STUDY OF OPEN ACCESS SYSTEM, AND SECURITY OF SCADA USING EA TOOL

Thesis submitted in partial fulfillment of the requirements for the award of the degree of

Master of Engineering

in

Power Systems & Electric Drives

Thapar University, Patiala

By

DITTIKA WALIA

Roll No: 800941007

Under the supervision of

Er.B.S. SINGLA
S.E, SLDC, ABLOWAL
PSEB

Mrs.Suman Bhullar
Assistant Professor,
EIED

NOVEMBER, 2011

ELECTRICAL & INSTRUMENTATION ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA-147004

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"STUDY OF SCADA IN POWER SYSTEM, AND SECURITY OF SCADA USING EA TOOL"** in partial fulfillment of the requirement for the award of degree of Master of Engineering in ***Power Systems & Electric Drives*** submitted in Electrical & Instrumentation Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out at SLDC, Patiala and under the supervision of **Er. B.S Singla, S.E, SLDC, ABLOWAL** and **Mrs. Suman Bhullar**, Assistant Professor, EIED.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Dittika Walia

(Dittika Walia)
Roll No: 800941007

It is certified that the above statement made by the student is correct and true to the best of my knowledge and belief.

15/11/11
(Er. B.S SINGLA)
SE, SLDC,
PSEB, Patiala

Bhullar 11/11/11
(Mrs.Suman Bhullar)
Assistant Professor, EIED,
Thapar University, Patiala

Countersigned by

S. Ghosh
14/11/2011
(Dr. Smarajit Ghosh)
Professor & Head
Electrical & Instrumentation Engg. Department
Thapar University

15/11/11
(Dr. S.K. Mohapatra)
Dean (Academic Affairs)
Thapar University,
Patiala

ACKNOWLEDGEMENT

First of all I thank the almighty who enabled me with this opportunity to carry out this work. I would like to express my profound gratitude to my guides **Er.B.S Singla SE,SLDC** and **Mrs. Suman Bhullar, Assistant Professor, (EIED)** for the opportunity to work under her guidance and untiring support and encouragement both academically and morally.

I would express my sincere thanks to **Dr.Samarjit Ghosh, Prof. & Head, (EIED)** for their valuable support and opportunity to complete my thesis work simultaneously. I also thank **Dr. Yaduvir Singh, P.G. Coordinator** and all faculty members of EIED for their encouragement.

I would also like to thanks the officers and employees' at **SLDC, Ablowal,** for their support to conduct my work related to **SCADA** system.

The paucity of words does not compromise for extending my thanks to my parents, faculty of EIED and friends of M.E. (PSED, EIC) and the one whose uninterrupted love, inspiration and blessings helped me in completing this research report.

Dittika Walie

Dittika Walia

800941007

ABSTRACT

The increase of dependendency of human being on automatic machines has no doubt reduced the human effort, but as almost every machine runs using power so there has been a great increase in load as well as demand. As there is increase in load more and more generating as well as controlling stations are being set up. Thus in controlling the power equipment using SCADA software has been very helpful in the recent past.

In this thesis, recent trends and advancements of monitoring various other systems through SCADA has been studied. These along with power system applications and using various sensors for monitoring of various other parmeters have been studied. The Open Access system has been studied for economic scheduling.

CONTENTS

CHAPTER-6 RESULTS AND CONCLUSIONS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

In the late 1960's and early1970's SCADA came into existence. SCADA stands for "Supervisory Control And Data Acquisition". This system is responsible for gathering, processing and displaying information about the state of the monitoring system. The system must be able to acquire and present large amount of data securely, and coherently, so that operator can make appropriate decision. The concept basically implies a remote controlling station, which monitors and controls system situated at some distance, multiple substations being controlled from the control room.[25]

Most of the industrial plants has a control center, where is installed a SCADA (Supervisory Control And Data Acquisition) application. At the moment, it exists as a great offer of acquisition, supervision and control of software and the evolution of this software follow a triple tendency: intercommunication between applications, standardization of the communications with the field devices and adoption of the communication surroundings.

In a SCADA infrastructure, the role of diagnosis is to be able to detect a fault and to assess the extent of the damage in individual system components, so to carefully identify fault treatment and system recovery actions, which are most appropriate.[32] Although diagnosis has been extensively studied, its application to SCADA infrastructures raises a variety of issues, which have not been addressed all together before. Such issues stem from a number of factors, which are briefly described in the following:[22]

i. The designer has limited control over individual components and subsystems, since for most of them the internal design is not known;

ii. Individual components are heterogeneous, whereas the targets of traditional diagnosis are homogeneous;

iii. Diagnostic activities must be conducted with respect to components which are large grained, whereas traditional applications typically consist of relatively fine grained components;

iv. Repair or replacement of system units is costly and in some cases not possible at all.

v.

A SCADA system performs the following function:

1. Data acquisition
2. Networked data communication
3. Data presentation
4. Control

These functions are performed by four kinds of SCADA components:

1. **Sensors** (either digital or analog) and **control relays** that directly interface with the managed system.
2. **Remote telemetry units (RTUs).** These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.
3. **SCADA master units.** These are larger computer consoles that serve as the central processor for the SCADA system. Master units provide a human interface to the system and automatically regulate the managed system in response to sensor inputs.
4. The **communications network** that connects the SCADA master unit to the RTUs in the field.

1.2FUNCTIONAL OVERVIEW

The purpose of the SCADA subsystem is as follows:

It maintains an up-to-date picture of the state of the monitored system in database. It allows operator to observe the state of the monitored process via CRT displays.

It allows operator to interact with the monitored process by transmitting controls to the process.

It also provides functions such as, Tagging, Load shedding, historical data recording and generalized calculations in a real time environment.

Typically, SCADA systems are used to automate complex industrial processes where human control is impractical in such systems where there are more control factors, and more fast-moving control factors, than human beings can comfortably manage.

Open access system is analyzed to study the scheduling method and recently developed enterprise analysis architectural tool is also studied.

Enterprise IT infrastructures are large, complex and rapidly evolving, making integration sometimes difficult; they must meet rigorous compliance requirements even as the portals and access points in their environments and across enterprise applications continue to increase in number.

A context where the enterprise information security is really critical is the energy market, involving a lot of SCADA systems. Because of the mission-critical nature of a large number of SCADA systems, cyber attacks could, in a worst case scenario, cause massive financial losses through loss of data or actual physical destruction, misuse or theft, even loss of life.[35]

The main advantage of this tool is its capability for system quality analysis. Although a number of enterprise architecture software tools are available on the market, where some of these provide possibilities to sum costs or propagate the strategic value of a set of modeled objects, none have capabilities for system quality analysis. [15]

1.3 LITERATURE SURVEY

A lot of literature is available on this topic. Here is the literature survey that is relevant with the work carried out for this thesis work.

According to Rick Dodd and Bob Berry in their white paper to ‘SCADA tutorial’ have said that “SCADA monitoring and control can save you a lot of money and increase profitability… but your SCADA implementation can be a sinkhole of cost overruns, delays and limited capabilities. This White Paper will explain the essentials of SCADA technology, give you guidelines for evaluating SCADA technology and help you decide what kind of SCADA system is best for your needs” new software tools have been introduced.[27]

In the paper of “The ABB Group: The evolution of SCADA/EMS,” have discussed he emergence of SCADA as a better and secured technology, as compared to previous vulnerabilities in SCADA systems. [2]

According to Sir Andrew West he focus on the use of current standard SCADA communication protocol under defense and their properties. It introduces a new paradigm of connecting substation devices. [6]

In Wright A.K, Kinast J.A and McCarty paper on ‘SCADA infrastructure communications’ Distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems were developed to reduce labour costs, and to allow system-wide monitoring and remote control from a central location. Control systems are widely used in critical infrastructures such as electric grid[28].

The paper by Rashed Dhaouadi, Darwish and Ali describes the development of a virtual SCADA (V-SCADA) system tool for testing and training purposes. Design engineers can test their system before the actual implementation. Fresh graduate engineers and senior students can be trained using this tool to visualize the pseudo real-time power substation equipment, operations procedures, and fault management.[18]

The paper on cyber security assessment for SCADA by ‘Permann Robert and Kenneth Rohde describes the development of a virtual SCADA (V-SCADA) system tool for testing and training purposes.’ Design engineers can test their system before the actual implementation. Fresh graduate engineers and senior students can be trained using this tool to visualize the pseudo real-time power substation equipment, operations procedures, and fault management.[16]

The paper presented on importance of awareness of SCADA by Johansson, et.al; states that “These SCADA-systems perform highly advanced logic that automatically controls the power distribution network as well as provide the operators with vital information and efficient support needed to make advanced decisions such as identifying emerging problems and take actions preventing them.”[13]

The architectural framework on SCADA has been studied from SCADA lab manual available at the SLDC which was a great help for study in detail of Supervisory Control and Data Acquisition (SCADA) systems. [20]

The first is a move to define standard interfaces and communications protocols in support of cross-vendor compatibility and modularity. The second is a move to connect nodes in a SCADA system to open networks such as the Internet.

The development of EA Tool for the decision making process and the PRM approach has been analysed by Markus Buschle,Ullberg John and Sommestad which has been utilized for cyber risk assessment.[34]

Under the paper;“Architectural analysis of secure communication under SCADA program” at the Sandia laboratory. Stated the growing dependence of critical infrastructures and industrial automation on interconnected physical and cyber based control systems has resulted in a growing and previously unforeseen cyber security threat to SCADA and DCS systems.[19]

1.4 OBJECTIVE OF WORK

The main objective of my work is to the study and access the SCADA system at the state load dispatch center and to understand and analyze the recent trends in a SCADA system and to monitor the control system under various conditions and to study in detail the working of various utilities at SCADA system.

The studies of various architectural models provide decision makers with a convenient tool to capture different aspects of information systems in abstract diagrammatic descriptions. Thereby factors of interest can be captured and interdependencies become visible. Architectural models are based on modeling languages that define how these models should look like.

1.5 ORGANIZATION OF THESIS

First chapter includes brief outline of the thesis.

Second chapter constitutes the basic theory of a SCADA system and its components.

Third chapter includes theory and analysis of the Open Access System and scheduling of power system.

Fourth chapter includes the study of meteorological sensors.

Fifth chapter includes the study of recently developed EA Tool

Sixth chapter includes the results.

Seventh chapter includes the conclusions as well as the future scope of work.

In the end the references are mentioned

CHAPTER 2

SCADA SYSTEM

2.1 SCADA

SCADA stands for Supervisory Control And Data Acquisition. SCADA is not a specific technology, but a kind of specific technology. Any application that gets data about a system in order to control and monitor that system is a SCADA application.

A SCADA application has two elements:

1. The process/system/machinery you want to monitor and control - may be a power plant, a water system, a network, a system of traffic lights, or in various other systems.
2. A network of intelligent devices that interfaces with the first system through sensors and control outputs.

Supervisory Control and Data Acquisition (SCADA) systems provide means for management, supervisory control, and monitoring of process control and automation systems via collecting and analyzing the real time data.[20]

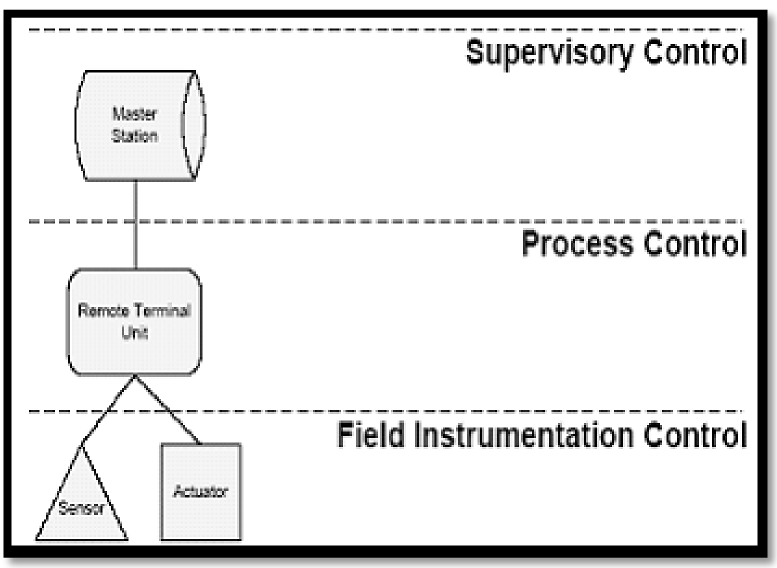

Fig.2.1 BASIC ARCHITECTURE OF SCADA SYSTEM

2.2 SCADA for Power Systems

SCADA systems have played an important role in supervision and control of electrical power system's transmission and distribution systems.

SCADA's Supervisory control function allows the operator and application programmer to control devices in the monitored systems. From the control center control commands can be issued to change the state of devices such as circuit breaker and switches.

