheme for data acquisition from Multifunction Meters located at the 4 generators, 4 transmission lines, 5 loads, PLC, Wireless Unit and computer system.

The archtecture of the figure 5 has been designed and used by the author in the construction of his Dynamic Monitor Reference [22] Ramleela Khare and Fillipe R. Melo.

Charles T. Lindeberg' and Wayne R. (1993) [1] describe a typical supervisory control and data acquisition (SCADA) system or Energy Management system (EMS) has an installed life of only 15 years. System operations' needs and the underlying technology are rapidly changing, so it is unlikely that the life expectancy will increase. Because it can take 5 years or more to implement a new EMS or SCADA system therefore, it motivates utility engineers to be familiar with the process of managing EMS or SCADA implementation projects. Implementing a new EMS SCADA is a challenge that can be met by using state-of-the-art project management tools.

D. Leslie', A. Hlushko', S. Abughazaleh. And Frank Garza (1994) [2] indicated that SCADA systems have been used by the manufacturing and process industries and many electric power utilities for energy management systems, including economic dispatch and the interconnection pricing of energy. However, the use of SCADA in smaller power generation systems is not quite *so* wide spread. This article explains how a SCADA system was custom developed for a standby power generation system recently installed in a commercial office building. Solving the user interface for the standby power generation system recently installed in a New York skyscraper could have been a serious engineering problem. The standby power system, which was installed after the building was constructed in response to a growing uncertainty in utility power reliability and rising losses in the event of power failure, was designed to distribute power into the building's electrical infrastructure through the top of existing vertical bus ducts.

The design incorporated a complex control sequence whereby standby power distribution circuit breakers were interlocked with the utility feed switches to prevent paralleling with the utility and also with transfer switches on each floor to prevent power from the standby generator system passing through utility company energy meters. The system user interface, therefore, required some form of switch/ breaker/ transfer switch position monitoring with annunciation close to the generator and paralleling switchgear equipment as well as remote annunciation in the building operations control room.

This requirement may not sound very difficult until you consider the amount of equipment to be monitored and controlled and the fact that this equipment was distributed throughout the 48 story building. The engine generator sets and paralleling switchgear were located on a roof setback at the 32nd-floor level. The utility service switches were located at cellar level, and 45 transfer switches were distributed on each floor throughout the building. All devices required monitoring of position (open, closed, normal, and emergency). In addition, transfer switches required remote control of position transfers, and utility switches required trip

Dimitris Th. Askounis and Emmanuel Kalfaoglou (2000) [3] indicate that the national electric utility of Greece has recently installed and put in operation a modern Energy Management System (EMS). This paper presents the development of the Supervisory Control and Data Acquisition (SCADA) system of EMS during its two years of commercial operation. It classifies all the improvements implemented during this period in three areas telecommunications, man-machine interface and core SCADA functions. They conclude that all computer based information systems are manmade systems that cannot be totally fault free. Information system faults can be hardware or software and from design faults to faults not corrected during testing. Part of these faults can be identified even after the start of the commercial operation of the systems and, if feasible, improvements have to be made to deal with them. This is particularly true for complex, custom made SCADA systems like the one presented in this paper. In the case of the Greek EMS-SCADA, part of the improvements implemented so far can be attributed to technical factors, while others have been realized in order to satisfy the needs of the dispatchers. Although the system developers (contractor) have involved the users (dispatchers) in the development process since the system design phase, it is expected that a number of changes will continue to be requested by the dispatchers. Of course, these changes will mainly refer to the adaptation of the system to its dynamically developing environment (new power stations, network topology, etc.). Furthermore, following the recent European Commission directives providing that the Member States' energy systems should adapt to open market principles, the role of the three control centers is expected to expand and gain increased importance.

Mini S. Thomas, *Senior Member, IEEE*, Parmod Kumar, and Vinay K. Chandna (2004) [4] Indicate that this paper reports a state-of-the-art Supervisory Control and Data Acquisition (SCADA) Laboratory facility for power systems at Jamia Millia Islamia, New Delhi, India. It has been designed to function as a research and training center for utilities, faculty members, and students. This paper covers the design, commissioning, and functioning of the SCADA/EMS laboratory facility, based on distributed-processing technology. The SCADA laboratory will provide experience to students and practicing engineers and give insight into the contemporary SCADA systems.

