ABSTRACT

KHANNA, MOHIT. Communication Challenges for the FREEDM System. (Under the direction of Dr. Wenye Wang).

The Future Renewable Electrical Energy Distribution and Management (FREEDM) Center's proposal to incorporate the renewable resources of energy as source of electricity into the existing power distribution system and allow for energy exchange between individual sites, is a revolutionary idea which will help us meet the energy needs of the future in an environment friendly manner. The renewable resources of energy have certain characteristics which make such an integration very challenging. They are available in large amounts but not concentrated at an area and are intermittent in nature. Thus a lot of them need to be deployed along with storage resources in order to obtain a steady source of electricity resulting in a distributed energy generation environment. To maintain the stability of such an electricity distribution grid, it is essential to monitor and control each site from a central location using agents. These agents also need to communicate with each other to execute any protection scheme or for energy management to utilize any excess electricity at a site. Therefore, a reliable communication backbone becomes an essential platform which would allow such a communication to take place. Since FREEDM is intrinsically a complex system, the communication backbone must be a fault-tolerant in that distributed devices and elements may become faulty or fail.

In this thesis, we investigate the challenges for such a communication backbone in a distributed energy generation and energy exchange environment within an electricity distribution system. We use the FREEDM system as a platform for our research. To our knowledge, a power system proposed by the FREEDM, does not exist, which makes our job more challenging. We need to identify the various communicating entities, communication scenarios and their timing requirements within the FREEDM system and propose a communication architecture which meets these criteria. We also need to identify the possible communication protocol standards which will be used for message exchange.

In order to understand the communication needs of power system applications which would be used in the FREEDM system, we conduct a survey of the existing power system communication architectures (the SCADA and substation automation systems) and communication protocols (DNP3 and IEC 61850).

Further we detail the various levels of communication and communicating entities within the FREEDM system. We apply our understanding of existing substation automation systems to the FREEDM system and identify the timing criticality and communication requirements for power system applications within the FREEDM system. In order to quantify the timing requirements and to identify the various networking technologies which will be used to support the communication backbone of the FREEDM system, we set up a distributed communication testbed using ZigBee, WiFi and Ethernet communication technologies. A Web, SNMP–based monitoring tool set up by us, as a means to keep track of the distributed devices forming the testbed is also presented. We conclude the thesis by presenting the results of experiments performed by us on the testbed and presenting a road-map for our future work.

This thesis, presents our first year efforts towards setting up of a communication backbone for the FREEDM system and identifying the communication challenges. The reliability and security aspect of the communication backbone, will be taken up in our future work. Our preliminary results have provided a fundamental platform to study unique challenges in the future design and development of a reliable and secure FREEDM system.

Communication Challenges for the FREEDM System

by
Mohit Khanna

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fullfillment of the
requirements for the Degree of
Master of Science

Computer Engineering

Raleigh, North Carolina

2009

APPROVED BY:

Dr. Subhashish Bhattacharya

Dr. Alex Dean

Dr. Wenye Wang
Chair of Advisory Committee

DEDICATION

To my father, Dr. K.K.Khanna, mother, Dr. Savita Khanna, my brother Rohit Khanna, my grandfather, Mr. V.D.Khanna. They have been a constant source of encouragement, inspiration and always ensured my well being !!

BIOGRAPHY

Mohit Khanna was born on June 16, 1983 in the city of Delhi, India. He did his schooling from Montfort School Delhi. He completed his Bachelors in Technology in Electronics and Communication Engineering from Guru Tegh Bahadur Institute of Technology, Guru Gobind Singh Indraprastha University, India. He worked as a software engineer with Xansa, India (now Steria) for 1.3 years. He also worked with Mtree Solutions for 8 months.

Mohit joined the Electrical and Computer Engineering Department at North Carolina State University in Aug'07 for Masters in Computer Engineering. He did his summer internship (May-Aug'08) with Qualcomm, San Diego with the WCDMA Integration team. Since Aug'08, Mohit has been working with Dr. Wenye Wang as a master's thesis student on the FREEDM project, with focus on a reliable and secure communication backbone for the FREEDM system.

Mohit intends to continue working with Dr. Wenye Wang on the FREEDM project and pursue his Ph.D. in Computer Engineering at NC State University after completing his master's degree.

ACKNOWLEDGMENTS

Working on my master's thesis has been a learning and a rewarding experience. When I began, I simply had no clue, as to how to approach a research topic and go about answering the key questions. I would like to take this opportunity to thank Dr. Wenye Wang, my academic advisor for showing me the way. She has always been a source of encouragement and guidance, helping me see the "the big picture" of the project instead of only focusing on a small aspect of it. She spent a lot of her time and energy in training me for my master,s thesis.

I would like to express my gratitude towards Dr. Alex Dean and Dr. Subhashish Bhattacharya for agreeing to be the committee members for my Master's thesis. I would like to thank Dr. Alex Dean for his insights and suggestions about the hardware platform we used for the testbed. I would like to thank Dr. Subhashish Bhattacharya, who helped me see the problem from the perspective of power systems. I would like to thank Dr. Mesut Beran and his students. Regular meetings with him helped me see the over all picture of the FREEDM project.

I would also like to thank my family and my girlfriend, Preeti, for their constant support. I would like to thank Subash and Shawqi, who worked with me on this project and helped me to come up with a paper for the FREEDM conference in May'09. My lab mates at the NetWIS lab have been very encouraging and always helped me whenever I was in need.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Current Power Systems and Renewable Energy - Issues

The current generation of power systems have served us for more than 50 years. However, the power systems in their current state cannot keep pace with the present day challenges, namely depleting oil resources, global warming, environmental pollution, increasing energy demands, need for energy independence from imported crude oil and an overall economic stability. To alleviate the problems mentioned above, towards a clean sustainable environment, the usage of renewable sources of energy for electricity generation is important. The same has also been stressed in the 'Energy Independence and Security Act of 2007' [1] approved by U.S. Congress. Besides the above benefits, the clean electricity produced from these resources can also be used to charge public transportation vehicles which rely upon batteries partially (plug-in hybrids) or completely (plugin-in electric). However, in the existing power systems, these resources account for only 7% of the total electricity generation [2] and focus on hydro electricity. Hence, there is a need to incorporate other renewable resources like solar and wind energy for electricity generation and to increase the overall utilization of these resources. It is projected that, the renewable generation, would increase by more than 100 percent from 2007 to 2030, when it would accounts for 14% of total generation [2]. We discuss the other advantages of using DRERs, their characteristics, communication needs and the obsolete features in the exiting systems which impede their deployment below.

DRER use can lower peak energy demand: The usage of solar energy sources like

the photovoltaic cells can be increased by setting them up along the electricity distribution networks. For example solar panels can be set up on rooftops of households and commercial buildings. If the solar energy is in excess at particular site, as of now, there is no straight way that this excess electricity can meet the demand of load at some other site or contribute to the distribution grid in general to meet the peak demand. Had it been possible, it will be useful for both the owner of excess electricity and the utility industry. The owner might benefit terms of the energy independence and some form energy credits from the utility company for his contribution of electricity and the utility will benefit as they will not have to bear the massive costs of running extra power plants in expectation of the peak demand. This bi-directional electricity exchange with the electricity distribution system forms the core objective of the proposed FREEDM system as discussed in Section 3.1.

DRER characteristics: The implementation of a bi-directional electricity exchange mechanism into the existing electricity distribution system is not very straight forward as the existing utility electric power systems were not designed for active generation and storage at the distribution level [3]. Moreover the renewable resources have certain characteristics which make their integration with the electricity grid very challenging. These sources are intermittent in nature and there is uncertainty about their times of availability. Thus they need an appropriate energy storage infrastructure which is used as an electricity source during times of their unavailability. As they are less intense in their capability to generate electricity, a lot of them need to be deployed making the electricity grid highly distributed. The use of a lot of plug-in vehicles adds to the distributed nature of the grid. These energy resources like the solar energy are generally referred to as *Distributed Renewable Energy Resources (DRERs)* in this thesis while the storage devices and plug-in vehicles are referred to as *Distributed Energy Storage Devices (DESDs)*.

DRER communication needs: To accommodate the DRERs and DESDs into the existing grid, there are changes required in the power system technology like e.g., use of solid state transformers, advanced semiconductor technology etc., and also a need of a communication infrastructure to support the electrical system. In this thesis, we investigate the communication needs for such an infrastructure which needs to

support a lot of electrical functions. For example, the distributed nature of the renewable resources calls for centralized monitoring and distributed autonomous fault protection and control. A two-way communication between the utility and the renewable resources (for reducing the peak demand) and between the renewable resources themselves (for energy exchange), would be required for information exchange. All the information must reach its destination reliably in a timely and secure manner. The reliability of the communication backbone is also critical.

DRER deployment impeded by obsolete features in existing grid: There are a lot of obsolete features in the present day electricity distribution grid which impede the deployment of DRERS and DESDs. Some of these are mentioned below:

- *Centralized generation and Unidirectional flow of electricity:* The present day power systems are centralized in nature. Because of the centralized generation, a glitch affecting one part of the grid might easily cause blackouts in a lot of distant areas. Practical difficulties in centralized power system expansion, limited power quality, security issues etc. are other problems faced by a centralized grid [4].
- *Lack of support for renewable sources of energy:* The electricity generation from renewable sources of energy can destabilize the grid. For example, the distributed and intermittent nature of these resources impacts the voltage and frequency levels on the grid and introduces protection issues [5]. Moreover, it is difficult to predict the availability of renewable resources and thus its difficult to co-ordinate the electricity generation from these resources with the electricity demand leading to grid instability.
- *Lack of support for bi-directional energy exchange:* As discussed above, the future DESD/DRER based electricity distribution grids will require a two-way energy exchange capability. The current iron/steel core based transformers in the distribution system are not efficient enough to meet this need. The FREEDM center will develop advanced solid state transformers which will provide a two-way energy exchange between the sites with loads and renewable resources of energy and electricity distribution grid. The paper [6] describes the design of the solid state transformer.

- *Lack of communication:* In present day power systems, there is only one way communication from the meter at the client site to the utility company. Thus the utility companies have no way to control or communicate with the loads at the client side. Lack of communication also provides limited information about the electrical utility equipment within the distribution grid.

1.2 Future Power Systems - The SmartGrid Vision

In Section 1.1, we enlist the obsolete features within the exiting power distribution grids and the communication needs for the use of renewable resources of energy for electricity generation. Hence there is a need for modernization of the grid using the state of the art technologies in power electronics and communication to overcome these shortcomings and to make the grid more reliable and efficient. A clear vision for the future power grid architecture is required before any investment or implementation work is carried out in the area. This comprises of the various aspects of the modern grid such as interconnection issues, communication protocols, communication medium, use of advanced solid state transformers etc. Such a vision has also been proposed and endorsed by a number of independent organizations all over the world [7][8] to transform the existing power distribution grid into a *SmartGrid*. For a complete realization of the vision and to ensure interoperability of the Smart Grids with the existing electric power systems, standardization of the new electrical and information technology is also required. For this reason, standard IEEE P2030 has been set up [9].

From a communication perspective, it is important for us to understand the Smart Grid vision, as the various applications and use cases listed by the vision would dictate the communication requirements and the architecture for the communication backbone supporting the vision. The main features of the SmartGrid vision have been discussed below:

- *Support for different forms of generation and storage devices:* Unlike the existing electricity distribution grid, the future grids are expected to accommodate different kinds of electricity generation and storage devices. Improved interconnection standards will allow seamless integration of distributed sources and storage options with different capacities, at all voltage levels. These will include the renewable sources of energy, like

the photovoltaic, wind, fuel cells, advanced storage batteries, plug-in hybrid vehicles etc. IEEE standard 1547-2003 species the procedures for information exchange, interconnection, control and monitoring of the distributed resources interconnected with the electricity grid. Large commercial central power plants including sun/wind farms and nuclear sources of energy, will continue to provide the major chunk of electricity. Efficient transmission lines will need to accommodate their remote locations. The grid will also provide for efficient transformers for a bi-directional energy exchange with the grid.

- *A Self-Correcting grid:* The SmartGrid is expected to detect, analyze and respond automatically to changes where human intervention may not be required or the action is too critical to wait for human intervention. Thus the grid will be able to detect the occurrence or the possibility of a fault in the transmission or distribution systems at the earliest. This would improve the reliability, power quality and efficiency of the grid and also minimize service disruption. The paper [10] suggests the use of an autonomous agent, communicating with the grid and controlling distributed energy sources, loads and storage devices.

- *A secure grid:* The future SmartGrids will make use of communication technologies for critical functionality such as control, protection and monitoring of electrical equipment. Hence the security of such a connected structure from any cyber attack is of paramount importance. Security against any physical attack would also be a concern. In case of any breach of security, it is expected that the grid will be able to detect, and isolate such a breach to minimize its affect and raise an alarm to speed service restoration.

- *Incentives for consumers:* In the future grids, the utility can have variable electricity pricing according to the load on the grid. For example, low electricity tariff for usage in off-peak times. If the consumers are well informed about the variable tariff and their electricity usage in real time, they can schedule their loads (the less critical tasks) to a time when the overall load on the grid is not at its peak capacity. This is referred to as *Demand Response*. An electricity usage profile for each consumer will make the process automated and customizable. Realization of demand response will have advantages for both the consumers and the utility companies. The consumers will be

able to keep their usage under check and reap the benefits of intelligently scheduling their electricity usage. They shall also be aware of electricity usage by individual appliances and may choose to replace the inefficient ones. The utility companies will benefit by avoiding the inefficient operation of the power plants and the transmission lines during times of peak electricity usage. Since by following such a system, the peak load on the grid would be under check, the utilities will not need to keep their generators running on standby and utilize their running assets to the maximum.

Implementation of demand response would require a two-way communication mechanism between the utility companies and the electrical appliances in households.

- *Superior power quality:* Power quality is the ability of the supplied electricity on the distribution grid to adhere to the specified levels of peak or RMS voltage. Any deviation in the level (e.g. increasing, decreasing or random R.M.S. voltage) can harm the loads attached to the grid which are generally designed to function at specified levels of electric voltage and frequency. The affected load in turn can harm the gird. For example, it might cause a dip in the voltage levels on the grid affecting other customers which share the infrastructure with the affected site. In severe cases, it might even lead to a power outage leading to loss of revenue. One of the ways to avoid such a situation is to make the loads more resistent to transients in the electric distribution network. The other way is to improve power quality.

  The modern grid will handle such problems by improving the power quality through power quality monitoring (using sensors) and power conditioning. It will provide power quality in accordance with load sensitivity. Thus there could be different levels of power quality at different prices. The digital appliances and gadgets require higher power quality than what is provided by the traditional grid.

1.3 Problem Statement and Contribution

In Section 1.1, we discussed the need for communication within a distributed electrical grid with DRERs and DESDs. Section 1.2 further lists the vision for Smart Grids and the various use cases where the communication would be useful. In this thesis, we focus on the communication between the agents controlling the DESD or DRER (e.g. for autonomous

control, protection and energy exchange) and between agents and a local substation (e.g. for centralized monitoring) and investigate the challenges for communication. Since deployment of DRERs, DESDs and two-way energy exchange in the electricity distribution grid are upcoming power system technologies, there are a lot of unanswered communication related research questions which motivate us to focus our research efforts in this area. We use the FREEDM system (described later in Section 3.1) as a platform for our research.

From the intermittent, distributed nature of the DRERs and DESDs (Section 1.1) and the vision of a self-correcting and secure communication for Smart Grids (as mentioned in Section 1.2), it is evident that a distributed, reliable and a secure communication backbone is required. Since the information for the electrical power systems functionality like protection and control is time sensitive, the timing requirements of these applications must also be met. Moreover, the communication backbone must be a fault-tolerant in that distributed devices and elements may become faulty or failed. The design of the communication backbone to be used for communication above poses us with the following questions, which we answer in this thesis.

- What is the communication architecture required to support communication between DRERs and DESDs?
- What communication protocols can be used for a distributed power system with DRERs and DESDs?
- What are the critical, time-sensitive applications and their timing requirements in such a system?
- What are the various networking technologies which can be used to meet the communication requirements of such a system?

In this thesis, we survey the existing power system communication architectures (SCADA and Substation Automation systems) and standardized communication protocols used in these systems (DNP3 and IEC 61850). This is because, a lot of electrical functions used in substation automation (protection, monitoring, and autonomous control) and SCADA systems (Power System Control and Tele-Protection) are also required for the communication between the agents controlling DESD or DRER devices within the electric distribution system. We also investigate the delivery time communication requirements for

substation automation and draw parallels for the FREEDM system. In this thesis, we detail the communication architecture for the FREEDM system and explain the various communicating entities involved in the system. The timing criticality for the FREEDM system has also been discussed.

In order to investigate the network technologies which may be used to support the communication backbone required by the FREEDM system, we set up a distributed testbed to based on WiFi, Ethernet and Zigbee communication technologies. These technologies were chosen because they are standardized and open source in nature. We test these communication technologies to quantify the throughput and end-to-end delay achievable through them.

A distributed system would require real time monitoring of the devices on the grid. In order to achieve this objective, we present a prototype monitoring tool based on Simple Network Management Protocol (SNMP) to collect various network and system parameter from the distributed devices on our testbed. SNMP is an application layer protocol which is an internet protocol standard used to monitor nodes on a network [11].

Our current research effort is more focused on the realization of the communication backbone and thus issues such as reliability and security have not been addressed yet in our current work.

1.4 Related Work

Incorporation of DESDs and DRERs into the existing electricity distribution system, has been an active research area with the power system community. There has been some research in the areas which we are trying to investigate. We look at work done in the area of power systems architecture in electricity distribution systems with DRER/DESD devices. We also look at the recent communication protocol standards proposed for Smart Grids. We also look at the network monitoring solutions and protocols proposed by the research community and widely used by the industry.

The paper [10] suggests the use of "Microgrids" [1] and an agent–based control frame work for incorporating the DRERs and DESDs into the traditional grid system.

[1]Mircrogrid: a distributed power system is comprised of different energy resources, energy storage elements and electrical loads

Such agents will be autonomous in nature and and can take action depending upon the sensed state of the system. Every DRER and DESD would be controlled by an agent to facilitate 'plug and play' of these systems into the primary distribution system. The paper [12] specifies the control strategy for the FREEDM system which is based on a hierarchical control frame work and uses agent technology. We consider this as a reference for our work. In context to microgrids, the research efforts in the power system community have primarily been focused on the control algorithms needed for incorporation of distributed resources and energy storage structures into the electricity distribution system. Issues like the communication architecture, performance analysis of the communication protocols, performance analysis of various communication technologies have not been dealt with.

In context to the communication protocols, the *IEEE P2030 Smart Grid Interoperability Communications Technology Task Force 3* [13], responsible for addressing the communication needs of the future SmartGrids was set up in March 09' by IEEE. The standard IEC 61850 has been recognized by National Institute of Standards and Technology (NIST) as a part of the initial SmartGrid Interoperability Standards Framework, Release 1.0 [9]. Similarly the DNP3 standard is also widely used for SCADA applications for control and monitoring and is a part of the NIST standards framework for Smart Grid interoperability. For this reason, we include IEC 61850 and DNP3 as a part of our survey of existing power system architectures.

For the monitoring system, we choose the SNMP, an application layer protocol which is an internet protocol standard used to monitor nodes on a network [11]. There are a number of such systems in the commercial market for power utility companies [14] and such solutions have also even been proposed in literature for other systems. For example, the authors in this paper [15] propose the use of SNMP and GPRS (General Packet Radio Service) for monitoring power system controllers used in power systems for telecommunication cellular networks. The paper [16] proposes the use of SNMP for power system telecontrol.

The organization of the thesis is as follows. In Chapter 2, we study and analyze the SCADA and Substation Automation systems for their communication architecture and requirements. Further, we detail the DNP3 and IEC 61850 protocols. The major differences between the two protocols have also been listed. Further, we brief about the recent trends in the power system industry towards the use of IEC 61850 as the main standard to

support the need of all of the electricity supply chain. Recent developments in the area of Interoperability for SmartGrids have also been mentioned.

In Chapter 3, we detail the objectives of the FREEDM project. We investigate the communication architecture of the FREEDM system and identify the communicating entities. The communication requirements of the FREEDM system have also been detailed. The timing criticality has been discussed for the FREEDM system. In Chapter 4, we give an overview of the WiFi and Zigbee networking technologies and explain our reasons for choosing these technologies for the FREEDM communication backbone. We also detail the communication backbone prototype set up by us. An SNMP-based monitoring tool - Cacti and the important statistics which need to be monitored to gauge the overall stability of the FREEDM system have also been explained. The experiments performed by us on the testbed and the corresponding results, learnings and inference derived from the experiments, have also been detailed. Chapter 5 concludes the thesis and gives directions for future research.

Chapter 2

Power Systems: Communication Functionality and Protocols

In Chapter 1, we explained the obsolete features in the present day power systems and the need to move towards the inclusion of DRERs and DESDs into the electricity distribution system. Even though the power grid needs to modernize, the essential functionality requiring communication in the future grid is similar to that of existing power systems. For example, similar to traditional SCADA systems (explained in Section 2.1.1), we need to monitor and control the DESDs and DRERs distributed all over the distribution grid. Similarly the automated protection and control functionality of the substation automation systems, (explained in Section 2.1.2) is required for fault detection and isolation to maintain the stability of the grid when various DRERs/DESDs of varying capacities are interconnected with the grid. Hence we conduct a survey of the communication functionality in SCADA and Substation Automation systems and their corresponding communication protocols (DNP3 and IEC 61850).

Fig. 2.1 shows the current power systems architecture and the different protocol standards being used. Substation-1 and Substation-2 are shown to be monitored and controlled by Control Center-1 using SCADA protocols. DNP3, IEC 60870-5-101, IEC 60870-5-104 and IEC 62445-2 are the various SCADA protocols being currently used. IEC 61850 is shown to be used inside a substation for automation purpose. Inter-Control Center communication is achieved using IEC 60870-6 protocol standard. IEC 61970 and IEC 61968 are the standards used for Energy Management and Distribution Management sys-

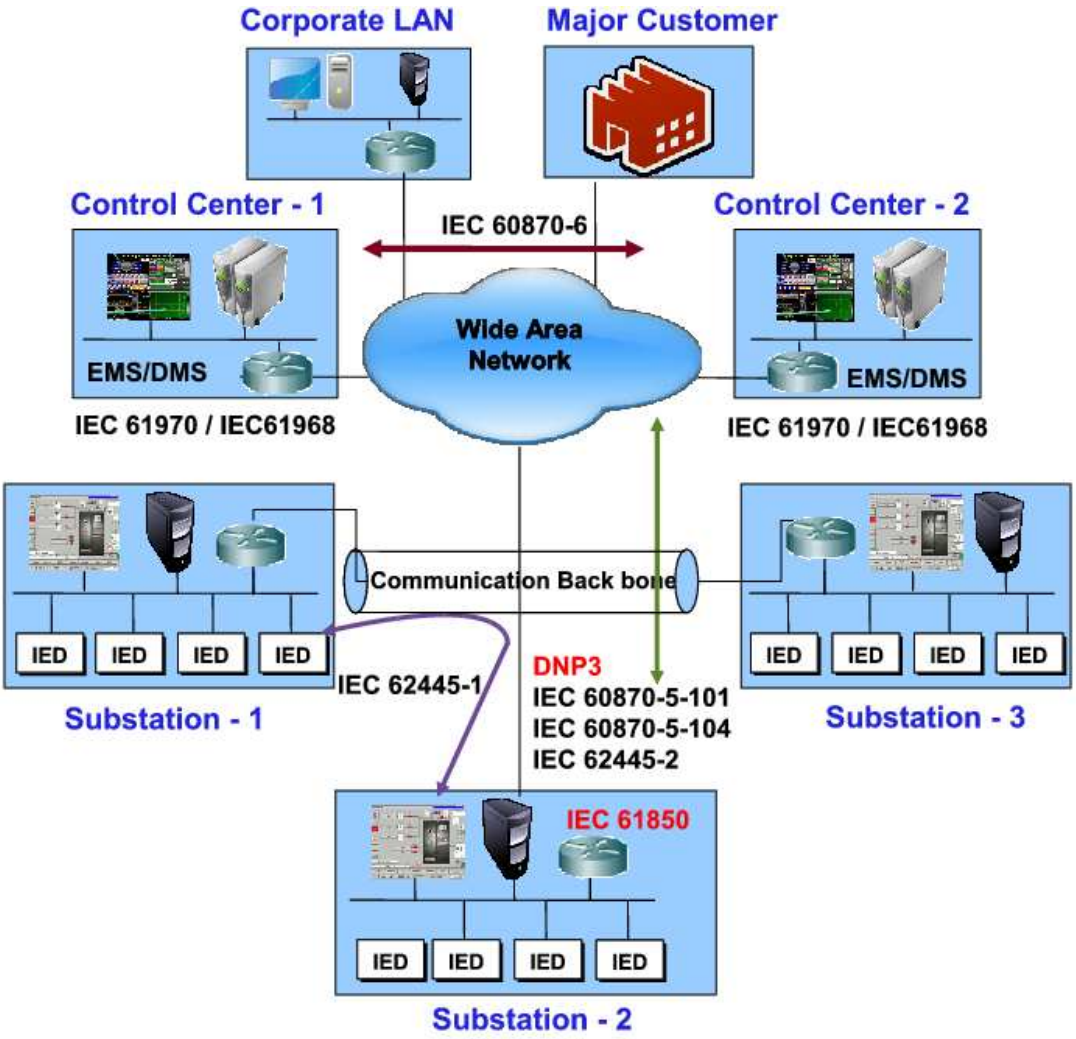

Figure 2.1: Existing Power Systems Architecture And Communication Protocols.

tems. IEC 62445-1 is used for inter-substation communication. Thus we have a lot of independent standards controlling various aspects of the power system architecture.

