Securing Communication of SCADA Components in Smart Grid Environment

Tai-hoon Kim[1*]

[*]Corresponding Author
[1]Multimedia Engineering Department, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
taihoonn@hnu.kr

***Abstract*—** SCADA is a Process Control Systems, designed to automate systems such as traffic control, power grid management, waste processing etc. Conventionally, SCADA is connected only in a limited private network because SCADA is considered a critical infrastructure, and connecting to the internet may put the society on jeopardy, SCADA operators hold back on connecting it to the public network like the internet. Connecting SCADA to the Internet can provide a lot of advantages in terms of control, data viewing and generation. SCADA infrastructures like electricity can also be a part of a Smart Grid. Connecting SCADA to a public network can bring a lot of security issues. In this paper, a SCADA communication security solution using crossed-crypto-scheme is proposed.

***Keywords*—** Smart Gird , SCADA, Security Issues, Encryption, Crossed Crypto-scheme.

I. INTRODUCTION

Smart Grid was built when energy was relatively inexpensive. While minor upgrades have been made to meet increasing demand, the grid still operates the way it did almost 100 years ago—energy flows over the grid from central power plants to consumers, and reliability is ensured by maintaining excess capacity. Infrastructures like electricity which is controlled by SCADA can play a big role on Smart Grids.

SCADA is a concept that is used to refer to the management and procurement of data that can be used in developing process management criteria. The use of the term SCADA varies, depending on location. In North America, SCADA refers to a distributed measurement and management system that operates on a large-scale basis. For the rest of the world, SCADA refers to a system that performs the same basic functions, but operates in a number of different environments as well as a multiplicity of scales. While the use of the term SCADA may not be uniform, many components are the same, regardless of the scale of the process.

On the Next parts of this paper, we discuss SCADA, the conventional setup and the Smart Grid. Advantages which can be attained using the Smart Grid are also covered. Security issues are being pointed out. We also suggest a security solution for a Web based SCADA using symmetric key encryption. Procedure for Paper Submission

II. SCADA SYSTEMS

SCADA systems are primarily control systems. A typical control system consists of one or more remote terminal units (RTU) connected to a variety of sensors and actuators, and relaying information to a master station.

For the most part, the brains of a SCADA system are performed by the Remote Terminal Units (sometimes referred to as the RTU). The Remote Terminal Units consists of a programmable logic converter. The RTU are usually set to specific requirements, however, most RTU allow human intervention, for instance, in a factory setting, the RTU might control the setting of a conveyer belt, and the speed can be changed or overridden at any time by human intervention. In addition, any changes or errors are usually automatically logged for and/or displayed. Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention.

One of key processes of SCADA is the ability to monitor an entire system in real time. This is facilitated by data acquisitions including meter reading, checking statuses of sensors, etc that are communicated at regular intervals depending on the system. Besides the data being used by the RTU, it is also displayed to a human that is able to interface with the system to override settings or make changes when necessary.

2.1SCADA Software

Supervisory Control and Data Acquisition software can be divided into proprietary type or open type. Proprietary software are developed and designed for the specific hardware and are usually sold together. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems are designed to communicate and control different types of hardware. It is popular because of the interoperability they bring to the system. [1] WonderWare and

Citect are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system.

2.1.1 SCADA Communication

SCADA systems have traditionally used combinations of radio and direct serial or modem connections to meet communication requirements, although Ethernet and IP over SONET / SDH is also frequently used at large sites such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry.

This has also come under threat with some customers wanting SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though. SCADA protocols are designed to be very compact and many are designed to send information to the master station only when the master station polls the RTU. Typical legacy 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 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced.

RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. A list of automation protocols is being compiled here.

Recently, OLE for Process Control (OPC) has become a widely accepted solution for intercommunicating different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network.

Central computer of the data acquisition system, located in the hydro power plant, provides measurements performance according to a preset program, the instrumentation existing at this time and remote communications by RS485 bus, using Master-Slave architecture and IEC1107, Modbus RTU, ASCII protocols.