The paper concludes that the SCADA/EMS Laboratory has been designed and commissioned to facilitate the understanding of real time monitoring & control of systems for Electrical Engineering. The Laboratory will provide experience on the on-line monitoring and control of the Electric Power System. The laboratory was conceived and designed after extensive consultation with Industries and utilities. The components of SCADA systems, master station, RTU, different communication channels and field equipments are available in the laboratory. The data acquisition is with time stamping, which will lead to sequence of events monitoring. A three phase transmission line model with on-load tap changer and static VAR are the highlights of the field equipments. The laboratory gets on-line data from the 11 KV substations feeding the Faculty of Engineering. The laboratory has two engineering stations and four operator stations at present, with 216 input/output units, which can be expanded to 1000. Overall, this laboratory will provide the undergraduate and post graduate students with a better understanding of industrial SCADA systems. They propose to add redundant data highway using fiber optic cable soon. The SCADA Laboratory will be primarily used for regular research and training programs for the benefit of Faculty and students of Jamia.

Donghyun Choi, *Student Member, IEEE*, Hakman Kim, Dongho Won, and Seungjoo Kim, *Member, IEEE (2009)* [5] indicates in this paper the authors review constraints and security requirements for SCADA systems and then investigate whether the existing key-management protocols for the SCADA systems satisfy these requirements. They propose an advanced key-management architecture provided with secure SCADA communications.

The contributions of their work are two-fold. First, our scheme supports both message broadcasting and secure communication. Second, by evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU), their protocol avoids any potential performance bottleneck of the system.

Is their paper highlights the key-management scheme for the SCADA systems among the security problems. Most SCADA systems require message broadcasting and secure communications. Although the existing key-management schemes for SCADA systems provide the secure communications, these schemes do not support the secure message broadcasting. In this paper, they have proposed a key-management architecture for secure SCADA communications.

The contributions of the work are two-fold. First, a scheme supports both the message broadcasting and the secure communications. Second, by evenly spreading much of the total amount of computation across high power nodes (MTU or SUB-MTU), the protocol avoids any potential performance bottleneck of the system while keeping the burden on low power nodes (RTU) at minimal.

Savas¸ S¸ ahin, Mehmet Ölmez, and Yalçın ˙Is¸ler, *Student Member, IEEE (2010)* [6] describes that in the field of automation technology, research and development for industrial applications has increased rapidly in recent years. Therefore, industrial automation and control education is a very important element of the industrialization process in developing countries. This paper gives a detailed description of some laboratory experiments in virtual-instrument aided supervisory control and data acquisition (SCADA) systems.

These experiments have been developed as part of education strategy in the Automation Laboratory of Ege Vocational School, Ege University, ˙Izmir, Turkey. The advantages and the challenging points of these experiments are also discussed and evaluated. A quantitative evaluation was achieved using a one-way ANOVA test performed on the exam results of the students. The qualitative evaluation was performed using a survey given to the students. The results indicated that the performance of the students was improved compared to the previous years' students.

M. Coates, Kenneth M. Hopkinson, *Member, IEEE*, Scott R. Graham, *Member, IEEE*, and Stuart H. Kurkowski, *Member, IEEE* (2010) [7] indicates that this paper discusses the use of a communications network security device, called a trust system, to enhance security of supervisory control and data-acquisition (SCADA). The major goal of the trust system is to increase security with minimal impact on utility communication systems. This paper concentrates on placing the trust system into a broader context, creates new trust system implementations to increase its flexibility, and demonstrates the trust system using TCP traffic. 1) The paper summarizes major threats against SCADA systems; 2) Discusses new trust system implementations, which allow the trust system to be used with a wider array of network-enabled equipment; 3) Discusses key SCADA security issues and shows how the trust system responds to such issues; 4) the paper shows the impact of the trust system when widely prevalent TCP/IP network communication is used; and 5) finally, the paper discusses a new hypothetical scenario to illustrate the protection that a trust system provides against insider threats.

The paper concludes that the proposed Trust system will comply with the strict requirements of the SCADA network while providing a secure environment. The trust system is flexible and can be implemented in whatever way best fits the needs of SCADA networks. The trust system enforces access restrictions between IP addresses that should not be allowed to communicate with one another via specific message types and interfaces.