2.1 Communication Functionality

2.1.1 SCADA Systems

SCADA stands for Supervisory Control and Data Acquisition. It generally refers to a process control application that collects data from the sensor devices at a remote

location (Data Acquisition) and sends them to a central computer (SCADA Master) over a physical communication medium for display. The SCADA Master computer is also used for centralized control of remote entities by initiating commands over the communication network (Supervisory Control). For power systems, a substation is considered to be the remote location. Fig. 2.2 shows the components of a typical SCADA system. These have been explained below:

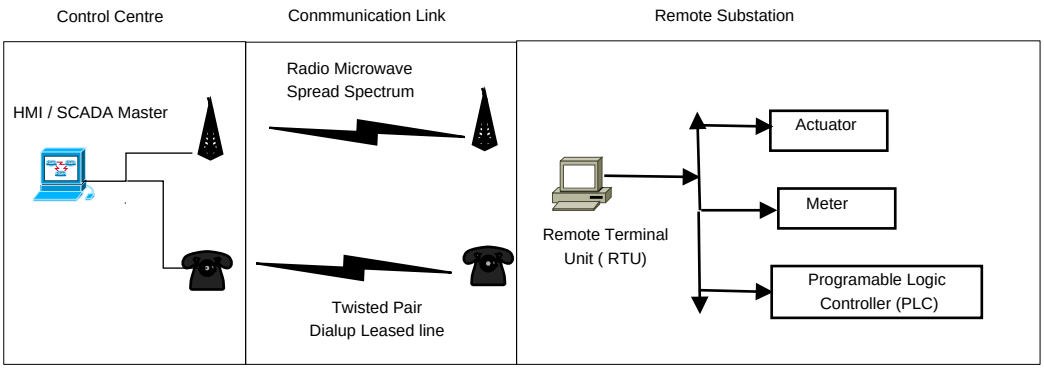

Figure 2.2: Components Of A SCADA System.

1. **Human Machine Interface (HMI):** consists of input and output devices for interaction between the user and the SCADA system. Keyboards and mouse are used as input devices. The output devices are generally a graphical display screen and printers for report printing. The graphical display for SCADA systems needs to be very intuitive and should have different levels of detailing depending upon what is needed by the operator. It should be able to display an overview of the complete SCADA system and also a detailed status of say a feeder.

2. **SCADA Master:** refers to the centralized computer running the SCADA protocol and other application software at the master site. It is connected to the IEDs/RTUs at the remote site (e.g. a substation). It requests/receives specific parameters from the SCADA slave device at the remote site to monitor it. It also sends command signals to control the analog and digital devices at the remote site. It is also connected to the HMI. A workstation with sufficient processing and memory capabilities is generally used as a SCADA master.

   SCADA Master is an important part of the SCADA system. There are a lot of software

modules which run on the SCADA master workstation to achieve the functionality of the SCADA system. The *Data Acquisition Module* acquires, processes and analyzes the data received from the substation and also sends it to HMI for display. The real time data is compared to user defined threshold values and an appropriate action may be taken if needed (e.g. raising an alarm). The *Control Software* generates requests for data or sends control signals to the RTU at the substation using the SCADA protocol. The data received from the substation is fed into a *Database* and archived regularly for fault finding, trend analysis and generating reports.

3. **RTU (Remote Terminal Unit):** connects to the actual IEDs. RTUs are linked to a SCADA master through a communication link. An RTU may have some autonomous control capabilities. The RTU acts as a SCADA slave device which collects electrical information from the devices connected to it and sends them to the SCADA master either in response to a request or unsolictedly when some predefined parameter changes at the substation.

4. **IED (Intelligent Electronic Device):** are the actual physical devices responsible for data acquisition and control of electrical equipment e.g. sensors, meters, actuators, PLCs (Programmable logic controllers). These devices receive the digital signals from the RTUs and convert them into electrical signals and vice versa. With the development in the digital electronics industry and the availability of memory and processing capability at cheaper prices, the RTU functionality is merging with the IED functionality.

5. **Communication Infrastructure:** consists of the physical communication media and the communication protocol. It connects the SCADA master to the RTUs through a wireless medium or a switched telephone network depending upon the need. A specialized communication protocol (e.g. DNP3) governs the data exchange between the SCADA master and remote devices. The link between the SCADA master and remote substations should be highly reliable and have high bandwidth for real time monitoring. Highly critical functions such as electrical protection are not dependant on the availability of the SCADA master and data is stored on the local IEDs in case of link unavailability. A SCADA master station may be used to control a single large substation (e.g. a high voltage power generation or a transmission substation). Fig.

2.2 depicts such an architecture. It can also be used to control smaller distribution stations. Such an architecture is shown in Figure 2.3.

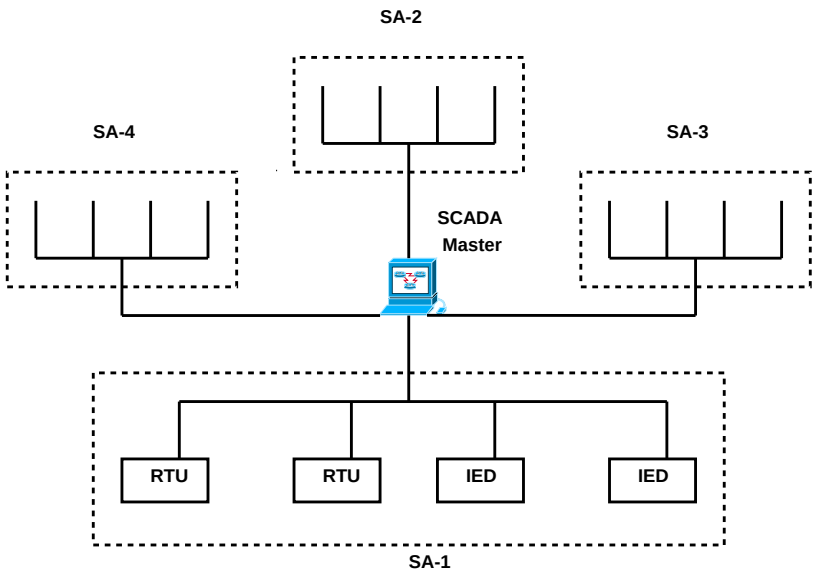

Figure 2.3: Single SCADA Master Controlling Many Substations.

Power System Utilities (power generation, distribution and transportation companies) are an excellent example of the application of SCADA protocols. Since the physiological conditions at such places are not conducive for human presence (high temperature, electromagnetic radiations etc.), there is a need to control/monitor such places remotely. This is where the SCADA protocols come into the picture. These protocols are used to remotely, monitor and control the power generation, transmission and distribution subsystems [17]. These systems have numerous components namely relay circuits, PLCs (Programmable Logic Controllers) etc. which regulate the system and also a lot of other components e.g. sensors, meters, actuators etc. which need to be constantly monitored by human personnel. The paper [18] classifies the power system communication requirements and lists *Teleprotection* and *Power system control(PSC)* as the main real-time communication requirements of power systems.

Such monitoring systems based on real time data, can help avert power blackouts which have happened in the past due to lack of complete information about the current functional state of a subsystem by taking automatic decisions [19]. Thus, besides monitoring

and control there is also a need to automate these systems for automatic corrective action in an abnormal condition. This is referred to as *Substation Automation*[20] (discussed in detail in Section 2.1.2).

Besides satisfying the needs of real time monitoring, the Utility Communication also faces the new challenges posed by the deregulated environment. As a result of deregulation, power utility companies need to exchange various kinds of real time data amongst themselves such as transmission capacity, scheduled power outages, operating constraints etc. Moreover, the merger of the companies also calls for integration of data from several substations, control centers and power plants [20][21]. The competitive deregulation environment also underscores the need of an effective communication network architecture for power system utilities to maximize system availability, minimize any unforseen outages and improve the quality of service of the system.

2.1.2 Substation Automation

Overview

The process of automatic corrective action in an abnormal condition in a substation environment is referred to as Substation Automation (SA). As discussed in Section 2.1.1, the SA systems together with SCADA systems, are useful in preventing electricity blackouts in a region. Here, we explain the architecture of typical SA systems, their advantages to the power system utility companies and their evolution over last decade.

Figure 2.4 illustrates the architecture of a typical SA system. Typically an automation system consists of *Primary Equipment* such as relays, circuit breakers, sensors, actuators etc. and *Secondary Equipment* for communication, protection, control and monitoring. Three levels of devices are generally defined. The primary equipment constitutes the devices at the *Process level*. The secondary equipment constitutes the device as the *Bay Level*. The Station Unit (SU), the Communication Unit (router or a modem) and the HMI form the *Station Level*. The primary equipment is connected to the secondary equipment using parallel wires whereas the secondary equipment is connected to the SU using serial communication. The SU acts as an intermediate data concentrator and may even act as a protocol translator if different protocols are used for communication within a substation and for communication with the Control Center[22].

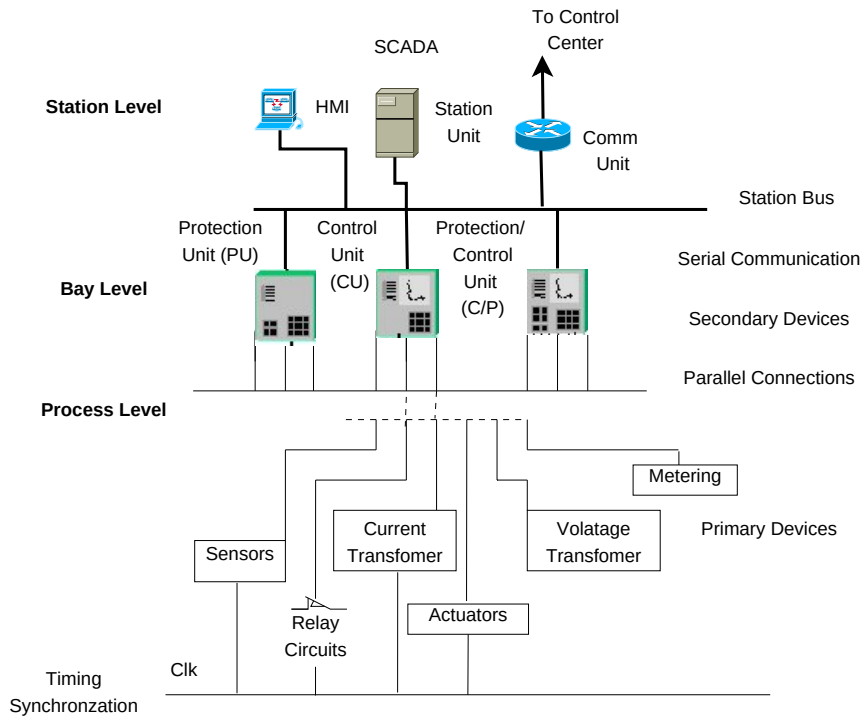

Figure 2.4: Typical Substation Automation Architecture.

A substation automation process typically comprises the following functionality:

1. **Protection:** This refers to the process of detection of abnormal conditions (e.g. failure of equipment) within a power system, localization of faults and removal of faulty equipment. All this is done to protect the other functional equipment from the damage due to the faulty part and to minimize the resulting revenue losses for the electric utility. Fuses, circuit breakers etc. form the components of an electric protection system. Electrical Protection is a local function and needs to function even if the substation automation process breaks down.

2. **Control:** It involves both local and remote control. Local control involves actions which can be taken by logical devices themselves, e.g. bay interlocking. This reduces human intervention and thus human error. Remote control implies the commands sent to the substation from a SCADA master at a remote location using SCADA protocols, for example, to close or open a circuit breaker. This can result in quick decision making thereby preventing losses.

3. **Measurement:** This refers to all the real-time digital and analog data generated by the various electrical devices at the substation. It includes voltage, current, power readings of different electrical equipment. It also includes the metering data. This huge amount of data generated is used for network studies like load flow, stability analysis etc. to prevent any major disruptions in the power network.

4. **Monitoring:** The data generated by measurements is stored in a database at the SCADA master site and displayed on a graphical interface for constant monitoring.

5. **Communication Network:** It forms the backbone of a Substation Automation system. It ensures reliable, error free communication between the bay level and the SCADA station level. The SCADA master may be located in the substation itself or at a remote control center.

Advantages of Substation Automation

Setting up a SA system is a big investment for any utility company. Hence the advantages should be carefully weighed against the costs. The following are the advantages of SA:

- To remain competitive in a deregulated market environment, the utility companies need updated information about the current state of the system.(eg, DISTCOs need to know about current transmission capacity, TRANSCOs need to know about current energy consumption by users etc). Improving SA can provide the necessary information needed to make a market decision, thereby improving profitability.

- Reduction in number of personal needed for monitoring and control and hence low operation costs can be achieved as now the substations are autonomous and can be monitored at a central place.

- Faster fault location and isolation, thereby decreasing the interruption time. This increases the reliability of the system.

- Reduction in installation costs can also be achieved as automated substations require less cabling. Installing new digital multifunctional IEDs would also remove the need for any dedicated equipment.

- An automated substation also allows for automated logging and documentation of each upgrade to the system.

Evolution of Substation Automation Communication Architectures

Over a period of last decade there has been a significant change in the way the substation automation architectures have been designed. This has been mainly due to the changes in the market models (deregulation) and has been made possible by the advancement in the communication, networking technologies and a shift towards the use of microprocessor based digital equipment in the substations (IEDs). The communication architecture has seen a change from the use of parallel wiring between all kinds of equipment, primary and secondary equipment to the use to LAN based networking technologies. The trend has also been to shift towards standardized protocols (like DNP3, IEC61850) and equipment rather than any proprietary protocol or vendor specific equipment for communication within a substation, between substations and from control centers to substations.

Fig. 2.4 (discussed above in this chapter) depicted the details of the *Current Generation SA Architecture*, which in a phase of transition from the old, 'wired' *Conventional SA Architecture* and proprietary protocols to the fully automated, networked SA architectures using standardized protocols. Hence at present only serial communication is used within a substation for communication and protocol converters are used for communication between standardized equipment and proprietary equipment.

Fig. 2.5 illustrates the *Next Generation Network Architecture* proposed by the IEC 61850 standard. In this case, the communication within and outside the substation is through IP based Ethernet LANs. Digital IEDs are used as bay level devices. They incorporate all the protection, control and monitoring capabilities. Hence the need of dedicated equipment for these functions is obviated. Merge Units (MU) are used to sample analog inputs from current transformers(CT), potential transformers (PT) etc. and get digitized data. The various protocols, used inside the substation are also shown (these have been explained in Section 2.2.2)

Table 2.1 summarizes differences between the various SA architectures, conventional monolithic architecture, current generation distributed architectures and the next generation fully networked architectures [22].

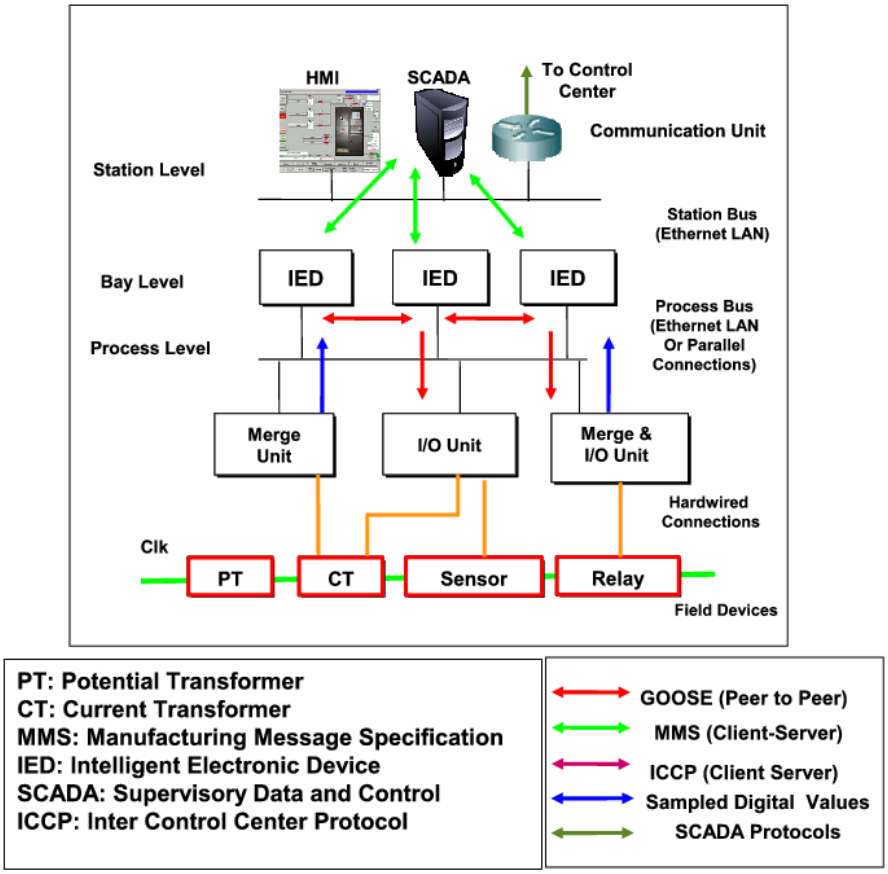

Figure 2.5: IEC 61850 Based Substation Automation Architecture.

Delivery Time Requirements between IEDs

As shown in Figure 2.5, in the new generation architecture for SA, Protection and Control are not considered to be embedded in separate devices but as applications and usually in the same IED. As new applications are added to the IED, it must ensured that the delay requirements for critical applications are always met. The real time data is either event driven or is periodic in nature. The Table 2.2 lists the relative delay requirements across various interfaces in a substation [23]. The analog values from the voltage and current transformers have the highest performance requirement. Performance requirement is also high for protection related functionality (event notification and messages to switch gear). On the other hand, messages from the substation computer for protection and control or to the Control Center have a low performance requirement. The timing requirements for

Table 2.1: Evolution Of Substation Automation Network Architectures.

Feature	**Conventional Arch.**	**Current Gen. Arch.**	**Next Gen. Arch.**
Architecture Characteristics	Monolithic Architecture, Proprietary Solutions, Vendor Specific equipment, Isolated Substations	Distributed Architecture, IED -IED communication, Substations on WAN , Controlled interaction with other control centers, entities	Networked, Internet based Open System Architectures
Communication Media	Leased Lines, Packet Radio, Data Rates in Kbps	Use of Frame Relay, Spread Spectrum Radio, Data Rates in Mbps	Gigabit Ethernet, Optical Fibre, Data Rates in Gbps.
Communication within Substation	Parallel wiring for all primary and secondary equipment	Parallel wiring between primary equipment and IEDs. Serial connection between Secondary equipment and Station Unit	Parallel wiring between primary equipment and IEDs. Ethernet based LAN between secondary equipment and station unit.
Communication Protocols	Proprietary Protocols, e.g. MODBUS, PROFIBUS	Standardized and Proprietary protocols, Protocol Converters, e.g. DNP3, IEC61850, IEC60870, IEC62056	Standardized protocols, e.g. IEC61850, IEC62056, TASE 2.0.

monitoring and control are less strict than the protection functions but stricter than file transfer and audio and video streams.

Table 2.2: Delivery Time Requirements Across Substation Communication Interfaces.

Communication Interface	**Performance Requirement**
Substation Computer to Protection	Low
Substation to Control	Low
Substation Computer or IED to Control Center	Low
Control to Protection	Medium
Control to Switch Gear	Low
Control to Control	Medium
Even Notification for Protection	High
Data Transfer for Protection	Medium
VT and CT Analog	Very High
Protection to Switch Gear	High

The timing requirements are explained as follows, Very-High-Speed: $< 2ms$, High-

Speed: $2 - 10ms$, Medium-Speed: $10 - 100ms$, Low-Speed: $> 100ms$.

The Table 2.3 shows the typical delay requirements for information exchange amongst IEDs for different categories of applications both inside and outside a substation. As shown in the table, the performance requirements are higher for communication inside a substation, than outside a substation. The protection function has the highest timing requirement and the audio and video data stream has the least timing requirement.

Table 2.3: Delivery Time Requirements For Communication Between IEDs.

Information Type	**Internal to Substation**	**External to Substation**
Protection Information, high speed	1/4 cycle	8-12 ms
Monitoring and Control Information, medium speed	16ms	1s
Operations and Maintenance Information, low speed	1s	10s
Text	2s	10s
Processed Data Files	10s	30s
Program Files	60s	10min
Audio and Video Data Stream	1s	1s

2.2 Communication Protocols

2.2.1 DNP3 Protocol - An Overview

DNP stands for *Distributed Network Protocol*. The DNP3 protocol provides rules for SCADA masters and RTUs for Supervisory Control and Data Acquisition (SCADA). It is used to monitor a number of physical processes and information like, kilowatt hour consumption, voltage, current, temperature etc. at the remote substation. It is also used to exercise control (e.g of circuit breakers) at the remote substations and transfer of any configuration files to/from SCADA master.

Originally developed by the company GE-Harris Canada based on IEC 60870-5 standard and released in 1993, it is currently managed by the DNP Users group [24]. IEEE

1379-2000 standard mentions the best practices for implementation of the protocol. Because of its features, it is included in the NIST-Recognized Standards Released for SmartGrid Interoperability [9]. DNP3 is an open, robust and an efficient SCADA protocol with the following features.

- Allows communication between the SCADA Master at the control center and RTUs in the substation.
- Specifically designed to operate reliably in harsh environment of the electric utility automation systems.
- Provides a layered architecture for reliable transmission of data and commands.
- Initially used for serial point to point communication, however it has been ported over TCP/IP protocol stack as well to be used over an IP network.
- Although, not initially designed with security in mind, the standard is now compliant with IEC 62351 "Power System Control and Associated Communications - Data and Communication Security"

DNP3 was initially proposed with only 3 layers. This was called as the *Enhanced Performance Architecture* by IEC. Later a fourth layer i.e. the Pseudo-Transport layer was added for message segmentation. Fig.2.6 shows the layered structure of the DNP3 protocol over a TCP/IP protocol stack. The SCADA Master is shown to receive different data types like binary, analog and counter. The SCADA Slave is shown to send the data requested by the SCADA Master. The SCADA Slave also receives control signals from the SCADA Master. The four main layers of the DNP3 protocol stack have been discussed below [25].

1. *Physical Layer:* The Physical layer deals primarily with the physical media over which the protocol is being communicated. The protocol was primarily specified for a serial physical layer such as RS-232 and RS-485 over communication media such as copper, radio, fiber etc.

   The serial physical layer must provide the following services to the link layer above it. The *Send* and *Receive* services are used to send and receive serial data, *Connect* and *Disconnect* are used to connect or disconnect from a Public Switched Network if

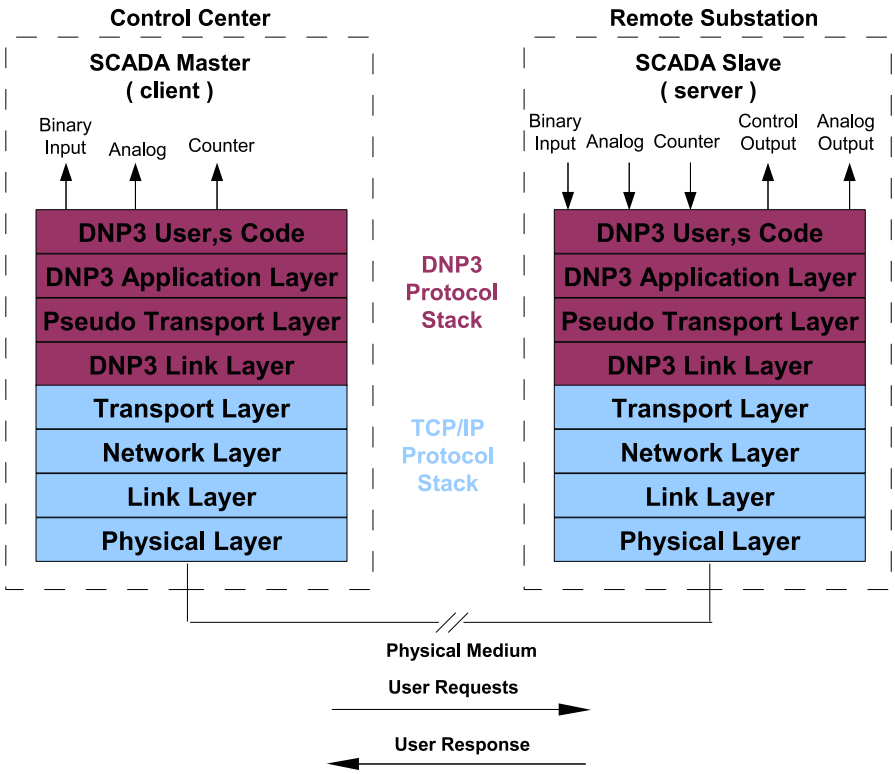

Figure 2.6: Layered Structure Of DNP3 Protocol.

required, and the *Status* service indicates whether the medium is busy or free for data transmission. Recent implementations of DNP3 over TCP/IP protocol stack use the Ethernet as the physical layer.