2.2 SCADA Hardware

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves. [2]

The communications system provides the pathway for communication between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station.

2.3 Human Machine Interface

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesired outputs to the human.

Ever since the increased use of personal computers and the relative decline in societal awareness of heavy machinery, the term user interface has taken on overtones of the (graphical) user interface, while industrial control panel and machinery control design discussions more commonly refer to human-machine interfaces.

The design of a user interface affects the amount of effort the user must expend to provide input for the system and to interpret the output of the system, and how much effort it takes to learn how to do this. Usability is the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying.

Usability is mainly a characteristic of the user interface, but is also associated with the functionalities of the product and the process to design it. It describes how well a product can be used for its intended purpose by its target users with efficiency, effectiveness, and satisfaction.

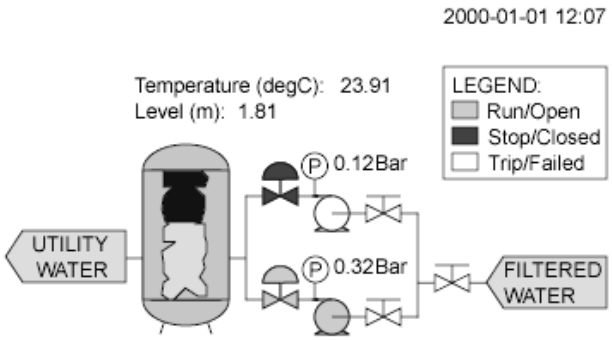

Figure 1. An Example of a SCADA Human Machine Interface

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

Alarm handling is an important part of most SCADA implementations. The system monitors whether certain alarm conditions are satisfied, to determine when an alarm event has occurred. Once an alarm event has been detected, one or more actions are taken (such as the activation of one or more alarm indicators, and perhaps the generation of email or text messages so that management or remote SCADA operators are informed). In many cases, a SCADA operator may have to acknowledge the alarm event; this may deactivate some alarm indicators, whereas other indicators remain active until the alarm conditions are cleared. Alarm conditions can be explicit - for example, an alarm point is a digital status point that has either the value NORMAL or ALARM that is calculated by a formula based on the values in other analogue and digital points - or implicit: the SCADA system might automatically monitor whether the value in an analogue point lies outside high and low limit values associated with that point. Examples of alarm indicators include a siren, a pop-up box on a screen, or a colored or flashing area on a screen (that might act in a similar way to the "fuel tank empty" light in a car); in each case, the role of the alarm indicator is to draw the operator's attention to the part of the system 'in alarm' so that appropriate action can be taken. In designing SCADA systems, care is needed in coping with a cascade of alarm events occurring in a short time, otherwise the underlying cause (which might not be the earliest event detected) may get lost in the noise. Unfortunately, when used as a noun, the word 'alarm' is used rather loosely in the industry; thus, depending on context it might mean an alarm point, an alarm event or an alarm indicator.

II. INSTALLATION OF SCADA SYSTEMS

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.[3][4]

3.1 Conventional Supervisory Control and Data Acquisition

The function of SCADA is collecting of the information, transferring it back to the central site, carrying out any necessary

analysis and control and then displaying that information on a number of operator screens. Systems automatically control the actions and control the process of automation.

Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU and other electronic devices, manufacturers incorporated digital electronics into relay logic equipment. Programmable logic controllers or PLC's are still the most widely used control systems in industry. As need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs (Programmable logic controllers) and DCS (distributed control systems) are used as shown in Figure 2.

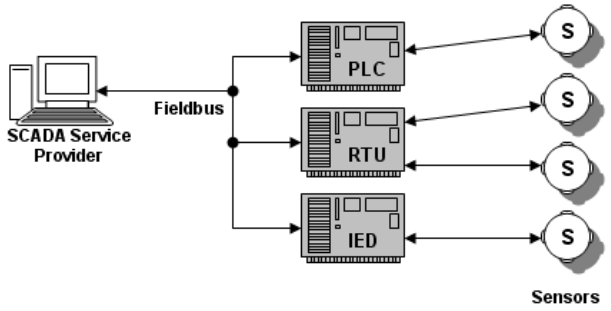

Figure. 2 Common SCADA Installation utilizing Remote Terminals (PLC/DCS, Sensors) and Master Station connected using a fieldbus.