The trust system, implemented in active mode, intercepts all malicious messages. Their research shows that a more secure network can be established, using a trust system, for the power grid. The trust system is a step toward security for the Utility network. In addition, there are a number of recommendations that can be made in order to strengthen security. Strict access controls should be enforced and only the minimum rights should be granted to an individual to accomplish their jobs. Passwords should be robust. Transmissions from RTU's, PLC's, and IED's should be protected by digital certifications and digital signatures to prevent unauthorized users from intercepting the information or introducing false data into the SCADA system. Finally, cyber security needs to be a priority for system administrators.

SCADA systems may be of interest to hackers and unauthorized users. Administrators should take precautions including closing unnecessary ports, keeping system patches up to date, and should keep up to date on current computer security practices. The trust system described in this paper can serve as an aid in many of these recommendations, but administrators also need constant vigilance to protect their portions of the electric power grid.

Donghyun Choi, *Student Member, IEEE*, Sungjin Lee, Dongho Won, and Seungjoo Kim, *Member, IEEE (*2010) [8] describes in this paper, authors propose are efficient scheme that decreases the computational cost for multicast communication. Reduces the number of keys to be stored in a remote terminal unit and provides multicast and broadcast communications.

Recently, in AKMA the authors proposed advanced key-management architecture for the secure SCADA communications and redefined security requirements for a SCADA system, analyzed the previous key-management protocols, and proposed a new key-management scheme suitable for secure SCADA communications. While SKE and SKMA do not meet the security requirements, AKMA satisfies the security needs, in that it supports message broad-casting and secure communications. Although the overall performance of ASKMA has many advantages compared to previous studies, it can be less efficient during the multicast communication process.

Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta (2011) [9] indicates that this paper presents an innovative approach to Intrusion Detection in SCADA systems based on the concept of Critical State Analysis and State Proximity. The theoretical framework is supported by tests conducted with an Intrusion Detection System prototype implementing the proposed detection approach.

The key elements of their technique are the concept of Critical State, and the assumption that an attacker aiming at damaging an industrial installation (like a Power Plant), will have to modify, for achieving that result, the state of the system from safe to critical. The critical state validation, normally hardly applicable in traditional ICT systems, finds its natural application in the industrial control field, where the critical states are generally well-known and limited in number.

Carlos Queiroz, Abdun Mahmood, and Zahir Tari (2011) [10] describes that recent attacks on SCADA systems highlight the need of stronger SCADA security. It is important to analyze the security risks and develop appropriate security solutions to protect such systems. However, a key problem is the lack of proper modeling tools to evaluate the security of SCADA systems. As widely accepted in academic and industrial communities, it is impractical to conduct security experiments on live systems. The authors proposed framework is a novel solution to create realistic simulations of SCADA systems based on a combination of network simulation and real devices connectivity. It solves a number of logical and implementation problems in the widely used OMNET++ simulation environment to allow real world devices (such as smart meters, RTUs, etc.) to be attached to the simulator. The simulation framework, SCADA Sim, also allows us to study the effects of malicious attacks on the devices and on the simulated network. Their proposed framework provides realistic evaluations of SCADA systems by adding real devices into the simulation. Two practical case studies on smart grid simulation were conducted with DDoS and spoofing attacks being presented. Results demonstrate that SCADA Sim closely simulates the realistic behavior of actual SCADA devices.

Tetsuo Otani, *Member, IEEE*, & Hiromu Kobayashi, *Member, IEEE (*2013) [11] Indicate that the authors examine a future distribution system capable of solving problems caused by the connection of numerous distributed generators. A supervisory-control-and-data-acquisition (SCADA) system for this distribution system should be economical, flexible, and reliable, and should execute a real-time process. In this paper, the authors propose a SCADA system using mobile agents for flexibility. In addition, they show two types of communication protocols that make agent migration more fault-tolerant, and perform experiments where the SCADA system executes earth fault protection within the required time. These results indicate that the SCADA system based on our proposed technologies should be capable to fulfill real-time processing requirement.