Data Acquisition means to collect data and to manipulate it. RTU sends the raw data to communication front ends which performs some conversion and checking of data before sending it to the Telemetry front end and then to the host.[1]

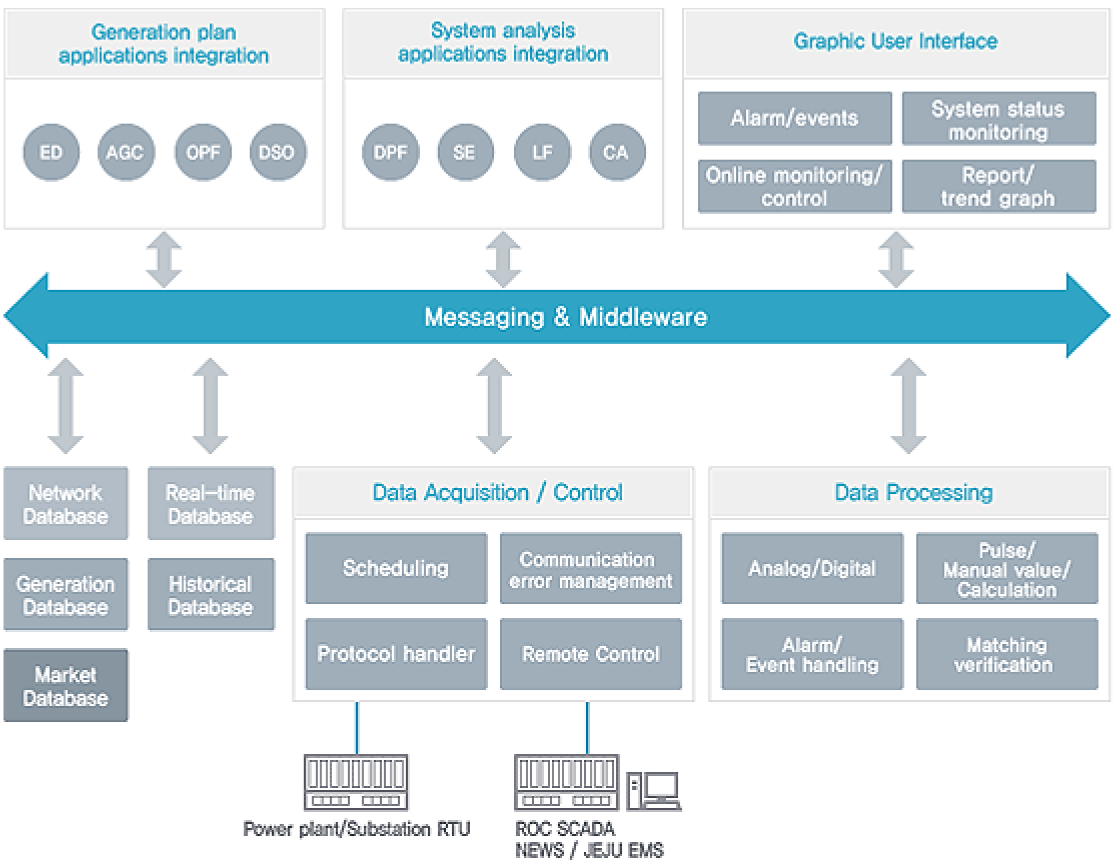

Fig. 2.2 BLOCK DIAGRAM OF SCADA

2.3 COMPONENTS OF SCADA SYSTEM

1. TRANSDUCERS:

Transducer provides a transformed output in response to a specific input measured value. They are used to measure or sense the change in parameters and to convert measured values from one form to another.

2. POTENTIAL TRANSFORMERS AND CURRENT TRANSFORMERS:

Instrument Transformers have a wide application in protection circuits of power systems for the operation of over current, under voltage, earth fault and various other type of relays. Transformers used for current measurement are called current transformers. Transformers used for voltage measurement are potential transformers.

3. REMOTE TERMINAL UNITS (RTUs):

Typical RTU has a network interface, a simple processor, some environmental sensors, some override switches, and, a bus. RTUs are basically distributed SCADA based systems.

An RTU,or Remote Terminal Unit is a microprocessor controlled electronic device which interfaces objects in the physical world to a distributed control system or SCADA system by transmitting telemetry data to the system and/or altering the state of connected objects based on control messages received from the system[20].

SCADA RTUs need to communicate with all your on-site equipment and survive under the harsh conditions of an industrial environment. Here’s a checklist of things you should expect from a quality RTU:

• **Sufficient capacities** to support the equipment at your site … but not more capacity than you actually will use. At every site, you want an RTU that can support your expected growth over a reasonable period of time, but it’s simply wasteful to spend your budget on excess capacity that you won’t use.

• **Rugged construction** and ability to withstand extremes of temperature and humidity. You know how punishing on equipment your sites can be. Keep in mind that your SCADA system needs to be the most reliable element in your facility.

• **Secure redundant power supply**. SCADA system needs to be up and working 24/7. Your RTU should support battery power and, ideally, two power inputs.

• **Redundant communication ports**. Network connectivity is as important to SCADA operations as a power supply. A secondary serial port or internal modem will keep your RTU online even if the LAN fails. Plus, RTUs with multiple communication ports easily support a LAN migration strategy.

• **Nonvolatile memory (NVRAM)** for storing software and/or firmware. NVRAM retains data even when power is lost. New firmware can be easily downloaded to NVRAM storage, often over LAN — so you can keep your RTUs' capabilities up to date without excessive site visits.

Intelligent Control: Sophisticated SCADA remotes can control local systems by themselves according to programmed responses to sensor inputs. This isn't necessary for every application, but it does come in handy for some users.

Real-time clock: For accurate date/time stamping of reports.

Watchdog timer: To ensure that the RTU restarts after a power failure.

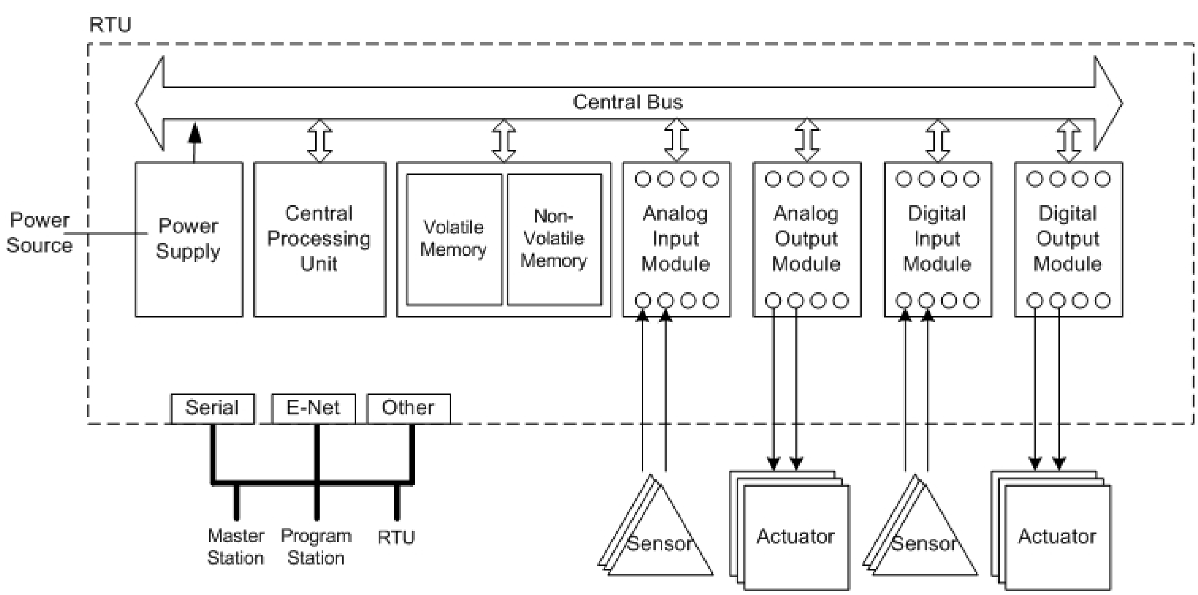

Fig 2.2 DETAILED COMPONENT STRUCTURE OF SCADA

RTUs can operate under command from a central computer or in standalone mode. RTU consists of a process module, analog and digital input modules and communication interface, power supply unit and screw termination on the rear of the panel for field connections. RTU basically performs the following functions:

- Collects power system data.
- Filters and processes the system data.
- Transmit data to the control center.
- Receive the control commands.

4. MODEM:

MODEM is acronym for Modulator-Demodulator. The primary MODEM function is to convert digital data into analog form, which is suitable for transmission on common carrier circuits. Modulation is the D/A conversion in which the digital data is placed on the transmission line by modulation of a carrier. Demodulation is the reverse process.

5. PLCC:

PLCC is abbreviated for Power Line Carrier Communication. Carrier current provides a means of conveying speech, metering indications, control impulses, etc. from one station to another by existing transmission lines without interfacing with their normal function of transmitting power.

The main elements of a carrier channel are as follows:

a) Sending terminal assembly
b) Coupling Capacitor
c) Line Tuning
d) Line Traps
e) Receiving station coupling
f) Power Line
g) Attenuation

6. FRONT END PROCESSOR:

COMMUNICATION FRONT END:

The communication equipment and software that links the computer to RTUs is referred as Communication Front End. CFE drives the serial communication lines connected to the RTUs.

TELEMETEREY FRONT END:

The software that communicates between the data server and CFE is called Telemetric Front End. It maintains information regarding the configuration of the communication components and facilitates interfacing with devices having a variety of communication protocols.

7. DATA DISPLAYS:

There are two types of data displays:

1. One line Display
2. Tabular Display

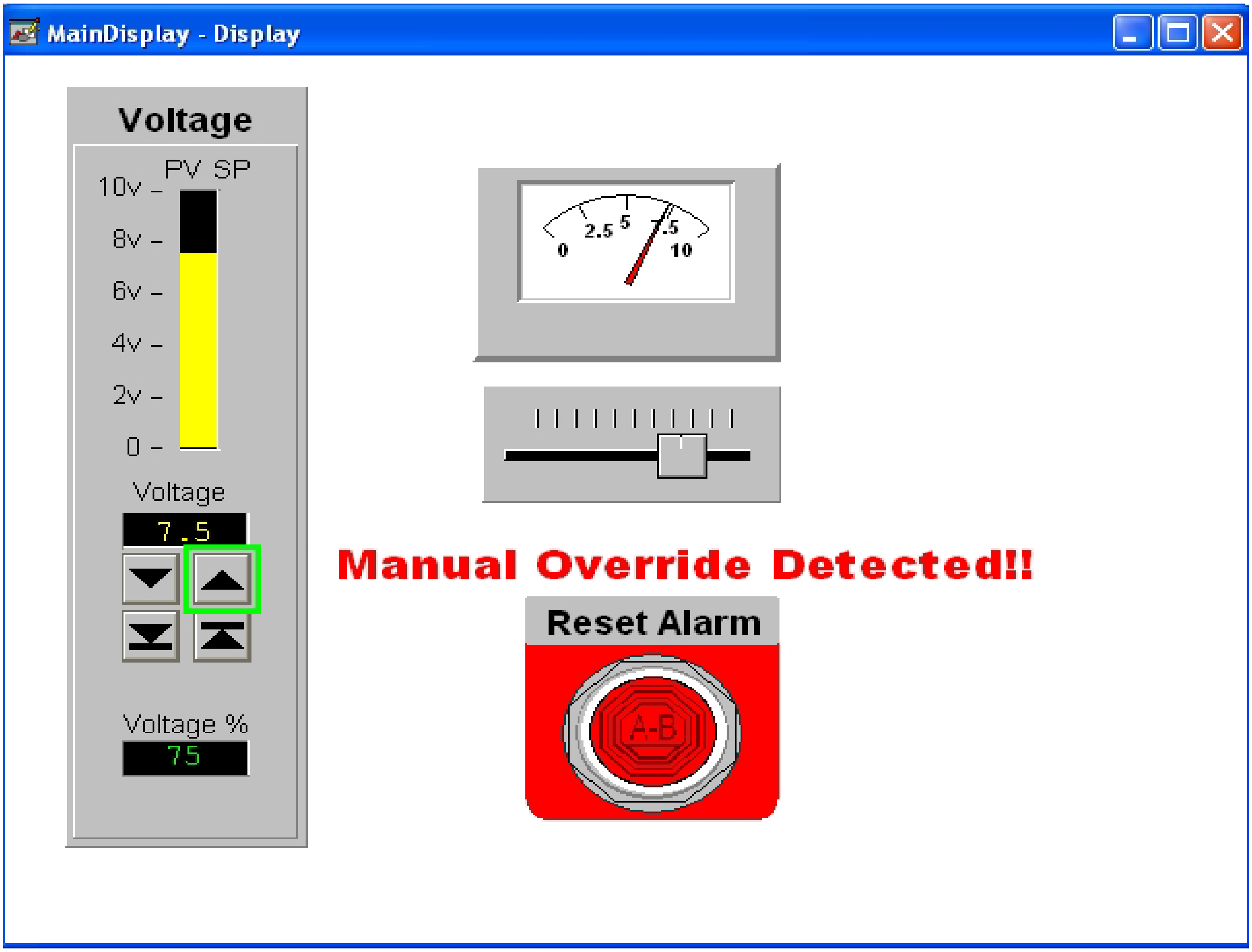

Fig.2.3 SHOWS DISPLAY SCREEN

In one line or single line display whole network is made up of single lines and graphical symbols are used for different components.

Tabular displays also give the state of operating devices and current data. In this data is displayed in tabular form.

8. LAN COMMUNICATION BETWEEN SERVER AND RTU:

In SCADA system, each control site has two host computers. Host computer will continue scanning. The host may switch communications from one path to an alternate path that is on another CFE or TFE without requiring a host failure. The VFEs communicate with RTUs and perform several functions to minimize data processing on the host computer.

2.4 SOURCES AND TYPES OF DATA

Each piece of data that SCADA acquires has a source from which data is acquired. The system has three different types of data:

ANALOG DATA

Analogs are numeric values representing the state of variable state devices, such as power lines, transformers, etc. All analog values are converted to host computer. For example: Voltage and Current measurements.

STATUS DATA

Status value represents the state of discrete state devices. All status point values are stored in point records in the SCADA database. For example: Status change of Circuit Breakers.

COUNT DATA

A count measurement is a value from pulse accumulator which is used to measure the total amount of energy. The pulse accumulator counts the contacts, changes and passes the count to SCADA.

DATA QUALITY

Data quality is a catch all term relating to information the SCADA operator may want to know about the values SCADA is displaying for monitored devices. SCADA has a group of five data quality indicators:

1. Data source flags
2. Detailed data quality flags
3. Composite data quality flags
4. State estimator flags
5. Data attribute flags

2.5 USER INTERFACE MANAGEMENT SYSTEM

UIM system primarily focuses on the SCADA displays and alarm functionality.

TYPES OF DISPLAYS

Data in the SCADA database and indications of changes are presented to the operator through the following displays:

1. **Menu Directory displays**- A display that lists all the menu displays.
2. **System Directory displays**- It lists all the SCADA system displays.
3. **Transmission System overview displays**- A graphic overview display of the transmission system.
4. **Substation displays**- The major operation displays.
5. **Interchange displays**- A schematic diagram showing power transfer between all constituent power systems.

2.6. DATA PRESENTATION

The only display element in our model SCADA system is the light that comes on when the switch is activated. This obviously would not do on a large scale because one cannot track a light board of a thousand separate lights, and you don't want to pay someone simply to watch a light board, either.[28]

A real SCADA system reports to human operators over a specialized computer that is variously called a master station, an HMI (Human-Machine Interface) or an HCI (Human-Computer Interface).