IV. SMART GRID

A smart grid includes an intelligent monitoring system that keeps track of all electricity flowing in the system. It also incorporates the use of superconductive transmission lines for less power loss, as well as the capability of integrating alternative sources of electricity such as solar and wind. When power is least expensive a smart grid could turn on selected home appliances such as washing machines or factory processes that can run at arbitrary hours. At peak times it could turn off selected appliances to reduce demand. Similar proposals include smart electric grid, smart power grid, intelligent grid (or intelligrid), FutureGrid, and the more modern intergrid and intragrid. In principle, the smart grid is a simple upgrade of 20th century power grids which generally "broadcast" power from a few central power generators to a large number of users, to instead be capable of routing power in more optimal ways to respond to a very wide range of conditions, and to charge a premium to those that use energy at peak hour.

The conditions, to which a smart grid, broadly stated, could respond, occur anywhere in the power generation, distribution and demand chain. Events may occur generally in the environment (clouds blocking the sun and reducing the amount of solar power, a very hot day), commercially in the power supply market (prices to meet a high peak demand), locally on the distribution grid (MV transformer failure requiring a temporary shutdown of one distribution line) or in the home (someone leaving for work, putting various devices into hibernation, data ceasing to flow to an IPTV), which motivate a change to power flow.

Latency of the data flow is a major concern, with some early smart meter architectures allowing actually as long as 24 hours delay in receiving the data, preventing any possible reaction by either supplying or demanding devices. [3].

The Smart Grid is the application of modern information, communication, and electronics technology to the electricity delivery infrastructure as shown in figure 3.

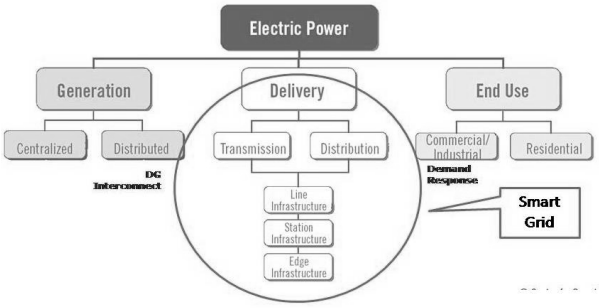

Figure 3. Smart Grid

The earliest, and still largest, example of a smart grid is the Italian system installed by Enel S.p.A. of Italy. Completed in 2005, the Telegestore project was highly unusual in the utility world because the company designed and manufactured their own meters, acted as their own system integrator, and developed their own system software. The Telegestore project is widely regarded as the first commercial scale use of smart grid technology to the home, and delivers annual savings of 500 million euro at a project cost of 2.1 billion euro. [5]

A smart grid is an umbrella term that covers modernization of both the transmission and distribution grids. The modernization is directed at a disparate set of goals including facilitating greater competition between providers, enabling greater use of variable energy sources, establishing the automation and monitoring capabilities needed for bulk transmission at cross continent distances, and enabling the use of market forces to drive energy conservation.

Many smart grid features readily apparent to consumers such as smart meters serve the energy efficiency goal. The approach is to make it possible for energy suppliers to charge variable electric rates so that charges would reflect the large differences in cost of generating electricity during peak or off peak periods. Such capabilities allow load control switches to control large energy consuming devices such as hot water heaters so that they consume electricity when it is cheaper to produce.

4.1 Smart Grid Functions

Before examining particular technologies, a proposal can be understood in terms of what it is being required to do. The governments and utilities funding development of grid modernization have defined the functions required for smart grids. Smart Grid must have the following functions:

4.1.1 Self-healing

Using real-time information from embedded sensors and automated controls to anticipate, detect, and respond to system problems, a smart grid can automatically avoid or mitigate power outages, power quality problems, and service disruptions.