They have proposed a SCADA system for the ADAPS using mobile agents and a wide-area Ethernet. It could be made economical and flexible due to the characteristics of these two technologies. In addition, the agents have QoS control methods; via which processing is scheduled according to three priorities, and communication congestion would be avoided. Two types of protocols for agent migration are provided in the SCADA system, one of which iteratively sends a datagram packet to a destination to contribute to real-time and reliable processing in this system. Conversely, wide-area Ethernet is composed of ADS and PON.

The Ethernet-ADS provides RSTP that is capable of establishing an alternative route in case of communication failure. Conversely, the Ethernet-PON economically connects DSIF in significant volume. We performed experiments to evaluate the real-time performance and reliability of the SCADA system we propose. The system completed earth fault protection within the required time (1 s) in cases where an alternative communication route was established within 550 ms by RSTP in the Ethernet-ADS. We considered the feasibility of the SCADA system based on the experimental results and state-of-the-art communication technologies. In terms of real-time performance with fault tolerance, the current RSTP performance should be rapid enough to complete earth fault protection within the required time. Also boosting the feasibility of the SCADA system is the use of the real-time specification for Java in the implementation of mobile agents.

The expandability of the SCADA system should be ensured by multicast used in the iterative transmission protocol and the roundtrip of rapid and best-effort agents. According to these results and considerations, we conclude that the SCADA system we propose should satisfy the requirements.

J. I. Escudero, J. Luque*, Member, IEEE*, and A. Carrasco (2004) [12] indicates that the study of the existing relationship between a measurement error and the time elapsed since that measurement was taken in the field, a period of time which can be called the *datum age*, will allow us to learn about its behavior in a supervisory control and data acquisition (SCADA) system. This study has allowed knowing that, in the case of electrical measurements, they quickly reach their maximum error value because of their age. Therefore, it is not necessary to send measurements to the control center at small intervals: it is possible to wait a given time without having a higher associated error. After getting these results, we have done an experimental study about electrical measurements, in which these measurements are sent to the control center only if they exceed a given percentage of the former measurement, what we call measurement tolerance.

In this paper, it has been experimentally proved that this send-by-tolerance method significantly reduces the transmission channel load, so the system can benefit from this because the bandwidth can be reused by more remote units, as well as performance of the existing ones is improved. In this paper, they have studied the behavior of the measurement with respect to its age (the elapsed time from taking the measurement in the field until the present moment). This study has showed how a measurement error due to datum age quickly reaches its maximum value, so this error does not grow even if the datum still remains at the remote unit before being sent to the control center. This outcome has allowed us to carry out an experimental study based on the tolerance of the measurements, on account of which only those measurements that go beyond a given percentage, relative to the last sent value, are sent. They have experimentally proved that this sending system drastically reduces channel occupation without altering the quality of the measurements being sent within SCADA systems.

J. I. Escudero, J. A. Rodríguez, M. C. Romero, and S. Díaz (2005) [13] indicates that this paper they analyze special characteristics and propose solutions so multimedia integration with SCADA is possible in power systems communication. More and more frequently, electric utilities are equipped with an underlying data network (usually one of optic fiber) whose bandwidth is suitable for video, audio and data transport. Also innovations on communications technologies like power-line communications and wireless networks are important factors to take into account for this integration. From a technical approach, this integration is feasible, such as they have described in this paper, and they are still working on the implementation of a specific system and about transmission of multimedia and tele control information. This integration extends functionality of SCADA system, and enriches existing tele control functions by adding new operation, maintenance support, and operators training functions.

Euan M. Davidson, Stephen D. J. McArthur, *Member, IEEE*, James R. McDonald, *Senior Member, IEEE*, Tom Cumming, and Ian Watt (2006) [14] indicates that their paper reports on the use of multi-agent system technology to automate management and analysis of SCADA and digital fault recorder (DFR) data. The multi-agent system, entitled Protection Engineering Diagnostic Agents (PEDA), integrates legacy intelligent systems that analyze SCADA and DFR data to provide data management and online diagnostic information to protection engineers. As the results presented in this paper demonstrate, PEDA supports protection engineers by providing access to interpreted power systems data via the corporate intranet within minutes of the data being received.