2. *Data Link Layer:* The Data link layer is responsible for maintaining the logical link between the sender and the receiver of information and keeping the information sent and received, error free. Each transmitted data link *Frame* has a 10 byte data link header and has a 16 bit CRC every 16 bytes of the Frame. Maximum size of the frame is 256 bytes. DNP3 link layer uses 16 bit source and destination addresses for data exchange. Fig. 2.7 depicts the format of the DNP3 frame. The individual fields have been described in Table 2.4, 2.5.

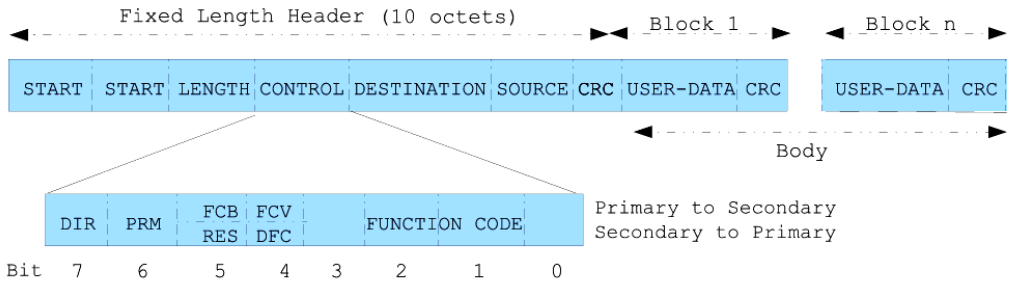

Figure 2.7: DNP3 Link Layer Frame.

Table 2.4: DNP3 Header Fields.

SYNC	2 starting octets of the header (0x0564)
LENGTH	1 octet count. Signifies user data in the header and the body. Includes control, destination address, and source address.
CONTROL	Frame control octet.
DESTINATION	2 octet destination address. Identifies the destination of the station the data is sent to.0xffff is defined to be an all stations address.
SOURCE	2 octet source address. Specifies the address of the station from which sends the frame.
CRC	2 octet cyclic redundancy check.
USER DATA	The link layer can accept a maximum of 249 octets of data from the application layer.

3. *Pseudo-Transport Layer:* The Pseudo-Transport layer has the following functions:

   - Segments and packs the application layer into multiple data link frames. Similarly it unpacks the multiple frames received from the data link layer into user data.
   - It inserts a function code into the frame, indicating whether its the first or the last segmented frame.
   - It also inserts an incrementing sequence number into the frame, so that the receiving node can detect the dropped packets if any. The sequence number ranges from 0 to 63.
   - Prioritized Delivery. The delivery can be EXPEDITED or NORMAL to indicate high or low priority request.

Table 2.5: DNP3 Link Layer Control Bits.

DIR	Physical Transmission direction. '1'implies master to some other station. '0' implies to master station.
PRM	Primary message. '1' implies from the initiating station to a responding station. '0'implies from the responding station to an initiating station
FCB	Frame Count Bit. Used for suppressing losses and duplication of frames to the same secondary station. This bit toggles for each SEND-CONFIRM command exchange between the same pair of stations
FCV	Frame Count Bit Valid. '0'implies the FCB bit is to be ignored. '1'implies the state of the FCB bit is to be checked against the last FCB bit received with FCV bit set.
DFC	Data flow control bit is used to prevent the overflowing of buffers in a secondary station. Bit value of 1 when received from a secondary station implies that the primary station should stop sending any further data. The primary station polls the secondary station continuously without sending any further data till DFC = 0 is received.
RES	Reserved Bit
FUNCTION CODE	Identifies the type of the frame.

- Quality Delivery. The frame can be set to either SEND-NO-REPLY or SEND-CONFIRM to indicate the need of a message acknowledgement.

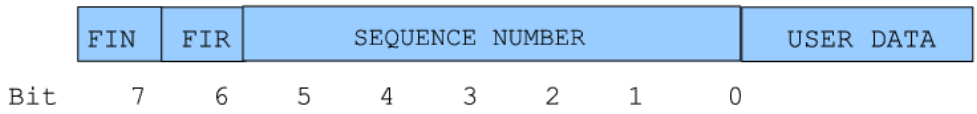

Figure 2.8: DNP3 Transport Layer Header and User Data.

Fig. 2.8 depicts the transport layer header structure. If the FIN bit is '0', it indicates that there are more frames to follow. FIN as '1' indicates the arrival of the last frame. If the FIR bit is set, it indicates that the frame is the first in the series of frames to follow. If both FIR and FIN are set, it indicates that the frame is the only frame to be received.

4. *Application Layer:* The DNP3 application layer messages from the Master DNP3 are called *Requests* while those from the DNP3 Slave are called the *Responses*. A Slave DNP3 station can also send an *unsolicited response*. As with the Data Link Layer, a

Slave or a Master DNP3 station can request for a *application layer confirmation*.

The Application layer in DNP3 has the following functions:

- It responds to the messages received from the Pseudo-Transport Layer and builds messages as per the availability of data. This built message is passed down the Pseudo-Transport layer.
- If the application layer data does not fit into a single application layer message, it divides the application layer data into fragments . Thus each fragment (excluding the last one) needs to indicate, if there are more fragments to follow.
- It provides timeout functionality in case a response is not received to a request. It also provides a retry count functionality, so that a request is tried again a fixed number of times in case no response has been received.

Fig. 2.9 shows the DNP3 Application Request Packet Format. Each request packet consists of a *Request Header* (which contains of Application Protocol Control Information - APCI) followed by one or more Object Header (Data Unit Identifiers - DUI) , Data (Information Object - IO) combinations. The DNP3 response packet is shown in Fig. 2.10. It follows the same structure as that of the request packet with a few additional fields (Internal Indication).

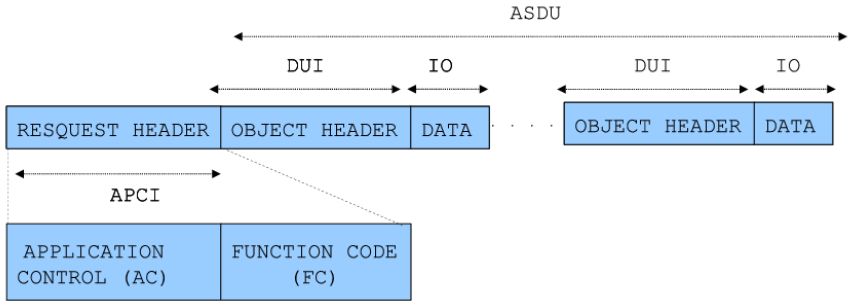

Figure 2.9: DNP3 Application Request Packet Format.

The individual fields in the DNP3 Application Response and Request Packets have been explained below.

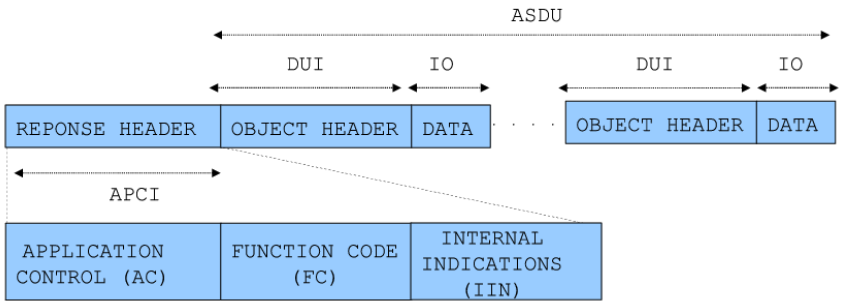

Figure 2.10: DNP3 Application Response Packet Format.

Request Header	-	Identifies the purpose of the message and consists of Application Protocol Control Information (APCI).
Object Header	-	Identifies the data objects that follow.
Data	-	Data Objects of the type specified by the object header.
Application Control (AC)	-	Provides information needed to construct multi-fragmented messages (FIR, FIN , SEQUENCE NUMBER bits as discussed before). It also has a CON bit to request for confirmation.
Functional Control (FC)	-	This indicates the purpose of the message. e.g. confirm, read, write, select, operate, warm restart etc.
Internal Indications (IIN)	-	Is a two octet field that follows the function code in all responses. In case a request cannot be processed, the IIN field is set, indicating the appropriate reason.

Fig. 2.11 shows an example of message exchange sequence between a SCADA Master and an Outstation, where a SCADA master requests the SCADA slave device for enabling of Unsolicited or Spontaneous Messages. The SCADA Master sends a *Spontaneous Message Enable Request* to the SCADA slave device, which responds by sending a *Spontaneous Message Enable Response* indicating that the spontaneous messages have been enabled. Now the SCADA slave can send aperiodic messages to the SCADA master. The slave device may ask for a confirmation of this message form the master.

```
SCADA Master -----Spontaneous Message Req-----> SCADA Slave
             <-----Spontaneous Message Res-----
SCADA Master<-----Unsolicited Response-------- SCADA Slave
            ---------Confirm Response---------->
```

Figure 2.11: SCADA Master Sending Spontaneous Message Enable Request.

2.2.2 IEC 61850 - An Overview

As mentioned in Section 2.1.2, the legacy SA systems were designed to work with the limited networking technologies (like serial communication) available at that time. The data rates/bandwidth of the communication medium was a constraint considered at the time of design of a SA protocol. However, with the developments in the networking technologies and digital electronic technology, the need of a "next generation" protocol for substation automation was felt.

With increase in data rates from Kbps (serial communication) to Mbps (ethernet), the "cost" component of the automation system became the configuration and documentation of the system. It was felt that various devices which are a part of the SA system, should have the capability of self description of data and services offered by it. With the presence of digital IEDs (Intelligent Electronic Devices), it was easier to move a lot of functionality into a single digital IED. Thus the specific protection devices and control devices were no longer required and could be replaced by a multipurpose IED capable of high speed communications. Other requirements that were considered in the design of the protocol were:

- Need of high speed IED-IED communication
- Guaranteed delivery times
- Standardized protocols
- Multi-Vendor operability
- Support for security

- Configuration support
- Support for voltage and current samples.

The work began with the development of *Utility Communication Architecture* (UCA) in 1988. This work became the starting point for the work of IEC Technical Committee - 57 (TC57) Working Group 10 (WG10) which eventually came up with the standard *IEC 61850 - Communication Networks and Systems in Substation* [26].

Scope and and Key Features

IEC 61850 was designed to be used primarily within a substation. The standard defines a set of 10 parts, which detail the various aspects of the standard. These are summarized in Table 2.6 and their use is explained in the following sections.

Table 2.6: Structure Of IEC 61850 standard.

1	Introduction and Overview
2	Glossary of Terms
3	General Requirements
4	System and Project Management
5	Communication Requirements for Function and Device Models
6	Configuration Description Language for Communication in Electrical Substations Related to IEDs
7	Basic Communication Structure for Substation and Feeder Equipment
7.1	Principles and Models
7.2	Abstract Communication Service Interface (ACSI)
7.3	Common Data Classes (CDC)
7.4	Compatible logical node classes and data classes
8	Specific Communication Service Mapping (SCSM)
8.1	Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
9	Specific Communication Service Mapping
9.1	Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link
9.2	Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

The following are the key features of IEC 61850 protocol standard.

- *Use of a Virtualized Model:* The standard defines a set of logical devices, logical nodes, abstract communication services and data classes for the description of data and services offered by an IED. These are independent of the actual protocol used to transmit the data over a network.

- *Standardized, Unique naming for all data:* All parameters/variables of a device have a unique name which correspond to the functional use of the variable. Legacy protocols did not have this feature. Moreover, these names have been standardized by the standard in relevance to the electrical functionality where the variable will be used.

- *Self-Describing devices:* The configuration of each device is stored in a configuration file, which can be downloaded by an IEC 61850 client to know the services offered by the device and corresponding parameters

- *Support for a wide variety of timing requirements:* The IEC 61850 standard allows for the use of different protocol stacks to be used to achieve different timing requirements. Even for the same protocol stack, there is a provision of specifying the transmission time requirement of a message.

- *Standardized Configuration Language (SCL):* The standard specifies an XML-Based language SCL which is used to specify the services offered by an IED and the corresponding parameters. This also allows system designers, to do the configuration process offline.

Modeling Approach

IEC 61850 standard provides a comprehensive data model for organization of data within the power systems. IEC 61850 Part-6 describes an XML based *Substation Configuration Language* which gives the description of a particular device, the various objects and functions performed by it. Thus in case a new device is to be added to the existing system, an engineer simply needs to connect the device to the substation communication network and import the SCL file of the device to configure it. An IEC 61850 client can extract the object definitions in the SCL file from the device over the network.

The IEC 61850 device model describes a *physical device* as the actual device which connects to the network. Each physical device may have one or more *logical devices*. This

allows each device to have more than one functionality. For example, the same device can act as a data concentrator and have the functionality of a circuit breaker. Each logical device has one or more *logical nodes.* A logical node is a named grouping of data and the functionality/services offered by a logical device (described in IEC61850 Part-7-4). Thus there are logical nodes for protection, sensors, power transformers, supervisory control etc. Each logical node has a predefined name, followed by an Instance-ID. For example, MMXU1 is the the name of the first logical node of a Measurement Unit.

Each logical node, contains one or more data elements, each with a unique name. These are generally related to the functionality of the logical node. For example, a circuit breaker modeled as an XCBR logical node will have data to define circuit breaker operating capability, block breaker open commands, remote or local operation etc. Each data element within a logical node, conforms to a a *Common Data Class (CDC)* (described in IEC61850 Part-7-3), which describes its type and structure.

The IEC 61850 device model is a virtualized model of the device and its data objects (specified in IEC61850 Part-7). A virtualized model is then mapped to a specific protocol stack as defined in IEC61850-8-1 based on MMS, TCP/IP or Ethernet (described further in next section). In case the MMS protocol stack is used, the standard specifies a method to transform the virtualized information model, into a unique MMS variable object. For example **"Relay1/XCBR1/STLoc$stVal$"** corresponds to a logical device named "Relay1", consisting of a circuit breaker logical node "XCBR1", its corresponding variable "Loc"and its value "Val".

Mapping to Protocol Stacks

The Abstract Communication Service Interface (ACSI) model (described in IEC61850 Part7-2) defines a set of services and possible responses to those services, which can be used by the IEDs to communicate with each other. The ACSI services are independent of the underlying protocol stack which defines how the data is to be transformed into packets and sent over the network. As shown in Fig. 2.12, IEC 61850 Part 8-1 maps the abstract services and objects specified by the ACSI into real objects and services of the Manufacturing Message Specification (MMS) protocol. For example, the "GetDataSet" and "SetDataSet" services of the ACSI are mapped to the "read" and "write" services of the MMS protocol. Other mappings specified by IEC 61850 Part 8-1 include the profiles for communication

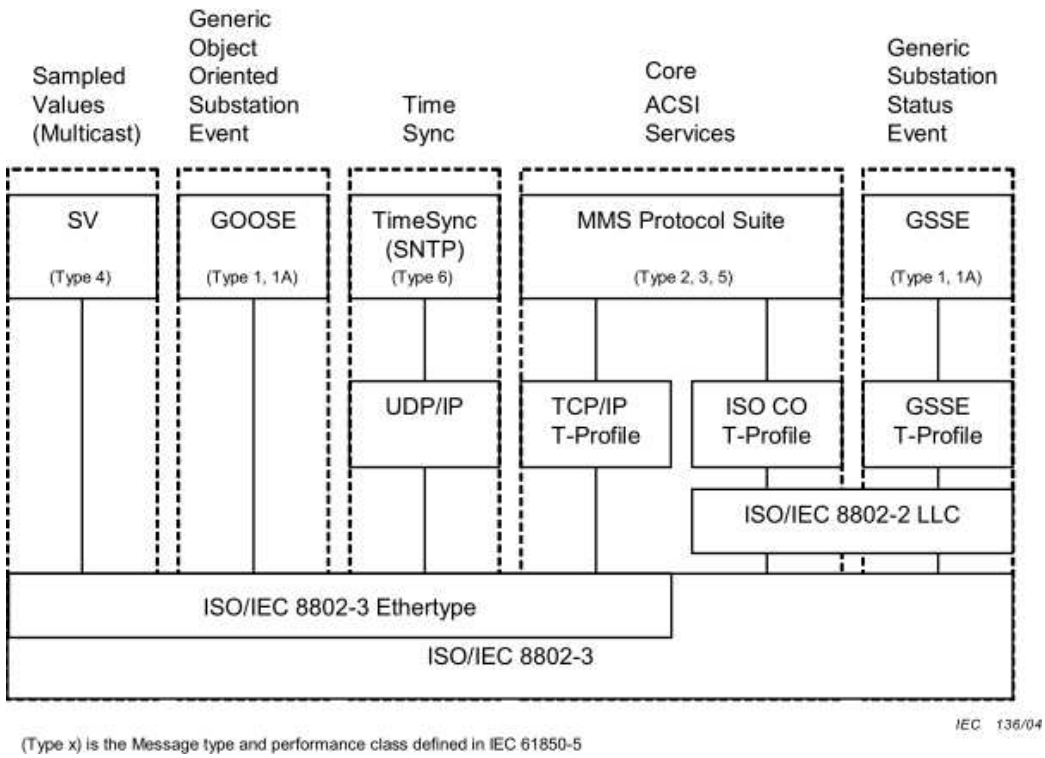

Figure 2.12: IEC 61850 Protocol Stack And Communication Profiles.

stacks, which are dependent on the service provided. For example, the Sampled Value and Generic Object Oriented Substation Event (GOOSE) services can be directly mapped on top of the Ethernet layer. Generic Substation Event Service (GSSE) is mapped on top of connectionless ISO services. SNTP (Simple Network Time protocol) has been mapped on top of UDP (User Datagram transport protocol). All data eventually maps onto an Ethernet data frame.

Message Performance Requirements

So far, we have described how the data is represented and how it is mapped to real communication protocol stacks. Here, we explain the mechanism of data exchange between two logical nodes, and how the performance requirement of a message is ensured by using different protocol stacks for different types of messages and message requirements. The IEC 61850 Part-5 describes the communication between logical nodes using *PICOMS (Piece of Information for Communication)*. The communication between two logical nodes

may consist of thousands of different PICOMs. The typical PICOM attributes are:

1. Data: describes the content of the information.
2. Type: describes the structure of the information
3. Performance: specifies the permissible transmission time as defined by the performance class, data integrity requirement, cause of transmission (request, periodic, event-driven)
4. Logical Connection: contains the logical source and the logical destination of the message.

The PICOMS transmitted consist of different types of messages depending upon the performance requirement of a message. For example, Type-1A is the most important of the messages with the most strict timing requirement from 3 - 10 ms. It is used for sending important commands like Trip, Close, Reclose etc. to the circuit breaker. Type-3 messages used for transmitting event records have transmission time requirement of less than 500 ms. Type-5 messages, used for file transfers have transmission time requirements of $>$ 1000ms. The standard also specifies different performance classes for each message type. Performance Classes P1, P2 and P3 are defined for control and protection messages, with P1 being the least and P3 being the most stringent. Similarly M1, M2 and M3 are performance classes for metering and power quality. Table 2.7 describes the various message types specified by IEC 61850 Part-5 and the corresponding transmission time requirements.

Figure 2.12 shows how different types of messages are mapped onto the different protocol stacks to attain the timing requirement. For example, Type 1, 1A messages with the most strict timing requirement have been specified to use the GOOSE and the GSSE protocol stacks. Type 2, 3 and 5 have been specified to use MMS services over a TCP/IP profile or a ISO profile. Type 4 messages, the sampled values, operate directly over the ethernet layer.

2.2.3 DNP3 Vs IEC 61850 - A Comparison

After having briefed DNP3 and IEC61850 in sections above, this section gives the important differences between the two protocols. The DNP3 protocol is primarily used for SCADA systems while the IEC 61850, though initially was developed for SA systems, it

Table 2.7: Message Types In IEC 61850-5.

Message Type	**Message Functionality**
Type 1 - Fast Message	Contains a simple binary code containing data or command. e.g., Trip, Close, Reclose, Start, Stop etc.
Type 1A - Trip	Most important message, more timing requirements than other messages. e.g 10 ms transmission time for P1, 3 ms for P2, P3.
Type 1B - Others	Less demanding than "trip", e.g. 100ms transmission time for P1; 20 ms for P2, P3 .
Type 2 - Medium Speed Message	The time at which a message originates is important, the transmission time is less critical. Transmission time $<$ 100 ms.
Type 3 - Low Speed Message	Used for speed auto control functions, transmission of event records. May or may not be time tagged. Transmission time $<$ 500 ms.
Type 4 - Raw data Message	Includes the raw data from the transducers, digital transformers
Type 5 - File Transfers	To transfer large files. Transmission time $>=$ 1000 ms.
Type 6 - Time synchronization messages	To synchronize the internal clock of the IEDs. Depending upon the application, different time classes may be used. T1 $\pm$1ms, T2 $\pm$ 0.1ms.

is being extended to other parts of the electricity supply chain as well (detailed in Section 2.2.4).

The DNP3 protocol architecture is layered and the standard specifies the actual packet header format at each layer which carries the data through the medium. DNP3 specification specifies its use with either serial (dial-up or microwave) or ethernet based communication medium.

On the other hand, the IEC 61850 protocol standard, stresses on the ease of logical representation of the devices, the data, the services provided by each device and the logical parameters exchanged for communication between similar logical nodes present on one or more physical devices in context to the power system operations. The standard uses different communication profiles (or protocol stacks) for carrying messages with different communication requirements. This separation between the representation of data and functions and the actual protocols carrying the data makes it easier for IEC 61850 to cope up with the advancements in communication technology by simply changing the mapping between the logical representation and the actual protocol stack carrying the information bits. The differences between the two protocol standards have been summarized in Table 2.8.

Table 2.8: Differences Between IEC 61850 and DNP3.

Feature	**DNP3**	**IEC 61850**
Focus Area	SCADA Applications	Aims at SA. Can be adapted for other domains
Design Philosophy	Optimized use of bandwidth and hardware	Simplified data engineering and integration, reuse of models and existing communication protocols
Protocol Stack	A layered architecture with Link layer Pseudo Transport layer and an Application layer the same stack is ported on top of TCP/IP stack to make DNP3 work over a LAN	A virtualized model of devices and objects which is mapped to a specific protocol stack based on MMS, TCP/IP and Ethernet,the standard defines profiles for other layers of communication stack that are dependent on services provided
Data Representation during communication	Use of a numbered list of data points	Exchange of I/O (actual data) and meta-data (named data objects)
Communication Medium	Serial (dial-up, microwave), IP communications over Ethernet	IP based communication over Ethernet, extensible over other media
Data Rates	Designed for low data rates(Kbps)	High speed IED to IED communication (100 Mbps)
Configuration Support	Uses config files but no configuration language	Uses xml based SCL (Standardized Configuration Language) to configure a device and define its role

2.2.4 Recent Trends

As mentioned in Section 2.2.2, IEC 61850 uses advanced modeling techniques to represent protection, control, monitoring devices, services and corresponding data used in SA systems. Moreover, the data and service modeling techniques are independent of the underlying protocol stack, which carries the actual data through the network. The same approach, is being extended to other parts of the power system industry in the form of different IEC standards, which use IEC 61850 as a base protocol and specify different the information models, depending on the needs of the applications. Some of these are specified below [27]. Fig. 2.13 shows pictographically the above mentioned standards.

- IEC 61850-7-410 specifies the logical nodes required to represent the complete control and monitoring system of a hydropower plant.
- IEC 61850-7-420 provides IEC 61850 extensions or logical nodes to be used to model decentralized resources. These are applicable to central-station generation installations that are comprised of groupings of multiple units of the same types of energy conversion systems e.g. photovoltaic and fuel cells. The communications for DER plants involve not only local communications between DER units and the plant management system, but also between the DER plant and the operators who manage the DER plant as a virtual source of energy.
- IEC 61400-25 gives the specifications of communications for monitoring and control of wind power plants. Besides information and information exchange models, the standard specifies mappings to IEC 60870-5-104 and DNP3 protocol standards.
- IEC 61850 TC57, WG10 is working on IEC 61850 extensions on power quality.
- IEC TC 57, AHWG07 is working on IEC 61850 extensions for information exchange between substations and control centers.
- Information models for advanced metering networks and demand response are being developed by the OpenAMI task force [28].
- IEC TR 61850-90-1 specifies the use of IEC 61850 for the communication between substations.