As applied to distribution networks, there is no such thing as a "self healing" network. If there is a failure of an overhead power line, given that these tend to operate on a radial basis (for the most part) there is an inevitable loss of power. In the case of urban/city networks that for the most part are fed using underground cables, networks can be designed (through the use of interconnected topologies) such that failure of one part of the network will result in no loss of supply to end users. A fine example of an interconnected network using zoned protection is that of the Merseyside and North Wales Electricity Board (MANWEB).

It is envisioned that the smart grid will likely have a control system that analyzes its performance using distributed, autonomous reinforcement learning controllers that have learned successful strategies to govern the behavior of the grid in the face of an ever changing environment such as equipment failures. Such a system might be used to control electronic switches that are tied to multiple substations with varying costs of generation and reliability.

4.1.2 Consumer participation

A smart grid, is, in essence, an attempt to require consumers to change their behavior around variable electric rates or to pay vastly increased rates for the privilege of reliable electrical service during high-demand conditions. Historically, the intelligence of the grid in North America has been demonstrated by the utilities operating it in the spirit of public service and shared responsibility, ensuring constant availability of electricity at a constant price, day in and day out, in the face of any and all hazards and changing conditions. A smart grid incorporates consumer equipment and behavior in grid design, operation, and communication. This enables consumers to better control (or be controlled by) “smart appliances” and “intelligent equipment” in homes and businesses, interconnecting energy management systems in “smart buildings” and enabling consumers to better manage energy use and reduce energy costs. Advanced communications capabilities equip customers with tools to exploit real-time electricity pricing, incentive-based load reduction signals, or emergency load reduction signals. There is marketing evidence of consumer demand for greater choice.

4.1.3 Resist attack

Smart grid technologies better identify and respond to man-made or natural disruptions. Real-time information enables grid operators to isolate affected areas and redirect power flows around damaged facilities.

One of the most important issues of resist attack is the smart monitoring of power grids, which is the basis of control and management of smart grids to avoid or mitigate the system-wide disruptions like blackouts. The traditional monitoring is based on weighted least square (WLS) which is very weak and prone to fail when gross errors (including topology errors, measurement errors or parameter errors) are present. New technology of state monitor is needed to achieve the goals of the smart grids.

4.1.4 High quality power

Outages and power quality issues cost US businesses more than $100 billion on average each year. It is asserted that assuring more stable power provided by smart grid technologies will reduce downtime and prevent such high losses.

4.1.5 Accommodate generation options

As smart grids continue to support traditional power loads they also seamlessly interconnect fuel cells, renewables, microturbines, and other distributed generation technologies at local and regional levels. Integration of small-scale, localized, or on-site power generation allows residential, commercial, and industrial customers to self-generate and sell excess power to the grid with minimal technical or regulatory barriers. This also improves reliability and power quality, reduces electricity costs, and offers more customer choice.

4.1.6 Enable electricity market

Significant increases in bulk transmission capacity will require improvements in transmission grid management. Such improvements are aimed at creating an open marketplace where alternative energy sources from geographically distant locations can easily be sold to customers wherever they are located.

Intelligence in distribution grids will enable small producers to generate and sell electricity at the local level using alternative sources such as rooftop-mounted photo voltaic panels, small-scale wind turbines, and micro hydro generators. Without the additional intelligence provided by sensors and software designed to react instantaneously to imbalances caused by intermittent sources, such distributed generation can degrade system quality.

4.1.7 Optimize assets

A smart grid can optimize capital assets while minimizing operations and maintenance costs. Optimized power flows reduce waste and maximize use of lowest-cost generation resources. Harmonizing local distribution with interregional energy flows and transmission traffic improves use of existing grid assets and reduces grid congestion and bottlenecks, which can ultimately produce consumer savings.