In this paper, the authors discuss their experience of developing a multi-agent system that is robust for continual online use within the power industry. The use of existing agent development toolsets and standards is also discussed. In this paper they have presented experience of implementing a system for deployment in the power industry. The results presented demonstrate state-of the- art and multi-agent system technology exhibits both the robustness and flexibility required for use within the power industry for the type of application described in this paper. The application of MAS technology to real-time power system control applications requires a greater level of robustness than that required for automated post-fault analysis; however, results from the trials of the PEDA system should be seen as a positive indication that MAS technology is maturing to the point where the realization of a range of meaningful applications can be achieved.

Igor Nai Fovino, Alessio Coletta, Andrea Carcano, and Marcelo Masera (2012) [15] describe that they present an innovative approach to the design of filtering systems based on the state analysis of the system being monitored. The aim is to detect attacks composed of a set of “SCADA” commands that, when considered in isolation on a single-packet basis, can disrupt the correct behavior of the system when executed in particular operating states. The proposed firewall detects these complex attacks Furthermore, they detail the design of the architecture of the firewall for systems that use the Modbus and DNP3 protocols, and the implementation of a prototype, providing experimental comparative results that confirm the validity of the proposed approach. This paper presents a new network filtering approach for the detection and mitigation of a particular class of cyber attacks against industrial installations. This technique is based on monitoring the evolution of the state of the protected system and on the analysis of the command packets between master and slaves of SCADA architecture.

The key elements of this technique are the concept of *critical state* and the observation that an attacker, in order to damage an industrial system, will have to modify its state from secure to critical. The critical state validation, normally hardly applicable in traditional ICT systems, finds its natural application in the industrial control field, where the critical states are generally well-known and limited in number. The introduction of the concept of critical state distance allowed extending the firewall features in the direction of a more complete early warning system.

The results of the tests conducted on a prototype implementing the described approach demonstrate the feasibility of the method. This approach presents advantages on traditional filtering techniques: 1) Since the network filtering is applied on the basis of the system evolution and not on the basis of the attack evolution (something unknown), for predefined critical state this approach allows to block “zero day attacks,” i.e., attacks based on unknown techniques. 2) The number of false positives results limited since the traffic is dropped only if the analyzed command will drive the system into a described critical state. Only two cases can have false positives or false negatives: the case in which a critical state has not been described (and this is an error performed by who configured the firewall rules) or if the real system and its virtual image are desynchronized (and this is due eventually to an error in the configuration of the auto synchronization time between the real system and the virtual system). This technique, being conceived to protect the SCADA devices, cannot protect from more traditional ICT attacks such as virus attacks to general purpose ICT systems. For this reason, we see the critical state based filtering as a technique complementary to the traditional firewall techniques, helping in enhancing the security of these systems. The configuration of the rule set is not cheap in term of effort; however, to facilitate this process, they are planning to develop a self-discovery engine able to automatically learn the configuration of the system to be protected. Moreover, for the future, they are planning to conduct a more extended campaign of tests on real production systems.

Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen (2013) [16] indicate that their paper aims to perform security threat assessment of networked control systems with regulatory and supervisory control layers. They analyze the performance of a proportional-integral controller (regulatory layer) and a model based diagnostic scheme (supervisory layer) under a class of deception attacks. They adopt a conservative approach by assuming that the attacker has knowledge of: 1) the system dynamics; 2) the parameters of the diagnostic scheme; and 3) the sensor-control signals. The deception attack presented here can enable remote water pilfering from automated canal systems. They also report a field-operational test attack on the Gignac canal system located in Southern France. They have conducted security threat assessment of hierarchically structured water SCADA systems, and presented results from a field operational test on the Gignac water SCADA system. They studied the effect of stealthy deception attacks on a PI control scheme (regulatory layer) and a UIO based diagnostic scheme (supervisory layer). Both schemes used downstream sensor measurements. This is typically the case when off takes are located at the downstream end of the canal pools. They find that, although the diagnostic scheme works well for non simultaneous random withdrawals but it is not robust to the deception attack. Our field operational test demonstrates that such attacks can be stealthy, i.e., they can bypass detection by the SCADA system.