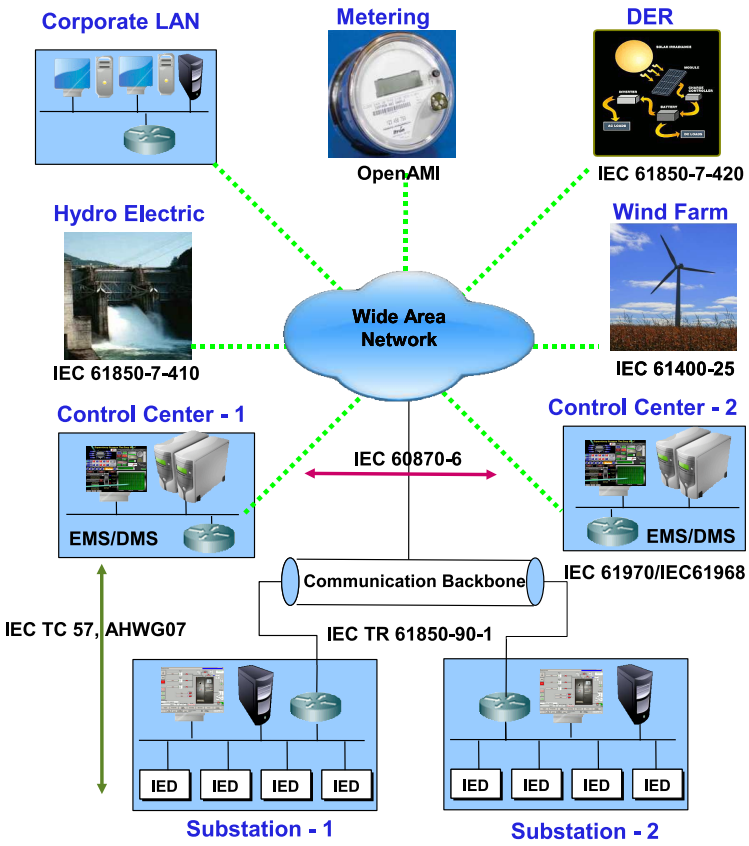

Figure 2.13: Upcoming IEC Protocol Standards For Future Power Systems.

Thus, IEC 61850 is being applied and extended to meet the requirements for applications even outside the substation for almost the whole electrical energy supply chain. A new title is also proposed for the standard - *IEC 61850 Communication networks and systems for power utility automation.*

Meanwhile, many efforts are being done by the IEC to extend the IEC 61850 to different parts of the electricity supply chain, however, these standards, do not satisfy the needs of SmartGrids such as bi-directional communication between utility and end users and between the agents controlling the DRERs/DESDs. Thus the standard IEEE P2030 was set up to provide guidelines for smart grid interoperability [13]. Specifically the Task Force -3 of IEEE-P2030 deals with the development of communication protocols, based on the already existing communication standards in power systems. The protocol standards identified by NIST [9] to have interoperability between SmartGrids are listed in Appendix-D.

IEC 61850, is a strong contender, to serve as the initial smart grid interoperability standard for SmartGrids. Because of the separation between the modeling approach and the actual protocol stack responsible for carrying the application messages, IEC 61850 can support a lot of different physical medium. For example, it can support 3G cellular technology, as well as the optic fiber as a communication medium.

Thus, as of now, there is no standardized protocol to be used specifically for Smart Grid like systems. However, making use of existing standardized protocols like IEC61850 would be a wise choice to implement the various applications for SmartGrid Systems. The challenge would be to model the various components of the SmartGrid (e.g the agents controlling the DERs, DESDs) based on existing node models and to develop communication profiles that would suit the needs of the SmartGrid. For example, to be used over a wide area network, IEC 61850 will have to be mapped to a communication medium that can support the required range.

Chapter 3

Reliable and Secure Communication Architecture for FREEDM

In Chapter 1, we mentioned our focus on the communication between the agents controlling the DRERs and DESDs, and between the agents and the substation for this thesis. In this Chapter, we describe the FREEDM system which we use as a platform for our research. We describe the FREEDM objectives and the various components constituting the FREEDM system. We also discuss the FREEDM communication architecture and requirements. We take learnings from Chapter 2 regarding timing criticality in SA systems and propose guidelines for the FREEDM system.

3.1 RSC and FREEDM - Objectives

Support for different forms of generation and storage devices is one of main objectives of the future smart grids. As a step towards achieving this objective, the *Future Renewable Electric Energy Delivery and Management (FREEDM)* Systems Center has recently been created by the NSF to develop technologies to incorporate distributed renewable resources of energy and storage devices into the existing power distribution systems [29]. *Reliable and Secure Communication (RSC)* subthrust is a part of the FREEDM project focusing on the communication requirements, architecture and communication protocols to

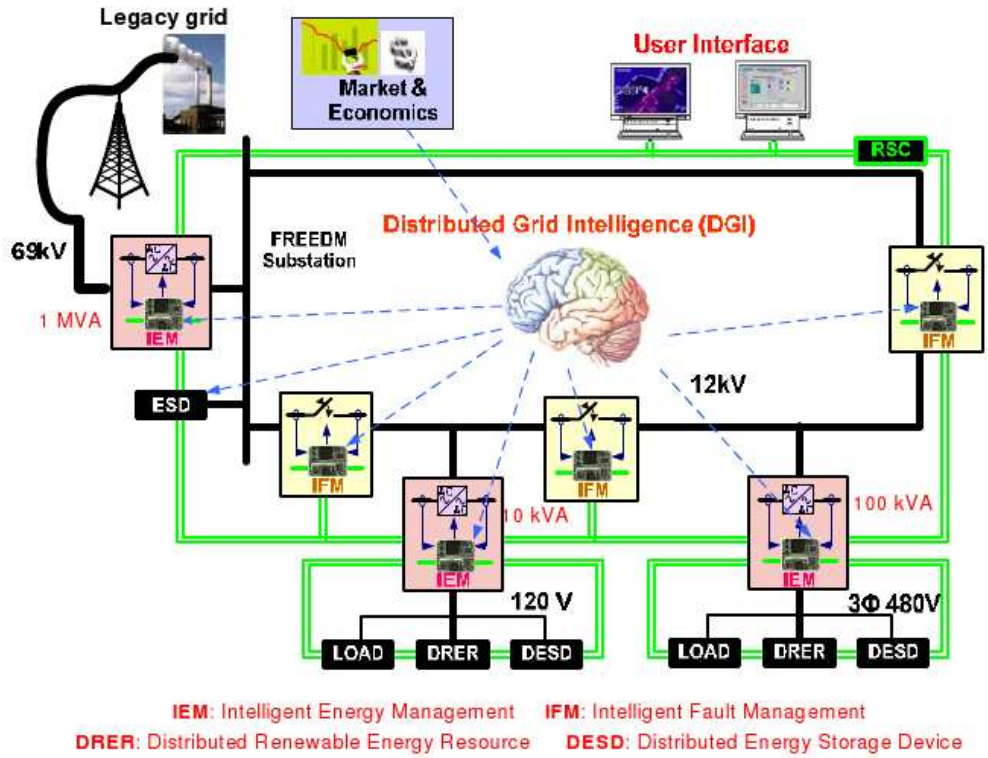

Figure 3.1: Proposed FREEDM System Architecture.

be used within the FREEDM system. The work in this thesis was carried out as a part of the RSC subthrust. In this section, we detail the FREEDM project. The main features of the FREEDM system have been described below:

1. *New delivery system*: The FREEDM center would develop power electronic technologies to improve the existing power distribution (delivery) system to allow the 'plug and play' operation of any Distributed Renewable Energy Resource (DRER), Distributed Energy Storage Device (DESD) or load. Since these devices may work at different voltage levels (e.g batteries of different voltage levels), they cannot be directly attached to the grid. The new delivery system will also allow for bi-directional energy flow on the power grid using an Intelligent Energy Management system (IEM) based on solid state transformers.

2. *Distributed grid intelligence (DGI):* The DESD and DRER devices in the FREEDM

system, will be distributed along the electricity distribution grid. Because of their large number, they need to be controlled autonomously (or intelligently) using a distributed agent based architecture with each agent controlling the devices at a site. Agents will also be needed to actively monitor the grid and take corrective action using an Intelligent Fault Management System (IFM). This would ensure to stability of the grid and its insulation from any faults at the user level.

3. *Reliable and secure communication backbone:* The intelligent agents controlling energy devices need to communicate with each other for energy management, with loads or DRERs or DESDs for control and to a control center for monitoring. Communication will also be required to support the critical IFM functionality. The distributed nature of the FREEDM system makes the support for reliable communication very challenging. Hence a fault-tolerant communication backbone is required to support FREEDM applications. Since the communication medium could be shared and readily accessible (e.g. wireless medium such as WiFi), the backbone needs to secure.

4. *Perfect power quality:* The future power grids will require to have superior power quality according to load sensitivity and to support the needs of new digital appliances (Section 1.2). However, with the integration of DRERs and DESDs into the grid, which operate intermittently at varying voltage levels, this objective of superior power quality becomes difficult. Renewable energy sources such as photovoltaic power systems are known to generate high harmonic levels which can destabilize the grid. The FREEDM system will develop modern solid state transformers and fault isolation and management devices which can control these resources, maintain grid stability and thus provide good power quality to end users.

5. *Improved efficiency and operation with unity power factor:* The FREEDM system will improve the efficiency of existing alternating current systems through active management and operation with unity power factor. Active management utilizes real time measurements of primary system parameters (voltage and current) for real-time control of generation and network devices [30]. This can result in an improved power factor of the system.

   Power Factor is the ratio of the resistive load (R) to the the total impedence (Z)

of an AC circuit. The average power consumption of the load is given by $VICos\varphi$, where φ is the power factor of the load and V, I are the instantaneous voltage and current respectively. Thus an AC load with a lower power factor will require more current for the same power use as a purely resistive load ($Z = R$), as the applied AC voltage is the same in both cases. This would result in more line losses for the utility making the overall distribution system inefficient. The increased current on the distribution network might even overload the transmission lines. The utilities need to guard against such issues by limiting them to a section of the grid. This is accomplished using active management as mentioned above.

It is also claimed that distribution networks using active management can accommodate up to three times as much DRERs [31]. The FREEDM project will use IFM technology for active management.

6. *Operation in isolation:* The FREEDM system will be capable of operation relying solely on DRERs and DESDs to meet the demand of the load devices. This capability is essential in future grids to provide insulation against glitches in the legacy power transmission grids, which if unchecked can cause widespread blackouts.

Fig. 3.1 illustrates the proposed structure of FREEDM system which is essentially an improved electricity distribution system. Thus the structure shown in the figure is replicated all along the electricity distribution feeder as *Subdivision Loops*. All the devices are spread all along subdivision loops, which form the traditional $12kV$ distribution grid, also called the *Primary Circuit*. The agents controlling the DRERs, DESDs and load devices are also attached to the $120V$ residential electricity network, also called the *Secondary Circuit*. They are called the *Intelligent Energy Management (IEM) devices* in the FREEDM system (shown as AC-AC converters). These devices are responsible for efficient two-way energy conversion and exchange between the primary and secondary circuits using a solid state transformer. Similarly, agents for active management, fault detection and isolation are called the *Intelligent Fault Management (IFM) devices* (shown as circuit breakers). The IFM and IEM devices have built-in intelligence (DGI) and communication capability (RSC). In the figure, the DRERs represent energy resources like the wind and the solar energy and the DESDs represent storage sources like the batteries to store solar power or used to run the plug-in electric vehicles. A central monitoring server ("User Interface" in

the figure) is also required to monitor the IEM or IFM operation. It is referred to as a control center (CC) in this thesis. The FREEDM system is connected to the legacy grid through a FREEDM substation.

From the objectives of the FREEDM system described above, it is clear that a reliable and secure communication backbone is an important part of the system supporting and enabling different forms of control (DGI) within the grid. We describe the architecture of such a communication backbone in the following section.

3.2 FREEDM Communication Architecture

The control strategy for the FREEDM system dictates its communication requirements and hence the communication architecture. Sathyanarayana et al. [12] suggest the use of a mix of agent–based control and hierarchical control for the FREEDM system. In agent–based control, autonomous agents with decision making capability are used to control the locally attached loads, DRERs or DESDs [10]. Some of the agents are used to monitor the grid itself and implement protection functionality. These agents need to communicate which each other for protection information exchange. This kind of control is easier to implement, requires only local communication and can avoid single point failures. However, local control cannot achieve global optimization. On the other hand, hierarchical control requires the agents to send monitoring information to the substations, which analyze the information and send control commands to the individual agents. Thus this form of control requires long-range communication and is capable of global optimization. *Hence, the communication architecture for the FREEDM system needs to allow for peer-peer communication between the IEM and the IFM devices, and also for centralized communication between IEM or IFM devices and the substation.*

Fig. 3.2 depicts a possible communication architecture of the FREEDM system. As shown in the figure, each IEM or IFM device comprises of a communication board and a control board. The communication board links each communicating device to the communication backbone through an RSC interface. In an IEM device, the control board controls the operation of a Solid State Transformer (SST) through a digital I/O bus [32]. In an IFM device, the control board monitors the attached electrical lines. It is also connected to a circuit breaker for protection operation. DGI processes running on each control board com-

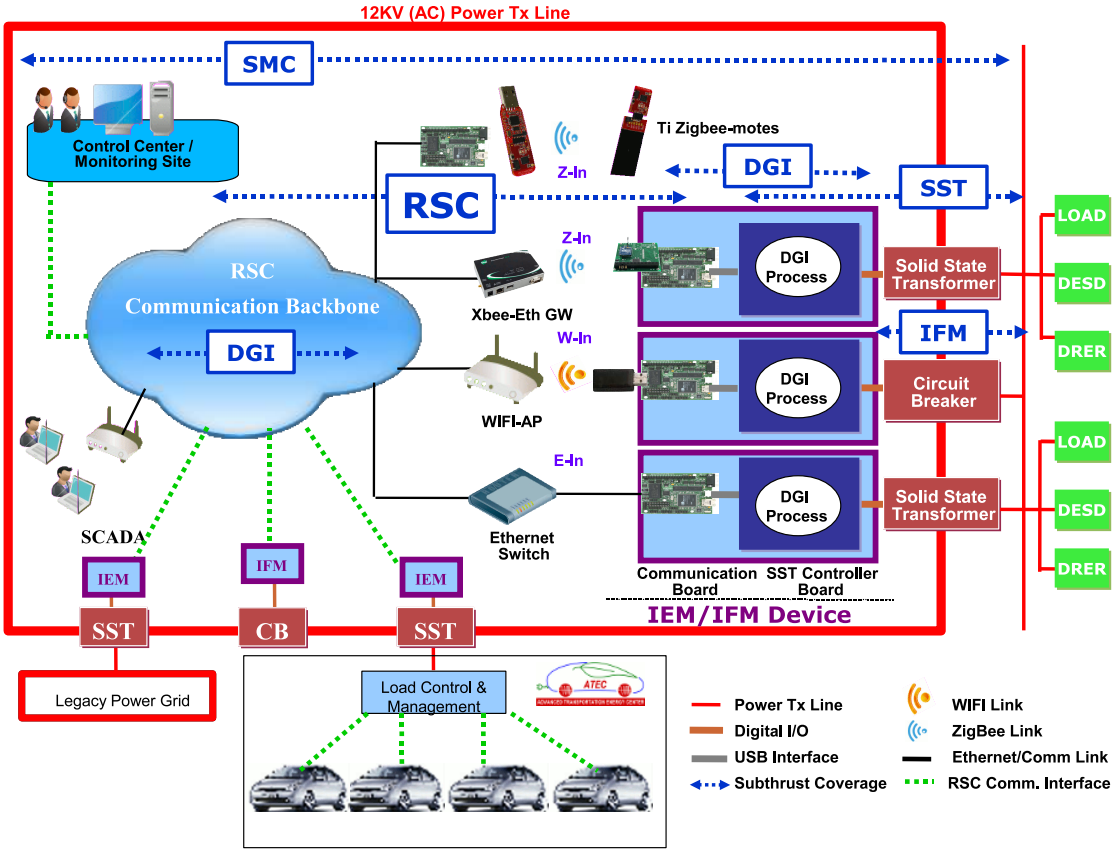

Figure 3.2: FREEDM System Communication Architecture.

municate with each other through the communication backbone. The DGI processes use information obtained from locally attached loads, DRERs and DESDs and global information, obtained from other peers in the network, for configuration or reconfiguration of nodes, on-line leader election, distributed state maintenance and control. Three kinds of control is mainly exercised by the DGI processes[1], *Short term control* (IEMs directly controlling the attached device), *Medium Term Control* (IEMs within the same leader communicate using explicit message passing or may use sensing from the attached power lines) and *Long Term Control* (Group leaders communicate with each other through explicit message passing). Based on the control strategies and different forms of control discussed above, various levels of communication and use cases have been identified below:

[1]Control Mechanisms and Grid Intelligence is being taken up by the DGI team

1. **Wide–Area Communication:** Wide–Area communication is required to support the following interactions within the FREEDM system.

   - IEM - IEM: This forms a part of the DGI system where IEM devices exchange information with each other for energy management. For example currently attached load, surplus power from DRER.
   - IFM - IFM: The IFM devices responsible for fault management need to communicate with each other to exchange protection data and commands.
   - IEM - CC or IFM - CC: All communicating devices send monitoring information using standardized communication protocols (SNMP or SCADA) to a centralized control center (CC) which may be co-located with the FREEDM substation.

   Thus, Wide–Area Communication will allow the agents controlling the DRERs, DESDs and the loads, spread all over the distribution grid of an area to communicate with each other and with the substation. It is over this communication backbone, that the time critical fault protection, monitoring and control applications will operate. Thus, *Wide–Area Level communication is characterized by larger distances (miles), high throughput requirement (Mbps), and strict timing constraints.* Since FREEDM is a complex system, the electrical system may become faulty. The communication backbone should be fault-tolerant so that command signals can be sent to rectify the faults from a remote location.

   Different networking technologies may be used for Wide–Area communication, namely, wireless mesh networking, 3G cellular networks, WiMAX, RF radios operating in licensed and unlicensed bands and Broadband over Power Line (BPL). The throughput and timing requirements of FREEDM system applications requiring wide–area communication need to be matched with the capability of the communication medium. As an initial step in this direction, we use the WiFi (W-In) and ethernet (E-In) communication technologies for this purpose (Fig. 3.2). Experiments carried out using these technologies have been discussed in Section 4.4.

2. **Local–Area Communication:** The control algorithms at the IEM devices require local communication to interact with the local loads, energy resources and storage devices. The interaction includes the commands initiated by the IEM device and

monitoring information obtained from the energy devices. This information exchange occurs through either a digital I/O bus (the entity being controlled, is directly attached to the IEM device) or through a communication interface compatible with the entity being controlled. For example, the ATEC center at NC State University, proposes to use ZigBee technology at the charging station to manage the charging of vehicles fixed with Zigbee devices [33]. Thus the IEM device managing the charging of vehicles at a charging station will have a ZigBee interface for local communication with PEVs and have an interface for wide–area communication with the substation, IEM or IFM. An IEM with "local control and management unit" for managing the PEVs at a charging station, having an RSC interface for both local–area and wide–area communication is shown in Fig. 3.2.

Thus, the communication needs of the load or the DRER or DESD being managed, will decide an appropriate communication technology for local–area communication. For this thesis, we use IEEE 802.15.4 communication standard for this purpose. Our initial experiments with IEEE 802.15.4 have been discussed in Section 4.4.

3. **Substation–Level Communication:** This consists of a SCADA interface between the legacy grid and FREEDM substation. Information aggregated from within the FREEDM system will be sent to the utility using SCADA protocols (e.g. DNP3 or IEC-61850). The FREEDM substation will be connected to the control center of the utility providing electricity to the substation. It may also be connected to peer substations for inter-substation communication.

In this section, we detailed the communication architecture of the FREEDM system and explained how it is influenced by the control strategy of the FREEDM system which is a mix of peer-peer control and hierarchical control. We also identified the various communicating entities and levels of communication within the FREEDM system. Now that we understand the different kinds of communication possible with IEM and IFM devices, we investigate the communication requirements of the FREEDM system in the following section.

3.3 FREEDM Communication Requirements

The FREEDM system shares a lot of electrical functionality with both SCADA and SA systems. For example, like the SCADA systems, remote monitoring and control capability from substation is required for the IEM and the IFM devices. Similarly, like the SA systems, we need automatic corrective action capability in both IEM and IFM devices. Hence, the communication and timing requirements for the FREEDM system applications are similar to these systems. In this section we describe the communication requirements of the FREEDM system (timing requirements have been described in Section 3.4).

The communication requirements for FREEDM system applications can be classified as either *Network Performance-Based* (e.g., network latency, time synchronization) or *Network Quality-Based* (e.g., quality of service, data delivery criticality, reliability, security and scalability) [23][34]. These are summarized below:

1. **Network Latency:** Network Latency implies the maximum time in which a particular message should reach its destination through a communication network. The messages communicated between various entities within the FREEDM system will have different network latency requirements (discussed in Section 3.4). For example, the protection information and commands exchanged between IFM devices will require a low network latency than the monitoring related messages between IEM or IFM devices and the FREEDM substation.

   Moreover, the messages exchanged can be event-driven (e.g., protection and control related) or periodic (e.g., monitoring related). The network architecture and communication medium must support the diverse requirements. The network architecture of the system will determine if the message sent from one communicating entity to the other will reach its destination in one or more hops. This will directly affect the latency. Similarly the data rates supported by the communication medium would dictate, how fast an entity can communicate a change observed or reply to a message received.

2. **Quality of Service (QoS):** The protocol suite used for communication (e.g., IEC 61850) must be able to differentiate between the high priority data and the low priority data. Example, a control signal from one IFM to the other to trip a relay needs to have

priority over unsolicited real-time data sent to the substation. A QoS parameter may be used to differentiate between various kinds of application data with varying QoS requirements. For example, IEC 61850-8-1 suggests the use of "priority tagging" in an ethernet MAC frame according to IEEE 802.1Q to differentiate between time critical protection related traffic from other low priority traffic in SA systems. This is especially useful for GOOSE or GSE messages (used for sending "trip" messages) and transmission of sampled values (digital current and voltage information from transformers to IEDs). By default, the GOOSE and sample value messages have a user-priority as four. Non-tagged messages have a user-priority one.

3. **Data Delivery Criticality:** The protocol suite must provide for different levels of data delivery criticality depending on the needs of the application. This need may be decided at the time of connection establishment between two applications. The following levels of data delivery criticality may be used:

   (a) High: is used where the confirmation of ETE data delivery is a must and absence of confirmation is followed by a retry. For example, this may be used for delivery of SCADA control commands for settings, change of switch gear position.

   (b) Medium: is used where no ETE confirmation is required, but the receiver is able to detect loss of data. E.g., measured current and voltage values and disturbance recorder data.

   (c) Non Critical: is used where loss of data is acceptable to the receiver. In this case, reliability can be improved by repetitive messages. For example, this may be used for periodic data for monitoring purpose.

4. **Reliability:** From a communication perspective, FREEDM is essentially a real-time distributed system with IEM and IFM devices as its components. These devices rely on the communication backbone to send and receive critical messages to maintain the stability of the FREEDM system. Hence, it is extremely important for the communication backbone to be reliable and fault-tolerant for successful and timely exchange of messages.

   The reliability of the communication backbone can be affected by a number of possible failures. These failures could be time-out failures, network failures and resource fail-

ures. A time-out failure can occur if the time spent in detecting, assembling, delivering and taking action in response to a control message exceeds the timing requirements. A network failure could occur when there is a failure in one the layers of the protocol suite used for communication. For example, a routing protocol failure might prevent a message from reaching its destination in spite of existence of a physical link. Noise and interference in the physical medium may also disrupt the communication. A resource failure implies failure of the end node which initiates communication or receives messages.

Hence, there is a need to assess the reliability of the FREEDM system and find ways to improve it.

5. **Time Synchronization:** The IFM and IEM devices will need to be synchronized in time for their operation. The requirements for time synchronization will depend on the criticality of the application. Tolerance (jitter) and resolution requirements for time synchronization will be stricter for IEDs which process time sensitive data. For example synchrophasors have the most strict need of time synchronization as they provide a real-time measurement of electrical quantities (voltage and current) from across an electricity grid for analysis, measurement and control [23].

   Time synchronization can be obtained through a number of ways depending upon the resolution and jitter requirements. Precision Time Protocol (PTP) defined by standard IEEE 1588 provides time synchronization with upto nanosecond precision over ethernet networks. Global Positioning Systems (GPS) and Simple Time Network Protocol (SNTP) are other ways of achieving time synchronization.

