Smart Grid – The new paradigm

Lecture Notes

By

Dr A K Tiwari

Central Training Institute
Jabalpur
# Contents

1. Smart Grid – The new paradigm 4  
2. IT Layer 12  
3. Communication Layer 21  
4. Advanced Metering Infrastructure 34  
5. Interoperability and Standards for Smart Grid 37  
6. Phasor Measurement Unit 45  
7. Technologies for distributed generation 48  
8. References 52
1. Smart Grid – The new paradigm

1.1 Background

The economic activity of any country supported by industrial growth, citizen’s life style, agriculture, trade and research is an impetus for sustained energy demand more in the form of electrical energy. Indian electrical energy generation was about 1600 MW in 1950s and 180000 MW in 2011. The augmentation is phenomenal but inadequate to meet the demand. This is typical situation in many countries. As per reports the current energy path is unsustainable and the world will need at least 50% more energy in 2030 than it uses today and since most of this energy is emanating from fossil fuels the carbon emissions are set to follow a similar track. This brings to the fore the inter dependence of economic activity, energy demand and greenhouse gas (GHG) emissions. The need for embracing low carbon energy through an innovative approach towards energy generation, distribution and utilization is found to be the key for the much needed transformation in the energy and power sector.

This is the essence of the much talked about –Smart Grid‖ perceived as panacea for the energy problem. The smart grid is a fall out of the growing concern on energy security, climate change and the urgency to embrace in a big way the renewable form of energy sources.

1.2 About Smart Grid

The word smart grid has many definitions. Simply put, it is the integration of information and communication technology in to electric transmission and distribution networks. The smart grid is “an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances.”

It may be looked upon as a reform process by which the balance is accomplished between available energy and demand by putting in place appropriate policies and operational framework. The Fig-1 depicts a smart grid scenario.

![Smart Grid Scenario](Image)

**Fig. 1 Smart Grid Scenario**
The figure shows central power plant, distributed energy resources like wind turbines, fuel cells, storage besides loads centers. Under the smart grid scenario the attributes of each one of these components are asserted automatically to increase power availability or decrease power demand.

The base layer of the smart grid is the robust distribution network with adequate energy resources. The intelligence is built over that by deployment of SCADA, AMI and Smart Meters and by leveraging the potential of ICT. The intelligence would reflect the business practices, policies and operational aspects of the Distribution Company. The policies also encompass pricing for distributed energy resources, smart pricing for consumers covering time of day metering, incentives for off peak times and other options.

The vital component of smart grid is the ‘demand side management‘ program which would provide variety of options for the customers and induce them to reduce the demand on the network especially during peak hours.

Simultaneously the concept of distributed resources would provide for proliferation of additional generation including renewable (virtual power plants) to be available as spinning resources at time of needs (peak period).

Therefore through the ‘Smart Grid‘, the distribution company can judiciously maneuver the ‘distributed generation‘ and ‘demand side management‘ in an optimal and efficient manner for providing power to all its customers without interruption.

1.3 Characteristics of Smart Grid:

The smart grid concept offers several characteristics and a few are given in Table 1:

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Healing and Adaptive</td>
<td>Rapidly detects re-configures and restores power supply.</td>
</tr>
<tr>
<td>Interactive with consumers and markets</td>
<td>Motivates and includes the consumer and stakeholders.</td>
</tr>
<tr>
<td>Optimized to make best use of resources and equipment</td>
<td>Improved operational efficiency through optimal utilization of resources and assets.</td>
</tr>
<tr>
<td>Predictive rather than reactive</td>
<td>The system behaviour can be analysed and predicted to initiate advanced corrective action, as opposed to responding to emergencies. This virtue makes system resilient to physical/cyber-attacks.</td>
</tr>
<tr>
<td>Distributed Generation</td>
<td>Accommodates all forms of generation like solar, wind, bio-mass and storage</td>
</tr>
<tr>
<td>Two-way communication across the grid</td>
<td>Both energy and information flow in either direction thereby enabling information based management.</td>
</tr>
</tbody>
</table>

1.4 **Benefits of the Smart Grid**

The philosophy of smart grid leads to several benefits some of which are:

1. Addressing energy security through distributed generation and efficient utilisation.
2. Provides near real time network information.
3. Information based operation, planning, forecasting etc.
4. Increasing power availability without interruptions.
5. Consumer savvy approach through information dissemination.
6. Improving network resilience, reliability and power quality.
7. Reduction of greenhouse gas.

1.5 **Functionalities:**

Having said that – Smart Grid provides for matching the available energy with demand, it is required to know as to how this can be accomplished. The traditional electricity value chain comprising of Generation, Transmission and Distribution continues to be main stay. The technical advances in Information and Communication Technologies and its confluence with power apparatus have made possible a bi-directional electricity value chain involving market, consumers and distributed generators feeding the network. The resultant chain would be as in Fig 2.
Fig 2 – Bi - directional electricity value chain.
Using this modified value chain involving electrical technology, communication technology and information technology the smart grid concept is rolled out through choice of functionalities. The functionalities are implementable tasks resulting in desired performance. The various functionalities can be grouped as system centric, customer centric and energy resource centric. This grouping is only to highlight the spread of smart grid concept. These functionalities are both standalone as well as mutually dependent. One or more functionalities are combined together to realise the overall objectives for a given network. The functionalities commonly referred are listed in Table – 2.

Table – 2

<table>
<thead>
<tr>
<th>System Centric</th>
<th>Customer Centric</th>
<th>Energy resource Centric</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI</td>
<td>Smart Pricing</td>
<td>Renewable sources</td>
</tr>
<tr>
<td>Smart Meters</td>
<td>Time Of Day Metering</td>
<td>Solar – PV</td>
</tr>
<tr>
<td>Meter Data Management</td>
<td>Incentive / disincentive</td>
<td>Wind</td>
</tr>
<tr>
<td>Remote Load control</td>
<td>User based tariff</td>
<td>Bio-mass</td>
</tr>
<tr>
<td>Theft detection &amp; control</td>
<td>Real time pricing</td>
<td>Renewable integration issues.</td>
</tr>
<tr>
<td>- AT&amp;C loss reduction</td>
<td>Pre-paid metering</td>
<td>Policies for usage</td>
</tr>
<tr>
<td>Smart distribution</td>
<td>Demand Side Management</td>
<td>Net Metering</td>
</tr>
<tr>
<td>Efficient fault detection, isolation &amp; restoration</td>
<td>- DSM</td>
<td>Hybrid / Electric Vehicles</td>
</tr>
<tr>
<td>Outage management</td>
<td>Energy Efficient</td>
<td>Charging requirements</td>
</tr>
<tr>
<td>Peak Management</td>
<td>Appliances &amp; control</td>
<td>Sourcing options</td>
</tr>
<tr>
<td>Two way communication</td>
<td>Home Area Networking</td>
<td>Storage</td>
</tr>
<tr>
<td>Network Monitoring and operations</td>
<td></td>
<td>Batteries</td>
</tr>
<tr>
<td>Business Process</td>
<td></td>
<td>Other storage options</td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load research</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory policies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What these functionalities mean and what can be achieved from each one of them is briefly described here.
1.5.1 Advanced Metering Infrastructure - AMI: The AMI enables working with the end use energy consumption data. The energy consumption is recorded with deployment of appropriate smart meters. The end use points are consumers, network points and power apparatus. The AMI also transports the recorded data over a seamless bi-directional communication channel in to the data base of Control Center (CC). The CC works with the data using analytical tools generally called Meter Data Management System (MDMS). The AMI provides the operator several services like - to assess the consumer consumption pattern, involve the consumer in the management process, know the network operating conditions and limits, Disseminate DSM / DR programs, Control of consumer appliances through HAN. The AMI is vital and essential in the implementation of smart grid and as such aids in sustenance of reliable power supply besides host of other quality services. AMI facilitates Remote load control, AT&C loss reduction, Theft detection also.