The SCADA master station has several different functions. The master continuously monitors all sensors and alerts the operator when there is an "alarm" — that is, when a control factor is operating outside what is defined as its normal operation. The master presents a comprehensive view of the entire managed system, and presents more detail in response to user requests. The master also performs data processing on information gathered from sensors.[20]

2.7 DATA COMMUNICATION SYSTEM

DATA COMMUNICATION

There are two types of data communication:

ASYCHRONOUS COMMUNICATION

Asynchronous communication can either be serial communication or parallel communication. In serial communication first and last bit of data is indicated by start and stop bit. The number of data bit is fixed depending on the selection of the mode. However, in case of parallel communication, a computer communicates to printer in parallel pattern along with some control signals.[1]

For asynchronous communication to send the data to data communication equipment ,one type of signal is required, while, for receiving data another signal is required.

SYCHRONOUS COMMUNICATION

Synchronous communication is similar to serial communication, for, each transfer bits from data communication equipment to data terminal equipment, a separate clock signal is required. Data can be transmitted either as current or voltage. Typically 20mA or 60mA current loops are used in teletype equipment logic 1 current flows, logic 0 current is interrupted.[9].The current signals are relatively noise free and are suitable for transmission when data required needs to be highly accurate as it forms the basis of the decision to be taken by the supervisor.

2.8 ARCHITECTURE

SCADA architecture is mainly in two parts:

HARDWARE ARCHITECTURE

The basic hardware of the SCADA system is distinguished into two basic layers: the "client layer” which caters for the man machine interaction and the "data server layer" which handles most of the process data control activities.[6] The data servers communicate with devices in the field through process controllers. Process controllers, e.g. PLC’s, are connected to the data servers either directly or via networks or field buses that are proprietary (e.g. Siemens H1), or non-proprietary (e.g. Profibus). Data servers are connected to each other and to client stations via an Ethernet LAN

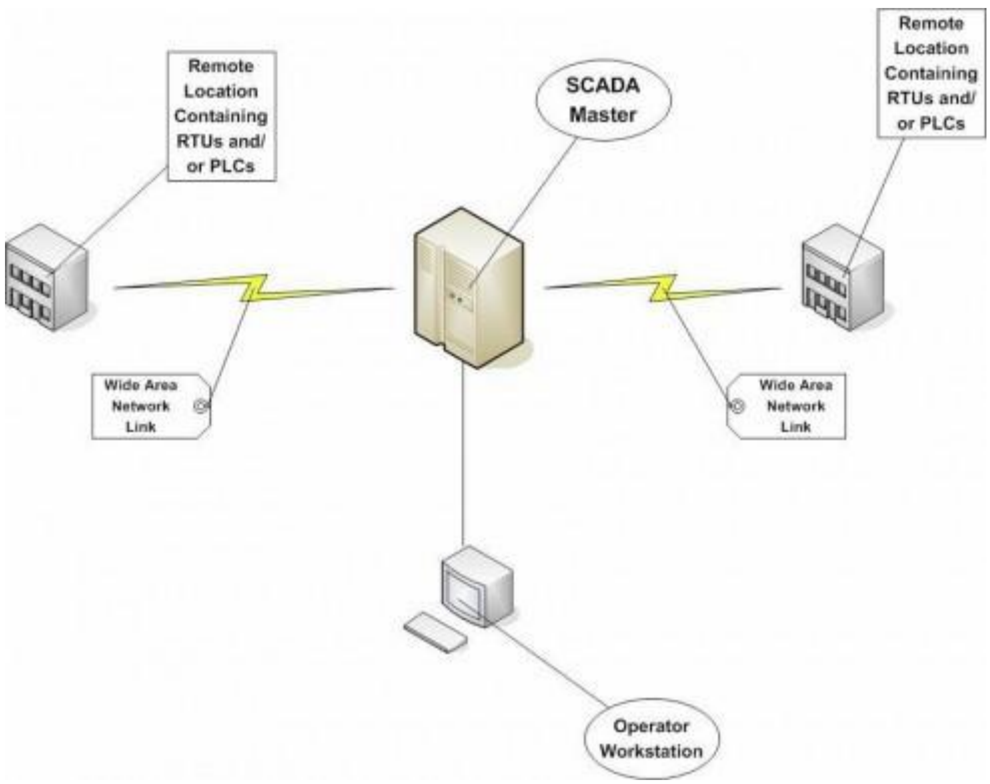

Fig 2.4 SHOWS HARDWARE ARCHITECTURE OF SCADA

SOFTWARE ARCHITECTURE

The SCADA products are multi-tasking and are based upon a real-time database (RTDB) located in one or more servers. Servers are responsible for data acquisition and handling (like polling controllers, alarm checking, calculations, logging and archiving) on a set of parameters, typically to which those are connected.

However, it is possible to have dedicated servers for particular tasks, e.g. historian, data logger, alarm handler.[2]

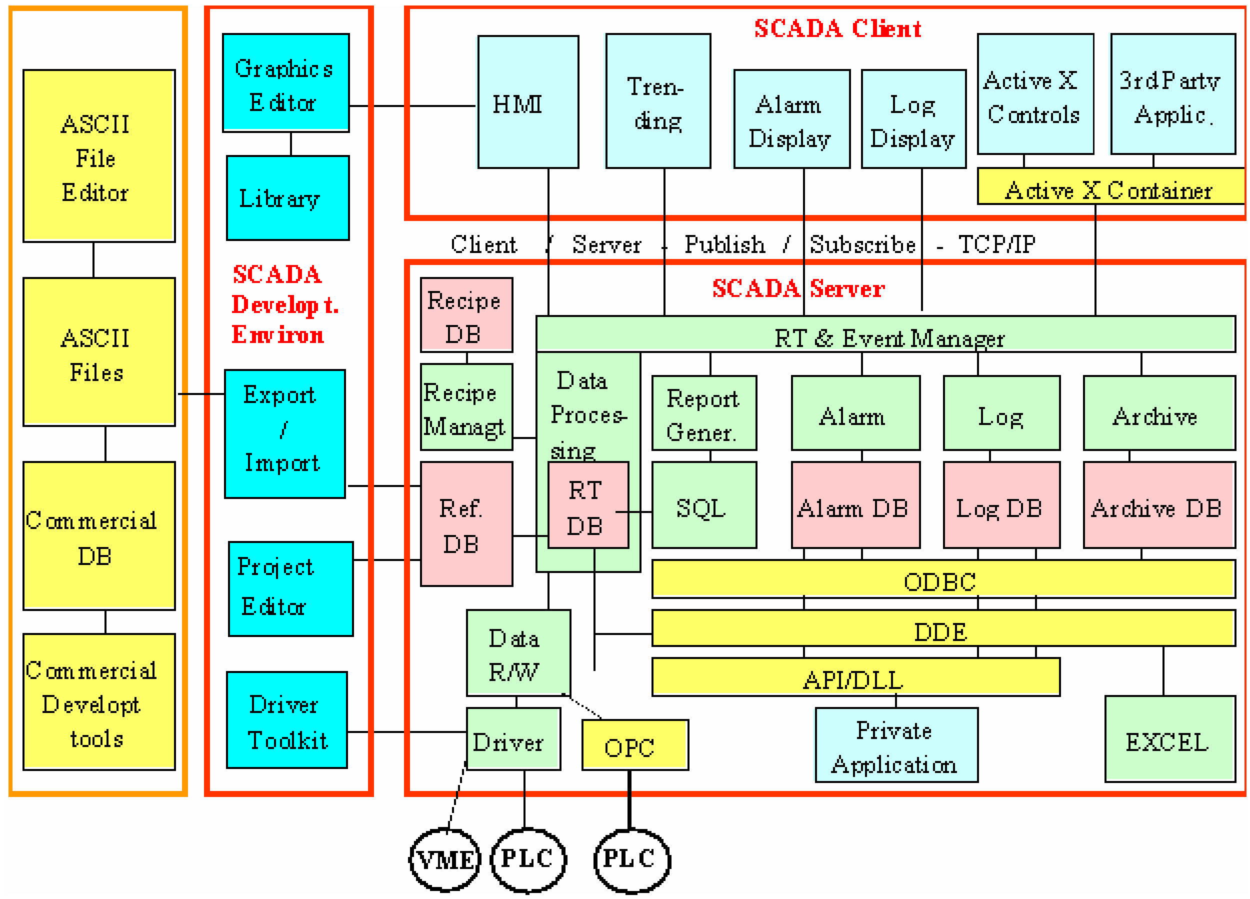

Fig.2.5 SHOWS SOFTWARE ARCHITECTURE OF SCADA

2.9 HUMAN MACHINE INTERFACE

A Human-Machine Interface or HMI is the apparatus which presents process data to a human operator, and through which the human operator controls the process.

An HMI is usually linked to the SCADA system's databases and software programs, to provide trending, diagnostic data, and management information such as scheduled maintenance procedures, logistic information, detailed schematics for a particular sensor or machine, and expert-system troubleshooting guides.[17]

The HMI system usually presents the information to the operating personnel graphically, in the form of a mimic diagram. This means that the operator can see a schematic representation of the plant being controlled.[35] For example, a picture of a pump connected to a pipe can show the operator that the pump is running and how much fluid it is pumping through the pipe at the moment. The operator can then switch the pump off. The HMI software will show the flow rate of the fluid in the pipe decrease in real time. Mimic diagrams may consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols.[2]

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 .[33]

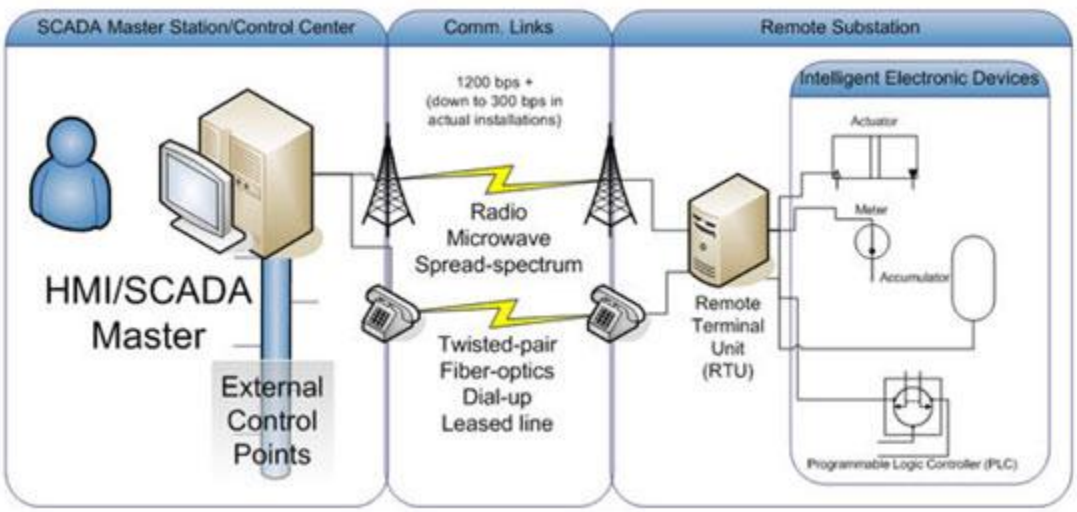

Fig.2.6SHOWS HMI

An important part of most SCADA implementations is alarm handling. 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.

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 indicator, or an alarm event. loge point lies outside high and low limit values associated with that point.[20]

2.10 SCADA Security Issues

The Supervisory Control and Data Acquisition System (SCADA) monitor and control real-time systems. SCADA systems are the backbone of the critical infrastructure, and any compromise in their security can have grave consequences. Therefore, there is a need to have a SCADA testbed for checking vulnerabilities and validating security solutions. In this paper we develop such a SCADA testbed.[33] The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems and office networks and the Internet has made them more vulnerable to attacks [5]. Consequently, the security of SCADA-based systems has come into question as they are increasingly seen as extremely vulnerable to cyber-warfare/cyber-terrorism attacks. [23]

In particular, security researchers are concerned about:

- the lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks.
- the belief that SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces.
- the belief that SCADA networks are secure because they are physically secured.
- the belief that SCADA networks are secure because they are disconnected from the Internet.

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society.[29] The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original compromise. For example, a blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen.[16]

There are two distinct threats to a modern SCADA system. First is the threat of unauthorized access to the control software, whether it be human access or changes induced intentionally or accidentally by virus infections and other software threats residing on the control host machine. Second is the threat of packet access to the network segments hosting SCADA devices.[31] In many cases, there is rudimentary or no security on the actual packet control protocol, so anyone who can send packets to the SCADA device can control it. In many cases SCADA users assume that a VPN is sufficient protection and are unaware that physical access to SCADA-related network jacks and switches provides the ability to totally bypass all security on the control software and fully control those SCADA networks.[18] These kinds of physical access attacks bypass firewall and VPN security and are best addressed by endpoint-to-endpoint authentication and authorization such as are commonly provided in the non-SCADA world by in-device SSL or other cryptographic techniques.[28]

Many vendors of SCADA and control products have begun to address these risks in a basic sense by developing lines of specialized industrial firewall and VPN solutions for TCP/IP-based SCADA networks.[21] Additionally, application white-listing solutions are being implemented because of their ability to prevent malware and unauthorized application changes without the performance impacts of traditional antivirus scans.[27] Also, the ISA Security Compliance Institute (ISCI) is emerging to formalize SCADA security testing starting as soon as 2009. ISCI is conceptually similar to private testing and certification that has been performed by vendors since 2007. Eventually, standards being defined by ISA99 WG4 will supersede the initial industry consortia efforts, but probably not before 2011.[16]

A communications network security device, called a trust system, to enhance supervisory control and data-acquisition (SCADA) security. The major goal of the trust system is to increase security with minimal impact on existing utility communication systems.[22]

The increased interest in SCADA vulnerabilities has resulted in vulnerability researchers discovering vulnerabilities in commercial SCADA software and more general offensive SCADA techniques presented to the general security community. In electric and gas utility SCADA systems, the vulnerability of the large installed base of wired and wireless serial communications links is addressed in some cases by applying bump-in-the-wire devices that employ authentication and Advanced Encryption Standard encryption rather than replacing all existing nodes.[12]

CHAPTER 3
OPEN ACCESS SYSTEM AND SCHEDULING

3.1 OPEN ACCESS SYSTEM

Open access means the partial privatization of the electricity sector. In this case different suppliers of electric energy are there and one can take supply according to one's choice. Indian Electricity act was revised in 2003 for open access system. Central Electricity Authority regulates the electricity supply act.[9]

3.2 OPEN ACCESS AND SCHEDULING

Scheduling is done for a state for 24 hours. To notify hourly/half hourly etc. generation to the utility is called scheduling. Bulk consumers give their 24 hour scheduling to the supplier. If they consume more or less power than their given scheduling, then they are penalized or vice-versa. The agreement between the consumer and the power supplier for purchasing power is called PPA, that is, Power Purchasing Agreement.[20]

3.3 UNSCHEDULED INTERCHANGE

Unscheduled interchange means more or less load than the given scheduled. It depends on the frequency, if, the frequency decreases we have to decrease the load and sometimes different units of the substation are to be shut down. In rainy season frequency increases so load has to be increased. The energy meters which record the online supply frequency, are called Special Energy Meters (SEM). For change in load ABT or Ability Based Tariff is taken for this. If supplier has no network in the region of the consumer then wheeling charges are taken from the consumer to lend a network in that region.