4.1.8 Enable high penetration of intermittent generation sources

Climate change and environmental concerns will increase the amount of renewable energy resources. These are for the most part intermittent in nature. Smart Grid technologies will enable power systems to operate with larger amounts of such energy resources since they enable both the suppliers and consumers to compensate for such intermittency.

4.2 Features

Existing and planned implementations of smart grids provide a wide range of features to perform the required functions.

4.2.1 Load adjustment

The total load connected to the power grid can vary significantly over time. Although the total load is the sum of many individual choices of the clients, the overall load is not a stable, slow varying, average power consumption. Imagine the increment of the load if a popular television program starts and millions of televisions will draw current instantly. Traditionally, to respond to a rapid increase in power consumption, faster than the start-up time of a large generator, some spare generators are put on a dissipative standby mode. A smart grid may warn all individual television sets, or another larger customer, to reduce the load temporarily (to allow time to start up a larger generator) or continuously (in the case of limited resources). Using mathematical prediction algorithms it is possible to predict how many standby generators need to be used, to reach a certain failure rate. In the traditional grid, the failure rate can only be reduced at the cost of more standby generators. In a smart grid, the load reduction by even a small portion of the clients may eliminate the problem.

4.2.2 Demand response support

Demand response support allows generators and loads to interact in an automated fashion in real time, coordinating demand to flatten spikes. Eliminating the fraction of demand that occurs in these spikes eliminates the cost of adding reserve generators, cuts wear and tear and extends the life of equipment, and allows users to cut their energy bills by telling low priority devices to use energy only when it is cheapest.

Currently, power grid systems have varying degrees of communication within control systems for their high value assets, such as in generating plants, transmission lines, substations and major energy users. In general information flows one way, from the users and the loads they control back to the utilities. The utilities attempt to meet the demand and succeed or fail to varying degrees (brownout, rolling blackout, uncontrolled blackout). The total amount of power demand by the users can have a very wide probability distribution which requires spare generating plants in standby mode to respond to the rapidly changing power usage. This one-way flow of information is expensive; the last 10% of generating capacity may be required as little as 1% of the time, and brownouts and outages can be costly to consumers.

4.2.3 Greater resilience to loading

Although multiple routes are touted as a feature of the smart grid, the old grid also featured multiple routes. Initial power lines in the grid were built using a radial model, later connectivity was guaranteed via multiple routes, referred to as a network structure. However, this created a new problem: if the current flow or related effects across the network exceed the limits of any particular network element, it could fail, and the current would be shunted to other network elements, which eventually may fail also, causing a domino effect. See power outage. A technique to prevent this is load shedding by rolling blackout or voltage reduction (brownout).

4.2.4 Decentralization of power generation

Another element of fault tolerance of smart grids is decentralized power generation. Distributed generation allows individual consumers to generate power onsite, using whatever generation method they find appropriate. This allows individual loads to tailor their generation directly to their load, making them independent from grid power failures. Classic grids were designed for one-way flow of electricity, but if a local sub-network generates more power than it is consuming, the reverse flow can raise safety and reliability issues. A smart grid can manage these situations.

4.2.5 Price signaling to consumers

In many countries, including Belgium, the Netherlands and the UK, the electric utilities have installed double tariff electricity meters in many homes to encourage people to use their electric power during night time or weekends, when the overall demand from industry is very low. During off-peak time the price is reduced significantly, primarily for heating storage radiators or heat pumps with a high thermal mass, but also for domestic appliances. This idea will be further explored in a smart grid, where the price could be changing in seconds and electric equipment is given methods to react on that. Also, personal preferences of customers, for example to use only green energy, can be incorporated in such a power grid.

V. SCADA AND SMART GRID

The function of an Electrical grid is not a single entity but an aggregate of multiple networks and multiple power generation companies with multiple operators employing varying levels of communication and coordination, most of which is manually controlled. Smart grids increase the connectivity, automation

and coordination between these suppliers, consumers and networks that perform either long distance transmission or local distribution tasks.