1.5.2 Smart Distribution - The smart distribution is concerned with uninterrupted power availability to the loads all the times. The smart distribution would improve KPIs like SAIDI, SAIFI and CAIDI. The components of smart distribution are

(i) **Self-Healing** - The self-healing is that part of automation which provides for auto routing of power flow, in the event of a fault, to the load. The FLISR (Fault Location Identification Service Restoration) is the core virtue by which the network is made resilient.

(ii) **Outage Management** – It is concerned with responding to power outages due to variety of causes. From the instant of knowing the outage and resolving the causes the typical approaches like isolating faulty section, alternate routing, deputing crew and the like will be chosen to restore normalcy.

(iii) **Peak Management**: The peak management is concerned with supplying the highest power demand on the network at any point of time. This is done either by bringing in additional resources or by rolling out DSM programme.

(iv) **LT Network Control**: The LT network has always been continuously expanding. Therefore to improve the supply reliability the network need to be monitored and controlled to sustain quality power and also ensure that proper tail end voltage. The LT network control covers Re-configuring of LT network, Re-conductoring, Shunt Capacitors, Fuse Gradation and Switching Optimisation, Back feeding.

1.5.3 Two way communication: - This functionality is concerned with providing path for flow (bi-directional) of data/information between control centre and consumer. This is one of the prime requirements for implementation of smart grid. The bi-directional data communication channel is vital for rolling out many of the functionalities. The communication medium could be technology mix of but the virtual seamless data channel must fall in place between the two ends. The other important aspect here is the interoperability when one or more technologies are deployed which is overcome by resorting to open systems.
In a similar manner the energy from distribute energy resources also will be required to flow from various points on the geographical area to the network.

1.5.4 Network Operations: - This functionality will change but remain central to the smooth functioning of the electricity supply industry. This will be information driven approach. The real time information about customers, their consumption pattern, network condition, apparatus load profile, resource availability, demand, tariff and other pertinent data will be used to analyse and predict the operational requirements.

1.5.5 Business Process: - This functionality is concerned with utilities business approach and will include MIS, Analytics & Reporting, Asset Management, Load research to name a few all of which will leverage the dynamic information form the network module.

1.5.6 Regulatory Policies: The smart grid regime will have many stakeholders including customers. The customer participation is essential in the management of network resources. The tariff variants, incentives, disincentives, technical considerations all need Regulator involvement. The customer while drawing power can become a supplier in which case the buy in price would also become a Regulator subject. This functionality would work towards evolving a frame work for dealing with challenges relating to economics and legal aspects of stakeholder participation.

1.5.7 Smart Pricing: - This functionality looks at evolving tariff structure which will induce the customer to opt for the beneficial tariff. The tariff structure generally is flat average at present. In the smart grid scenario the tariff structure will have several options for the day, season, peak period, off peak period etc. The structure is arrived at with inputs like cost of energy, cost of technology, cost of network components, cost of operations and the like. The cost of input energy will be dynamic as that would depend on source / type and time (for instance peak time or when availability is scarce) of purchase. The smart grid aims at fixing higher tariff at peak demand times and lower tariff level at off peak times and with gradation over the day spread over multiple time zones of usage (ToU). This type of pricing is often referred as Time of Day (ToD) pricing. Similarly for some category of consumers incentives on reducing demand during peak time are an option and disincentives or penalties if the demand is exceeded. Also pre-paid meter as an smart price option could be a pick for some category of customers. The other types of smart prices are Real time pricing and critical peak pricing.

The Smart Meter is an important component for introduction of smart prices. The smart meter connects the consumer to utility with two way communication. A smart meter is usually an electrical meter that records consumption as per programmed interval and communicate the data captured CC. It will have TOU registers for recording consumption over different time zones. It can also record various types of information related to the quality of electricity, abnormal events etc.
1.5.8 Demand Side Management: - The electricity has long become an essential commodity. The industrialization, agriculture, life style of people all has pushed the consumption and the demand for more and more energy. The DSM a customer centric functionality is concerned with moderating the demand through various options. The typical options are ToU pricing, voluntary shut down of loads by consumers, remote control of loads by utility, Response of consumers for price signals and incentives which is also termed as Demand Response (DR) and improvement in energy efficiency. The notion is consumer may not be able to decrease the demand but would be willing to change the consumption pattern with respect time. This shifting of consumption is the desired response which will make utilities tide over the increasing demand. This responsiveness can bring substantial savings to utilities.

1.5.9 Energy Efficient Process & Appliances:- The end use energy efficiency would have a direct impact on demand and energy requirement. If users can be encouraged for going in for improvements in improving the efficiency of process or deploy efficient appliances in all category of customers an appreciable benefit is achievable. Generally the energy efficiency is handled outside the purview of smart grid.

1.5.10 Home Area Networking:- The Home Area Networking (HAN) is meant to monitor and control the appliances in the home environment. HAN is a technology with which the electric utility can resort to DSM measures. There are standards for implementing the HAN. But design may require customization.

1.5.11 Renewable sources: - The smart grid encourages proliferation of distributed generation which by and large takes the form of renewables like Solar – PV, Wind and Biomass. These sources are normally considered in small capacity which can be installed in the consumer premises. Roof top solar PV, wind generators, micro turbines and bio mass plants (rural) are typical examples. The technology supports stand alone as well as grid tied versions. The grid integration of these generators requires study and standardization. The policies for their usage including feed in tariff are part of regulatory aspects.

(i) **Plug in Electric Vehicles:** - The quest for environmentally clean energy has become a key driver for rolling out of plug in electric vehicles (PEV). These PEVs are sinking load while charging and sourcing load while sourcing power to grid. The PEVs are potential sources for peak management.