6. **Security:** The FREEDM system will be implemented in the existing electricity distribution networks of a region spread over a considerable area (tens of miles). Hence physical and cyber security from intruders is of utmost importance. Moreover, if a wireless communication medium (like WiFi or Zigbee) is used to support the communication backbone, because of the shared and accessible nature of the medium, security concerns are increased. Hence, to provide complete security for the FREEDM system, we need to identify various communication use cases (like demand side management, advanced meter reading-AMI, communication between IEM or IFM devices, local–area communication by an IEM device) and find appropriate security solutions to

each of those use cases. For example, authorized access to the FREEDM real time data and control functions, use of encryption algorithms for wide–area communication to prevent any spoofing.

The need for security in smartgrid systems has even been recognized by the upcoming smart grid interoperability standard IEEE P2030 [9]. The standard identifies the use of security standards like AMI-SEC System Security Requirements (Advanced metering infrastructure - AMI and smartgrid end-to-end security), IEC 62351 Parts 1-8 (Information security for power system control operations), IEEE 1686-2007 (Security for intelligent electronic devices) etc.

7. **Scalability:** Scalability of a telecommunication network is considered as its ability to gracefully handle increasing amounts of data and end nodes. In case communication technology like the cellular networks, is used for communication within the FREEDM system, the scalability issues are handled by the service provider. However, if open communication standards like wireless mesh networks, Zigbee are used, a lot of scalability issues may arise. For example, wireless mesh networks are known to have scalability issues [35], namely, decrease in application throughput with increase in network size, failure of routing protocols to form a reliable routing path, loss of connection in transport protocols etc. Thus to ensure scalability, all the protocols from the MAC to the application layer need to be scalable. Hence we must design a scalable communication backbone with use of standardized communication protocols for the FREEDM system.

8. **Multicast support:** The multicast concept is crucial for power system applications in which a given analog value, state change, or command may have to be communicated to several peers at the same time [36]. Thus, instead of multiple individually addressed messages, a single multicast message is sent to a switch, which would normally forward it to all outgoing ports. Receiving devices are simply configured to listen to a particular multicast address, thus making it possible to disregard the unwanted network traffic. In the FREEDM system, multicast functionality will be required when an IFM device needs to inform its peers of a particular event in the electricity distribution network.

In this section, we described the communication requirements for the FREEDM

system and the various scenarios where they are applicable. These requirements need to be taken into account while designing the communication backbone for the FREEDM system. Network latency or timing constraint is one of the main requirement for power system applications. We discuss this requirement in the next section.

3.4 Timing Issue - A Critical Factor

"Timing" is a critical factor in power system applications. It is generally specified using a protocol variable, *Delivery Time* which is the maximum time in which an application message should reach its destination. This is particulary important for "trip" messages which need to timely change the position of a circuit breaker. The paper [18], describes Tele-protection and Power system control (PSC) as the main real-time communication requirements of power systems. Section 2.1.2 details the timing requirements between various interfaces in SA systems and also for different types of information exchange between IEDs, both inside and outside of a substation. Even the recent communication protocol standard for SA, IEC 61850 has provisions to ensure message performance requirements using PICOMS.

The time requirements for power system applications are directly dependent on the medium used for communication. Power systems in their early years of operation used dedicated communication media. E.g., SCADA systems used telephone lines while the SA systems used serial communication links. A dedicated medium makes it easier to predict the delivery time of messages and confirm that the timing requirement of the power system application is met. However, in recent times, with advances in microprocessor technology, microprocessor based digital IEDs, advances in communication technologies like the ethernet and TCP/IP protocols, the power systems have moved to the use of shared wired (e.g., ethernet in SA systems) or wireless (e.g, microwave for SCADA) communication medium because of advantages of networked systems over wired systems. However, a shared communication medium (e.g. ethernet) allows every node connected to the medium to transmit data at any time. Hence, there is a possibility of simultaneous packet transmission and hence packet collision. This is followed by retransmission of lost data. Retransmission of packets adds to total message delivery time required for the packet. A shared wireless medium adds more challenges for packet transmission like interference, which also leads to

packet losses and retransmission of data.

Similar challenges of a shared communication medium also pose the timing requirements and the wide–area and local–area communication needs of the FREEDM system (Section 3.2). Thus, there is need for a rigorous assessment of a communication medium used to support the RSC communication backbone for FREEDM to make sure that it meets the diverse delivery time requirements of FREEDM. The paper [37] follows a similar approach and compares the performance of wired and shared communication (ethernet) solutions to confirm that IEC 61850 can be used to successfully replace the conventional (wired) substation control and protection systems without any degradation of system performance (i.e. the timing requirements).

The FREEDM system has various logical communication interfaces with different timing requirements. For example, the interface between IEM-IEM, IFM-IFM, IEM-DRER, IEM-DESD, Control Center(CC)-IEM, CC-IFM. IFM devices are primarily used for fault management and protection, hence the IFM-IFM interface has strict timing requirements. Similarly the analog and digital values from the DRERs and DESDs need to reach the IEM devices at the earliest. They would also require high speed communication. Control commands sent by the IEM devices to DRERs and DESDs may have medium speed communication. Communication between the control centers and the IEM or IFM devices would be mainly the monitoring information or the configuration file upload or download. These would require low speed communication. The different communication interfaces and relative communication requirements according to the needs of the application running on each interface are listed in Table 3.1.

The timing requirements listed in Table 3.1 are the limiting timing requirement for an interface. Timing requirements may be different for different types of information on the same interface. The timing requirements listed are only relative and would be less strict than in SA systems because of the physical scale of the FREEDM system. Moreover, it will not be possible to deploy a fast communication medium like the ethernet (used in SA systems) which would add more latency to the messages.

The exact communication delay and throughput requirements for various applications used within the FREEDM system, have not been ascertained as yet. This is because the IEM applications and the protection schemes are still under development by other teams. Hence a logical way to come up with possible message timings in the absence of message

Table 3.1: Delay Requirements For The FREEDM System.

Interface	**Example of communication**	**Delay Requirement**
IEM - IEM	Energy Exchange Information	Medium Speed
IFM - IFM	Protection	High Speed
IEM - LOAD	Control	Medium Speed
LOAD - IEM	Analog / Digital Values	High Speed
IEM - DRER	Control	Medium Speed
DRER - IEM	Analog / Digital Values	High Speed
IEM - DESD	Control	Medium Speed
DESD - IEM	Analog / Digital Values	High Speed
CC - IEM CC - IFM	Control Information, Configuration files	Low Speed
IEM-CC IFM - CC	File upload, Updates ,Control Responses	Low Speed

requirements is to test different probable communication media which are candidates to support the communication backbone of the FREEDM system. This approach has been applied in Chapter 4. Appendix E gives an example of the expected timing requirements for communication between DER systems as suggested by Siemens.

Chapter 4

RSC Testbed and Measurements

One of the objectives of this thesis is to find out the communication technologies which could be used for communication within the FREEDM system (Section 1.3). This Chapter describes the communication hardware platform for the FREEDM system set up by us to achieve this objective. We first brief the communication technologies used by us in the testbed. Further, we describe the RSC testbed and its components. We also describe the various experiments carried out using the testbed to find out the limiting timing requirements possible from the use of a particular communication medium. The results from the experiments and important lessons learnt have also been detailed.

4.1 Overview of Networking Technologies

Wide–Area communication and local–area communication within the FREEDM system (Section 3.2) have different communication requirements, applications and hence technologies used for communication. For our year 1 efforts, we focus on WiFi and Zigbee communication technologies. These technologies are IEEE standards and are open source in nature with ample of hardware and software support available. In this section, we detail the main features and protocol stacks of these technologies.

4.1.1 IEEE 802.11 - WLAN

IEEE standard 802.11, is a standard for Wireless Local Area Networks (WLANs) [38]. The standard has many components (e.g., IEEE 802.11i - Security, 802.11e - Quality

of Service etc.) which add different features. Some of the main features of IEEE 802.11 have been outlined below:

- *Protocol layer:* Specifies MAC procedures for wireless local area network computer communications.
- *Frequency:* Operates in 2.4 GHz or 5 GHz ISM band.
- *Data Rate:* IEEE 802.11g provides a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 19 Mbit/s average throughput.
- *Range:* Supports an indoor Range of about 35 m and outdoor range of about 140 m.
- *Networking modes:* Supports Infrastructure and Ad-hoc Modes.
- *Security:* Specifies the security mechanisms for communication (IEEE 802.11i). Commercially it is called WPA2. Most of the commercial products available implement the security standard partially and provide 64-bit or 128-bit WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access).
- *QoS*: Provides Q0S support (IEEE 802.11e) to time sensitive application. However, as of now, most of the commercial products do not support this standard.

Fig. 4.1 shows the different network topologies possible with WiFi. Two *Infrastructure WLANs*, connected by a Wired LAN have been shown. The Infrastructure WLANs are characterized by the presence of nodes called *Stations* connected to an *Access Point (AP)* using wireless access mechanisms (specified by IEEE 802.11) and a wireless radio. A group of nodes connected to an AP form a *Basic Service Set (BSS)*. BSS connected via a wired network, called a *Distribution System* form an Extended Service set (ESS) having an identifier, ESSID. A *Portal* within a distribution system forms the interworking unit to external LANs. Two Ad-hoc WLANs are also shown in the figure. In this case, stations tuned to the same frequency band can form an Independent BSS (IBSS) and communicate with each other directly without needing an AP.

Fig. 4.2 shows the protocol architecture and management for WLANs. The IEEE 802.11 standard covers the physical layer (PHY), the Medium Access Control layer (MAC) and the management procedures. The Logic Link Control layer (LLC), which is the upper

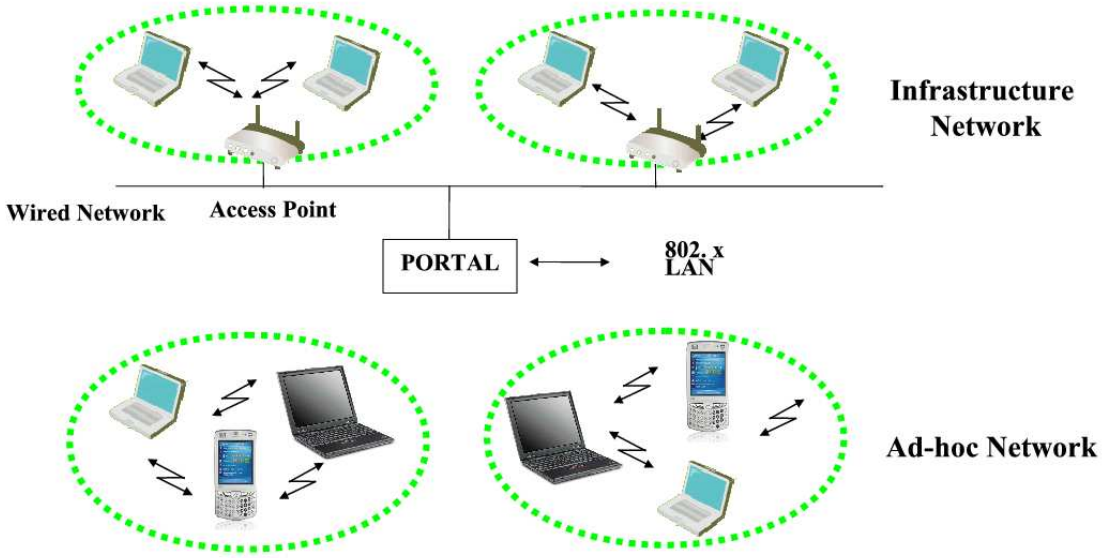

Figure 4.1: Wireless LANs - Infrastructure And Ad-hoc Modes.

part of the Data Link Control Layer, is not a part of the standard. The various layers have been described below.

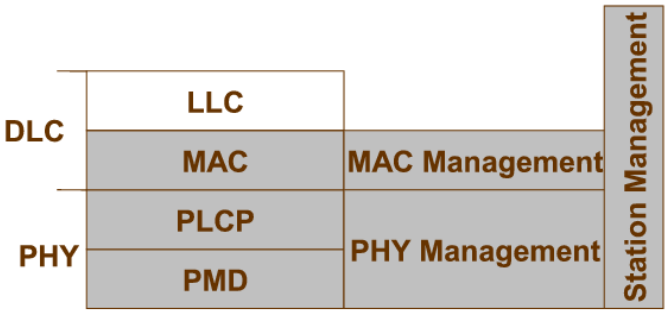

Figure 4.2: Wireless LANs - Protocol Architecture And Management.

1. *Medium Access (MAC) Layer*: The MAC layer has the following features:

   - It is responsible for controlling medium access to the shared wireless medium.
   - It provides asynchronous data service and an optional time bound service. The former is available in both infrastructure and ad-hoc modes, while the later is available in only infrastructure modes.
   - It is responsible for authentication, roaming and power management.

- It also preforms message fragmentation and message retries.

2. *MAC Management*: The MAC Management layer provides the following features:

   - It provides synchronization support for finding of WLANs, clock synchronization and generation of beacon signals.
   - It is responsible for power management functions e.g., periodic sleep.
   - It provides support for roaming, scanning of access points.
   - It maintains the current state of the network using a Management Information Base (MIB).

3. *Physical Layer Convergence Protocol (PLCP)*: The PLCP layer provides a Clear Channel Assessment Signal (CCA) for carrier sensing. It also provides a Service Access Point (SAP) independent of the transmission technology to the MAC layer above it.

4. *Physical Medium Dependent Layer (PMD)*: The PMD layer handles the actual modulation, encoding and decoding of signals over the wireless medium.

5. *PHY Management*: The PHY management layer is responsible for channel selection and maintaining the Management Information Base (MIB) which has all the information regarding the physical characteristics of a station, e.g., transmission rate, power level, antenna type.

6. *Station Management*: The station management layer co-ordinates with the PHY and MAC management layers.

4.1.2 Zigbee

Zigbee is a specification for a suite of high level communication protocols based on the wireless radio IEEE 802.15.4-2003 standard for *Wireless Personal Area Networks* (WPANs) [39]. The technology was developed to meet the needs of applications like consumer electronics, industrial control, medical sensor applications, home networking and energy conservation etc., which require a low cost, low power, low data rate and a limited range networking technology. The IEEE standard 802.15.4 specifies the PHY and the MAC layers for Zigbee while the Zigbee alliance [40] (which is an association of companies working

together) defines and maintains the higher layers. The Zigbee technology has the following main features:

- Limited range personal area networks (10 - 75m).
- Global ISM band operation, 2.4 GHz, 915 MHz, 868 MHz.
- Low data rates (10 - 115Kbps) and low duty cycle networks to maximize battery power.
- Two years battery life using standard alkaline batteries.
- Co-located networks, i.e. more than one PAN using different frequencies can co-exit at a place.

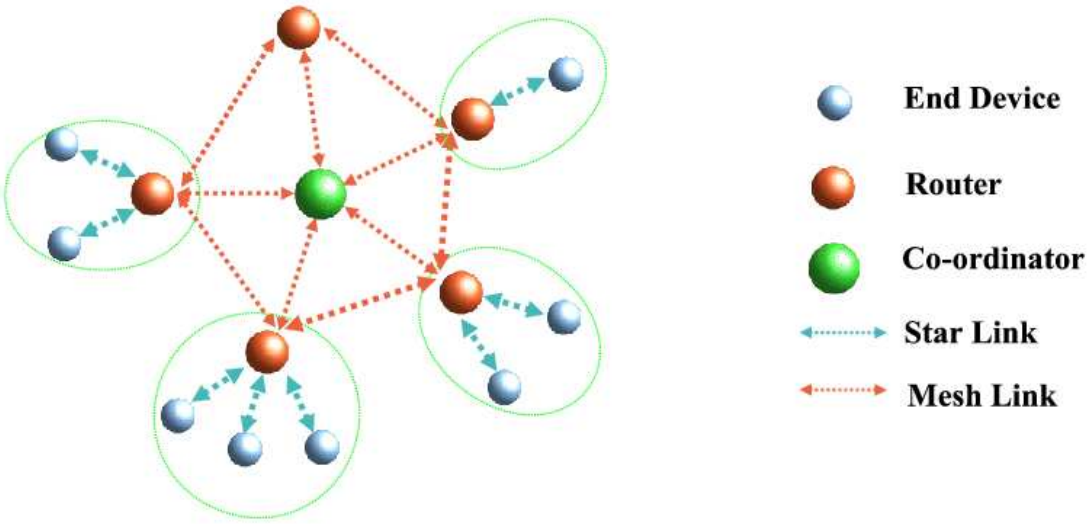

Figure 4.3: Zigbee Network Architecture.

Fig. 4.3 shows the network architecture of a Zigbee network. There are three types of devices as shown, *End Devices, Routers and Coordinators.* The end devices can be fully functional devices (FFD) or reduced functional devices (RFD). The routers and the coordinators are always FFDs, i.e. they have the capability to perform all the network functions. There is always one coordinator per network which is responsible for starting a network and choosing certain networking parameters and informing others about them.

End devices are generally arranged in a star topology around a router or a coordinator. They get instructions from a coordinator. In case an end node is outside the range of a coordinator, they communicate through a router. The routers and the coordinator can form a mesh like network where a router can send (or receive) data to any other router or coordinator it its range. In this manner, the range of a network gets extended.

All the devices governed by a coordinator form a Personal Area Network with a PAN-ID. Zigbee specifies communication between only intra-PAN networks, i.e. the data begins and terminates within a single PAN. The coordinator may also be linked to a gateway for communication with IP based networks.

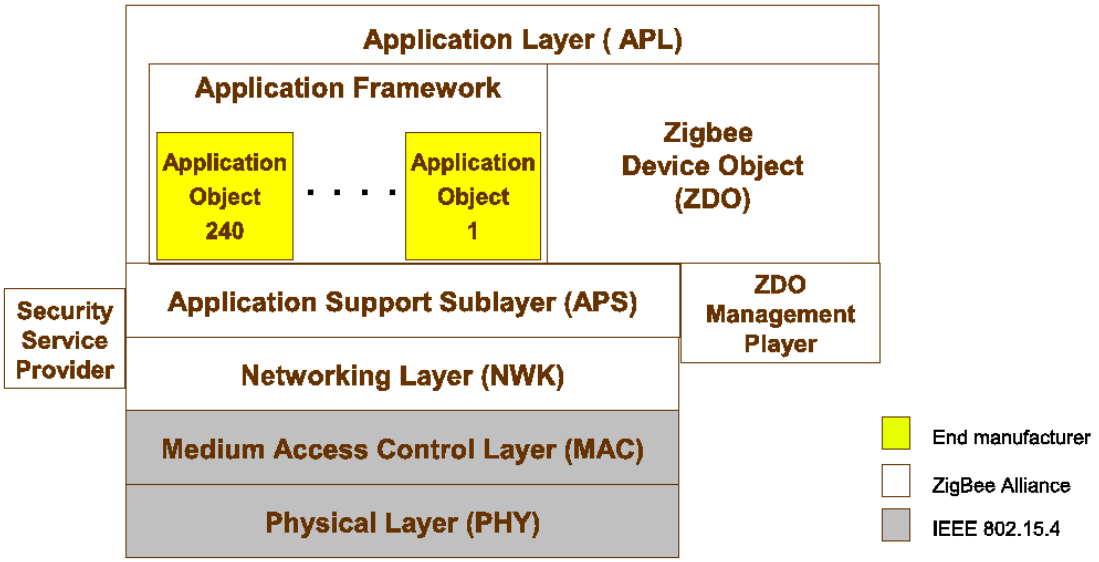

Figure 4.4: Zigbee Protocol Architecture.

Fig. 4.4 shows the layered architecture of the Zigbee stack. The stack identifies a data entity (used for data transmission services) and a management entity (provides other services) at each layer. Each service entity provides an interface to the layer above it through a Service Access Point (SAP). The layers have been briefed below.

- *Physical Layer:* This layer as specified by the standard IEEE 802.15.4 provides two PHY layer choices, one which can work on 868/915 MHz band and the other which works on 2.4 GHz ISM band. The former PHY layer provides good coverage and better

sensitivity at the cost of reduced data rate of 20-40 Kbps while the later provides a good throughput of 250 Kbps and can attain lower duty cycles and lower latencies.

- *MAC layer:* The MAC layer controls access to the radio channel using CSMA-CA mechanism. It is responsible for beacon transmission, synchronization, frame validation and providing a reliable transmission medium. This layer also provides a 16-bit short or a 64-bit extended, device addressing mechanism. The standard specifies three security levels at MAC layer: no security, access control lists, symmetric key security using AES-128.

- *Network Layer:* This layer, as specified by the Zigbee alliance provide two service access points to the application layer above it, namely Network Layer Data Entity (NLDE) and Network layer management entity (NLME). The NLDE is responsible for generating the network layer protocol data unit (NPDU) from the application layer data, transmitting the routing data to its next destination. The NLME provides for services like, configuring a new device when it joins the network (i.e. will the device join an existing network or start a new network and be the network coordinator); joining, leaving and rejoining a network; addressing of the end nodes by the network coordinator; neighbor discovery and route discovery and routing mechanism.

- *Application Support Sub-layer (APS)*: This layer acts as an interface between the network and the application layer and provides a set of services which are used by the application layer objects and the ZDO Management layer. The layer has two entities which provide the service through their access points, the APS data entity (APSDE), APS Management Entity (APSME). The APSDE provides data transmission services between two or more application entities location on the same network, while the APSME provides services to application objects like the security services and binding of devices. It also maintains a database of managed objects.

- *Application Framework:* The application framework provides an environment, in which the application objects are hosted on the Zigbee devices. The framework can host about 240 application objects with their end point addresses ranging from 1 - 240. An Application Profile is an agreements for messages, message formats, and processing actions that enable developers to create inter-operable, distributed applications

communicate between various end devices. The Application Objects are specified by the equipment manufacturer for a particular application.

- *Zigbee Device Objects (ZDO)*: The ZDO provide the common requirements of all applications using the Zigbee stack, and interfaces between the Application Objects, the device profile and the APS.
- *Security Service*: The security services for ZigBee provide for: methods for key establishment, key transport, frame protection and device management. These services form the building blocks for implementing security policies within a ZigBee device.

In this section, we gave an overview of WiFi and Zigbee communication technologies which we use in this thesis to form a communication backbone prototype for the FREEDM system. The WiFi technology can be extended using mesh networking to support wide–area communication, while the zigbee technology can be used to support local-area communication. The communication backbone prototype has been described in the next section.

4.2 RSC Communication Backbone Prototype

In this section, we explain the testbed set up by us, to demonstrate the distributed computational capability needed for the FREEDM system. We have set up prototype IEM devices to communicate with each other using Zigbee, WiFi and ethernet interfaces by using the NCSU network as a backbone. Various experiments performed by us using the testbed have been detailed in Section4.4.

4.2.1 Hardware Platform

Fig. 4.5 shows the testbed with prototype IEM devices and there interfaces. These have been detailed in the following subsections. We use Technologic Systems TS-7250 embedded computers (200 MHz ARM-9 CPU, 64MB RAM, USB, Ethernet, Linux OS)[41] as communication boards for the prototype IEM devices. This device supports Z-In (Zigbee and IEEE 802.15.4), W-In (WiFi) and E-In (Ethernet) interfaces. Only one of these interfaces would be used by the device to reach the NCSU network at a time. Other devices which are a part of the testbed include TS-7250 Xbee board (IEEE 802.15.4 compliant

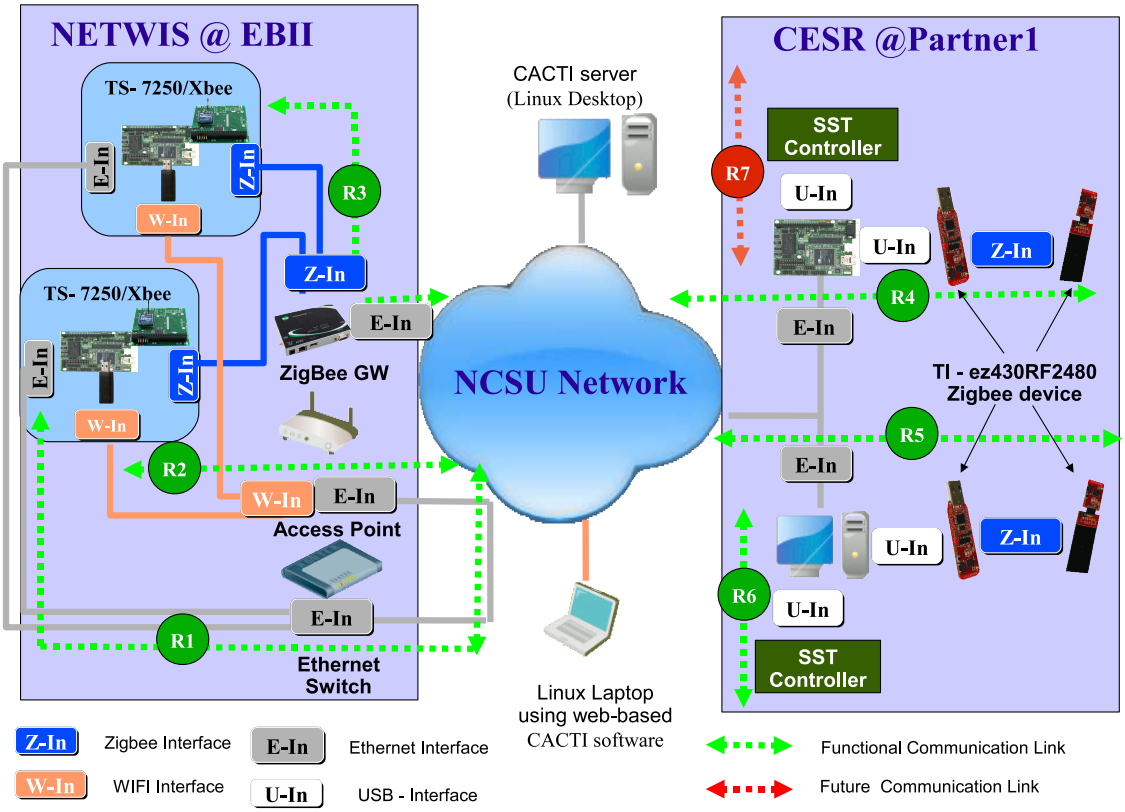

Figure 4.5: RSC Prototype For FREEDM.

device) [42], Digi IEEE 802.15.4 - Ethernet gateway [43], IOGEAR WiFi dongles (IEEE 802.11g compliant), WiFi Access Points, Ethernet switches, Linux workstations and laptops. We also use SST controller boards which are high performance embedded computers with fast signal processing capability. These have been developed at NCSU by the DGI team [32].