ABSTRACT OF UNSCHEDULED INTERCHANGE FOR THE YEAR 2010-2011

Month	Schedule (LU)	Actual Drawl (LU)	UI (LU)	Actual UI (Rs.lac) (Billed Amt.)	Avg. Unit Charge (Rs/unit)
Apr	8853.78	11815.56	2961.78	21350.57	7.21
May	16175.11	19158.63	2983.52	16402.60	5.50
June	23439.92	24982.89	1542.96	6284.91	4.07
July	26611.06	27421.22	810.17	3026.38	3.74
Aug.	27743.90	29701.20	1957.30	4913.86	2.51
Sept.	24999.37	25727.64	728.28	487.01	0.67
Oct.	17019.90	16542.27	-477.62	-1013.21	2.12
Nov.	10072.57	9259.02	-813.55	-1575.85	1.94
Dec.	10364.75	10202.71	-162.04	-62.51	0.39
Jan.	9295.23	9570.94	275.71	937.52	3.40
Feb.	8719.68	8668.95	-50.72	481.72	-9.50
Mar	12838.13	12512.78	-325.35	-803.18	2.47
TOTAL	**196133.40**	**205563.82**	**9430.42**	**50429.82**	**5.35**

Fig.3.1 SHOWS UI DIVISIONAL PIE

Let us consider that a state is divided into ‘n’ number of regions. Each region has its own generating load G1,G2,G3,G4…Gn. There is a Holding Company (HC) which regulates the generating units. HC manages the overall system.

TOTAL= G1+G2+G3+………..+Gn+ (IS1+IS2+……….)

IS is the net exchange Inter-state Schedule

Thus total availability is the sum of inter-state feeder and its own generation. If consumers are in G1 region, they can take supply from any other supplier. But wheeling charges have to be paid, if supplier has no network in that region. Consumers at borders can take supply according to their requirements.[7]

3.4 ACTIVITIES TO BE DONE TO ESTABLISH OPEN ACCESS SYSTEM

1. Identification of state boundaries, interstate point of 220 KV, 132 KV, 66KV and thus designing of meter code- based on voltage level and based on line code.[2]
2. Identification of generating points. Designing of meter code for calculating total generation .
3. Defining distribution company border and thus to identify meter and to design meter code.

METER CODE SHOULD IDENTIFY THE FOLLOWING:

a.) Owner of the company

b.) Interstate

c.) Holding Company

d.) Generating Unit

e.) Distribution Company

METER REQUIREMENTS ARE:

1.) It should be capable of composite current transformer/potential transformer ratio errors.

2.) It should have sufficient storage capacity.

3.) It should be programmable according to host server requirement.

CHAPTER 4

METEOROLOGICAL SENSORS

4.1 INTERFACE UNIT

An interface unit is used for conversion of various meteorological sensors' output to standard 4 to 20 mA output. It can work on battery as well as mains. The unit accepts six meteorological inputs, that is, wind speed, wind detection, air temperature, relative humidity, atmospheric pressure and rainfall. A separate PCB is provided for each sensor. Each card is provided with signal conditioner, D/A converting circuit for pulse sensors and a 4 to 20mA converting unit.

This unit accepts 230V AC/24V DC and provides necessary power to the sensor and interfacing circuits. One can connect a 24V rechargeable battery to the unit. The recommended battery is 12V 7AH battery two in series. To power it from an external DC source, we must need to put a diode in series so that the charger circuit will not force power, when it is operated on 230V AC. The input signals from the sensors are driven through a suspension circuit so that the atmospheric discharges and noise are filtered.[18]

The interfacing unit sources 4 to 20mA through the output line. In the receiving circuit one must provide a load resistanceR1. The load resistance can be from 100ohms to 600ohms.

If the unit is operated from an external DC supply, the voltage should not fall below 24V and the noise on the supply line should be minimum to get the output with specified accuracy.

4.2 WIND SPEED SENSOR

Anemometer here used is a fast response, low threshold OPTO electronic anemometer. When rotated by wind, a chopper on the anemometer shaft interrupts an infrared beam 118 times per revolution, generating pulses from a phototransistor. The signal is amplified and fed through a line driver which can drive up to 500 meters of cable. The frequency is proportional to wind speed.

TABLE-1 SHOWS SPECIFICATIONS OF WIND SPEED SENSOR:

WIND SPEED SENSOR	3 Cup Anemometer
SENSING	3 Cup assembly mounted on friction free shaft
STARTING THRESHOLD	0.3 meter per second
RANGE	0 to 65 meter per second
OUTPUT	TTL pulse output proportional to wind speed
ACCURACY	± 2%
DIAMETER OF CUP ASSEMBLY	165 mm
CUP MATERIAL	ABS plastic
CONSTRUCTION OF BODY SENSOR	Brass housing and shaft
SIZE OF BODY	260(h)*50 diameter
WEIGHT	800gm. (approx.)
OPERATING TEMPERATURE	-20 to +70 Degree

4.3 PRESSURE SENSOR

A pressure sensor measures pressure, typically of gases or liquids. Pressure is an expression of the force required to stop a fluid from expanding, and is usually stated in terms of force per unit area. A pressure sensor usually acts as a transducer; it generates a signal as a function of the pressure imposed.

Pressure sensors can alternatively be called pressure transducers, pressure transmitters, pressure senders, pressure indicators and piezometers.

Some pressure sensors, such as those found in some traffic enforcement cameras, function in a Binary (on/off) manner, i.e., when pressure is applied to a pressure sensor, the sensor acts to complete or break an electrical circuit. These types of sensors are also known as a pressure switch.

TYPES OF PRESSURE SENSORS

1. ABSOLUTE PRESSURE SENSOR

This sensor measures the pressure relative to perfect vacuum pressure (0 PSI or no pressure). Atmospheric pressure, is 101.325 kPa (12.7 PSI) at sea level with reference to vacuum.

2. GAUGE PRESSURE SENSOR

This sensor is used in different applications because it can be calibrated to measure the pressure relative to a given atmospheric pressure at a given location. A tire pressure gauge is an example of gauge pressure indication. When the tire pressure gauge reads 0 PSI, there is really 12.7 PSI (atmospheric pressure) in the tire.

2. VACUUM PRESSURE SENSOR

This sensor is used to measure pressure less than the atmospheric pressure at a given location. This has the potential to cause some confusion as industry may refer to a vacuum sensor as one which is referenced to either atmospheric pressure (ie measure Negative gauge pressure) or relative to absolute vacuum.

3 .DIFFERENTIAL PRESSURE SENSOR

This sensor measures the difference between two or more pressures introduced as inputs to the sensing unit, for example, measuring the pressure drop across an oil filter. Differential pressure is also used to measure flow or level in pressurized vessels.

4. SEALED PRESSURE SENSOR

This sensor is the same as the gauge pressure sensor except that it is previously calibrated by manufacturers to measure pressure relative to sea level pressure.

APPLICATIONS OF PRESSURE SENSORS

• PRESSURE SENSING

This is the direct use of pressure sensors to measure pressure. This is useful in weather instrumentation, aircraft, cars, and any other machinery that has pressure functionality implemented.

• ALTITUDE SENSING

This is useful in aircraft, rockets, satellites, weather balloons, and many other applications.

All these applications make use of the relationship between changes in pressure relative to the altitude. This relationship is governed by the following equation:

$$h = (1 - P/P_{ref})0.190284)*145366.45 \text{ feet}$$

This equation is calibrated for an altimeter, up to 36,090 feet (9,000 m). Outside that range, an error will be introduced which can be calculated differently for each different pressure sensor.

These error calculations will factor in the error introduced by the change in temperature as we go up.[20]

Barometric pressure sensors can have an altitude resolution of less than 1 meter, which is significantly better than GPS systems (about 20 meters altitude resolution). In navigation applications altimeters are used to distinguish between stacked road levels for car navigation

• FLOW SENSING

This is the use of pressure sensors in conjunction with the venturi effect to measure flow.

Differential pressure is measured between two segments of a venturi tube that have a different aperture. The pressure difference between the two segments is directly proportional to the flow rate through the venturi tube. A low pressure sensor is almost always required as the pressure difference is relatively small.

• LEVEL / DEPTH SENSING

A pressure sensor may also be used to calculate the level of a fluid. This technique is commonly employed to measure the depth of a submerged body (such as a diver or submarine), or level of contents in a tank (such as in a water tower). For most practical purposes, fluid level is directly proportional to pressure. In the case of fresh water where the contents are under atmospheric pressure, 1psi = 27.7 inH20 / 1Pa = 9.81 mmH20. The basic equation for such a measurement is

$$P = p * g * h$$

Where,

P = Pressure,

P = Density of the Fluid,

g = Standard Gravity,

h = Height of fluid column above pressure sensor

• LEAK TESTING

A pressure sensor may be used to sense the decay of pressure due to a system leak. This is commonly done by either comparison to a known leak using differential pressure, or by means of utilizing the pressure sensor to measure pressure change over time.

TABLE 2 SHOWS SPECIFICATIONS OF PRESSURE SENSOR:

SENSOR	Stainless steel bellows coupled to a strain gauge.
RESOLUTION	0.1 milli-bar
ACCURACY	0.25% of full scale reading
RANGE	600 to 1100 milli-bars
OUTPUT	1 to 5 volts
POWER REQUIREMENT	10 V DC
HOUSING	SS 316
OPERATING TEMPERATURE	-20 to +70 degree Celsius

4.4 WIND DIRECTION SENSOR

Wind vane is a counter balanced, low threshold wind vane, linear wire round endless potentiometer is coupled to the vane by a shaft. As the vane turns it rotates he steel shaft, which is coupled to the potentiometer. The potentiometer has excellent linearity, very low torque. The use of single wiper increases the life expectancy of the potentiometer.

Sensor gives minimum resistance at the north that is at 0 degree approximately 20 ohms. The position of the vane is proportional to the resistance.

TABLE 3 SHOWS SPECIFICATIONS OF WIND SENSOR

WIND DIRECTION SENSOR	Wind vane
SENSING	Vane coupled to linear endless potential
STARTING SENSOR	Better than 0.5m/s
RANGE	0 to 357 degrees
OUTPUT	0 to 5kohm resistance
RESOLUTION	1 degree
ACCURACY	±3 degrees
WEIGHT	1300gm. Approx.
SIZE OF BODY	260(h)*70mm diameter
OPERATING TEMPERATURE	-20 to 70 degree

CHAPTER-5
ENTERPRISE ARCHITECTURE ANALYSIS

5.1 INTRODUCTION

Enterprise architecture is a model-based approach. The core of this model-based approach is diagrammatic descriptions of the systems and their environment. However, there is not a clear definition of what constitutes a “good” enterprise architecture model because the “goodness” of a model is not an inherent property, but contingent on what kind of analysis it is. The overall security concern for an ICS typically originates from malicious threat agents attempting to disrupt an industrial process such as to interfere with it specified operation (e.g. to create a power outage) or to negatively impact on the environment and/or personnel safety.[1]

In Bucher et al. contribute to Enterprise Architecture methodology providing a systemization of the Enterprise Architecture Analysis techniques. The Enterprise Architecture Analysis is defined as the application of property assessment criteria on enterprise architecture models.[14]

The Enterprise Architecture Tool (EAT) consists of two main functional components: the Abstract Modeler, a component supporting the creation of Abstract Models and the Concrete Modeler that supports the creation of Concrete Models, taking abstract models as input. The typical user of the Abstract Modeler function is a researcher who, reading through sources of information, defines Abstract Model determining the goals of the assessments.[17] The typical user of the Concrete Modeler function, instead, is the information systems decision maker, or a data collector/investigator/assessor, who, moving from the previously created Abstract Models, can instantiate those into Concrete Models detailing the decision alternatives. The Enterprise Architecture Analysis Tool (EAT) was developed in Java with intentions to achieve platform independence and portability. It uses Java core API’s like Java swings and JAXB (Java Architecture for XML Binding) along with some additional API’s to enhance the functionality.

EAT is comprised of two major components: the Abstract Modeler and the Concrete Modeler. They are executed separately and they are independent of each other. Both parts have their own mechanisms for handling and saving models.[14]

5.2 ABSTRACT MODELER:

The Abstract modeler is first component of EAT. It facilitates the user to construct abstract models for desired architectures. The user can construct modeling languages in the form of classes and attributes of classes. The abstract modeler also supports the inheritance phenomenon along with features like attribute overriding.

Currently EAT supports three types of attributes.

• Discrete Attributes

• Continuous Attributes

• Textual Attributes

5.3 CONCRETE MODELER:

The concrete Modeler is the second major component of EAT. The fundamental functionality of concrete modeler is to instantiate modeling languages. To start, the user has to provide a modeling language to concrete modeler or the user can also reopen previously saved concrete models.