The characterization of stealthy attacks is important because it can guide the deployment of IT-specific security mechanisms and enable the design of better attack diagnostic schemes. Their analysis is extended to the case when multiple sensor measurements *ydi* are subject to attacks. A possible stealthy attack strategy is to first compromise the most downstream sensor measurement *ydm*, and systematically proceed to compromise upstream sensor measurements. An interesting research question is then to characterize the relation between the resources required by the attacker and the impact of the resulting attack. Such analyses can ultimately lead to a rigorous framework for security threat assessment of NCS/SCADA systems.

Jonathan Kirsch, Stuart Goose, Yair Amir, *Member, IEEE*, DongWei, *Member, IEEE*, and Paul Skare, *Member, IEEE (*2014) [17] indicate that this paper reports on the experience designing, architecting, and evaluating the first *survivable* SCADA system—one that is able to ensure correct behavior with minimal performance degradation even during cyber attacks that compromise part of the system. They describe the challenges they faced when integrating modern intrusion-tolerant protocols with a conventional SCADA architecture and present the techniques they developed to overcome these challenges. The results illustrate that the survivable SCADA system not only functions correctly in the face of a cyber attack, but it also processes in excess of 20, 000 messages per second with a latency of less than 30 ms, making it suitable for even large-scale deployments managing thousands of remote terminal units. In addition to the conventional challenges to availability, such as hardware crashes, power failures, and network partitions, SCADA providers must also anticipate the consequences of cyber attacks. Whereas conventional enterprise security techniques have sought to build increasingly sophisticated perimeter defenses, in this research we sought to answer whether it is possible to build a SCADA system that is able to operate correctly giving performance even if a cyber attack was successful at evading these conventional defenses. As the compromise of the highest value asset, the SCADA Master, can have potentially disastrous consequences, their work has focused on protecting this entity via intrusion-tolerant replication. In effect, intrusion tolerance allows the SCADA Master application to act as its own firewall, thus providing protection in the event of a security breach. This paper reports on our experience designing and evaluating the first survivable SCADA system. We described the unique requirements imposed by the SCADA architecture and gave an overview of several new techniques facilitating the integration of intrusion-tolerant replication and SCADA. Our experimental results illustrate that our replication engine performs sufficiently well to meet the needs of even large-scale SCADA systems containing thousands of RTUs.

Shyh-Jier Huang, *Senior Member, IEEE,* and Chih-Chieh Lin (2002) [18] describe in this paper, an asynchronous transfer mode (ATM)-based network is applied as the communication backbone between geographical information system (GIS) and supervisory control and data acquisition (SCADA). Because the ATM network is a true multiservice network that provides broadband services and meets the different quality of service requirements, this technique is increasingly important in a modern communication system. The paper begins with the event generator that brings different messages to the ATM network from various local area networks. A statistical evaluation is then employed to examine the amount of message flow and the quality of service, where the outcome is assessed based on traffic, capacity and performance of the proposed method. Test results help solidify the effectiveness of the approach for power system communication applications. In this paper, an ATM based communication network was proposed to serve as the backbone between the GIS and SCADA system.

The paper begins with the event generator that brings different messages to the ATM network from various local area networks. This is followed by a statistical evaluation for investigating the amount of message flow and the quality of service in different applications. To investigate the effectiveness of the approach, the communication network performance was also evaluated when the integrated system operates with other software systems. Test results demonstrated the feasibility and practicality of the proposed method.

Verónica Medina, Isabel Gómez, Joaquín Luque, *Member, IEEE*, and Sergio Martín (2002) [19] indicate that this paper presents the use of ESTELLE, a formal description technique, as a method to calculate automatically the performance of telecontrol protocols in SCADA systems. Some specific primitives are added to the ESTELLE description language in order to achieve that goal. As an example, we analyze the performance of a telecontrol protocol. The results from this method are compared to performance measurements obtained from analytical and simulated solutions The optimization of telecontrol protocols can reduce the installation costs of telecontrol systems in power utilities. FDTs are used to specify protocols, for which ESTELLE is more suitable than other methods in the electrical sector. Primitives added to ESTELLE make it possible to measure the performance of such protocols; therefore, telecontrol protocols can be improved. These improvements could simply consist of setting up some new parameters for an existing telecontrol protocol or replacing them with better ones (for instance, standardized ones). In this paper, this alternative method for studying the performance of a telecontrol protocol has been presented.