4.2.2 Testbed Functionality

To implement a distributed system, the testbed was set up at two sites at NCSU (shown in Fig. 4.5). At Site "Netwis@EBII" [1] routes R1, R2 and R3 are set up while at site "CESR@Partner1" [2] routes R4, R5 and R6 are set up. The purpose of the routes is

[1]NETWIS: Networking of Wireless Information Systems Lab at EbII building, NCSU.
[2]CESR: Center for Efficient, Scalable and Reliable Computing at Partners 1 building, NCSU.

to link the prototype IEM device to the NCSU network. The routes comprise of various interfaces, E-In, W-In or Z-In, which are meant to link two devices. Route R1 connects the E-In interface on the TS-7250 board to the NCSU network through an ethernet switch. Route R2 connects the W-In interface on the TS-7250 device to the NCSU network through the WiFi access point. The TS-7250 board has been configured to receive IP addresses dynamically from the network routers for both the E-In and W-In interfaces. Route R3 connects the TS-7250 board to the NCSU network via Z-In interface.

To develop the Z-In for the TS-7250 device, we use an expansion board which links the TS-7250 device to an Xbee board via serial port (UART). Using the Z-In interface, the Xbee devices connect to a Zigbee-Ethernet gateway using IEEE 802.15.4 technology to form a personal area network (PAN). Xbee device forwards all information received on the UART to the gateway transparently. Similarly the Xbee device forwards all data received on its wireless interface to the UART, which is received by the TS-7250 board. Different Xbee devices can communicate with each other using 64bit (pre-assigned) or 16bit (assigned) MAC addresses. The Zigbee Gateway has an ethernet interface and a Zigbee interface. The gateway maps predefined TCP port numbers to the MAC addresses of the Xbee devices using a *perl* script and allows any device on the NCSU network to 'telnet' to these ports and exchange data with the corresponding Xbee device. The Xbee devices used to develop route R3 can only be used as interfacing devices, but not as end nodes. Hence we used highly power efficient EZ430-RF2480 devices [44] from Texas Instruments as Zigbee end nodes. We refer to them as TI-Motes[3].

Like the Xbee devices, the TI-motes also use IEEE 802.15.4 technology for their lower layers of communication. However, unlike the Xbee devices, they can be configured into a large number of network topologies defined by the Zigbee protocol. For the testbed, we set up a PAN using three TI-motes with one of them acting as a coordinator (sink) and while the other two are used as end devices (source). The source devices have been configured to send voltage and temperature readings to the sink at regular intervals. The sink forwards the incoming data from the end nodes to the attached TS-7250 through the UART interface (route R4). As an alternative, the data packet from the source TI-motes could also be captured by a sink attached to a workstation using the same communication

[3]The work on TI-motes was carried out by other members of the RSC team. We brief it here to give a complete picture of the testbed.

Table 4.1: Summary Of Communication Routes In The Testbed.

Route	**Devices**	**Working or Future Work**
$R1$	TS-7250, Ethernet Switch, NCSU Network Router	Working
$R2$	TS-7250, NCSU WiFi Router	Working
$R3$	TS-7250, Zigbee-Ethernet Gateway,NCSU Network Router	Working
$R4$	TI-Mote(Source), TI-Mote(Sink), TS-7250, NCSU Network Router	Working
$R5$	TI-Mote(Source), TI-Mote(Sink), Linux Workstation, NCSU Network Router	Working
$R6$	SST Controler Board, Windows PC, NCSU Network Router	Working
$R7$	SST Controler Board, TS-7250, NCSU Network Router	Future Work

method (route R5). Each data packet sent from the source TI-mote carries its 16-bit address. The TS-7250 (or the workstation) uses this address to find out the source the data. This data is forwarded to the TS-7250 at NetWIS lab using its E-In interface and socket based TCP/IP streams over the NCSU network. Similarly the TS-7250 nodes at the NetWIS lab can send data to the TI-motes at the CESR lab over the NCSU network through any of the R1, R2 or R3 interfaces. *Thus we were able to establish a two-way communication between the prototype IEM devices (TS-7250 boards) at NetWIS lab and sensor nodes (TI-motes) at the CESR lab through the NCSU network.*

Route R6 comprises of SST controller boards (Section 3.2) interfaced with a workstation using a USB interface. This work was done in co-ordination with the DGI team. The work for route R7 (SST controller board linked to the USB on TS-7250) would be taken up in future. Table 4.1 summarizes the different routes.

4.3 SNMP-Based Monitoring Tool

In order to keep track of a distributed computing environment, there is a need of a centralized monitoring system which is able to collect vital statistics from the IEM/IFM devices. As a first step towards achieving this goal, we set up an SNMP based statistics collection system coupled with a web-based graphing solution. SNMP is an application layer protocol which is an internet protocol standard used to monitor nodes on a network [11]. There are a number of such systems in the commercial market for power utility companies [14] and such solutions have also even been proposed in literature for other systems. For example, the authors in this paper [15] propose the use of SNMP and GPRS (General Packet Radio Service) for monitoring power system controllers used in power systems for telecommunication cellular networks. The paper [16] proposes the use of SNMP for power system telecontrol. In this section, we also identify the various statistics within the FREEDM system, which could be of use for monitoring purpose.

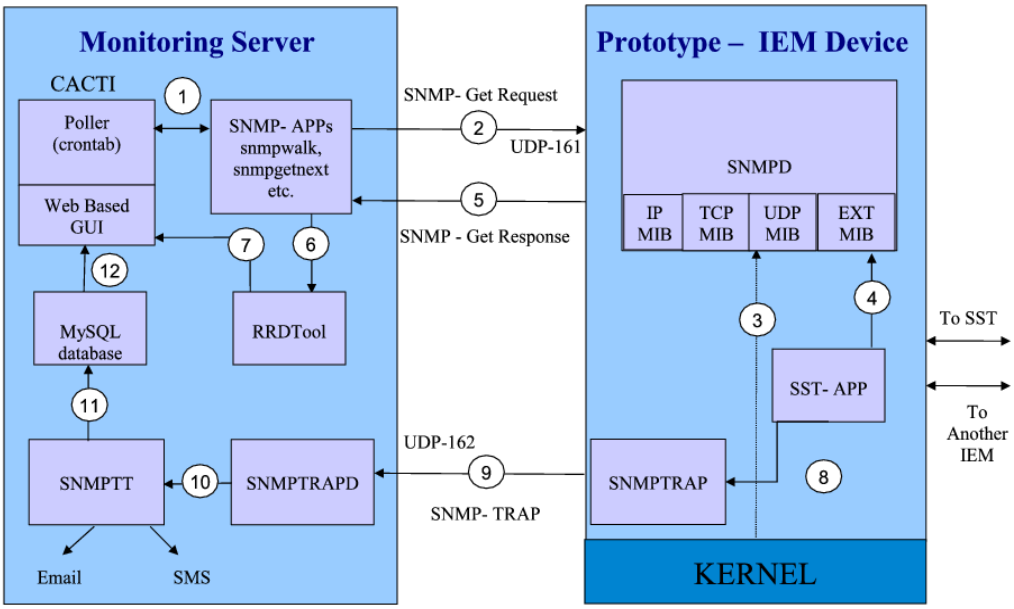

Figure 4.6: Block Diagram Of Cacti, SNMP-Based Monitoring Tool.

We have set up an SNMPv1-based statistics collection system [45] and used the Cacti tool [46] to view the statistics through a web interface. Cacti is web-based graphing solution using the RRDTool. RRDTool is the open source industry standard, a data logging

and graphing system for time series data [47].

4.3.1 Functions of the Monitoring Tool

The functioning of the complete system has been explained in Fig. 4.6. Two types of functionality have been implemented for the monitoring tool: *Periodic Polling and Trap-Handling.*

Periodic Polling

In this case, the monitoring tool polls the end nodes running the SNMP daemon periodically to retrieve pre-configured parameters. Steps 1 - 7 in the Fig. 4.6 depict the periodic operation of Cacti tool using SNMP protocol.

- **Step 1** : The Cacti tool polls the SNMP clients (prototype IEM devices) for statistics information periodically. This is done using a periodic poller. The poller is controlled by the application through a system scheduler such as 'crontab'. By default, the poller is configured to run every five minutes.

- **Step 2** : The poller uses the standard SNMP tools like *snmpgetnext* and *snmpwalk* to generate a *SNMP-GetNext* packet for the information needed by Cacti. These packets contain the Object Identifier (OID) of the variable to be read from the SNMP client. The *SNMP-GetNext* packet is received by the SNMP daemon (process) running on the SNMP client on well known UDP port 161. An example of "snmpwalk" command has been shown below.

  ```
  snmpwalk -v 1 -c mycommunity poplar.ece.ncsu.edu .1.3.6.1.4.1.2021.8
  ```

  In this example, the monitoring server executes this command to receive the SNMP related data from the "poplar.ece.ncsu.edu" node where an SNMP daemon is running. "mycommunity" is the password required by the SNMP daemon to process the "snmpwalk" command. "1.3.6.1.4.1.2021.8" is the OID or the parameter which is requested. The SNMP daemon will reply to this request with an appropriate SNMP-Response, containing the value of the OID requested.

- **Step 3** : The SNMP daemon process running on each SNMP client collects information from the system based on the variables mentioned in the *Management Informa-*

tion Base (MIB) files present on the system. The MIB file describes the structure of Management data using a hierarchial namespace containing *Object Identifiers*. For example the IP-MIB, TCP-MIB, UDP-MIB as shown in Fig. 4.6. The different variables as mentioned in MIB files are stored in variables of different data types as specified by the *Structure of Management Information (SMI)*. Related objects and variables are stored in MIB tables. The hierarchial namespace permits management across all layers of the OSI reference model. Thus the SNMP daemon can collect information from the operating system kernel of the device and also any application running on the device.

- **Step 4** : This step represents the collection of information from a test application like 'SST-APP' running on the SST controller as shown in the Fig. 4.5. As of now, the application is essentially a shell script which outputs random voltage and power values. The SNMP daemon has been configured to collect application data using the *extend* module and *exec* directive of 'snmpd.conf' file. The values from the shell script are stored in the tables whose structure is governed by the 'EXT-MIB'.

- **Step 5** : The SNMP daemon packs the information requested by the *SNMP-GetNext* packet into a *SNMP-GetResponse* packet and sends it back to the application which requested the data (*snmpwalk* or *snmpgetnext*).

- **Step 6** : The information received in the SNMP response packet is stored by the Cacti application using *Round Robin Database Tool (RRDTool)*. The RRDTool stores information in a compact manner which does not expand over time. It is also capable of performing functions such as maximum, minimum, average over the stored data.

- **Step 7** : The RRDTool has built-in graphing functions. The Cacti tool integrates this functionality into a web browser so that the graphs can be viewed from any workstation over an internet connection.

Trap-Handling

The Cacti tool can also be configured to receive SNMP traps. This will be useful to generate alarms or exceptions at the control center or a monitoring server in case of an

unlikely event (e.g., voltage sensed from the SST rising beyond a threshold). Steps 8 - 12 in Fig. 4.6 indicate the flow of this alarm capturing capability.

- **Step 8**: A test application like 'SNMP-APP' as discussed above can also be configured to generate an SNMP trap using *snmptrap* command. Using SNMP traps, any abnormal condition detected can be sent to the monitoring server immediately. This would alert a personnel at the monitoring site so that the requisite action may be taken in time.

  Step 9: The *snmptrap* command sends the information about the trap to a particular workstation on which the SNMP trap daemon (SNMPTRAPD) is running. The structure of the trap information is defined by the SMI information present in the MIB file for the trap. An example of "snmptrap" command has been shown below.

  ```
  snmptrap -v 1 -c mycommunity poplar.ece.ncsu.edu
  UCD-TRAP-TEST-MIB::demotraps.0 "" 6 17 "" SNMPv2-MIB::sysLocation.0
  "Just at poplar"
  ```

  Here an snmptrap is being sent by the node "poplar.ece.ncsu.edu" to the snmptrap server as mentioned in the configuration file. "mycommunity" is the password which is required by the snmptrap server to process the trap. "UCD-TRAP-TEST-MIB" is the MIB which specifies the structure of this trap. The remaining items are all its arguments.

  Step 10: SNMPTRAPD, is an application program which runs as the SNMP trap daemon and listens on UDP port 162 for any incoming traps. On receiving a trap, the SNMPTRAPD has been configured to send the trap information to SNMPTT daemon.

- **Step 11**: *SNMPTT (SNMP Trap Translator)* is an SNMP trap handler which is capable of displaying information obtained from SNMPTRAPD in a user friendly manner. For this setup, SNMPTT has been configured to log the SNMP trap information in *plugin_camm_snmptt* table of the 'cacti' MYSQL database.

- **Step 12**: The Cacti tool has been configured with a plugin 'Cacti Message Management' (CAMM) to read the table *plugin_camm_snmptt* table of the 'cacti' MySQL

database and display the traps in a web browser. The plugin also supports 'email-alerts' on receiving a trap.

4.3.2 Statistics

SCADA protocols can monitor only the electrical aspects of the IEM and IFM devices. However, it is also important to measure other critical aspects of the FREEDM system which are not covered by the SCADA protocols. This includes the network performance (ping latency, UDP and TCP traffic, packet losses etc.), the system performance in terms of computational capability of devices (memory usage, CPU usage etc), the temperature information from the sensors (TI-motes) and other electrical information not captured by the SCADA protocol. These critical aspects, which are vital to gauge the stability of the FREEDM system can be captured using the Cacti tool described above. They have been have been summarized below:

1. **Network Statistics:** These are the network protocol (e.g., IP, UDP, TCP and SNMP) related statistics. We use built-in SNMP MIBs to capture such information. It is critical to measure the network statistics for the following reasons.

   - To make sure that the communication interfaces and network protocols for the IEM devices are up and running.
   - To keep an eye on the network traffic at each IEM or IFM device to make sure it is below a certain threshold. This also ensures that the IEM can respond to the messages from their peers IEMs within the required timing requirements.

   As an example of a network statistic, we obtained the Ping-Latency values for one of the prototype IEM devices in NetWIS lab, Avg: 291.25 μs, Max: 919.20μs. Ping-Latency was measured from the Cacti server to the end device (TS-7250 board). The average ping latency gives an indication of average traffic in the network. The peak value indicate the maximum end-to-end delay that could occur. The graph shows a peak in ping latency of 919.20 μs between 7.30-8.00 AM in a 24hr period.

2. **System Statistics:** These are obtained for the IEM device which indicate the overall computational performance of the device (for example, CPU usage, memory usage,

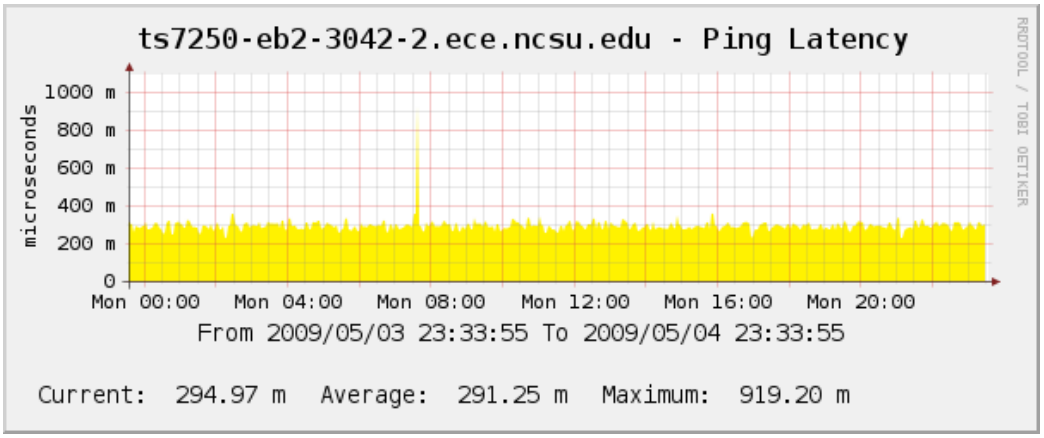

Figure 4.7: Ping Latency Of A Prototype IEM Node.

free disk space). As before we use built-in SNMP MIBs to capture this information. These statistics need to be monitored for the following reasons:

- To ensure the hardware has enough processing capability to run all the applications needed to support IEM functionality.
- To ensure the ARM boards have sufficient real and virtual memory to run the IEM applications.

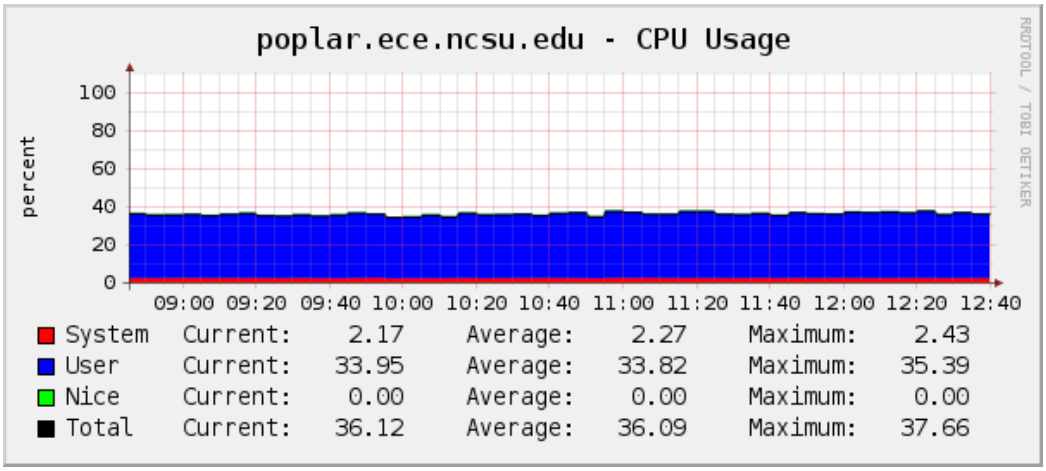

Figure 4.8: CPU Usage Of The Monitoring Server.

Fig. 4.8, shows the CPU-Usage values, for the monitoring server in the NetWIS lab. Avg: 36.09 %, Max: 37.66.3 %. The graph also differentiates between the User CPU

usage and the system CPU usage. The Max System CPU usage is 2.43%, while the Max User CPU Usage is 35.39%.

3. **TI-Mote Statistics:** The TI-Motes as shown in Fig 4.5 can also be used as temperature sensors. This will be useful to know the operating conditions of IEM or IFM devices. In our testbed, the TI-motes have been configured to send temperature information to the sink attached to a TS-7250 device. The TS-7250, in turn forwards this data to the Cacti server for remote monitoring. In our experiments, we obtained the following readings at the monitoring server (at NetWIS lab) from one of the TI-motes (in the CESR lab), Temperature Avg: 30.2'C, Max: 33'C.

4. **IEM Statistics:** These are obtained from the test application "SST-APP" running on the SST controller boards (Section 4.3. These statistics would include information about the working of the SST device and also about the IEM applications. These statistics also use NetSNMP "extend" capability to capture information from SNMP clients. An example of IEM statistics could be the normalized voltage and current readings of point of common coupling at IEM. This is the point where the IEM device is linked to the primary distribution circuit.

In this section, we described the SNMP, web-based monitor tool (Cacti) set up by us with periodic polling and trap handling capability. We also described the various statistics which are vital in determining the state of the FREEDM system from a communication perspective.

4.4 Experiments and Results

In this section, we explain the various tests carried out to measure and quantify the communication capability of the TS-7250 device. We run the tests to find out the *End-To End delay* and the *Throughput* for the TS-7250 boards. The parameters have been measured for the IEEE 802.15.4, WiFi and Ethernet interfaces for the device as mentioned in Section 4.2. The parameters in context of our experiments are defined here for clarity.

1. *End-To-End Delay (ETE):* is the total time taken by an application packet to reach from an application on one IEM prototype device to the other. We use packets of

different sizes $(16, 32, 64....4096$ bytes) to measure ETE delay. The total ETE delay can be decomposed into the following parts:

$$T_{ETE} = T_{PROC1} + T_{TX1} + T_{PROP} + T_Q + T_{TX2} + T_{PROC2}$$

where,
- T_{ETE} - Total Application packet ETE,
- T_{PROC} - Application packet processing delay at one IED,
- T_{TX} - Transmission delay at one IED,
- T_{PROP} - Propagation delay for the packet (or packets) in the medium,
- T_Q - Queuing Delay at the intermediate router or access point.

2. *Throughput:* is defined as the rate at which an application is able to transmit data from one IEM prototype device to the other. This would be useful while downloading reports or uploading configuration files to these devices. We used 5MB of data transfer to measure the throughput for tests using WiFi and Ethernet and use 1024KB for calculations with IEEE 802.15.4.

We use round-trip time to calculate the above parameters. The calculations are done in this manner to avoid any error due to the difference in the clock time of the two boards. We have taken ten readings for each test to be sure of the results. We choose to use TCP as the transport layer for our test application. This is because IEC 61850 uses TCP for MMS mappings. Before running the tests, we made sure that all the unnecessary processes which could be consuming CPU time and consuming the network bandwidth were halted. The transport layer protocol, TCP is being used with its default parameters of 1448 bytes of Maximum Segment Size (MSS). Hence any packet greater than the MSS would be segmented by the TCP layer. The experiments were also analyzed using the Wireshark packet capturing utility. We plot the average, maximum and minimum values of ETE delay to check the variability. The $log_{10} - graph$ of the ETE delay has also been plotted to examine the relation between ETE delay and byte size.

The results obtained for the various experiments have been summarized in Table 4.2. The measurements from the experiments have been detailed in Appendix F. The following experiments were performed:

1. *PC - PC communication via ethernet:* As a first test, we first measure the parameters for two Linux workstations (2.6 Ghz processor, 1.5 GB RAM, 10/100 Mbps ethernet

interface), connected via an ethernet switch (10/100 Mbps). We used CAT-6 cables to connect the devices. The PC-PC measurements were taken to test the correctness of the application program written to perform calculations and to serve as a reference when gauging the capability of the TS-7250 boards. The setup for the test is depicted in Fig. 4.9. We use two of our lab workstations, 'poplar' and 'sycamore', which are connected to an ethernet switch. The ethernet switch is in turn connected to the NCSU network. Connection to the NCSU network is important for Domain Name System (DNS) name resolution and Dynamic Host Configuration Protocol (DHCP).

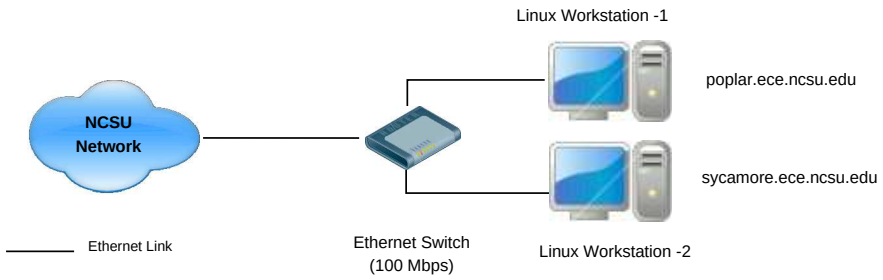

Figure 4.9: PC - PC Communication Via Ethernet.