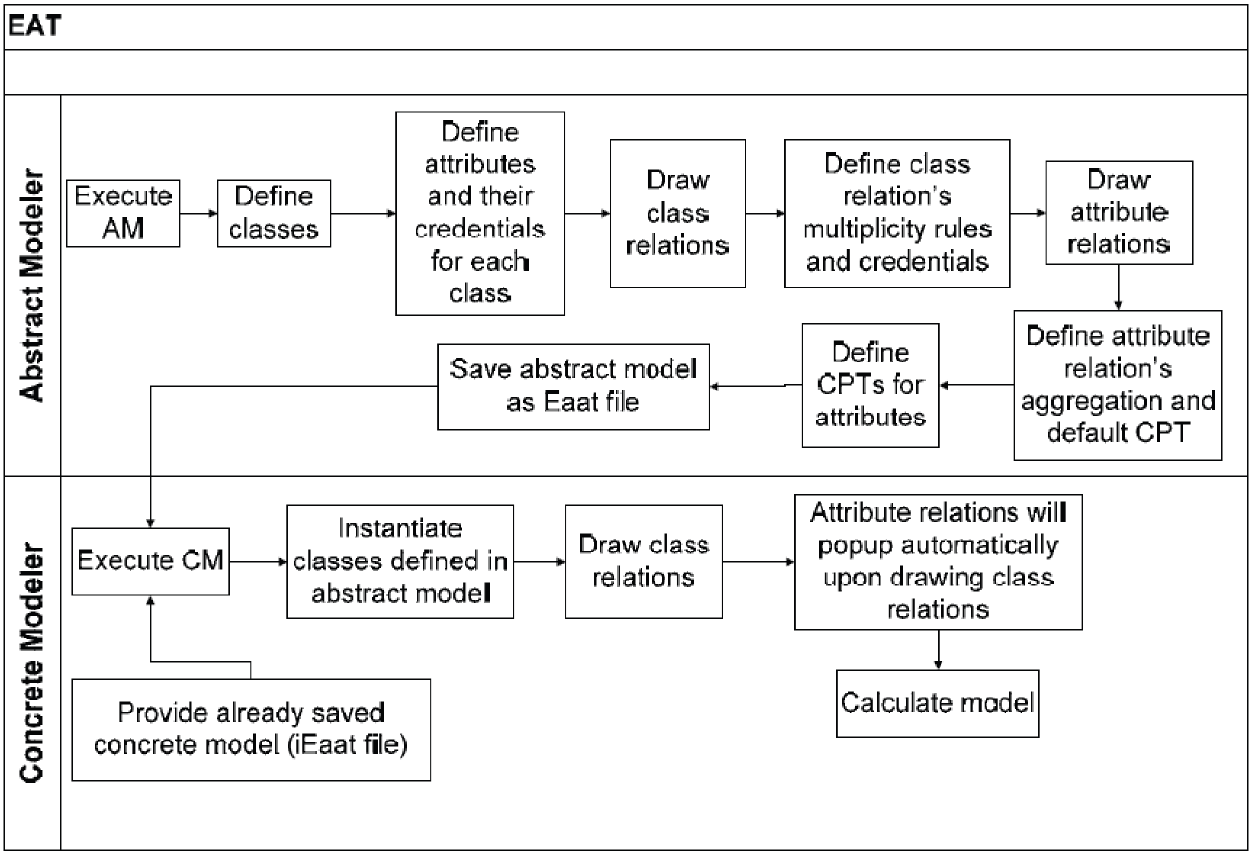

Fig 5.1 SHOWS APPLICATION PROCESS OF EAT

5.4 EAT FAMILIARIZATION

The EAT is written in Java to enable platform independence and thus requires Java JRE to run For windows users the program is started by from the command line using the command java–jar Or by clicking on the AbstractModellerPrm.jar.[15]

5.4.1 Getting familiar with the user interface

When starting the abstract modeler the following window is displayed. This view is dominated by the large modeling area, the white part of the window. Apart from this there is the menu bar and the tool bar at the top of the screen and the info palette at the right side.

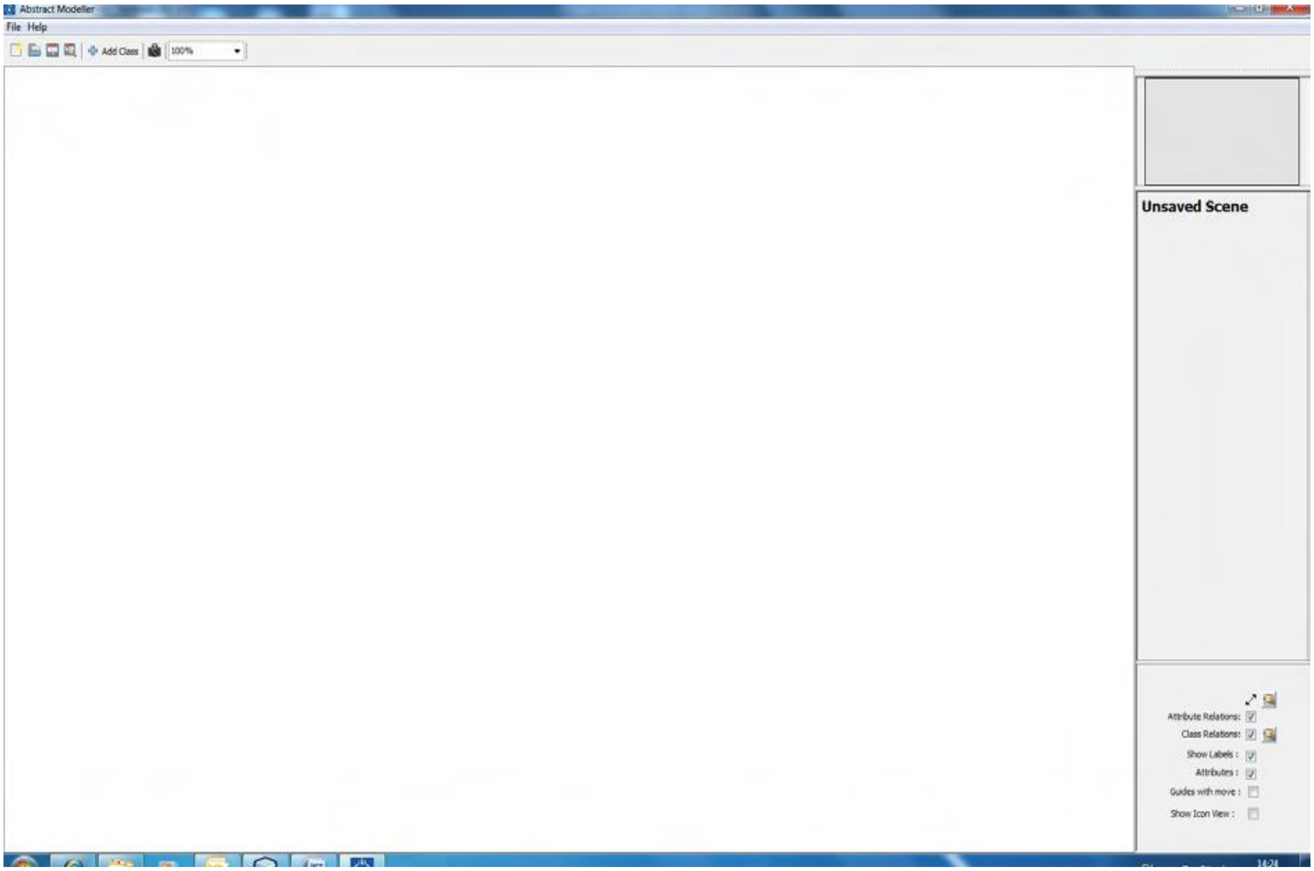

Figure 5.2 SHOWS THE MAIN WINDOW OF THE EAT ABSTRACT MODELLER WITH MODELING PANE, MENU BAR, TOOL BAR AND STATUS BAR. (ABSTRACT MODELLER)

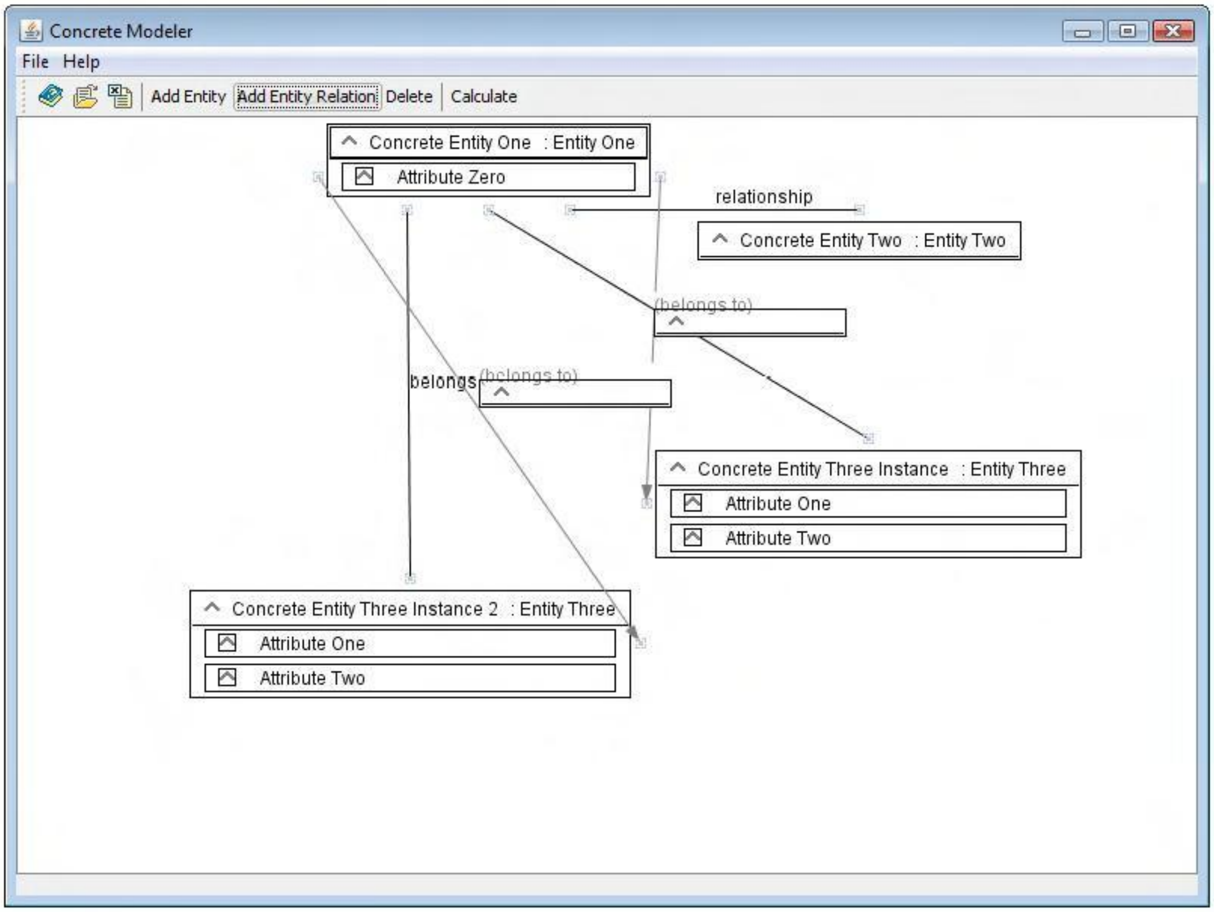

FIGURE 5.3 SHOWS THE MAIN WINDOW OF THE EAT CONCRETE MODELLER WITH MODELING PANE, MENU BAR, TOOL BAR AND STATUS BAR. (CONCRETE MODELLER)

Following is a short description of the menu choices and buttons in the tool bar, as well as the Info. palette.

5.4.2 Menu bar

The menu consists of two top menus, the file menu and the help menu. The file menu offers to “Export to XML” on the one hand and to “Import From XML” on the other hand. Executing the export function creates an xml document that reflects the content of the model, whereas the import allows reading a model from an xml file, which has been created earlier. Additionally the program can be closed from the file menu.

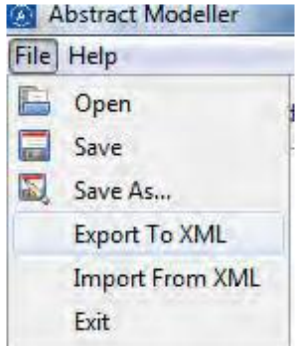

Fig.5.3 SHOWS THE FILE MENU OF ABSTRACT MODELLER.

5.4.3 Tool bar

The toolbar, as displayed below, allows for easy access to the most common functions of the tool.

Fig.5.4 SHOWS THE TOOLBAR OF THE EAT CONCRETE MODELLER, CONTAINING THE MOST COMMON COMMANDS.

Starting from the left there is a possibility to clear the scene and thereby to start with a new model. The second function allows opening of an existing model. These are followed by both save and save as functionality. Turning to the modeling tools, a button to add classes is offered. Next, screenshots of the model can be made and finally the zoom level can be adjusted.

5.4.4 Info palette

Information on the current model is presented in the information area on the left-hand side of the modelling pane.

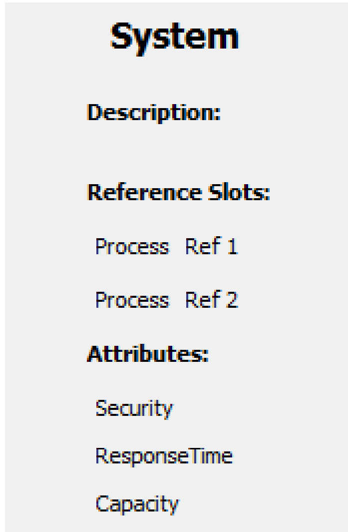

Fig. 5.5 SHOWS THE INFORMATION PALETTE OF EA.

At the top of the info palette a satellite-view can be found. This presents an overview of the model and is meant to help orienting and navigating within large models. Below information panel can be found. Here a short summary of the selected model-element is presented. In the lowest part of the info palette several filters can be switched on or off.[19] They are:

- To show the connections on top of the entities
- To show the relations between attributes
- To show the relations between classes
- To show the labels of the relationships
- To show attributes

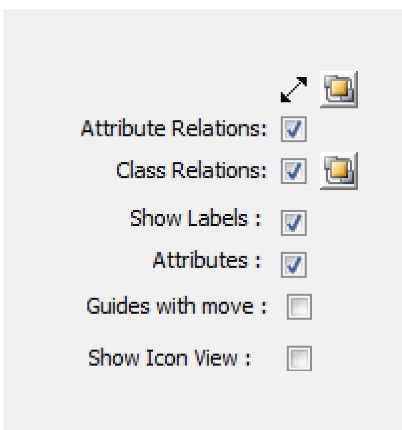

Fig. 5.6 SHOWS THE FILTER PANEL.