Savaş Şahin and Yalçin İşler, *Member, IEEE* (2013) [20] describes that this paper describes how supervisory control and data acquisition (SCADA) and robotics experiments in control and automation education can be conducted at reasonable cost. These setups consist of a fluid tank, a Cartesian robot with a three-axis robot arm, and serial, parallel, USB, and TCP/IP communication ports. The presented experiments were also quantitatively evaluated using the one-way ANOVA test on the exam results, and qualitatively evaluated by a discussion session and survey. The results indicated that student performance improved when microcontroller-based experimental setups were used.

Amit Shrivastava and Anand Khare (2014) [21] have discussed the Micro Grid model which simulates a power system and has the features of SCADA automation to study its advantages and to finally implement it in real power system. It suggests the approximate cost to build the model along with the SCADA Architecture. It also suggests some experiments which can be done on this proposed smart GRID Model.

Ramleela Khare and Filipe R E Melo (2014) [22] Automation provides optimized solution to problems of storage and distribution of water. The chapter highlights low cost new equipment and new techniques for reliable and efficient management of this technology. The entire network including a standby generator has features of SCADA (Supervisory Control and Data Acquisition) automation to control and monitor water supply and in case of power failures to maintain continuity of power supply. The scheme of automation is such that the Manager of water project is able to implement it with full understanding of the project without being dependent on contractors and suppliers.

3. CONCLUSIONS

The rapid increase in research and development in automation technology has led to a gap between education and industry. Developing countries need to keep in touch with the latest developments; this poses some difficulties for education in industrial automation, such as cost, lack of student motivation, and insufficient laboratory infrastructure. Low-cost experimental setups may overcome many of these challenges described by the author in his paper "Economic and Efficient Management of Transmission and Control of Electrical Power - Design of A SCADA Power System Monitor". The author has developed the Power System Monitor described in details elsewhere in chapter 4 see reference for details [23] which demonstrates the application of SCADA architecture for automation. Supervisory Control and Data Acquisition (SCADA) has been demonstrated on the Dynamic model of Power System Monitor constructed for the purpose. One can get clear understanding of how to implement SCADA automation in industry to improve economic and efficient management of all activities.

ACKNOWLEDGEMENT

I would like to thank The MRPC Company for funding the project for research on SCADA Automation. I would also like to thank Mr. Ravi Kumar for making the diagrams on coral draw software.

REFERENCES

[1] *Charles T. Lindeberg' and Wayne R. (*1993) Project Planning For Ems & SCADA Systems *Block2 lEEE Compiler Applications in Power* ISSN 08950156/93/$3.0001993 IEEE

[2] *David Leslie', Andrew Hlushko', Samer Abughazaleh. And Frank* Garza3 (1994) Tailoring SCADA Systems for Standby Power Applications, IEEE *Computer Applications in Power* ISSN 08954156/94/$4 OID1994 IEEE

[3] Dimitris Th. Askounis and Emmanuel Kalfaoglou (2000) Greek Ems-SCADA: From the Contractor to the User IEEE Transactions on Power Systems, VOL. 15, NO, 4, November 2000

[4] Mini S. Thomas, *Senior Member, IEEE*, Parmod Kumar, and Vinay K. Chandna (2004) Design, Development, And Commissioning Of A Supervisory Control And Data Acquisition (SCADA) Laboratory for Research And Training IEEE Transactions On Power Systems, VOL.19, NO.3, AUGUST 2004

[5] Donghyun Choi, *Student Member, IEEE*, Hakman Kim, Dongho Won, and Seungjoo Kim, *Member, IEEE (2009)* Advanced Management Architecture For Secure SCADA Communications IEEE

Transactions On Power Delivery, VOL. 24, No. 3, JULY 2009

[6] Savas¸ S¸ ahin, Mehmet Ölmez, and Yalçın ˙Is¸ler, *Student Member, IEEE (2010)* Micro-controller-Based Experimental Setup & Experiments for SCADA Education IEEE transactions on education, VOL.53, NO.3, August 2010

[7] Gregory M. Coates, Kenneth M. Hopkinson, *Member, IEEE*, Scott R. Graham, *Member, IEEE*, and Stuart H. Kurkowski, *Member, IEEE* (2010) A Trust System Architecture For SCADA Network Security IEEE Transactions On Power Delivery, VOL. 25, NO. 1, January 2010 Gregory