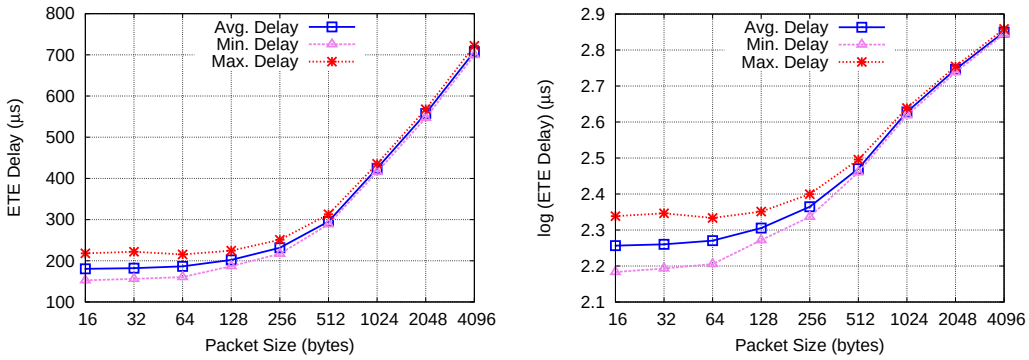

Figure 4.10: PC-PC ETE TCP/IP Ethernet Delay.

The experimental measurements of ETE delay for packet sizes of varying length are depicted in Fig. 4.10. As is shown in the graph, the ETE delay remains of the order of 200 μs for 16 - 256 byte packets, when it starts increasing. A variation in the ETE delay for a packet of particular size is also observed. For example, for a 32 byte packet, the minimum ETE delay is 156 μs and the maximum ETE delay is 222μs, which is a variation of about 66μs. It is also observed that for packets of size greater than 1024 bytes, the slope of the log-graph increases. This indicates some extra contributing

factor to the ETE delay besides the expected processing and transmission delays.

The increase in the slope of the log-graph is due to the processing required for fragmentation and re-assembly of packets with size greater than 1024 bytes by the TCP layer. Using Wireshark packet capturing utility, it was observed that the packets of size greater than 1024 bytes are fragmented before transmission over the ethernet network. This is because the default Maximum Segment Size (MSS) used for TCP is 1448 bytes (MTU - Maximum Transmission Unit for ethernet is 1500 bytes), hence packets greater than 1024 bytes (i.e. 2048 and 4096 byte packets) are fragmented to be accommodated within an ethernet MAC frame. For example, a 4096 byte packet is fragmented into 1448, 1448 and 1200 byte packets.

2. *TS7250 - TS7250 communication via Ethernet:* For this test, we use TS-7250 boards as prototype IEM devices to take the measurements. The boards were connected using a 100 Mbps switch and CAT-6 cables. The setup for the test is depicted in Fig. 4.11. The experimental measurements for ETE delay for packet sizes of varying length are depicted in Fig. 4.12. The graph shows a marked increase in ETE delay for the same packet size when compared to Experiment-1. This can be attributed to the low processing capability of the TS-7250 device.

   The ETE delay follows a similar pattern as in Experiment-1, with an increase in slope of the log-graph for packet sizes greater then 1024 bytes. The ETE delay ranges from 750 μs for a 16 byte packet to 1.6 ms for a 4096 byte packet. Variation is observed in the ETE delay for a packet of particular size.

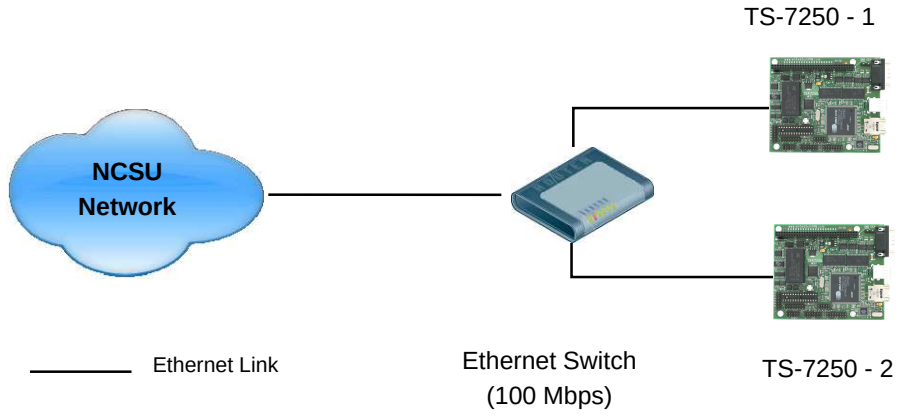

Figure 4.11: TS7250 - TS7250 Communication Via Ethernet.

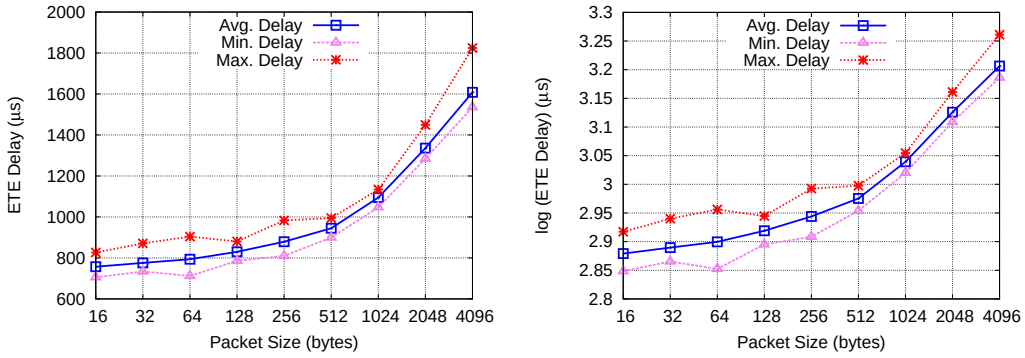

Figure 4.12: TS7250 - TS7250 ETE TCP/IP Ethernet Delay.

3. *TS7250 - TS7250 communication via WiFi:* For this test, we connect the IOGEAR WiFi dongles with the USB interface on the TS-7250 boards. The WiFi dongles have been configured to connect to a Cisco (IEEE 802.11 b) WiFi access point. The maximum physical data rate supported by IEEE 802.11b is 11Mbps. The setup for the test is depicted in Fig. 4.13. The experimental measurements of ETE delay for packet sizes of varying length are depicted in Fig. 4.14. The ETE delay ranges from 3.2 ms for a 16 byte packet to 16.66 ms for a 4096 byte packet. As expected, there is an increase in the average ETE delay for a packet of particular size, when compared with Experiment-1 and Experiment-2. From the log-graph, it can be observed that the slope of the ETE delay as in previous cases increases for data packets of size greater than 1024 bytes. This trend can be attributed to the default segment size of the TCP protocol.

   It should be noted that the IEEE 802.11 standard allows a maximum data frame of size 2304 bytes at the MAC layer (or a maximum of 2304 - (20 + 20) = 2964 bytes of application layer packet). Hence improvements in delay and throughput can be attained by increasing the default MSS of TCP for WiFi. Moreover, we are using a IEEE 802.11b compliant access point, however the WiFi dongle supports IEEE 802.11g (max physical layer data rate 54 Mbps). Hence, further improvements in delay and throughput can be made by using an IEEE 802.11g compliant access point.

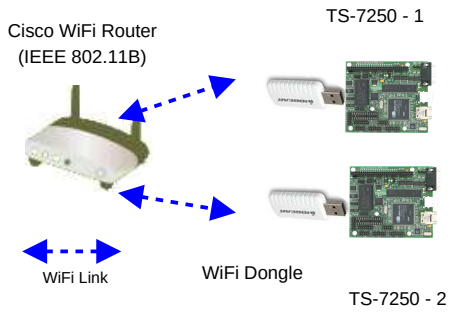

Figure 4.13: TS7250 - TS7250 Communication Via WiFi.

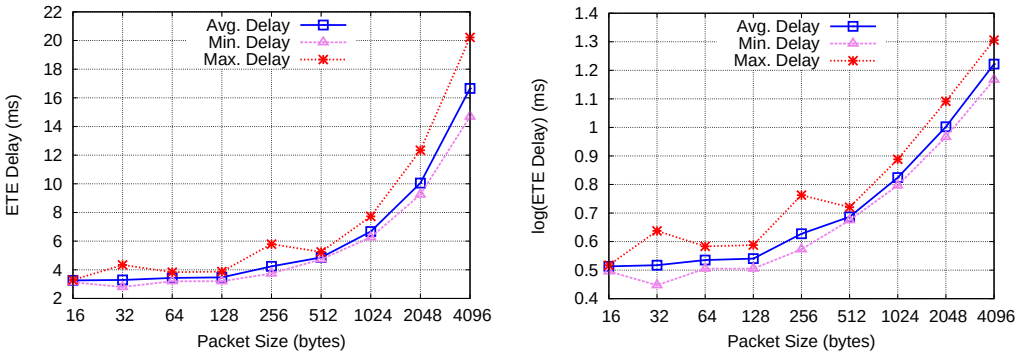

Figure 4.14: TS7250 - TS7250 ETE TCP/IP WiFi Delay.

4. *TS7250 - TS7250 communication via IEEE 802.15.4:* For this test, we set up a Personal Area Network (PAN) using a Xbee-Pro device and a TS-7250 board, with a Ethernet - IEEE 802.15.4 gateway acting as a network co-ordinator. The serial link between the TS-7250 board and the Xbee-Pro board is configured at 115200 baud. The setup for the test is depicted in Fig. 4.15. For the IEEE 802.15.4 link, we took measurements till only 512 byte packet sizes, as the ETE delay got very large ($>$ 100ms) beyond this point. The throughput was measured for 1024 bytes of data exchange. In order to see, how the ETE delay and throughput scale with distance, we took measurements at 1m, 42m and 96m line of sight distance between the TS-7250 board (with the Xbee-Pro interface) and the gateway.

   The experimental measurements of ETE delay for packet sizes of varying length are depicted in Fig. 4.16. The ETE delay ranges from 11.61 ms for a 16 byte packet to 86.11 ms for a 512 byte packet when the devices are in close range of less than a meter. It is observed that the slope of the log-graph for ETE delay is constant unlike

the previous cases. It is also observed that the ETE delay increases as the distance between the TS7250 and the gateway is increased from 1m to 96m. For example, the average ETE delay for a 512 byte packet at 1m distance from the gateway is 86.11 ms and at 96m is 95.04 ms, which is a 10.3 % increase. This can be attributed to the increased interference and decreased receiver power with the longer path.

It should be noted that the Xbee-Pro module has a different way than TCP to deal with larger packet sizes. The data fed to the Xbee-Pro module (through the serial interface with the TS-7250 device) is stored in a DI buffer. The buffer transmits the data through the RF interface either if no data arrives from TS-7250 for 3 character times, or if the total number of characters received is 100. Thus packets of size greater than 64 bytes are broken down into packets of size 100 bytes or less. The fragmentation is necessary as, the maximum payload allowed by the MAC layer of IEEE 802.15.4 is 102 bytes.

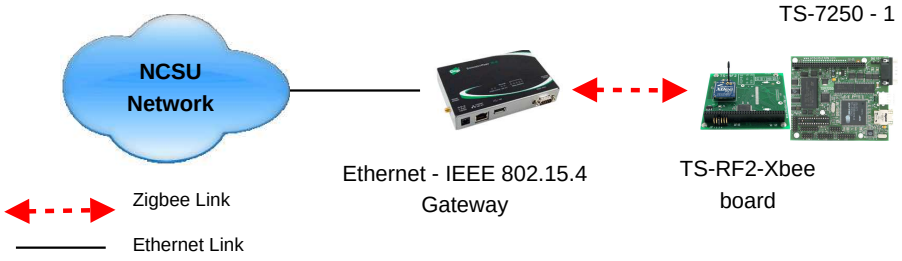

Figure 4.15: TS7250 - TS7250 Communication Via IEEE 802.15.4.

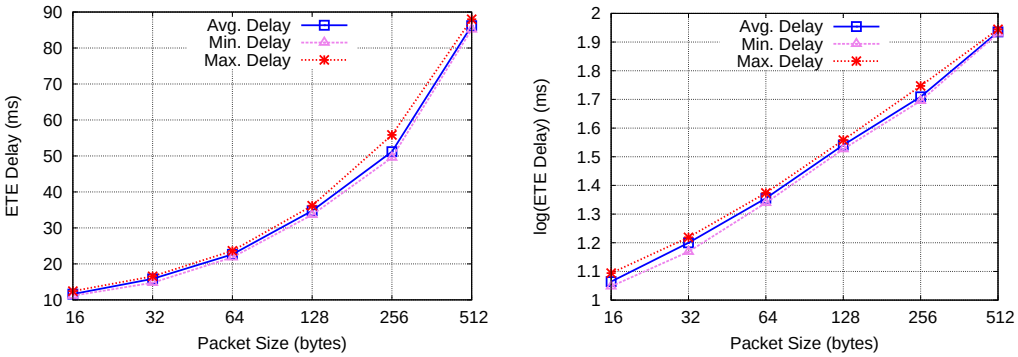

Figure 4.16: TS7250 - Xbee Gateway ETE IEEE 802.15.4 Delay.

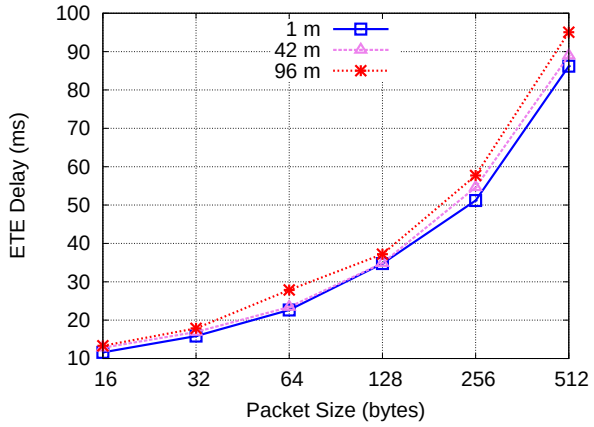

Figure 4.17: TS7250 - Xbee Gateway ETE IEEE 802.15.4 Delay vs Distance.

5. *PC - TS7250 communication via IEEE 802.15.4 - Ethernet Gateway:* This test was carried out to measure the capability of the IEEE 802.15.4 - Ethernet gateway to perform IEEE 802.15.4 - IEEE 802.3 protocol conversion and send packets from the Xbee Pro device (connected to TS-7250 boards) to a Linux workstation connected to the ethernet interface of the gateway and vice versa. The setup for the test is depicted in Fig. 4.18. The experimental measurements of ETE delay for packet sizes of varying length are depicted in Fig. 4.19. As expected, the ETE delay is higher in this case than Experiment - 4. This is because of the additional time taken for protocol conversion and the transmission, propagation delay added by the Ethernet medium. The ETE delay ranges from 31.5 ms for a 16 byte packet to 173.15 ms for a 512 byte packet when the gateway and the Xbee-Pro devices are in close range of less than a meter.

   The increase in the slope of the log-graph of ETE delay for data packets of size greater than 64 bytes can be attributed to the fragmentation of the packets as explained for Experiment -4. Thus the multiple packets are generated for packets of size greater than 64 bytes. These traverse the IEEE 802.15.4 interface and then the ethernet interface to reach their destination and follow the same way back.

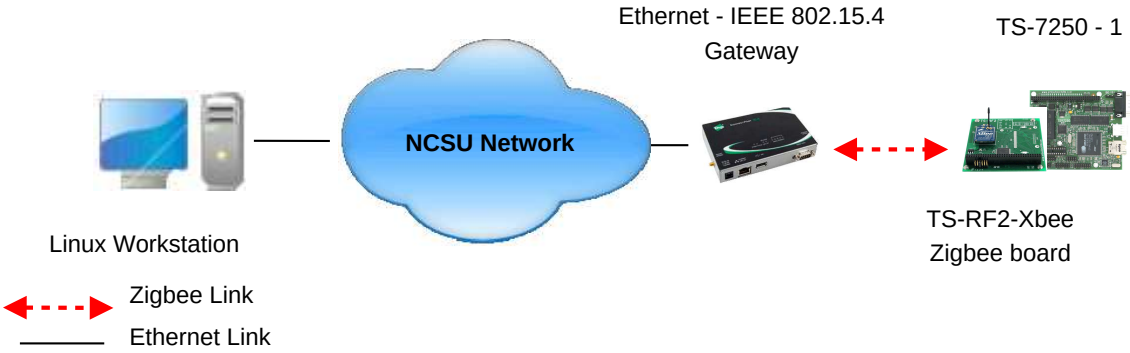

Figure 4.18: PC - TS7250 Communication Via IEEE 802.15.4 - Ethernet Gateway.

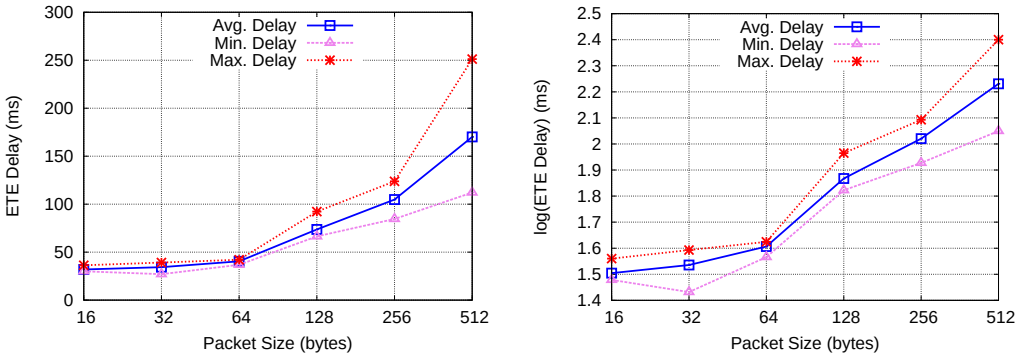

Figure 4.19: TS7250 - PC ETE Delay Over IEEE 802.15.4 And Ethernet Interface.

Table 4.2: Average ETE Delay And Throughput Summary Of Experiments.

Test No.	**Test Description**	**Avg ETE Delay (ms) (for 512 byte pkt)**	**Throughput**
1	PC - PC via Ethernet	0.29	93.93 Mbps
2	TS7250 - TS7250 via Ethernet	0.94	18.84 Mbps
3	TS7250 - TS7250 via IEEE 802.11b	4.8	2.6 Mbps
4	TS7250 - TS7250 via IEEE 802.15.4	86.2	53.97 Kbps
5	TS7250 - PC via Gateway	170.14	25.88 Kbps

4.5 Lessons Learnt

In Section 4.4, we tested the WiFi and IEEE 802.15.4 technologies for throughput and ETE delay as a part of our year-1 effort towards the architecture of a communica-

tion backbone for the FREEDM system. This section discusses the inference from our experimental work. As we draw inference, we keep in mind our goal of Wide–Area and Local–Arear Communication (as discussed in Section 3.2) in the FREEDM system, which is essentially an improved electricity distribution system. We also take into consideration the "High" timing requirement of protection information as discussed in Section 2.1.2 which is 2 - 10 ms for use inside a substation automation system and 8 - 12 ms when external to a substation. As discussed in Section 3.4, these requirements would be expected to be less strict for the FREEDM system because of the physical scale of the system (spread along the electric distribution feeder in a particular region). *For now, we take 3 ms as our target which is the timing requirement for the "Type 1A Fast trip" messages for priority class P2 and P3* (refer Section 2.2.2).

Our year-1 experimental testbed does not provide a complete solution to the communication problem in the FREEDM system. However, we consider it to be a stepping stone towards achieving our goal. From the study of WiFi technology, it appears that the traditional WiFi devices have a lower range of about 140 m outdoors. Typical Electricity Distribution networks in cities are spread over a few miles. The low range of WiFi infrastructure networks will make it unsuitable for Wide–Area Level Communication in the FREEDM system. However, the ETE delay measured using WiFi IEEE 802.11 b is 4.8 ms for a 512 byte packet. This is quite close to our target. *Hence, we conclude that advances in WiFi technology like the Wireless Mesh networks and improved range devices should be investigated for their suitability to support the communication backbone of the FREEDM system.*

From experiments with IEEE 802.15.4, it is evident that the ETE for a 512 byte packet at 86.2 ms is the highest and the throughput is the lowest at 53.97 Kbps. The advertised range of the product we tested is 1 mile and we tested the ETE delay degradation to be 10.3 % at 96 m of distance. The Zigbee technology, even though may be able to increase the range further by its networking capabilities, the one-hop throughput is expected to be still lower due to additional processing and increased packet size. *Hence, we conclude that IEEE 802.15.4 or Zigbee are unsuitable to meet the needs of Wide–Area Level Communication in the FREEDM system. However it would be an ideal candidate to support Local-Area Level Communication to support use cases like plug-in electric vehicle (PEV) charging, demand response, load control etc.* The "Smart Energy Profile" requirements document [48]

prepared by Zigbee Alliance and the HomePlug Powerline Alliance details the use of ZigBee for the above mentioned use cases.

From our experiments with different packet sizes and different networking technologies, we conclude that it is advisable to use application packet sizes less than 1448 bytes while using the ethernet medium to transfer critical time sensitive messages. Similarly for WiFi packet sizes less than 1448 bytes (when used along with an Ethernet medium) or 2964 bytes (when the end node is a WiFi node with no intermediate Ethernet medium) would yield lower ETE delays. For IEEE 802.15.4 the same limit is 102 bytes.

Analysis of the networking technologies and the hardware platform using the test bed to realize the FREEDM communication backbone revealed a lot of implementation issues and leanings for the future. These are discussed below:

- It was observed that the computational capability of the board affected the communication capability and hence the measurements. The ETE delay observed using the TS-7250 boards communicating via Ethernet medium, was lower than the delay observed when using Linux workstations for the experiment. This suggests that a faster communication board (high processing capability) could be a way to improve the ETE delay.

- The timing resolution of the TS-7250 board was only 10ms in its default operating system. This was improved to microsecond precision with assistance from other members of the RSC subthrust.

- We used IEEE 802.11b access point for our experiment. Using an IEEE 802.11g access point will improve the ETE delay and throughput.

- For WiFi, improvements can also be made by increasing the default MSS of TCP (1448 bytes) as the IEEE 802.11 standard allows for a maximum of 2304 bytes frame at the MAC layer.

- The range of Zigbee can vary depending on the antenna used. For our experiments, we used long range antennas and got a range which goes beyond 96 m using our Xbee boards and the gateway. However, the TI-motes which use a smaller antenna have a lower range of about 10 m.

- For our experiments, we used Xbee boards which were purchased from the same vendor as the TS-7250 ARM boards for compatibility issues. These boards are IEEE 802.15.4 compliant and do not have any of the networking capabilities of the Zigbee stack. We can have the advantage of enhanced range if we use Zigbee.

In this Chapter, we discussed the RSC Communication testbed set up by us to quantify the ETE delays which are possible using Ethernet, WiFi and IEEE 802.15.4 communication technologies. We also presented a SNMP, web-based network monitoring tool to keep track of the distributed devices. The inference from the experiments and implementation issues have also been described. This concludes our work for this thesis. We present an overall conclusion from our work in the following section and give a road map for our future works.

Chapter 5

Conclusions and Future Work

Throughout the course of this thesis, our goal has been to understand the needs of the FREEDM project, study the existing state of art systems and find solutions for the communication challenges facing the FREEDM system. In this section we summarize the work done in this thesis.

5.1 Conclusions

The present times are a beginning of a new era for the power systems. The FREEDM vision of integration of the renewable resources of energy into the existing distribution grid, will revolutionize the power systems grid, making it an internet of energy. However, this poses a lot of new challenges like the communication architecture of the system, the communication protocols, the requirements of time sensitive applications and the various networking technologies to be used to support the backbone. We have reached the following conclusions regarding these questions from our current work. We also brief our reasoning for the conclusions.

- **Communication Protocols for FREEDM:** As a first step in this thesis, we study existing communication protocols (DNP3 and IEC 61850) and communication functionality (SCADA and Substation Automation systems). IEC61850 uses advanced modeling techniques to represent logical devices, services and corresponding data used in substation automation systems, with a clear separation between the logical models/services and the actual protocols used to carry the data. The same techniques

are being used and logical nodes for newer systems are being defined (Section 2.2.4). The power industry is harmonizing its efforts to have a single standard based on IEC 61850 for all the communication needs of the electricity supply chain. Talking about DNP3, as discussed in Section 2.2.1, it is an efficient and a robust protocol which has been adapted to work over IP based networks. It even has provisions to provide security. The DNP3 protocol, continues to be used for SCADA systems. At the same time, the newer IEC 61850 extensions (e.g IEC 61400-25) are using DNP3 protocol to carry the data specified by their logical nodes. Although, at present, work is going on to develop the IEEE standard P2030 for interoperability in SmartGrids, however, because of its features, IEC 61850 is a strong contender to serve as the initial smart grid interoperability standard for SmartGrids. *Hence, it is logical to deploy IEC 61850 and its extensions to meet the Local–Area Communication, Wide–Area Communication and Substation Level Communication needs of the FREEDM system.*

- **Communication Architecture and Timing Criticality:** The communication architecture of the FREEDM system has been detailed in this thesis (Section 3.2). We describe the communication functionality in IFM and IEM devices. The applications running on these devices can be classified into different levels as Wide–Area Level communication, Local–Area Level communication or Substation–Level Communication. Different communication technology will be required for Wide–Area level and Local–Area level communication. One of the main contributions of this thesis is to underscore the timing criticality of the applications to be used in the FREEDM system, identify various communication interfaces and categorize them according to the timing criticality of the applications using the interface (detailed in Section 3.4). We use 3 ms as our target for ETE delay which is the timing requirement for the trip message in SA systems.