As mentioned before, enterprise architecture analysis is to support decision making in the field of enterprise information systems. The method to apply enterprise architecture analysis on enterprise architecture models with EAT.[17]

CHAPTER 6

RESULTS AND CONCLUSIONS

6.1 STARTING EAT

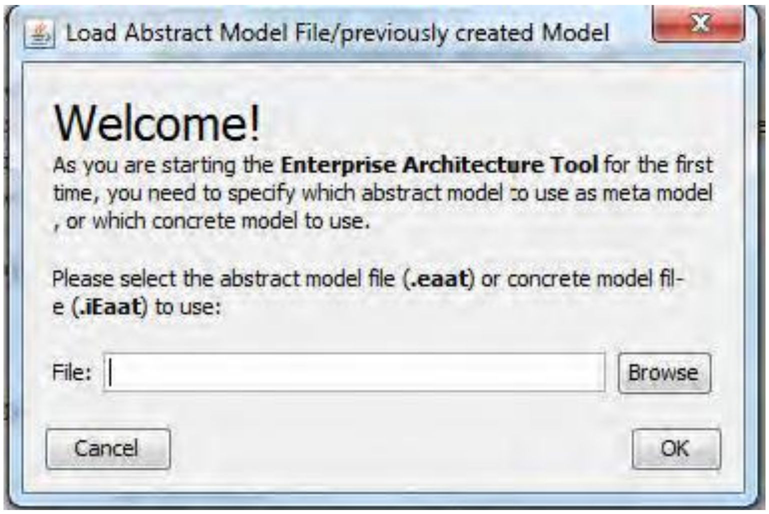

Fig 6.1 SHOWS START UP DIALOG BOX

6.2 EAT PROCESS: It is a three step process:

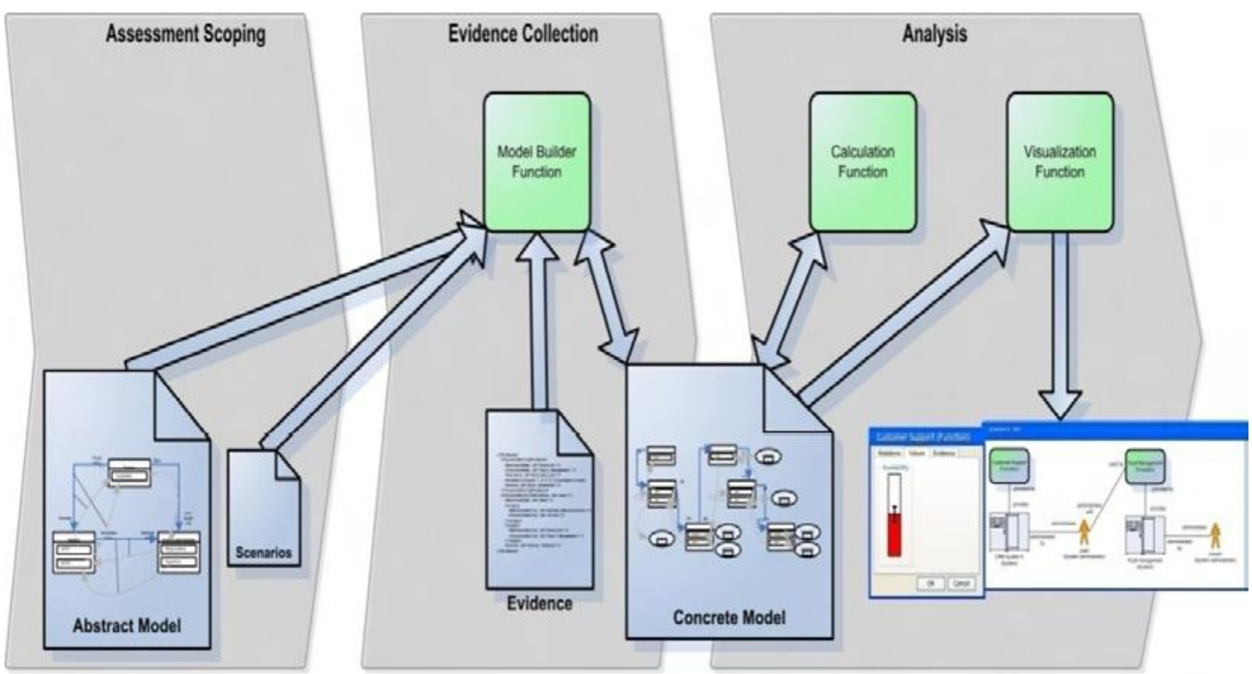

Fig. 6.2 SHOWS ENTERPRISE ARCHITECTURE ANALYSIS PROCESS

A Probabilistic Relational Model (PRM) for Control system cyber security risk analysis for SCADA using EA is studied. The first step is the Assessment Scoping where the problem is described in terms of enterprise information system potential future scenarios and in terms of the assessment criteria (the Abstract Model in the figure) with which the scenarios will be evaluated. The scenarios are detailed in the second step through a process of Evidence Collection. The results of this Evidence Collection are the Concrete Models of different scenarios.[34]

The third and final step is the analysis step. Here quantitative values of the models' quality attributes are calculated. The models, then, are visualized in the form of Enterprise Architecture Diagrams through the Visualization Function. In the Assessment Scoping step, the decision maker identifies the available decision alternatives, for example, in this case study, the cyber security framework scenarios.[14]

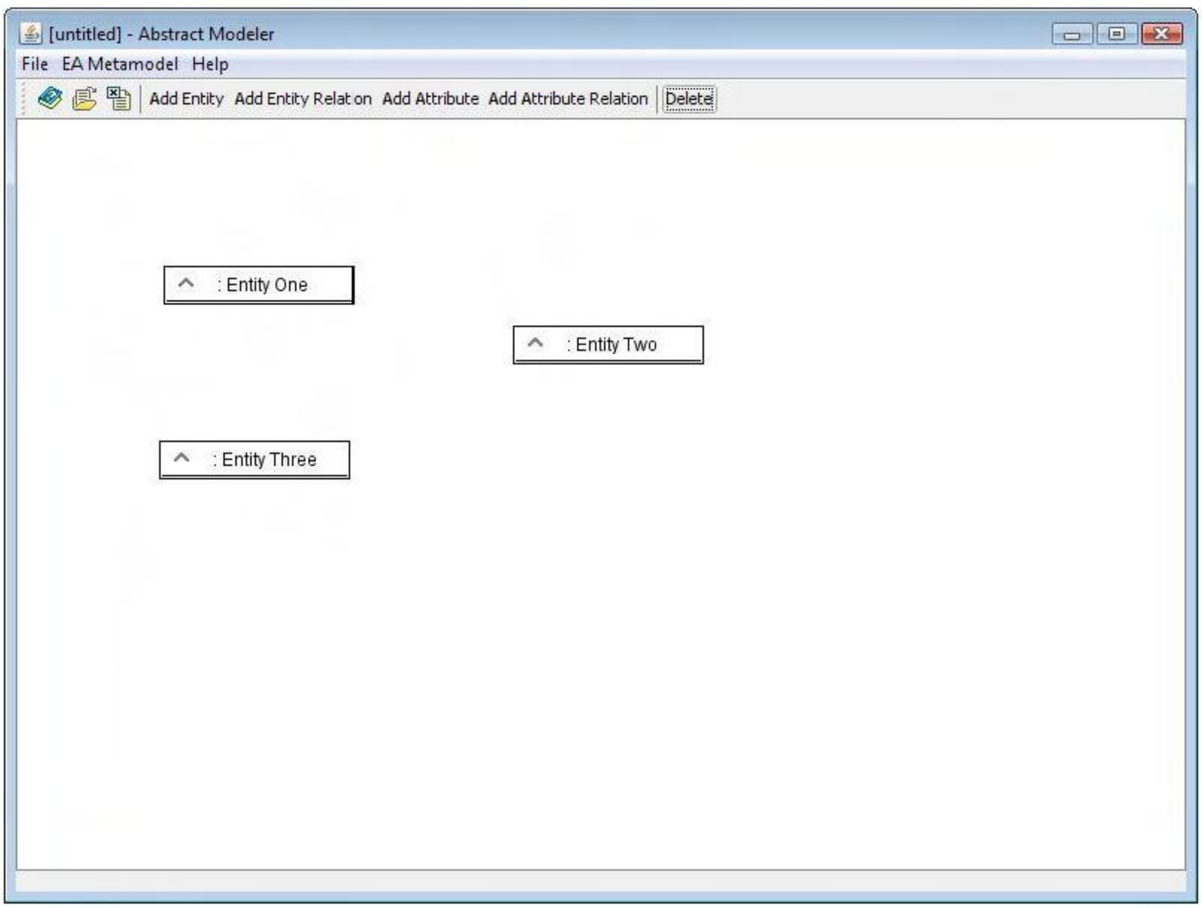

Fig 6.3 SHOWS EAT's GUI WITH AN ABSTRACT MODEL DEFINING THREE ENTITIES

The box has the name of the entity at the top, then there is a line separating the name area from the rest of the box. The entities can be connected to each other. These connections among entities are the entity relationships.

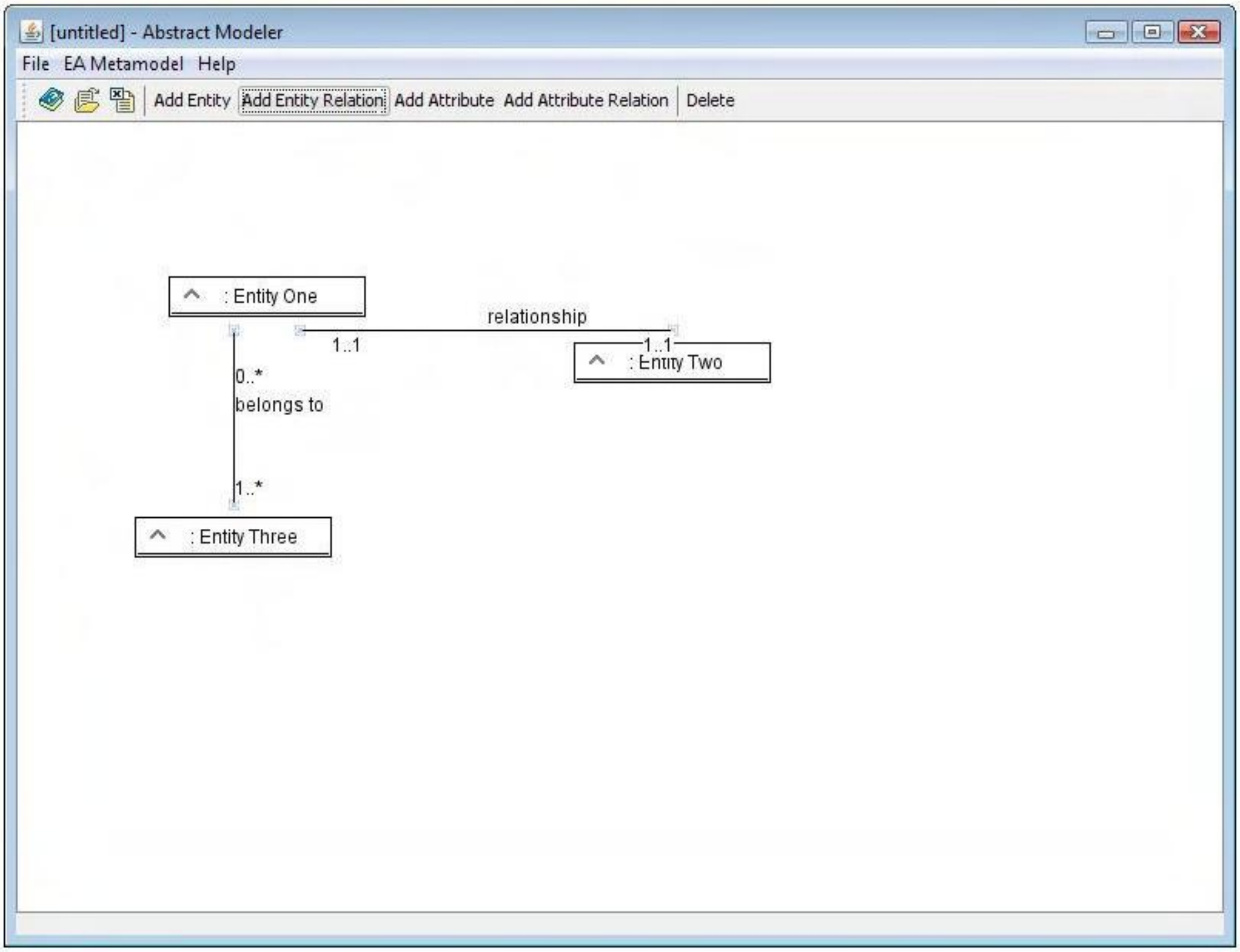

Fig.6.4 SHOWS RELATION BETWEEN TWO ENTITIES

The entities can contain attributes. Differently from UML the attributes of the abstract model are random variables. This allows introducing values to manage the probabilistic inference. The attributes may assume values from a finite domain such as the predefined ones:

{High, Medium, Low}, {True, False}, {0, 1, 2, 3, 4, 5} or they may assume value from a finite, but customizable domain.