(ii) **Storage Batteries:** - Large capacity storage batteries are available for deployment at grid level and used for peak management.

The functionalities described until now are more commonly sought in the design of smart grid projects. One or many functionalities are picked depending on the overall objective of the smart grid project.
The implementation of a smart grid project for chosen functions requires an infrastructural platform designed and implemented with appropriate Electrical Technology, Information Technology and Communication Technology. These three technologies complement each other. The generic smart grid platform will look like as shown in Fig – 3.

The IT layer is concerned with the IT hardware and software including the various application programmes that are required to be installed for the purpose of realizing the objectives.

The Communication layer is concerned with facilitating two-way data communication between the Smart grid control center and the intelligent equipment like Smart meters, DCU (Data Concentrator Unit), Automation components HAN (Home Area Network) etc.

The Network Infrastructure layer refers to electrical distribution network, smart meters, Distribution Generation resources etc.

The features and technology of each of the three layers is discussed in the subsequent chapters.
2. IT layer

The IT layer consists of appropriate hardware and software. This layer is located in a control center often called as Smart Grid Control Center.

2.1 Generic Architecture of Smart Grid Management Centre

Smart Grid Architecture is the conceptual structure and overall organization of the Smart Grid functions. It depicts the overall perspective of technology deployed for accomplishing the end objectives like uninterruptible power, reliable power, more green power and the like.

In order to realize the smart grid functionalities the typical system architecture is as shown in Fig 2.1.

Fig 2.1 – Typical IT Architecture

The IT layer is concerned with the IT hardware and software including the various application programmes that are required to be installed for the purpose of realizing the objectives.
2.2 Smart Grid Management Centre – SGMC

The SGMC is the complete monitoring and control of the Smart Grid network. The control center architecture generally is a conceived as dual LAN (Local Area Network) architecture with redundancy. The typical components include:

- Smart Grid Application Server for Meter Data Management System (MDMS):
- Development Server
- Consumer Portal Server
- Front End Server
- Home Area Network (HAN) server
- Information Storage and Retrieval (ISR) Server
- NMS (Network Management System) Communication
- ICCP (Inter Control Centre Communication) Server
- BI (Business Intelligence)/ Analytic/ Reporting Server
- Work Stations
- Printer
- Routers, Firewall and other LAN components.

It will have connectivity provisions for the external systems like Smart Meter Network, DCU, HAN and other utility applications running in other external environment.

Fig – 2.2 Smart Grid Management Control Center
2.2.1 Smart Grid Management Centre Application Servers:

2.2.1.1 Meter Data Management System (MDMS) is the heart of AMI. MDMS is a critical component to realizing the full potential of advanced metering infrastructure (AMI) MDMS is the single repository of all meter data. It is built on open standards with SOA principle.

This module running on an exclusive server support the following features:

1. Rule based Validation, Estimation & Editing (VEE) of consumption data
2. Detect & publish abnormal consumption events and patterns
3. Interface with any existing billing system
4. Schedule based or on-demand reading from meters
5. Receive tamper events from meters and take appropriate action
6. Receive power loss/restoration events from meters and take appropriate action
7. Receive, store and present data from non-meter sources, including customer equipment, distribution automation devices, Home Area Networks, RE sources, Network components.
8. Support different pricing plans, including ToU.
9. Support import as well as export of energy from consumer premises
10. Enterprise class reporting engine.
11. Scalable to support chosen interval reads for million plus meters without performance degradation.
12. Load analysis / research for decision support.
14. Process and generate billing for customers of project area.
15. Required Security and Controls
16. Support consumer portal services.
17. Interface with other IT systems.

2.2.1.2 The other types of applications are:

i. Business Intelligence
ii. Analytics & Reporting
iii. Consumer portal service
iv. Network Management system (NMS) – Monitoring of network resources
v. Communication Servers – data exchange modules as per open standards.

2.2.1.3 SCADA and DMS Functions

When smart grid covers MV and LV network the SCADA and DMS functions with distribution automation and substation automation is required to accomplish high level of reliability. The typical SCADA functions are:
i. Data Acquisition from RTUs at S/S, FRTUs at RMUs / sectionalizer & FPIs
ii. Time synchronization of automation components
iii. Event processing
iv. Supervisory Control
v. GIS
vi. Information Storage & Retrieval (ISR)
vii. Data recovery (DR)

2.2.1.4 DMS Functions

The typical DMS functions are

i. Loss Minimization via Feeder Reconfiguration (LMFR)
ii. Load Balancing via Feeder Reconfiguration (LBFR)
iii. Fault Management and System Restoration (FMSR)
iv. Outage Management
v. Peak Management
vi. Workforce Management
vii. Voltage VAR control (VVC)
viii. Network Connectivity Analysis (NCA)
ix. State Estimation (SE)
x. Load Flow Application (LFA)
xi. Operation Monitor (OM)
xii. Distribution Load forecasting (DLF)
xiii. Distributed Planning
  • Operational planning
  • Assessing planned outages
  • Storm condition planning
  • Short-term distribution planning
  • Short term load forecast
  • Long term distribution planning
  • Long term load forecasts by area
  • Optimal placements of switches, capacitors, regulators, and DER
  • Distribution system upgrades and extensions
  • Distribution financial planners

2.2.1.5 Distribution Automation

The distribution automation includes any automation that is used in the planning, engineering, construction, operation, and maintenance of the distribution power system, including interactions with the transmission system, interconnected distributed energy resources (DER), and automated interfaces with end-users.
The smart distribution which claims –Self –healing‖ as an inherent virtue to increase reliability or respond to emergencies provide for

- Remotely open or close automated switches
- Remotely switch capacitor banks in and out
- Remotely raise or lower voltage regulators
- Block local automated actions
- Send updated parameters to feeder equipment
- Interact with equipment in underground distribution vaults
- Retrieve power system information from smart meters
- Automate emergency response
- Provide dynamic rating of feeders

2.2.1.6 Substation Automation

Automation within substations involves monitoring and controlling equipment in distribution substations to enhance power system reliability and efficiency. The present hard wired substation is becoming networked with IEDs based in IEC 61850 standard. This standard enables interoperability.

2.2.1.7 Distributed Energy Resources Management

Under the smart grid scenario distributed energy resources and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system.

- Direct monitoring and control of DER
- Shut-down or islanding for DER
- PEV management as load, storage, and generation resource
- Electric storage charge or discharge management

2.2.1.8 Load Management

As part of DSM, load curtailment may be resorted to by the utility. This module to support:

- Load management provides active and passive control by the utility of customer appliances (e.g. air conditioner, water heaters, and pool pumps) and certain C&I customer systems.
- Direct load control and load shedding
- Demand side management
- Load shift scheduling
- Curtailment planning
- Selective load management through home area networks (HANs)
2.3 Smart Grid Security

Increased connectivity presents challenges, especially in security. Because of the critical nature of the technology and the services it provides, the grid becomes a prime target for acts of terrorism and vandalism.