  The exact communication structure and layout of the system has not been described, as we are still in the process of experimenting with different networking technologies.

- **A Hardware Platform for FREEDM:** One of the other achievements of the thesis is the establishment of the communication hardware platform for the FREEDM

system i.e. the TS-7250 ARM boards. This is very crucial for the project, as the time sensitive communication protocols are going to run on this hardware platform. While deciding the communication platform, a lot of factors were considered. Processing and memory requirements of IEC 61850 from protocol stack manufactures, support for WiFi, Zigbee and Ethernet communication interfaces, open source platform are some of these. Similarly, the other products like the Zigbee Gateway, the Xbee boards, were considered and bought after careful deliberation.

- **Communication Technologies:** We were able to make the communication board (TS7250) and the communication interfaces (Ethernet, WiFi and IEEE802.15.4) fully functional. We were also able to establish IED-IED communication between the CESR and the NetWis lab. The experiments performed by us using the testbed give us useful insights into the capabilities of the TS-7250 ARM boards and the WiFi and the Zigbee communication technologies. It was observed that the Zigbee gave us a low throughput and good range, whereas the WiFi had a good throughput and a relatively low range. For the FREEDM system we would need good range and good throughput. Hence these technologies alone cannot be used for Wide–Area Level Communication in the FREEDM system. We need to look at other technologies like the 3G Cellular or the Long range Wireless Mesh for this purpose. Zigbee is an ideal candidate for Local–Area Level Communication e.g., for PEV or PHEV vehicles or for implementing demand response in households.

- **SNMP-Based Monitoring Tool for FREEDM:** The SCADA protocols are used to measure the state of the electrical devices from a remote location. It is equally important to monitor other aspects of a device such as the network and system statistics as discussed in Section 4.3. SNMP is a standardized internet protocol for this purpose. More over, there is a drive in the power utility industry to integrate the SCADA and SNMP systems based on IEC 61850-7 standard. However, as of now both the systems continue to co-exit. The Web-Based SNMP tool - Cacti, is useful to monitor the state of all the devices from one location. This will be very useful, once the scale of the testbed increases and can present the real time state of the IEM/IFM devices present all along the electricity distribution network. This can be further improved by adding some network visualization and security features.

The research in this thesis represents our year-1 efforts towards a complete reliable and secure solution to the FREEDM communication problem, we believe that our preliminary results have provided a fundamental platform to study unique challenges in the future design and development of a reliable and secure FREEDM system.

5.2 Future Work

During the course of our research work we came across a lot of issues which we could not focus on and we intend to pursue them as future work. We intend to extend our work in future in the following directions.

- When we started off with the FREEDM project, our main objectives were to analyze the performance of DNP3 and IEC-61850 protocol standards.

  However, as we learnt more about the project, we realized the importance of IEC 61850 protocol standard and shifted our focus towards it. IEC 61850 protocol, though its an open standard, its not an open source protocol. Thus we had to approach a lot of protocol vendors like Triangle Microworks, Kalkitech and Sisconet and obtain the details of their products and negotiate with them for the IEC-61850 protocol. This process is still on and we are in talks with Kalkitech to obtain the IEC61850 software stack.

  Thus, the realistic measurements in various IEM scenarios using IEC-61850 is a part of our future work.

- Analyze and test other communication technologies like 3G-Cellular and Wireless Mesh, which could be used for Wide–Area Level communication. A lot of factors need to be considered before a technology is adopted for the communication backbone of the FREEDM project. E.g., throughput, QoS support, licensed or unlicensed band operation, security support, open source or proprietary communication technology, operational costs etc.

- Assessing the reliability and security needs of the FREEDM communication architecture. We need to analyze the possible communication related faults in the FREEDM system to improve the system reliability. Security protocols will be used at various

layers to secure the FREEDM system. We will need to analyze and quantify the impact of these security protocols over system performance, especially for time sensitive applications like fault protection.

- Adding security to the monitoring system i.e. using SNMPV3 which adds security features to the SNMP protocol standard like message integrity, authentication and encryption of packets. As the wireless medium is shared, adding security to SNMP is a must.

Bibliography

[1] U.S. Energy Independence and Security Act of 2007. http://www.thomas.gov/cgi-bin/query/z?c110:H.R.6.ENR:, 2007.

[2] Energy Information Administration. Annual Energy Outlook 2009 with Projections to 2030. http://www.eia.doe.gov/oiaf/aeo/electricity.html, 03 2009. Report, DOE/EIA-0383(2009).

[3] IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems. "http://ieeexplore.ieee.org/servlet/opac?punumber=8676".

[4] C. Marnay and G. Venkataramanan. Microgrids in the evolving electricity generation and delivery infrastructure. In *Power Engineering Society General Meeting, 2006. IEEE*, pages 5 pp.–, 0-0 2006.

[5] C.J. Mozina. Impact of green power generation on distribution systems. In *Rural Electric Power Conference, 2009. REPC '09. IEEE*, pages A3–A3–8, April 2009.

[6] Subhashish Bhattacharya, Tiefu Zhao, Gangyao Wang, Sumit Dutta, Seunghun Baek, Yu Du, Babak Parkhideh, Xiaohu Zhou, and Alex Q. Huang. Design and Development of Gen-1 Silicon based Solid State Transformer. In *Proceedings of the FREEDM systems center Annual Conference 2009*, 05 2009.

[7] L. D. Kannberg, M. C. Kintner-Meyer, D. P. Chassin, R. G. Pratt, J. G. DeSteese, L. A. Schienbein, S. G. Hauser, and W. M. Warwick. GridWise: The Benefits of a Transformed Energy System. Technical report, Pacific Northwest National Laboratory under contract with the United States Department of Energy, 11 2003. http://www.pnl.gov/main/publications/external/technical_reports/PNNL-14396.pdf.

[8] Smartgrids Advisory Council. Driving Factors in the Move Towards SmartGrids. http://www.smartgrids.eu/documents/vision.pdf, 2006. European Smartgrids Technology Platform: Vision and Strategy. European Commission.

[9] IEEE P2030 Inagural working group meeting. http://grouper.ieee.org/groups/scc21/2030/docs/P2030-20090603-AM-SLIDES.pdf, 06 2009.

[10] Zhenhua Jiang. Agent-Based Control Framework for Distributed Energy Resources Microgrids. pages 646–652, Dec. 2006.

[11] J.D. Case, M. Fedor, M.L. Schoffstall, and J. Davin. RFC-1157, Simple Network Management Protocol (SNMP). http://www.rfc-editor.org/rfc/rfc1157.txt, May 1990.

[12] Bharadwaj R. Sathyanarayana, Gerald T. Heydt, Mariesa Crow, and Fanjun Meng. Test Bed Evaluation of Future Power Distribution Systems with Renewable Resources for the FREEDM System. In *Proceedings of the FREEDM systems center Annual Conference 2009*, 05 2009.

[13] IEEE P2030 Smart Grid Interoperability Task Force 3: Information Technology. http://grouper.ieee.org/groups/scc21/2030/TF3.html, 2009.

[14] DPS Telecom. NetGuardian 832A G5: High Capacity SNMPv3 Alarm Collector. "http://www.dpstele.com/products/ne/netguardian_g5/".

[15] Rotharmel S. IP based telecom power system monitoring solution in GPRS networks. pages 769–774, 30 2007-Oct. 4 2007.

[16] S. Diaz, J. Luque, M.C. Romero, and J.I. Escudero. Power systems monitoring and control using Telecom network management standards. *Power Delivery, IEEE Transactions on*, 20(2):1349–1356, April 2005.

[17] Ericsson G. Communication utilization in power system control. A state-of-the-practice description. *Power Delivery, IEEE Transactions on*, 13(4):984–989, Oct 1998.

[18] Ericsson G. N. Classifilcation of Power Systems Communications Needs and Requirements: Experiences from Case Studies at Swedish National Grid. *Power Engineering Review, IEEE*, 22(2):61–61, Feb. 2002.

[19] J. Hauer, D. Trudnowski, G. Rogers, B. Mittelstadt, W. Litzenberger, and J. Johnson. Keeping an eye on power system dynamics. *Computer Applications in Power, IEEE*, 10(4):50–54, Oct 1997.

[20] A.-R. Khatib, Zuzhu Dong, Bin Qiu, and Yilu Liu. Thoughts on future Internet based power system information network architecture. In *Power Engineering Society Summer Meeting, 2000. IEEE*, volume 1, pages 155–160 vol. 1, 2000.

[21] M. Adamiak and W. Premerlani. The role of utility communications in a deregulated environment. In *System Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on*, volume Track3, pages 6 pp.–, 1999.

[22] The automation of new and existing substations: why and how. Technical report, International Council on Large Electric Systems, 08 2003. Sponsored by the CIGRE Study Committee B5, `www.grouper.ieee.org/groups/1525/CIGRE34.07/Document/Final%20Report%20r2.doc`.

[23] IEEE Standard 1646 for Communication Delivery Time Performance Requirements for Electric Power Substation Automation. `"http://standards.ieee.org/reading/ieee/std_public/new_desc/subst/1646-2004.html"`.

[24] DNP3 - Distributed Network Protocol User Group. `http://www.dnp.org/`.

[25] Malcolm Smith and Jim McFadyen. DNP3 Product Documentation Library V 3.0. Technical report, DNP3 Executive Committee, 3 2004.

[26] International Electrotechnical Commission. Communication networks and systems in substations Part 1: Introduction and overview. `http://webstore.iec.ch/`.

[27] Karlheinz Schwarz. IEC 61850 outside the substation for the whole electrical power system. `http://www.montefiore.ulg.ac.be/services/stochastic/pscc05/papers/fp678.pdf`, 08 2005. Power Systems Computation Conference.

[28] OpenAMI Task Force. `http://osgug.ucaiug.org/OpenAMI/default.aspx`.

[29] Future Renewable Electrical Energy Distribution and Management (FREEDM). `"http://www.freedm.ncsu.edu/"`.

[30] R.A.F. Currie, G.W. Ault, C.E.T. Foote, G.M. Burt, and J.R. McDonald. Fundamental research challenges for active management of distribution networks with high levels of renewable generation. In *Universities Power Engineering Conference, 2004. UPEC 2004. 39th International*, volume 3, pages 1024–1028 vol. 2, Sept. 2004.

[31] Strbac G., Jenkins N., Hird. M., Djapic P., and Nicholson G. Integration of operation of embedded generation and distribution networks. Technical report, 2002.

[32] Balasubramanya Bhat and Frank Mueller. FREEDM Software Controller Architecture for a Solid State Transformer. In *Proceedings of the FREEDM systems center Annual Conference 2009*, May 2009.

[33] Preetika Kulshrestha, Kaushik Swaminathan, Mo-Yuen Chow, and Srdjan Lukic. Evaluation of ZigBee Communication Platform for Controlling the Charging of PHEVs at a Municipal Parking Deck. In *FREEDM SYSTEMS CENTER ANNUAL CONFERENCE*, May 2009.

[34] Jerry Melcher Mark Adamiak, Ron Patterson. Inter and Intra Substation Communications: Requirements and Solutions.

[35] I.F. Akyildiz and Xudong Wang. A survey on wireless mesh networks. *Communications Magazine, IEEE*, 43(9):S23–S30, Sept. 2005.

[36] V. Skendzic and A. Guzma. Enhancing Power System Automation Through the Use of Real-Time Ethernet. In *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006. PS '06*, pages 480–495, March 2006.

[37] A. Apostolov and B. Vandiver. Functional testing of IEC 61850 based IEDs and systems. In *Power Systems Conference and Exposition, 2004. IEEE PES*, pages 640–645 vol.2, Oct. 2004.

[38] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pages C1–1184, 12 2007.

[39] IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pages 1 – 305, 2006.

[40] ZigBee Alliance. `http://www.zigbee.org/`.

[41] Technological Systems. TS-7250, Single Board Computer. `"http://www.embeddedarm.com/documentation/ts-7250-manual.pdf"`.

[42] Technological Systems. TS-RF2-ZIGBEE, Zigbee compatible wireless radio. `"http://www.embeddedarm.com/products/board-detail.php?product=TS-RF2-ZIGBEE"`.

[43] DIGI. Zigbee-Ethernet Gateway. `"http://www.digi.com/products/"`.

[44] Texas Instruments. Z-Accel Demonstration Kit. `"http://focus.ti.com/docs/toolsw/folders/print/ez430-rf2480.html"`.

[45] Net-SNMP. Open Source Implementation of SNMP (Simple Network Management Protocol). `"http://www.net-snmp.org/"`.

[46] CACTI - RRDTool based network graphing Solution. `"http://www.cacti.net/downloads/docs/pdf/manual.pdf"`.

[47] RRDTool - OpenSource industry standard for high performance data logging and a graphing system for time series data. `"http://oss.oetiker.ch/rrdtool/"`.

[48] HomePlug Allinace ZigBee Alliance. ZigBee+HomePlug Smart Energy marketing requirements document. `http://www.zigbee.org/LinkClick.aspx?link=449&tabid=431`, March 09.

Appendices

APPENDIX A: Acronyms

DESD Distributed Energy Storage Device

DHCP Dynamic Host Configuration Protocol

DRER Distributed Renewable Energy Resource

DESD Distributed Energy Storage Device

DGI Distributed Grid Intelligence

DNS Domain Name System

IEM Intelligent Energy Management

IFM Intelligent Fault Management

DNP3 Distributed Network Protocol

ETE End-To-End Delay

FREEDM Future Renewable Electrical Energy Distribution and Management

MSS Maximum Segment Size

PEV Plug-in Electric Vehicle

RSC Reliable and Secure Communication

SA Substation Automation

SCADA Supervisory Data Acquisition and Control

SNMP Simple Networking Management Protocol

APPENDIX B: Testbed Device Specifications

The following are the major devices which are a part of the RSC Backbone testbed.

1. **TS-7250 Single Board Embedded Computers:** These are single board embedded boards manufactured by Technologic Systems [41]. These devices have the following specifications.

   - 200MHz ARM9 CPU
   - PC/104 expansion bus
   - 64MB SDRAM
   - 128MB FLASH
   - 1 10/100 Ethernet port
   - 2 USB 2.0 (12 Mbit/s max)
   - 2 COM ports
   - 20 DIO lines
   - 5 12-bit ADC
   - Watchdog timer, SPI bus
   - WiFi, Zigbee support,
   - Redboot bootloader, Linux out-of-the-box
   - Temp Sensor, Real Time Clock

2. **TS-RF2-ZIGBEE:** These are Zigbee compatible PC/104 Peripheral Boards that provide an IEEE 802.15.4 long-range wireless interface to the TS-7250 boards [42]. These devices have the following specifications.

   - XBee-PRO, IEEE 802.15.4 compliant OEM RF Module from Digi.
   - 250 kbps RF data rate
   - 2.4 GHz operating frequency
   - Upto 1 mile range (line of sight)
   - Suitable for point-to-multipoint/peer-to-peer networking

- Transparent radio interface via serial port
- Supports 128-bit AES encryption

3. **ConnectPort X4 Zigbee-Ethernet Gateway:** The gateway provides direct communication with end nodes forming a PAN to an application running over an IP ethernet network. These have the following features and specifications.

   - Acts as a Networking Co-ordinator for a IEEE 802.15.4 compliant network.
   - Ethernet port to connect with applications over an IP network.
   - Python development environment.
   - Support for network protocols UDP/TCP, DHCP.
   - IPsec and SSL VPNs over WAN connections.
   - Real time clock.
   - HTTP/HTTPS web interface.

APPENDIX C: Components of Power Systems

Power systems mainly consist of three major components. These are the Generation, Distribution and Transmission. These components have been described briefly below.

1. **Generation:** Power Generation is the process of producing electricity from a resource such as coal, gas, petroleum, water flow, uranium etc. In most of these cases, a turbine is used to extract the energy of the resource into rotational energy of the turbine. This turbine is generally coupled with an AC generator to convert the rotational energy of the turbine into electrical energy. The operating cost of generating electricity is determined by the fuel cost and the efficiency of the power station. Power generation plants deploy sophisticated protection, control and monitoring techniques to maintain the stability of the generators and avoid network faults and overloading.

2. **Transmission:** Power transmission is the process of transferring generated power at high voltage using transmission lines to the locations where it is needed. The voltages are kept high to minimize the power losses due to transmission. A lot of transmission substations form the part of a transmission network. Protection schemes for transmission networks are more complex as the faults on the long transmission lines may not be discernable due to high reactance on these lines.

3. **Distribution:** Power distribution, is the process of distributing the power received from a number generating power plants over long transmission lines to the loads. Power distribution stations are located near to the points of power consumption. The high voltage electricity received from the transmission lines is converted to a lower voltage for distribution. The insulation properties of the three phase cables used to distribute power makes the usage of lower voltages, economical over short distances.

   The high voltage distribution substations have high voltage switch gear and power transformers. Substation automation techniques are deployed to protect and control these expensive and critical equipment to avoid any blackouts.

APPENDIX D: NIST-Recognized Standards for SmartGrid Interoperability

Standard	**Application**
AMI-SEC SystemSecurity Requirements	Advanced Metering Infrastructure (AMI) and Smart Grid end-to-end security
ANSIC12.19/MC1219	Revenue metering information model
BACnet ANSI ASHRAE 135-2008/ISO16484 − 5	Building Automation
DNP3	Substation and feeder device automation
IEC60870-6/TASE.2	Inter-control center communications
IEC61850	Substation automation and protection
IEC61968/61970	Application level energy managementsystem interfaces
IEC62351Parts1-8	Information security for power system control operations
IEEEC37.118	Phasor measurement unit (PMU) communications
IEEE1547	Physical and electrical interconnections between utility and distributed generations(DG)
IEEE1686-2007	Security for intelligent electronic devices (IEDs)
NERC IP 002-009	Cyber security standards for the bulk power system
NIST Special Publication (SP) 800- 53, NIST SP 800-82	Cyber security standards and guidelines for federal information systems, including those for the bulk power system Open Automated Demand Response (Open ADR) Price responsive and direct load control
OpenHAN	Home Area Network device communication, measurement, and control
ZigBee/HomePlug Smart Energy Profile	Home Area Network (HAN) Device Communications and Information Model

APPENDIX E: Example of Timing Requirements for Smart-Grid Systems

The following table gives an example of Timing Requirements for communication between distributed renewable sources of energy as suggested by Siemens.

Expected Timing Requirements For DERs

Application	**Expected Timing Requirement**
Control with return Information	2 s
Target Value (P, Q)	2 s
Alarm	1 s
Status Information	5 s
Metered Value	2 s
Measured Value	2 s
Target Profile P, Q (96 Values)	20 s
Parameter Setting	10 s
Fault Record	1 minute

As is evident from the table, even the minimum of the values are in range of seconds. This is expected because the communication between IEDs controlling the DER resources would take place over a Wide–Area Network. However, different applications still have different timing requirements with the Alarm functionality having maximum timing requirement of 1 sec and fault recording functionality having timing requirement of about 1 min.

APPENDIX F: Measurements From Experiments

Measurements of Average End-To-End Delay (μs) for PC-PC Communication via Ethernet

Bytes	**16**	**32**	**64**	**128**	**256**	**512**	**1024**	**2048**	**4096**
1	332	379	362	392	463	599	836	1136	1440
2	344	312	333	406	456	580	841	1111	1419
3	343	366	367	374	460	577	831	1113	1404
4	341	328	321	405	442	626	859	1101	1407
5	305	352	412	383	455	580	848	1094	1409
6	345	319	347	393	434	583	848	1115	1408
7	309	337	430	385	461	581	846	1126	1399
8	436	405	349	449	465	599	868	1119	1414
9	427	444	431	408	494	594	844	1102	1416
10	429	400	377	445	502	588	871	1133	1444
RTT	**361.1**	**364.2**	**372.9**	**404**	**463.2**	**590.7**	**849.2**	**1115**	**1416**
ETE	**180.55**	**182.1**	**186.45**	**202**	**231.6**	**295.35**	**424.6**	**557.5**	**708**

Measurements of Average End-To-End Delay (μs) for TS7250-TS7250 Communication via Ethernet

Bytes	**16**	**32**	**64**	**128**	**256**	**512**	**1024**	**2048**	**4096**
1	1653	1739	1708	1743	1966	1958	2266	2899	3649
2	1600	1467	1605	1635	1724	1828	2123	2569	3256
3	1561	1475	1591	1739	1696	1953	2133	2607	3240
4	1470	1469	1431	1693	1827	1821	2268	2595	3178
5	1411	1499	1729	1586	1764	1893	2130	2684	3121
6	1432	1742	1637	1571	1620	1799	2267	2861	3166
7	1568	1516	1808	1598	1710	1813	2094	2596	3271
8	1471	1474	1424	1761	1667	1956	2204	2616	3071
9	1414	1651	1467	1682	1820	1989	2167	2676	3096
10	1562	1481	1474	1588	1786	1887	2247	2614	3115
RTT	**1514.2**	**1551.3**	**1587.4**	**1659.6**	**1758**	**1889.7**	**2189.9**	**2671.7**	**3216.3**
ETE	**757.1**	**775.65**	**793.7**	**829.8**	**879**	**944.85**	**1094.95**	**1335.85**	**1608.15**

Measurements of Average End-To-End Delay (ms) for TS7250-TS7250 Communication via WiFi

Bytes	16	32	64	128	256	512	1024	2048	4096
1	6.56	7.51	6.85	7.44	9.02	10.51	15.46	19.56	40.43
2	6.26	6.23	6.4	6.4	8.26	10.23	13.23	18.95	32.25
3	6.56	5.61	6.7	6.66	7.64	9.57	12.53	18.51	30.18
4	6.54	5.69	6.8	6.66	11.58	9.55	12.66	24.68	29.38
5	6.55	6.56	7.56	7.67	8.58	9.55	13.5	18.52	35.37
6	6.52	5.77	6.67	7.74	8.45	9.66	12.7	19.22	30.87
7	6.56	6.51	6.68	6.58	7.48	9.5	12.57	19.95	29.6
8	6.56	6.6	6.66	6.58	7.6	9.47	13.58	20.76	32.73
9	6.57	6.7	6.64	6.77	8.45	9.63	13.67	20.12	36.34
10	6.56	8.69	7.66	6.95	7.67	9.61	13.48	20.8	36.13
RTT	**6.52**	**6.59**	**6.86**	**6.94**	**8.47**	**9.73**	**13.34**	**20.11**	**33.33**
ETE	**3.26**	**3.29**	**3.43**	**3.47**	**4.24**	**4.86**	**6.67**	**10.05**	**16.66**

Measurements of Average End-To-End Delay (ms) for TS7250-TS7250 Communication via IEEE 802.15.4

Bytes	16	32	64	128	256	512
1	23	29.49	44.5	72.33	111.68	174.12
2	23.03	29.6	44.12	67.25	99.09	171.85
3	24.84	32.01	43.91	70.04	100.12	173.09
4	23	32.87	43.65	70.66	102.34	172.14
5	22.42	31.66	46.34	67.33	100.35	175.99
6	23.12	32.56	44.79	70.96	104.8	172.64
7	22.79	33.1	46.77	70.95	100.43	170.6
8	23.17	31.87	45.81	68.8	101.83	172.34
9	24.35	32.27	47.28	67.51	101.52	170.32
10	22.33	31.31	46.1	69.27	101.39	170.96
RTT	**23.2**	**31.67**	**45.33**	**69.51**	**102.35**	**172.4**
ETE	**11.6**	**15.84**	**22.66**	**34.75**	**51.18**	**86.2**

Measurements of Average End-To-End Delay (ms) for TS7250-Gateway-PC Communication via IEEE 802.15.4 and Ethernet

Bytes	**16**	**32**	**64**	**128**	**256**	**512**
1	72.62	65.37	83.76	148.56	169.19	279.8
2	61.85	70.24	81.94	134.47	247.6	389.04
3	60.16	67.21	82.68	134.52	228.83	227.05
4	60.81	67.95	78.55	134.17	188.06	335.79
5	64.65	68.73	84.23	142.6	235.25	417.15
6	61.59	54.06	76.4	154.63	226.83	274.05
7	60.63	78.33	73.61	132.87	186.72	414.9
8	67.01	77.3	82.24	184.44	219.81	224.28
9	64.6	67.47	83.21	156.06	225.43	338.29
10	64.86	69.67	81.73	151.32	169.15	502.37
RTT	**63.88**	**68.63**	**80.84**	**147.36**	**209.69**	**340.27**
ETE	**31.94**	**34.32**	**40.42**	**73.68**	**104.84**	**170.14**