- Transmission networks move electricity in bulk over medium to long distances, are actively managed, and generally operate from 345kV to 800kV over AC and DC lines.
- Local networks traditionally moved power in one direction, "distributing" the bulk power to consumers and businesses via lines operating at 132kV and lower.

This paradigm is changing as businesses and homes begin generating more wind and solar electricity, enabling them to sell surplus energy back to their utilities. Modernization is necessary for energy consumption efficiency, real time management of power flows and to provide the bi-directional metering needed to compensate local producers of power. Although transmission networks are already controlled in real time, many in the US and European countries are antiquated by world standards, and unable to handle modern challenges such as those posed by the intermittent nature of alternative electricity generation, or continental scale bulk energy transmission.

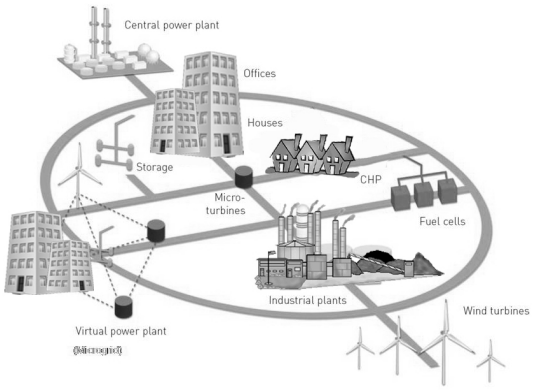

Figure 4. Vision of Smart Grid

Central & distributed generation Virtual aggregation of generators and loads for system management Grid components connected by both electrical and data networks Bi-directional power flows. The following figure shows how Smart Grid will look like.

5.1 Advantages of SCADA in Smart Grid

- The Tolerant of attack – mitigates and stands resilient to physical and cyber attacks
- Provides power quality needed by 21st century users
- Fully enables competitive energy markets – real-time information, lower transaction costs, available to everyone
- Optimizes assets – uses IT and monitoring to continually optimize its capital assets while minimizing operations and maintenance costs – more throughput per $ invested.
- Accommodates a wide variety of generation options – central and distributed, intermittent and dispatchable.
- Empowers the consumer – interconnects with energy management systems in smart buildings to enable customers to manage their energy use and reduce their energy costs.
- Self-healing – anticipates and instantly responds to system problems in order to avoid or mitigate power outages and power quality problems.

VI. CROSSED-CRYPTO SCHEME FOR SCADA IN SMART GRID

In cryptography, there are major types of encryptions: the symmetric encryption and the asymmetric encryption. From the two major types of encryptions we can say that Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost. On the other hand symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be considered as the correct and most appropriate security solution for many applications. [6] In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption. Diagram of a crossed crypto-scheme is shown in Figure 5.

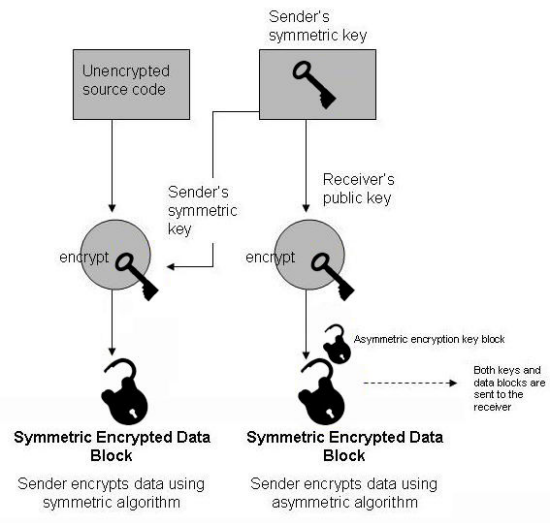

Figure 5. Crossed crypto-scheme

The crossed crypto-scheme can be integrated in the communication of the SCADA master and SCADA assets. The algorithm presented here combines the best features of both the symmetric and asymmetric encryption techniques. The plain text data is to be transmitted in encrypted using the AES algorithm. Further details on AES can be taken from [7].