Therefore, the transformation of traditional energy networks to smart grids requires an intrinsic security strategy to safeguard this critical infrastructure. As a result, a security vision must include a sound design for proactive security as well as resilience in the event of a security breach.

2.3.1 Security Challenges

The smart grid is unique in several ways that present significant security challenges:

- Scale: The communications infrastructure necessary to support the global power grid has the potential to be larger than the Internet. As we’ve learned from the Internet experience, securing such a large network presents challenges such as segmentation, identity management for a large number of entities, the management of keys for data integrity and confidentiality, as well as integrating multiple wired and wireless communications mechanisms.

- Legacy devices: Unlike corporate IT systems that typically have a life span of three to five years, many devices in the smart grid have service lives measured in decades. Any attempt to design security for the smart grid must enable integration of legacy systems, many of which have only basic, if any, communications capabilities, and provide a long-term migration strategy to smarter devices.

- Field locations: The power grid contains millions of field devices, such as meters, transformers, and switches. While physical security of these field devices is an important design consideration, the fact that they are potentially vulnerable requires that network security design not rely on them for grid integrity.

- A culture of security through obscurity: Today’s grid security often assumes that if the location or access method of a vulnerable point isn’t widely known, it won’t be exploited. Some people believe that the smart grid data communications network will be secure if it is built with proprietary, non-routable protocols, which would make it more difficult to access than a standards-based network. In reality, vulnerabilities cannot remain hidden for any length of time. History has shown that public availability of security algorithms that are subject to peer review has increased the security of these systems. Some examples are the Advanced Encryption Standard (AES) cryptographic standard, Diffie-Hellman asymmetric encryption keys, and the Internet Engineering Task Force (IETF) IP Security (IPSec) security standard. Flaws are discovered and resolved more quickly than in proprietary systems.

- Evolving standards and regulations: In this early phase of smart grid implementation, vendors are implementing security controls using a variety of standard and proprietary mechanisms. This leads to poor interoperability and difficult management. Early efforts suffer from a lack of independent testing and from frequently insecure implementations. As the smart grid standards landscape matures, through efforts by the National Institute of Standards and Technology (NIST) and others, we will see a gradual transition to a common set of security standards and testing. Government and industry bodies are working to address smart grid security concerns by creating
and updating security regulations and standards. The North American Electric Reliability Corporation (NERC) has published a set of regulations for critical infrastructure protection (CIP).

The smart grid gives energy customers the tools to manage their energy consumption—and thus their energy bills—more precisely to meet their individual needs. Using smart grid technology such as Advanced Metering Infrastructure (AMI), real-time information about electricity price changes will be transmitted to smart meters, home energy controllers, or thermostats, which will then automatically adjust their own settings, and change settings on appliances—or even turn them off—according to guidelines set by the customer or learned by the home energy systems themselves.

The customer operations security zone contains the devices and processes that extend energy management to customers. This zone defines policies and procedures for customer energy management and demand response, load shedding, and automated meter reading. Among the systems and devices are smart meters, customer portals, and demand response systems that collect and process customer data and have unique security requirements, such as:

- Fraud prevention. In addition to physical meter tampering, utilities must ensure that meters are not replaced by rogue devices, and that meter data cannot be manipulated.
- Grid integrity. In the event that field devices are compromised, the grid must protect the upstream network from unauthorized commands, access to the network, and denial of service attacks.
- Privacy. Customer energy usage patterns can reveal personal information and vulnerabilities, such as whether an electric car is plugged into the house, or whether a family is away on vacation. Utilities must ensure that customers’ energy usage information remains private both in transit to the utility and in storage in the utility data center.

To provide this level of security, access to home systems and to the data gathered by them must be limited to authorized people and devices. To do this, customer energy management systems must be able to assure integrity of command and meter data, authenticate devices, and protect the grid from compromised devices.

The smart grid security system must also ensure authentication of commands, and guarantee the integrity of telemetry data and commands, ensure data confidentiality, and protect upstream assets. The telemetry and control systems security zone defines the processes that are used to manage the routing of energy from generation plant to consumer and the reliability of the energy delivery systems. This zone contains the data centers involved in the generation, transmission, and distribution of energy, and the intelligent end devices (IEDs) such as transformers, relays, feeder breakers, capacitors, voltage regulators, line switches, reclosers, and sensors/phasors that are used to control energy flow and ensure the reliability of the grid. This zone also contains energy substations that use SCADA systems to manage the grid. Information collected and processed in this zone supports equipment maintenance and troubleshooting, load capacity, and power re-routing in the case of outages. Because this information is crucial to the delivery of quality power to customers, the unique security requirements for this zone include:

**Availability.** System availability is the overarching priority of smart grid security. To maintain availability, security measures should be employed, including:

- Technician and device authorization
• Access control to network services by time of day and function for both users and devices

• Isolation, rerouting, and resilience in the event of a cyber security incident

• Protection from denial of service attacks

**Data integrity.** The integrity of telemetry data and control commands is critical to the proper functioning of the smart grid, and supports the availability requirement. Measures include:

• Technician and device authentication

• Computer health

• Integrity of telemetry data and SCADA commands

• Correlation of alarm data with other sensors to prevent false positives

**Confidentiality.** To ensure regulatory compliance and enable forensic analysis, telemetry and control data must be collected and stored for time periods specified by regulating agencies. However, this information is very sensitive, and may reveal details that could be used to compromise the power grid. Therefore data encryption, intrusion prevention, and intrusion detection are essential.

### 2.3.2 Data Center Security

As mentioned earlier, the smart grid will capture and analyze real-time data about individual customer energy usage patterns. This will enable customers to adjust their power demands, and will enable utilities to adjust the power supply and design services to better meet customer needs. Such massive amounts of information require not only more data storage than utility companies have ever managed, but also the highest security to prevent unauthorized use and ensure safe, timely disposal in compliance with regulations.

All data centers must enable secure information sharing both within a specific data center and between data centers. Different types of data centers have different levels of security. Proper definition and enforcement of security policy ensures that appropriate access is granted, only authorized communication is granted between systems with different levels of trust, and that overall grid integrity is maintained.

### 2.3.3 Network and Data Security

The following items need to be considered for adequate security at different levels i.e. systems, data, network and security.

### 2.3.3.1 Physical Security:

The smart grid control room and data center should have tight physical security controls implemented in order to avoid any possible physical security threats. The entrances for smart grid control room and data center should have exclusive physical access control systems (swipe card / biometric)
implemented. This will be in addition to the access control systems implemented at the building level. The access control system shall be able to define the access levels based on the roles and designations of employees. Further, the access control system shall be able to apply access control based on timings so that employees working in shifts shall have access to the facility only during their allotted shift timings. The access control management software shall be integrated with identity and access management system.