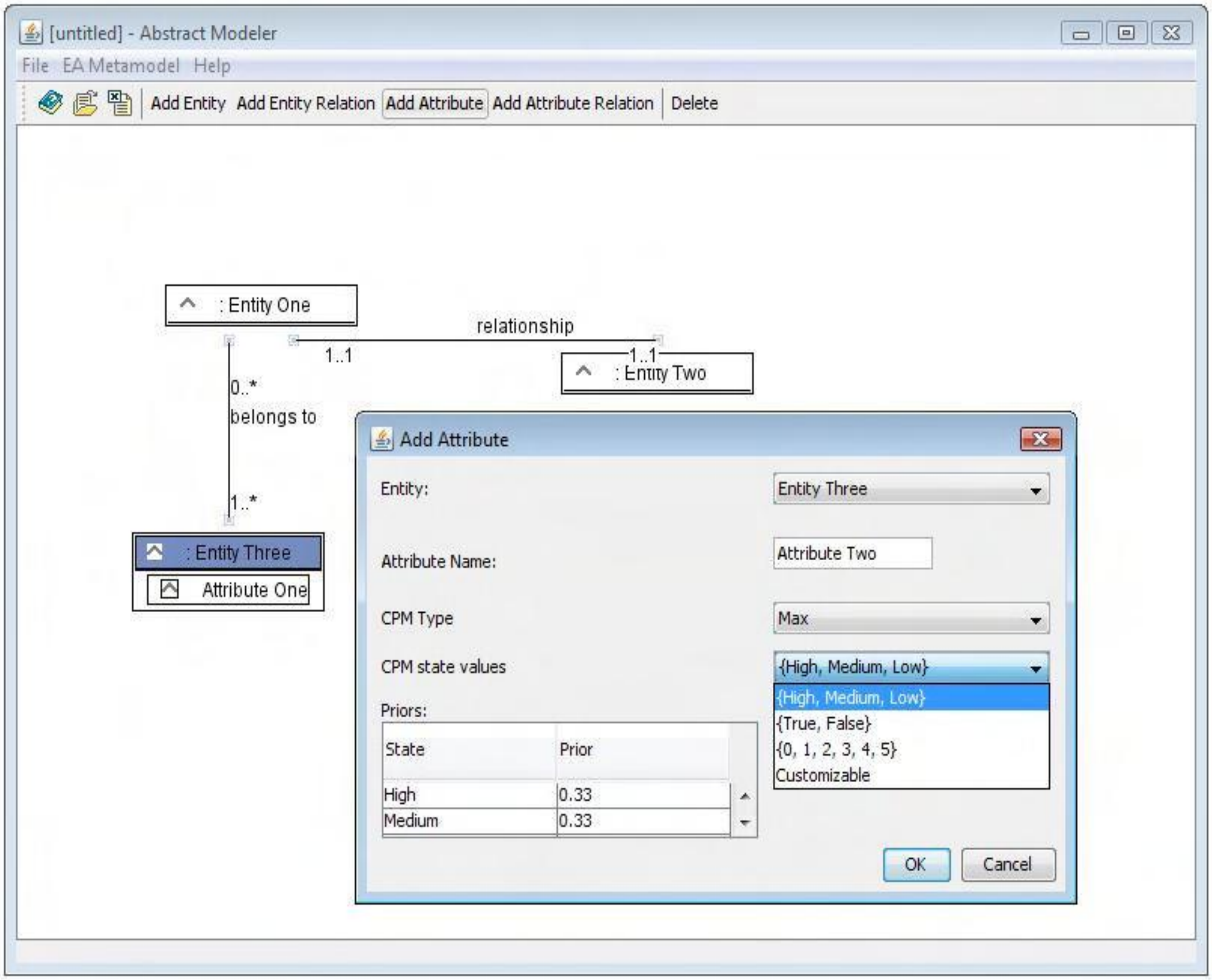

Fig.6.5 SHOWS EAT GUI SHOWING THE DIALOG TO ADD ATTRIBUTES

Attributes can represent concepts as "Logs exist", "Are Logs retained for thirty days", "Is documented". For example P(Logs exist=True) represents the probability that the attribute "Logs exist", associated to a certain entity, will assume the value 'True' stating the probabilistic existence of Logs for that entity. Graphically, attributes are depicted as rectangles inside the entities. The last component of the Abstract Model is the attribute relationship. They are graphically depicted as gray arrows between the attributes rectangles.

6.3 SCADA PROCESS OBJECTS

For the analysis the communication between the RTU and the SCADA system was investigated. The device process objects that are created by standard function tool can be freely chosen the protocol, but Secured With 5BO's must be chosen in order to get a proper set of select and execute objects for ICCP.[26]

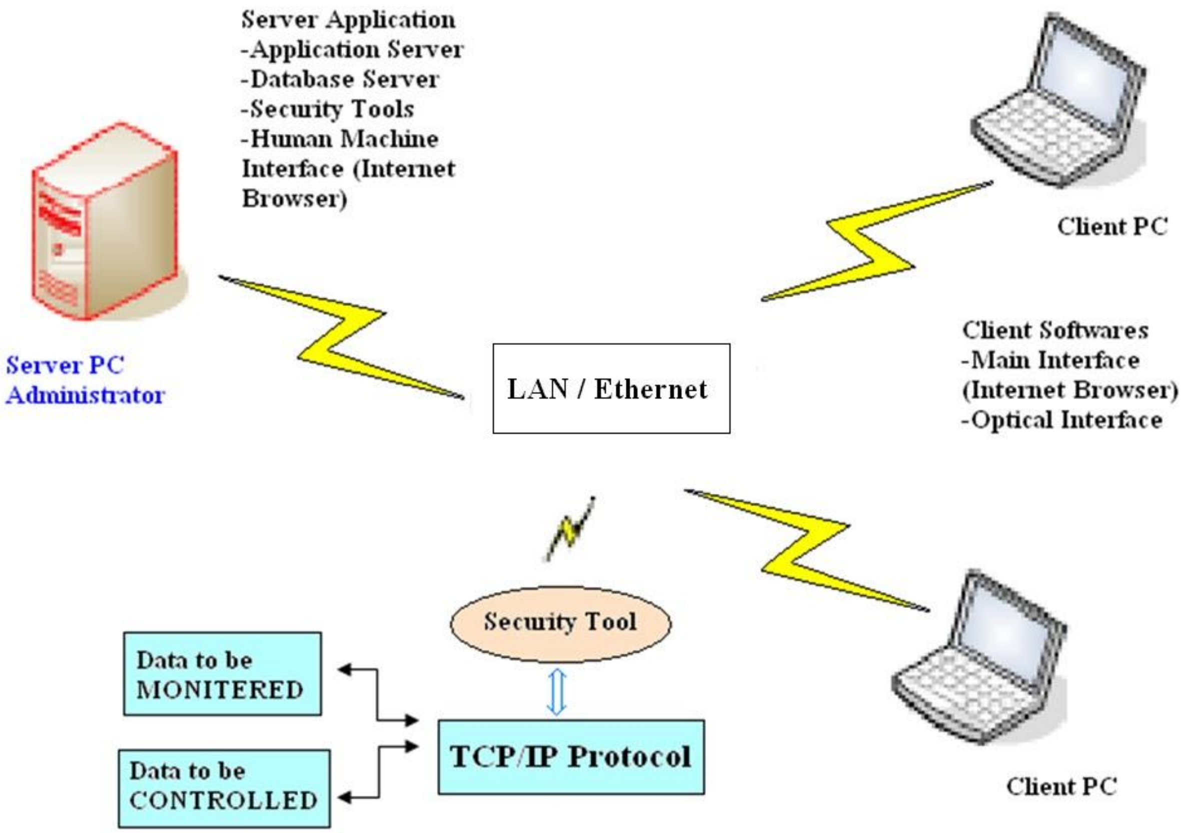

Fig.6.6 SHOWS ICCP SCADA COMMUNICATION

5.4 SCADA PROCESS SECURITY OVERVIEW WITH EA

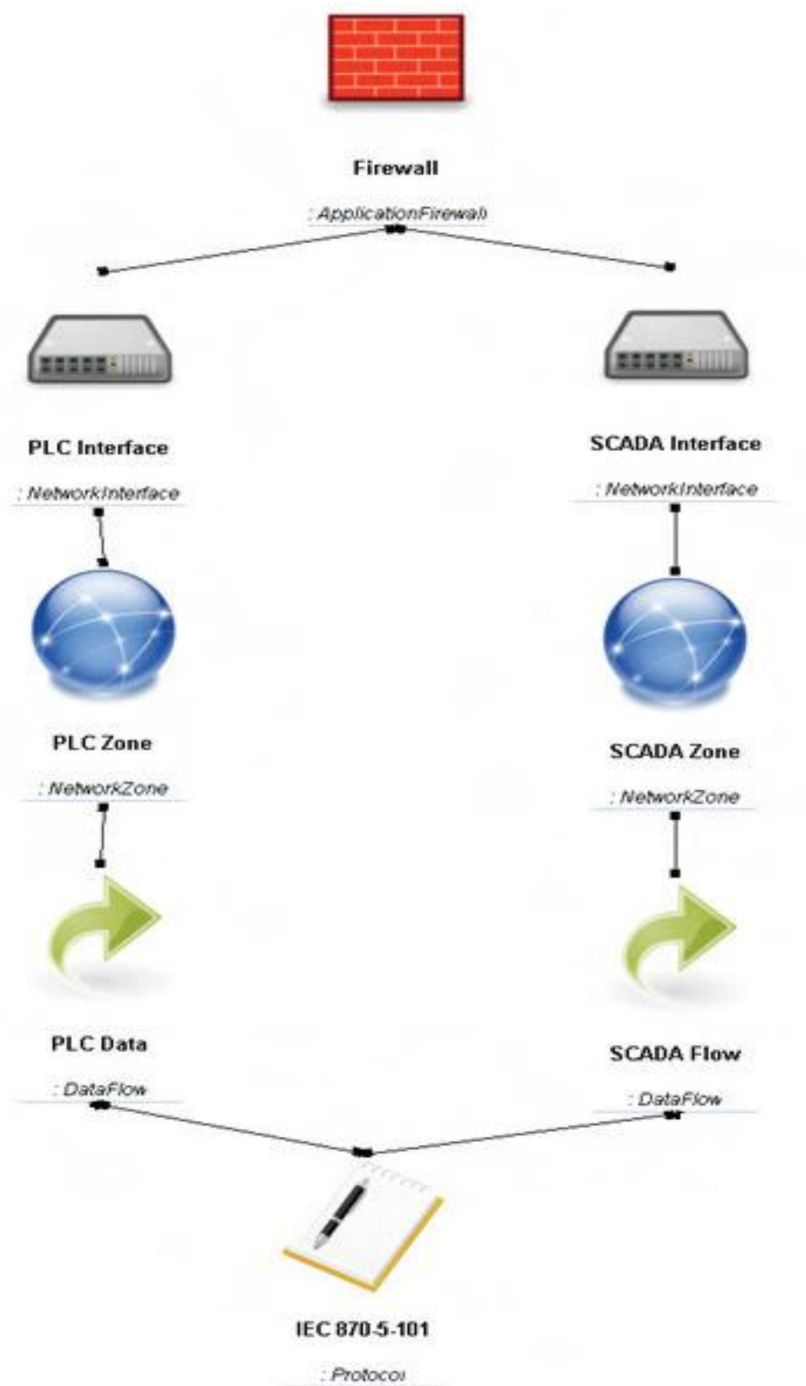

Fig5.7 SHOWS EA-SCADA PROCESS

SCADA process objects thus in consideration with the ICCP protocol test was then investigated. The red rectangle marked area represents an additional objects which are needed for the ICCP and are mapped to the OPC client as illustrated below [3]

LN	IX	UN	[OA]/IN	[OB]/EH	OI	OX	AN	FI
TSTH01C1	10				ICCP2 H01 C1	Current L1		3
TSTTR1Q1	10				ICCP2 TR1 Q1	Breaker position indication	ICCP_WRITE	1
TSTTR1Q1	11				ICCP2 TR1 Q1	Breaker open select command		0
TSTTR1Q1	12				ICCP2 TR1 Q1	Breaker close select command		0
TSTTR1Q1	13				ICCP2 TR1 Q1	Breaker open execute command		0
TSTTR1Q1	14				ICCP2 TR1 Q1	Breaker close execute command		0
TSTTR1Q1	15				ICCP2 TR1 Q1	Breaker device control block		0
TSTTR1Q1	16				ICCP2 TR1 Q1	Breaker open interlocked		0
TSTTR1Q1	17				ICCP2 TR1 Q1	Breaker close interlocked		0
TSTTR1Q1	18				ICCP2 TR1 Q1	Cause of interlocking		0
TSTTR1Q1	19				ICCP2 TR1 Q1	Breaker selection on monitor		0
TSTTR1Q1	20				ICCP2 TR1 Q1	Breaker command event		0
TSTTR1Q1	25				ICCP2 TR1 Q1	Breaker cancel command		0
TSTTR1Q1	101	2	1	0	ICCP2 TR1 Q1	Select Indication	ICCP_DEVICE_SELECT_2	0
TSTTR1Q1	102	2	1		ICCP2 TR1 Q1	Select CheckBackId		0
TSTTR1Q1	103	2	2		ICCP2 TR1 Q1	Select Send Response		0
TSTTR1Q1	104	2	2		ICCP2 TR1 Q1	Select Status		0
TSTTR1Q1	105	2	1	1	ICCP2 TR1 Q1	Operate Indication		0
TSTTR1Q1	106	2	3		ICCP2 TR1 Q1	Operate Send Response		0
TSTTR1Q1	107	2	3		ICCP2 TR1 Q1	Operation performed from: ICCP1		0
TSTTR1Q1	108	2	1		ICCP2 TR1 Q1	Operate Value	ICCP_DEVICE_OPERATE_2	0
TSTTR1Q1	109	2	1		ICCP2 TR1 Q1	Operate RVCC		0

Fig.6.8 SHOWS SCADA PROCESS OBJECTS

The measurement value is mapped with Custom STA and Free Integer between the OPC client and Micro SCADA. In order to make the circuit breaker controllable from the remote site there are three SCIL command procedures needed.