The AES key which is used to encrypt the data is encrypted using ECC. The cipher text of the message and the cipher text of the key are then sent to the SCADA assets. The message

digest by this process would also be encrypted using ECC techniques. The cipher text of the message digest is decrypted using ECC technique to obtain the message digest sent by the SCADA Master. This value is compared with the computed message digest. If both of them are equal, the message is accepted otherwise it is rejected. You can see this scenario in figure 6.

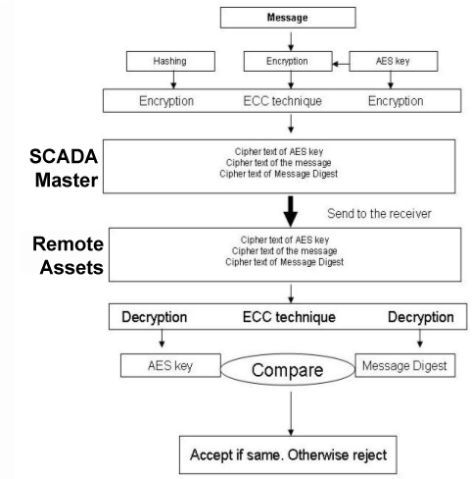

Figure 6. Chain of operation

VII. CONCLUSION

In summation, it is easy to observe that SCADA technology holds a lot of promise for the future. The economic and performance advantages of this type of system are definitely attractive. The security of any future Smart Grid is dependent on successfully addressing the cyber security issues associated with the nation's current power grid. The implementation of Smart Grid will include the deployment of many new technologies and multiple communication infrastructures. In this paper, we propose the integration of the Crossed crypto-scheme to the SCADA system in Smart Grid environment.

REFERENCES

[1] D. Bailey and E. Wright (2003) Practical SCADA for Industry
[2] Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems
[3] http://earth2tech.com/2008/05/01/silver-springs-the-cisco-of-smart-grid/ Accessed: May 2010
[4] http://earth2tech.com/2009/05/20/utility-perspective-why-partner-with-google-powermeter/ Accessed: May 2010
[5] National Energy Technology Laboratory (2007-08) (pdf). NETL Modern Grid Initiative — Powering Our 21st-Century Economy. United States Department of Energy Office of Electricity Delivery and Energy Reliability. p. 17. http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Modern%20Grid%20Benefits_Final_v1_0.pdf. Accessed: May 2010
[6] M.Balitanas, R.J. Robles, N. Kim, and T. Kim, "Crossed Crypto-scheme in WPA PSK Mode," Proceedings of BLISS 2009, Edinburgh, GB, IEEE CS, August 2009, ISBN 978-0-7695-3754-5
[7] Federal Information Processing Standards Publication 197 (2001) Announcing the ADVANCED ENCRYPTION STANDARD (AES) http://csrc.nist.gov/publications/fips/fips197/fips -197.pdf Accessed: January 2009
[8] THOMAS JAMPEN, MANUEL GU¨ NTER, TORSTEN BRAUN, "A Java API for Using a Native PGP Implementation", 6th WSEAS CSCC (CSCC 2002) MULTICONFERENCE
[9] SERENA PASTORE, "Internet technologies and the grid paradigm: designing a custom environment for web service-based applications", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006, pp. 693-698
[10] COSTIN CEPISCA, HORIA ANDREI, EMIL PETRESCU, CRISTIAN PIRVU, CAMELIA PETRESCU, "Remote Data Acquisition System for Hydro Power Plants", Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006, pp. 59-64
[11] RAMÓN MARTÍNEZ-RODRÍGUEZ-OSORIO, MIGUEL CALVO-RAMÓN, MIGUEL Á. FERNÁNDEZ-OTERO, LUIS CUELLAR NAVARRETE, "Smart control system for LEDs traffic-lights based on PLC", Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006, pp. 256-260

Prof. Tai-hoon Kim received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.