2.3.3.2 Application Security:

There shall be an identity and access management system which shall control the access control of all employees to the smart grid systems. The identity and access management system shall be able to define the access control levels of each employee based on his/her roles, responsibilities or designation. Further, the identity and access management system shall be able to define which employee can access which function of the individual systems. For example, the identity and access management system shall define which employee can initiate a load disconnect function for a particular consumer, and therefore rest of the unauthorized employees will not be able to perform load disconnect function. The identity and access management system shall be integrated with rest of the smart grid systems.

2.3.3.3 Network Security:

Since SGMC has to access external environment through GPRS and Internet cloud it is important to have adequate network security systems. There shall be intrusion detection and prevention systems deployed at the data center layer. There shall also be firewalls which will be a separate system from the intrusion prevention system. The firewall shall control the demilitarized zones in the data center and control room, and also the systems and ports which will be open to public network/VPN.

2.3.3.4 Systems and Data Security:

The data flowing from the field to enterprise shall be encrypted as per the industry standard security measures. This shall include encryption technologies like AES, public-private key etc.

The systems deployed shall also have the application scanning, hardware scanning tools in order to identify any vulnerability so as to mitigate any potential security threats. The application databases shall have exclusive security tools in order to prevent any potential internal attacks like SQL injection etc.
3. Communication Layer

The potential of communication technology is known and has been put to use in power sector since the days of EHV transmission. But the evolution of new communication technology and its adaption in power sector has made possible automation of Transmission and Distribution systems. The smart grid eco system would require bi-directional communication technology for effective implementation of various functionalities. This chapter discusses the Communication Technology options for Smart Grid eco system.

3.1 Background

The present trend globally in the electricity business is in providing quality and uninterrupted power supply with greater level of customer satisfaction at optimum cost to both customer and company. Since the deregulation of electric utilities globally, the requirements for interconnection of power networks at all levels and data sharing to various stakeholders has become necessary and complex due to existing infrastructure and diverse practices among utilities. The utilities are looking for technology support for to improve the operational efficiency, meet the regulatory requirements and enhance customer satisfaction besides other performance parameters. The automation and integration of Information System at both enterprise and engineering levels leading to ‘Smart Grid’ is the current thought process. This requires an appropriate communication technology or mix of communication technologies for end to end connectivity at levels of operation. and plant (here ‘plant’ is referred to mean a generating plant, substation, Distribution Transformer Centre, load dispatch centre).

Smart Grid in general, is implementation of modernization of the delivery of electricity from suppliers to consumers utilizing new technologies (digital). Smart Grid technologies cover power sources, power storage, power distribution and improvements in energy efficiency. The potential benefits of Smart Grid to consumers, industry, the environment and the electrical utility promise to revolutionize how power is distributed and electricity consumption is managed.

One of the technology areas requiring the greatest level of innovation is the communications systems at the core of every Smart Grid deployment. Each end-point device (e.g. power breaker, Smart Meter, mobile workforce unit, etc.) in the Smart Grid must be able to reliably and securely communicate with applications that manage the processes, these typically being located at one or more central locations.

To serve the emerging needs of the Smart Grid, these grid communications solutions must be pervasive, rapid, robust (even in emergency conditions), scalable, and most of all secure. Considering the varying operating environments, the vast number of systems involved and the locations where end-points may exist, the challenge of establishing a suitable Smart Grid communications network is immense.
3.2 Smart Grid Communications Requirements

The Smart Grid communications network implemented by the Utility will potentially be subject to many demanding communication needs, including but not necessarily limited to the support of:

- Advanced Metering Infrastructure (AMI);
- Supervisory Control And Data Acquisition (SCADA) equipment;
- Fault management equipment;
- Grid-to-vehicle applications;
- Critical asset management;
- Mobile workforce;
- Synchrophasor monitoring;
- Security communications and surveillance.

The smart grid phase will rely on extensive information exchange. The operation and maintenance of power distribution will be information based procedure. A predictive approach based on information will replace the present reactive approach.

---

**Fig. 3.1 Exchange of information at various levels in Electricity Business**

The Fig. 3.1 shows the information emanating from different segments of Electricity Business. The deluge of information exchange requires robust, suitable and cost effective communication technology at various levels so as to provide the seamless connectivity of all end points with central controller.
The source of information and its integrity is to be maintained wherever required in the eco system. This emphasizes the need for secured transportation of data / information over the communication channels. The security is also vital for association and access to a data source. The Fig – 3.2 shows the end-to-end communication security and management layers, cutting across each Smart Grid communication domain.

![Communications Network Security Layer](image)

Fig 3.2 End- to –end Smart Grid Communications Model (courtesy IEEE)

### 3.3 Challenges Faced By the Utility

In addition to the diverse communications requirements that the Smart Grid communications network must support, the Utility faces a number of other potential challenges when implementing such a network. These could include one or more of the following:

- Lack of suitable spectrum to implement the communications solution;
- The wide area, near ubiquitous, extent of required communications coverage across the Utility service territory;
- The demanding requirements of regulatory and other statutory bodies’ compliance;
- The Utility preference for private rather than public communications networks;
- The Utility requirement to meet the needs of shareholders, state / central government;
- The Utility preference for CAPEX centric implementations;
- The fact that standards are not yet fully defined for Smart Grid communications networks;
- Limited equipment ecosystems and the short commercial track record of many suppliers;
• The lack of suitable internal resources and experience within the Utility relating to state-
of-the-art communications technologies;
• The migration of users and devices from legacy communications solutions.

There are various communication technologies including simple telephone and PLCC to advanced Mobile (cellular) 3G and Satellite communication technologies are available for utility applications. Considering the most commonly available in today’s market and which are predominately recommended for distribution utilities are only considered in this paper.

3.4 Communication Technologies

3.4.1 Wireless (Radio) Communications

Radio communication systems basically owned by utility with licensed band and it includes both point to point and point to multipoint network. This system is being in use for many years for SCAD projects in utility.

Digital microwave systems are licensed systems operating in several bands ranging from 900 MHz to 38 GHz. They have wide bandwidths ranging up to 40 MHz per channel and are designed to interface directly to wired and fiber data channels such as ATM, Ethernet, SONET, and T1 derived from high-speed networking and telephony practice. Application of these systems requires path analysis to avoid obstructions and interconnection of multiple repeater stations to cover long routes. Each link requires a line-of-sight path.