When the execution queue starts to increase rapidly, the data transfer limit is reached. It is not serious if the queue is loaded to some extent or it oscillates. As long as the number of objects in the execution queue does not get bigger all the time and the average number of objects stays in the moderate level, it is a sign that OPC can handle the queue. When the execution queue starts to increase rapidly and endlessly, it is a sign of overflow and OPC is a blocked.[14]

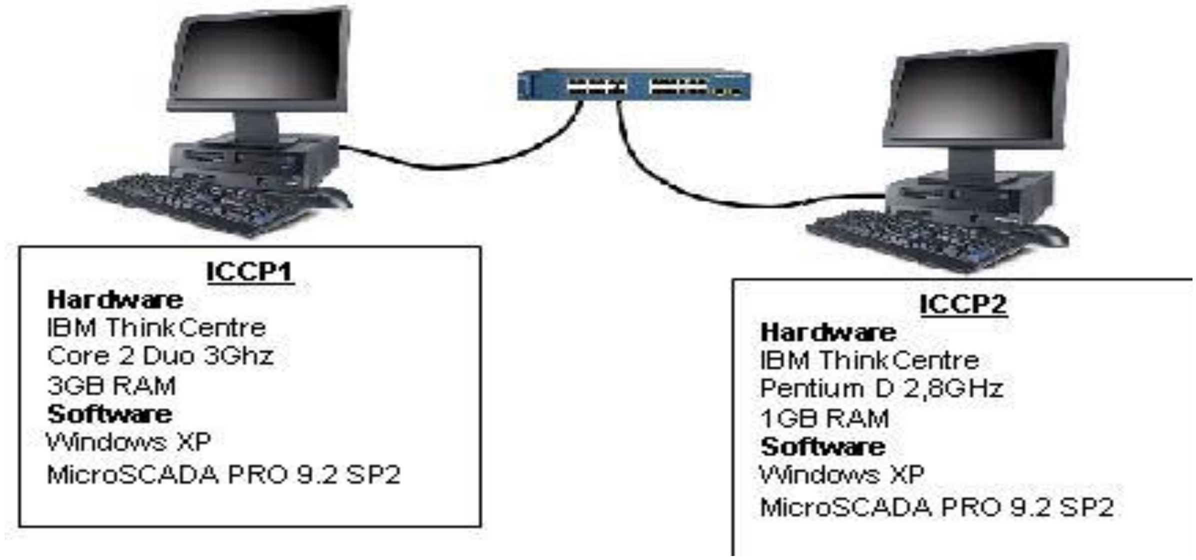

Fig.6.9 SHOWS THE TEST SETUP

The data exchange between the control centers with the ICCP protocol was tested with the above mentioned test setup. However, the performance was measured with ICCP2 computer, which has a lower performance. Therefore, it can be confirmed that the performance will not anyway decrease, in a real solution in a field. Nowadays the Micro SCADA is running on powerful server class computers, whereupon the performance should increase.

	Level 1	Level 2	Level 3	Level 4	Noncompliance Level
002 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
003 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
004 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
005 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
006 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
007 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
008 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
009 CIP	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1	True: 0 False: 1
Standards					True: 0 False: 1

Fig.6.10 SHOWS THE SNAPSHOT OF RESULT STUDY OF SLDC STANDARDS [20]

6.5 PERFORMANCE CURVE

Because the OPC client used was so-called external OPC client, it means that it is sort of external software and thus it can be monitored with Windows own performance monitor as illustrated in the curve. The red curve represents computer processor time that the OPC client uses. As it can be seen it shows a growing trend when updated objects are added. The yellow curve does not need to be taken into consideration.

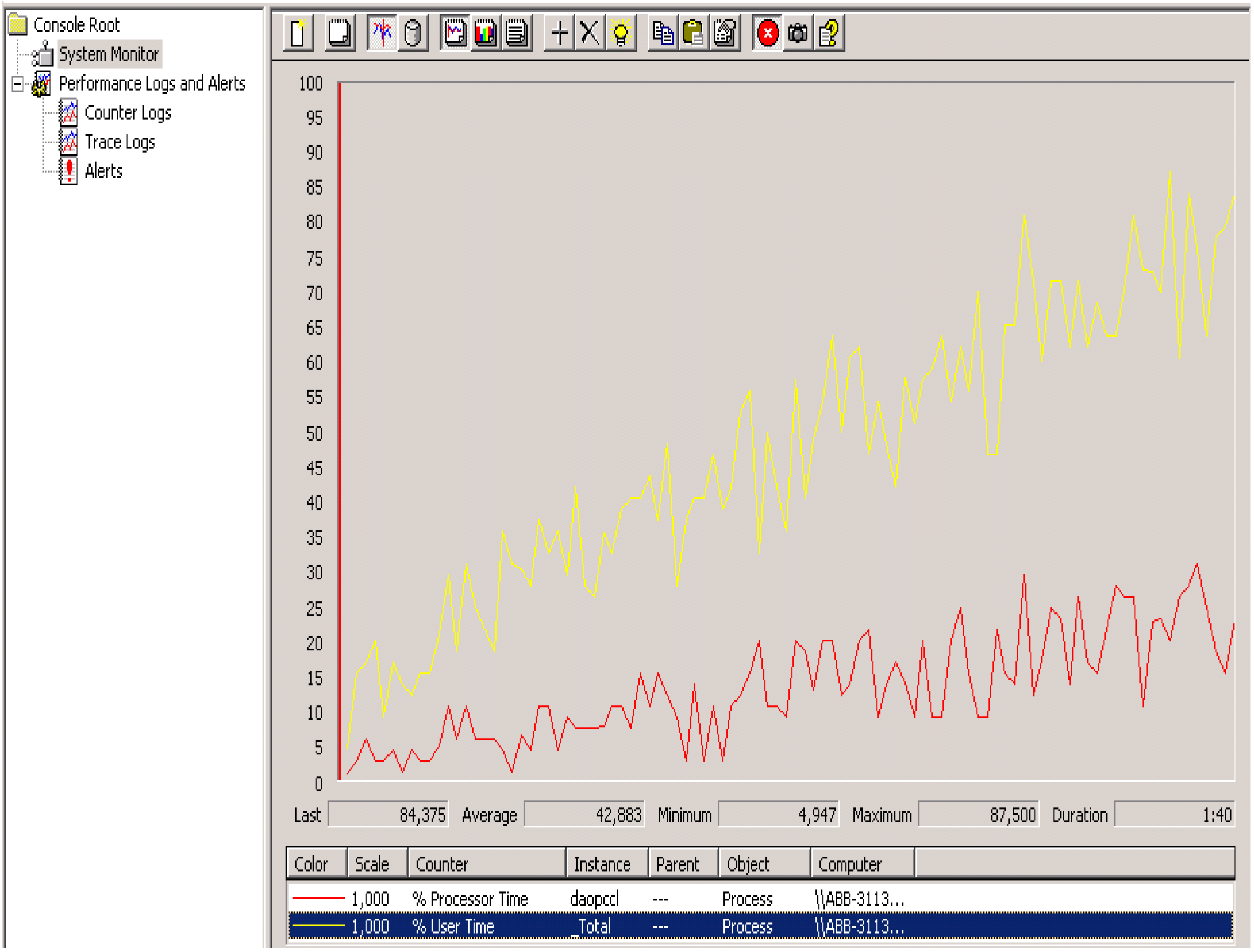

Fig. 6.11 SHOWS THE PERFORMANCE CURVE

6.6 CONCLUSIONS

A SCADA system and its components must be evaluated in terms of nine considerations, for both operational functions and managerial functions. As a part of my work at the load dispatch center the configuration and installation of the components at the center control room were initiated. The purpose was to find a solution how to implement external ICCP software into the MicroSCADA system and study of EA technology in the use of SCADA security systems. The use of this technology has definitely raised the standards of cyber security risk assessment. The results were evaluated as a guideline in order to compare the state of SCADA cyber security framework to the ideal position. The EA tool helped to build the abstract and concrete model for assessing the data available. The GUI makes the tool easier for the user to initiate and finalize the process. The computation is further done by double- clicking the attribute function of the result button. The tool has made it easier for the assessment of the cyber risks and their study.

6.7 FUTURE WORK

SCADA systems currently in operation have to be re-evaluated against the framework presented in this thesis to determine if they meet minimum requirements for security.

New SCADA system designs should be evaluated with this framework as a guide to understand the security implications of the design. Further research should be conducted on the implications of intersecting boundaries, and the effect on conflicting policies. Research on how best to systematically define boundaries should be conducted.

A formal analysis of the various open and proprietary communications protocols should be conducted to determine their suitability for high assurance SCADA systems. In order to make the EA tool easier to apply and to increase the number of users it needs to get more self-explanative. This should be addressed in terms of extensions of the user-interface that guide users through the tool-application.

Additionally help-functions, automatic wizards, auto-corrections, and a homogenous look-and feel should guide the user through the tool application. The changes should be made in close cooperation with the end users in order to specifically tailor the application.

REFERENCES

[1] AGA Report No.12, Cryptographic Projection of SCADA CommunicationsPart1: Background,

[2]“The ABB Group: The evolution of SCADA/EMS,” [Online]. Available: http://www.abb.com/cawp/gad02181/7ff771bfb4d81e96c1256e390052582f.aspx[Accessed:Aug. 28, 2008].

[3] Bailey David and Wright, Practical SCADA for industry, pp. 46-48, IDC Technologies, 2003 Communication Gateway, COM 500i. User’s Guide. ABB

[4] Cyber security of PCS/SCADA Networks: Half-baked Homeland Security, June, 2006 http://www.bechteltelecoms.com/docs/bttj v4n2/Article04.pdf

[5] Cisco Systems White Paper; Understanding Remote Worker Security: A Survey of User Awareness vs. Policies and Test Plan, American Gas Association, March,2006

[6] Department of Defense Architecture Framework Working Group: DoD Architecture Framework, version 1.5. Technical report, Department of Defense, USA (2007)

[7] EPRI Anomaly-Based Intrusion Detection in SCADA (Supervisory Command and Data Acquisition; http://www.epriweb.com/public/RS 1002598.pdf

[8] Heady et al; The architecture of a network level intrusion detection system; 1990

[9]Hughes, J., the Integrated Energy and Communication Systems Architecture, Electric Power Research Institute, 2004

[10] Henner Jakob “Securing Pervasive Computing Systems by Design: A Language Approach” in Recherche (2011)

[11] I Nai Fovino, A Carcano, M Masera “A Secure and Survivable Architecture for SCADA Systems” in 2009 Second International Conference on Dependability (2009)

[12]Jones J; Estimating Software Vulnerabilities; Security & Privacy, July-Aug 2007

[13]Johnson, P., Ekstedt, M.: Enterprise Architecture Models and Analyses for Information Systems Decision Making. Student literature, Sweden (2007)

[14] Markus Buschle, Ullberg John, Ulrik Franke, Lagerström Robert, Teodor Sommestad: A Tool for Enterprise Architecture Analysis using the PRM formalism In: Proc. CAiSE Forum 2010

[15] Pontus Johnson, Erik Johansson, Teodor Sommestad, and Johan Ullberg. A Tool for Enterprise Architecture Analysis. In Proceedings of the 11th IEEE International Enterprise Computing Conference (EDOC 2007), October 2007.

[16]Robert Permann, Raymond K.Fink, David F. Spencer, Rita A. Wells. "Lessons Learned from Cyber Security Assessment of SCADA and Energy Management Systems'',National SCADA TestBed(NSTB),2006,

http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf

[17] Robert Dacey, "Critical Infrastructure Protection: Challenges in Securing Control Systems," Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform, GAO-04-140T, October 2003.

[18]Rached Dhaouadi, Khalid Darwish; Virtual SCADA simulation for power substation" 2000, IEEE, Volume 3.

[19]SANDIA, "Securing dialup communications with encryption modems," Tech. Rep., 2003.[3] R Carlson, "Sandia SCADA program: High-security SCADA LDRD final report," Sandia National Laboratories, Tech. Rep., 2002.Thomas Robert. NSF/OSTP Workshop on Information Technology Research for Critical Infrastructure Protection for SCADA, September 2002.

[20] SCADA Manual book,, PSEB.

[21]Sebastian Jeckel, Abdelmajid Khelil, Daniel Germanus "Benchmarking of P2P Technologies from a SCADA Systems Protection Perspective" CIIP at Mobilight, 2010 in Techniques (2010)

[22] Seoksoo Kim,Giovanni Cagalaban, " Improving SCADA Control Systems Security with Vulnerability Analysis in Parallel and Distributed Computing and Networks" SCADA summitt (2011)

[23] Seog-Joo Kim, Dong-Joo Kang, Jong-Joo Lee,Jong-Hyuk Park "Analysis on cyber threats to SCADA systems" in 2009 Transmission Distribution Conference Exposition Asia and Pacific (2009)

[24]T. Bucher, et.al,"Enterprise Architecture Analysis and Application – An Exploratory Study," Institute of Information Management, University of St. Gallen Zocco L, "SEL and electric power utilities working to safeguard the electric power grid," in Power Systems World, 2002.

[25] Tai-Hoon Kim, Randy S Tolentino, " Distributed System Network Architecture for Securing SCADA system"in International Journal of Smart Power (2010)
[26] Thomas Robert. NSF/OSTP Workshop on Information Technology Research for Critical Infrastructure Protection for SCADA, September 2002.
[27] Vilanov Ramon,Pere Ponsa , A Pérez , Bojan Andonovski "SCADA design in automation systems" in Human System Interactions HSI 2010 3rd Conference on (2010)
[28] Wright, A.K., Kinast, J.A. and McCarty, J. (2004) 'Low-latency cryptographic protection for SCADA communications', Proc. 2nd Int. Conf. on Applied Cryptography and Network Security, ACNS 2004, LNCS 3809, Springer, pp.263–277.
[29]Wright-Patterson AFB, OH, USA, Coates, G.M.; Hopkinson, et.al; Dept. of Electr. & Comput. Eng., Air Force Inst. of Technol., "Communication network security device"; Power Delivery, IEEE Transactions; Issue Date: Jan. 2010 ,Volume: 25 Issue:1 ,On page(s): 158 - 169
[30]Wells Robert, Fink R., D. Spencer 2006, Lessons Learned From Cyber Security Assessments of SCADA and Energy Management Systems, US Department of Energy.
[31]Wildman Luke, Jörn Guy Sub, Peter, et.al; "Integrated Model-Driven Testing of SCADA Systems Using the Eclipse Modeling Framework and Modelica" in October (2008)
[32] Wang Yongge "sSCADA: securing SCADA infrastructure communications" in IACR Eprint (2004)
[33] Wiley Jon; Annarita Giani, Gabor Karsai, Tanya Roosta, Aakash Shah, Bruno Sinopoli, "A testbed for secure and robust SCADA systems" in ACM SIGBED Review (2008)
[34]Yung Suu, Sommestad, T., Ekstedt, M., Johnson, P.: A probabilistic relational model for security risk analysis. Computers & Security (February 2010)
[35] Yemen Rolad, Johansson Elbert, 2007, "Assessment of Enterprise Information Security How to make it Credible and efficient", The Royal Institute of Technology, Stockholm.