[8] Donghyun Choi, *Student Member, IEEE*, Sungjin Lee, Dongho Won, and Seungjoo Kim, *Member, IEEE (*2010) Efficient Secure Group Communi-cations for SCADA IEEE Transactions on Power Delivery, VOL.25, NO.2, April 2010

[9] Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, and A. Trombetta (2011) A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems IEEE Transactions on Industrial Informatics, VOL. 7, NO. 2, MAY 2011

[10] Carlos Queiroz, Abdun Mahmood, and Zahir Tari (2011) Scadasim—A Framework for Building SCADA Simulations IEEE Transactions on Smart Grid, VOL.2, NO.4, DECEMBER 2011

[11] Tetsuo Otani, *Member, IEEE*, and Hiromu Kobayashi, *Member, IEEE (*2013)

A SCADA System Using Mobile Agents For Next-Generation Distribution System IEEE Transactions On Power Delivery, Vol.28, No.1, January 2013

[12] J. I. Escudero, J. Luque, *Member, IEEE*, and A. Carrasco (2004) Experimental Study on The Transmission of Measurements by Tolerance in SCADA systems IEEE transactions on power delivery, vol. 19, no. 2, April 2004

[13] J. I. Escudero, J. A. Rodríguez, M. C. Romero, and S. Díaz (2005) Deployment Of Digital Video And Audio Over Electrical SCADA Networks IEEE Transactions On Power Delivery, Vol. 20, no. 2, April 2005

[14] Euan M. Davidson, Stephen D. J. McArthur, *Member, IEEE*, James R. McDonald, *Senior Member, IEEE*, Tom Cumming, and Ian Watt (2006) Applying Multi-Agent System Technology In Practice: Automated Management And Analysis Of SCADA and digital fault recorder data IEEE transactions on power systems, vol. 21, no. 2, may 2006

[15] Igor Nai Fovino, Alessio Coletta, Andrea Carcano, and Marcelo Masera (2012) Critical State-Based Filtering System For Securing SCADA Network Protocols IEEE transactions on industrial electronics, vol.59, no.10, October 2012

[16] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M. Bayen (2013) Cyber security of water SCADA systems—part i: analysis and experimentation of stealthy deception attacks IEEE transactions on control systems technology, vol. 21, no. 5, September 2013

[17] Jonathan Kirsch, Stuart Goose, Yair Amir, *Member, IEEE*, Dongwei, *Member, IEEE*, and Paul Skare, *member, IEEE (*2014) survivable SCADA via intrusion-tolerant replication IEEE transactions on smart grid, vol. 5, no. 1, January 2014

[18] Shyh-Jier Huang, *Senior Member, IEEE,* and Chih-Chieh Lin (2002) Application of ATM-Based Network for An Integrated Distribution SCADA-GIS System IEEE Transactions on Power Systems, Vol.17, No.1, February 2002

[19] Verónica Medina, Isabel Gómez, Joaquín Luque, *Member, IEEE*, and Sergio Martín [2002] Estelle: A Method to Analyze Automatically The Performance Of Telecontrol Protocols In SCADA Systems IEEE Transactions On Power Delivery, Vol.17, No.3, July 2002

[20] Savaş Şahin and Yalçin İşler, *Member, IEEE [*2013] Microcontroller-Based Robotics and SCADA Experiments IEEE Transactions On Education, Vol.56, No.4, November 2013

[21] PhD thesis Communication with Amit Shrivastava and Dr. Anand khare with reference to the PhD thesis submitted to Bhagwant University 2014

[22] Ramleela Khare, Dr Filipe Rodrigues E Melo, "Automation of Water Distribution Plant", IJREAT International Journal of Research in Engineering & Advanced Technology, Vol. 2, Issue 1, Feb-Mar, 2014, ISSN 23208791

[23] Ramleela Khare, Filipe Rodrigues e Melo "Economic And Efficient Management of Transmission And Control of Electrical Power - Design of A SCADA Power System Monitor", Sinhgad International Business Review, Vol. - V, Issue - II, January 2012 - June 2012, ISSN No. : 0974-0597.