3.4.1.1 Multiple Address System

Multiple Address (MAS) Radio is popular due to its flexibility, reliability, and small size. A MAS radio link consists of a master transceiver (transmitter/receiver) and multiple remote transceivers operating on paired transmit/receive frequencies in the 900 MHz or allocated licensed band. The master radio is often arranged to transmit continuously, with remote transmitters coming up to respond to a poll request. Units are typically polled in a "round-robin" fashion, although some work has been done to demonstrate the use of MAS radios in a contention-based network to support asynchronous remote device transmissions.

The frequency pairs used by MAS must be licensed by the FCC (WPC in India) and can be reused elsewhere in the system with enough space diversity (physical separation). Master station throughput is limited by radio carrier stabilization times and data rates limited to a maximum of 9.6 kbps. The maximum radius of operation without a special repeater is approximately 15 km, so multiple master radios will be required for a large service territory. MAS radio is a popular communication medium and has been used widely by utilities for SCADA (supervisory control and data acquisition) systems and DA (distribution automation) systems. MAS radio is susceptible to many of the security threats including Denial of Service (radio jamming), Spoof, Replay, and Eavesdropping. In addition, the licensed frequencies used by these systems are published and easily available in the public domain. For this reason it is important that systems
using MAS radio be protected against intrusion using proper techniques like encryption / scrambling.

3.4.1.2 Spread Spectrum Radio and Wireless LAN’s

New radio technologies are being developed as successors to traditional MAS and microwave radio systems which can operate unlicensed in the 900 MHz, 2.4 GHz, and 5.6 GHz bands or licensed in other nearby bands (at present 2.4 GHz is unlicensed in India). These systems typically use one of several variants of spread spectrum technology and offer robust, high-speed point-to-point or point-to-multipoint service. Interfaces can be provided ranging from 19.2 kbps RS232 to Ethernet. Line-of-sight distances ranging from 1 to 20 miles are possible, depending on antenna and frequency band choices and transmitter power. Higher-powered devices require operation in licensed bands. This technology has been successfully used both for communication within the substation fence as well as communication over larger distances between the enterprise and the substation or between substations. An example of communication within the substation is adding new functionality, such as transformer condition monitoring, to an existing substation. An internal substation radio connection can make such installations very cost-effective while at the same time providing immunity to electromagnetic interference which might otherwise arise from the high electric and magnetic fields which are found in a substation environment.

As contrasted to traditional radio systems, spread spectrum radio transmits information spread over a band of frequencies either sequentially (frequency hopping spread spectrum – FHSS) or in a so-called "chirp" (direct sequence spread spectrum – DSSS). Other closely related but distinct modulation techniques include Orthogonal Frequency Division Multiplexing (OFDM), which sends data in parallel over a number of sub-channels. The objective in all of these systems is to allow operation of multiple systems concurrently without interference and with maximum information security. The existence of multiple systems in proximity to each other increases the apparent noise background but is not immediately fatal to successful communications. Knowledge of the frequency hopping or spreading "key" is necessary for the recovery of data, thus at the same time rendering the system resistant to jamming (denial of service) and eavesdropping attacks.

Variants of DSSS, FHSS, and OFDM are being offered in commercial products and are being adopted in emerging wireless LAN standards such as the several parts of IEEE 802.11 (Wireless LAN) and 802.16 (Broadband Wireless Access). This is a rapidly changing technology.

3.4.1.3 ZigBee

Zigbee is a new wireless technology enabling networking of end user devices in industrial, residential and commercial establishments. This wireless network brings with it benefits like better life style, energy conservation, automation and the like. This has the potential for last mile connectivity.

Zigbee is a new wireless technology built on the IEEE 802.15.4 networking standard for wireless personal area networks (WPANs). ZigBee is targeted at RF applications that require a low data
rate, long battery life and secure networking. Worldwide ZigBee operates in 2.4 GHz, the Industrial Scientific and Medical (ISM) radio bands which do not require license.

The composite IEEE standard (Physical and Mac layers) and Zigbee (network and application layers) standard has enabled enormous applications for home automation, wireless sensors, automatic meter reading etc. The salient features like long battery life, low cost, small size and mesh networking.

**Zigbee Device types**

The Zigbee system is a network of three different types of generic devices namely ZigBee coordinator (ZC), ZigBee Router (ZR) and ZigBee End Device (ZED).

The ZC is the root of the network tree and is generally one per network. It is meant to store information about the network, monitor performance and configure parameters.

The ZR runs an application function as a router and can act as an intermediate router, passing data from other devices there by stretching the reach. These devices are also called FFDs (Full Function Devices).

The ZED can only discharge its designated function, for example controlling a light. ZED can talk to ZC or ZR and cannot relay data from other devices. This later function of ZED allows the node to be asleep a significant amount of the time giving the much quoted long battery life. These devices are also called RFDs (Reduced function devices).

**Topology**

![Zigbee Topologies](image-url)

Fig-3.3. Zigbee Topologies
The “Topology” is the configuration of the hardware components and how the data is transmitted through that configuration. The Zigbee networking supports three topologies as shown in Fig-1. They are Star, Mesh and Cluster Tree.

The ZigBee network begins with a process called “association”. In this process the ZC and a few ZRs play the appropriate role of routing the information to the desired ZED.

In a Star topology (point-to-point) all devices are within direct communication range to the coordinator, through which all messages are routed. A device sends a message to the coordinator, which then passes it on to the destination device. Direct communication between the end devices is not supported. The advantage is simplicity meaning, Star topology does not require a complex network layer or routing protocols and packets require only two hops to reach their destination. The limitations are no alternative paths between the device and coordinator and the radius is limited (typically 30—100 meters).

The Mesh topology is a maze of interconnected routers and devices. This is also called peer-to-peer network. Each router is typically connected through at least two pathways, and can relay messages for its neighbours. It supports multi-hop communications, through which data is passed by hopping from device to device using the most reliable links and most cost-effective path until its destination is reached. The advantages are this topology is “self-configuring and self-healing”, highly reliable, robust and increased range. The main limitations are higher communications overhead and increased power consumption and costs.

When data reliability is the key, a mesh network topology offers the best protection through its self-configuring and self-healing capabilities. The removing and adding of ZR or ZED make the mesh alive through alternate paths. Through the self-configuring capabilities the mesh network identifies a new device including its neighbours.

The cluster tree topology which is a mix of star and mesh is rarely used.

**ZigBee Applications**

The ZigBee targets applications "across consumer, commercial, industrial and government markets worldwide". Unwired applications are highly sought after in many networks that are characterized by numerous nodes consuming minimum power and enjoying long battery lives. ZigBee technology is designed to best suit these applications. For instance in a typical home environment entertainment units, security systems, fire alarm, smoke detector, burglar alarm, air-conditioners, the heater, kitchen appliances and the lighting all within throw away distance from each other can be controlled with a single hand held unit from anywhere within the home premises.
The electrical power sector has been adopting modern technology to address some of the issues being faced in the power distribution. One such issue is the reading of large number of consumer energy meters automatically. The Zigbee system is expected to find favor for this application.

The Zigbee specification such as low power, low data rate, long battery life, two way communication, wireless medium, unlicensed frequency band, mesh network, security, small foot print and plug and play are indeed great virtues. So the availability of technical support (HW/SW, tools and skills), the necessity for solutions to new or existing problems and the commercial considerations all tilt the balance in favor of Zigbee.

A typical control scheme for home appliance control is shown in Fig. 3.4

![Fig: 3.4 HAN Architecture](image)

Some of the ZigBee applications include:

- Wireless home security, Remote thermostats for air conditioner, Remote lighting controller, Industrial and building automation and control (lighting, etc.)

Communications rate The technology can operate in any one of three bands, the ISM band at 2.4 GHz worldwide, the European 868 MHz band, and the US 915MHz ISM band. The data rate at 2.4 GHz is 250 kbps; for the lower bands it is 20 kbps and 40 kbps respectively.

ZigBee based technology is becoming popular for remote meter reading applications and Home Area Networking (HAN).

### 3.4.1.3 Mobile Communications system

Though, Mobile communication system is basically wireless or Radio communication system and synonymous to wired telephony system with advanced features. This includes Global Standard for Mobile Communication System (GSM) and Code Division Multiple Access (CDMA) systems. Basically these systems started with voice applications and the present systems include triple play support (voice, data and video). Here only the GPRS the 2.5 G of GSM is discussed keeping its use in power sector for data communication applications like AMR / AMI and trouble call system.

GPRS (General Packet Radio Service) is a packet based communication service for mobile devices that allows data to be sent and received across a mobile telephone network. GPRS is a step towards 3G and is often referred to as 2.5G. Here are some key benefits of GPRS:
Speed

GPRS is packet switched. Higher connection speeds are attainable at around 56–118 kbps, a vast improvement on circuit switched networks of 9.6 kbps. By combining standard GSM time slots theoretical speeds of 171.2 kbps are attainable. However in the very short term, speeds of 20-50 kbps are more realistic.

Always on connectivity

GPRS is an always-on service. There is no need to dial up like you have to on a home PC for instance. This feature is not unique to GPRS but is an important standard that will no doubt be a key feature for migration to 3G. It makes services instantaneously available to a device.

New and Better applications

Due to its high-speed connection and always-on connectivity GPRS enables full Internet applications and services such as video conferencing straight to desktop or mobile device. Users are able to explore the Internet or their own corporate networks more efficiently than they could when using GSM. There is often no need to redevelop existing applications.

GSM operator Costs

GSM network providers do not have to start from scratch to deploy GPRS. GPRS is an upgrade to the existing network that sits alongside the GSM network. This makes it easier to deploy, there is little or no downtime of the existing GSM network whilst implementation takes place, most updates are software so they can be administered remotely and it allows GSM providers to add value to their business at relatively small costs. The GSM network still provides voice and the GPRS network handles data, because of this voice and data can be sent and received at the same time.

Simple GPRS Technical Overview
As mentioned earlier GPRS is not a completely separate network to GSM. Many of the devices such as the base transceiver stations and base transceiver station controllers are still used. Often devices need to be upgraded be it software, hardware or both. When deploying GPRS many of the software changes can be made remotely.

There are however two new functional elements which play a major role in how GPRS works. The Serving GPRS Support Node (SGSN) and the Gateway GPRS support node (GGSN). These 2 nodes are new to the network with the other changes being small if any. Before explaining what these 2 new members of our network do it is important to ask how does the network differentiate between GSM (circuit) and GPRS (packet)? In simple terms there are in practice two different networks working in parallel, GSM and GPRS. In any GSM network there will be several BSC’s (Base Station Controllers). When implementing GPRS, a software and hardware upgrade of this unit is required. The hardware upgrade consists of adding a Packet Control Unit (PCU). This extra piece of hardware differentiates data destined for the standard GSM network or Circuit Switched Data and data destined for the GPRS network or Packet Switched Data. In some cases a PCU can be a separate entity. From the upgraded BSC there is a fast frame relay connection that connects directly to the newly introduced SGSN.

**SGSN**

The Serving GPRS Support Node, or SGSN for short, takes care of some important tasks, including routing, handover and IP address assignment. The SGSN has a logical connection to the GPRS device. One job of the SGSN is to make sure the connection is not mobility changes from cell to cell. The SGSN works out which BSC to route the connection through. If the user moves into a segment of the network that is managed by a different SGSN it will perform a handoff of to the new SGSN, this is done extremely quickly and generally the user will not notice this has happened. Any packets that are lost during this process are retransmitted. The SGSN converts mobile data into IP and is connected to the GGSN via a tunneling protocol.

**GGSN**

The Gateway GPRS Support Node is the last port of call in the GPRS network before a connection between an ISP or corporate network’s router occurs. The GGSN is basically a gateway, router and firewall rolled into one. It also confirms user details with RADIUS servers for security, which are usually situated in the IP network and outside of the GPRS network. **Connectivity Between the SGSN & GGSN.** The connection between the two GPRS Support Nodes is made with a protocol called GPRS Tunneling Protocol (GTP). GTP sits on top of TCP/IP and is also responsible for the collection of mediation and billing information. GPRS is billed on per megabyte basis unlike GSM. In practice the two GSN devices may be a single unit.

**HLR**

The HLR or Home Location Register is a database that contains subscriber information, when a device connects to the network their MSISDN number is associated with services, account status information, preferences and sometimes IP addresses.
Problems with GPRS

Although GPRS has many benefits there have been a few problems. Low connection speeds like around 12Kbps, a far below from the expected. Another problem sometimes encountered is customer expectation. Many companies have applications running on a 10 megabyte LAN and expect the same performance from their GPRS devices. Although the connection speeds these days are pretty good it still is not as fast as ISDN or Local Area Networks.

GPRS roaming has not been implemented in many countries on a lot of networks as yet. This is where a user can use the GPRS service from any network operator. At the moment although GSM mobile will work, GPRS may not work at all. Accesses by third party application providers are having a lot of difficulty obtaining an APN from providers to offer their own GPRS services. This somewhat limits services to that provided by the GPRS operator. Though this feature may not be of interest to power sector application, the present day 3G technologies has most these problems fixed.

3.5 Wired (Radio) Communications

3.5.1 Power Line communications systems

The implementation of access technology is a challenge in both developed and developing countries. Traditional Power Line Carrier Communication (PLCC) on High Voltage lines was one of the earliest communication technology used extensively by power utilities for both voice and low speed data communications. In view of developments in Smart Grid, the power line is best candidate for communication as every apparatus working on power can be accessed. The utility can also offer additional value added services other than own usage.

Researchers have widely investigated the applicability/feasibility of Power line Network for communication and found that they have enough bandwidth for communication at nearly any data rate. A limitation hindering the communications through such media is the regulations by communication authorities, e.g. in Europe, CENELEC standard have regulated the operation frequencies and maximum power to be transmitted in power line communication (PLC) environment. These led to review of PLC systems with regards to frequency band of operations and maximum operating power in various countries, because PLC systems radiate like antenna and can cause interference to other electronic instruments.

PLC network is divided into three categories, indoor PLC, low voltage PLC, and medium voltage PLC. The low and medium voltage PLC is called access network. Generally, PLC technology can be divided into two groups so called narrowband and broadband technologies. The narrowband technology allows the data rates up to 100kpbs while the broadband technology allows data rates beyond 2Mbps. The narrowband services include office and home automation, energy information systems, transportation systems, etc. Currently, there is a growing deployment of PLC technologies in various countries and a number of manufacturers offer PLC products with claimed data rates up to 45Mbps or more.
There are a number of standards activities available today such as IEEE P1675 –Standard for Broadband over Power-line Hardware(a group working on hardware installation and safety issues, IEEE P1775 –Power-line Communication Equipment – Electromagnetic Compatibility (EMC) Requirements – Testing and Measurement Methods(a working group focusing on PLC equipment, electromagnetic compatibility requirements, testing and measurement methods, and IEEE P1901 –IEEE P1901 Draft Standard for Broadband over Power-line Networks: Medium Access Control and Physical Layer Specifications(1. The OPERA has also published results of R&D and pilot trials carried out in the European Union on the use PLC and results were encouraging.

The BPL technology uses OFDM technique. The coupling of high frequency data signal onto the LT line is either through capacitive or inductive.

### 3.5.2 Fiber Optics

Fiber optic cables offer at the same time high bandwidth and inherent immunity from electromagnetic interference. Large amounts of data as high as gigabytes per second can be transmitted over the fiber.

The fiber cable is made up of varying numbers of either single- or multi-mode fibers, with a strength member in the center of the cable and additional outer layers to provide support and protection against physical damage to the cable during installation and to protect against effects of the elements over long periods of time. The fiber cable is connected to terminal equipment that allows slower speed data streams to be combined and then transmitted over the optical cable as a high-speed data stream. Fiber cables can be connected in intersecting rings to provide self-healing capabilities to protect against equipment damage or failure.

Two types of cables are commonly used by utility companies: OPGW (Optical Power Ground Wire which replaces a transmission line’s shield wire) and ADSS (All Dielectric Self-Supporting). ADSS is not as strong as OPGW but enjoys complete immunity to electromagnetic hazards, so it can be attached directly to phase conductors.

Although it is very costly to build an infrastructure, fiber networks are highly resistant to undetected physical intrusion associated with the security concerns outlined above. Some of the infrastructure costs can be recovered by joint ventures with or bandwidth sales to communication common carriers. Optical fiber networks can provide a robust communications backbone for meeting a utility’s present and future needs.

### 3.6 Summary

A broad review of communication requirements and technologies for Smart Grid implementation is presented. Communication is vital link for success of Smart Grid. The data requirements for specific needs of utility like for automation, meter data and other business applications are different in terms of traffic (bandwidth) and latency. For complete end-to-end communication, a mix of communication technologies considering the utility’s existing communication infrastructure and future requirements may be required. The power line communication (both
narrowband and broadband) and ZigBee based wireless mesh technologies have the desired feature for smart grid implementation along with GPRS and Fiber optic (through service provider) systems.
4 Advanced Metering Infrastructure (AMI)

4.1 AMI and its role:
The AMI is the nerve center of any smart grid implementation. AMI constitute
- Smart meters at consumer premises.
- Two way communication network between CC and end points.
- MDAS that will act as Front end to field devices and MDMS
- IT system comprising of HW and SW running MDMS located at the SGMC.

The role of AMI is vital and would facilitate
- Periodic flow of customer meter data and network data in to the data base.
- Disseminate DSM / DR programs
- Facilitate MDM
- Customer empowerment through consumer portal

The generic architecture of an AMI is shown in Fig 4.1

![Generic AMI network diagram](image)

**Fig – 4.1 Generic AMI network.**

The generic architecture has HAN at the bottom layer. The HAN confines to the customer premises and helps SGMC in reaching to appliances for monitoring and control. It may also have a HDU for disseminating customer specific information like TOU tariff rates, incentives, penalties, energy consumption etc. The HAN may be Zigbee based. But the PLC based broadband technology also has the potential to support home automation.
The layer above HAN is the SMN. The SMN is a cluster of smart meters at customer premises networked through a suitable communication medium with the DCU. The Smart Meters comprise of single or three phase (direct or CT/PT connected) electricity meters with port for communication with DCU. The DCU will have two communication ports one for SMN connectivity and other for SGMC connectivity. The number of smart meters per DCU depends on SMN design. The SMN may again based on Zigbee (Mesh) or PLC.

The third layer is GPRS the IP based WAN bridging the SMN and the upper layer MDMS which will reside in the SGMC.

The above given generic AMI architecture may have variants depending on the AMI features.

4.2 Smart Meters:

The Smart Meter is an important component of Smart Grid. This meter is one which connects the consumer to utility with two way communication. A smart meter is usually an electrical meter that records consumption as per programmed interval and communicate the data captured to the SGMC. It can also record various types of information related to the electricity consumption over time. The smart meters are provided with time of use (TOU) registers. With the addition of two-way communications between the meter and the electricity distributor the consumer will be provided with information about consumption pattern, time based tariff and alerts. This will enable the consumer to use the electricity in the preferred time so as to reduce the bill.

The smart meters shall have the following minimum features:

1. Measure and Compute electrical parameters.
2. Store and communicate requested data as per programmed interval.
3. Detect, resolve abnormal & tamper events and store the same
4. Inbuilt memory to store all relevant meter data, events for a required period.
5. Meter communication protocol shall be as per open standard.
6. Options for both Prepaid and postpaid metering.
7. Shall be configurable remotely.
8. Interface to a Home Display Unit
9. Support remote firmware upgrade
10. Support remote load management
11. Load Reconnect / Disconnect switch

4.3 AMI application

It includes Meter Data Management (MDM) with customization. MDM is the most valuable subcomponent of AMI and backbone of the successful large scale AMI deployment because it
controls, validates and cleanses the core meter values before the data is made available to any other system. This module running exclusive server will have the following features:

1. Rule based Validation, Estimation & Editing (VEE) of consumption data
2. Detect & publish abnormal consumption events and patterns
3. Interface with any existing billing system
4. Schedule based or on-demand reading from meters
5. Receive tamper events from meters and take appropriate action
6. Receive power loss/restoration events from meters and take appropriate action
7. Receive, store and present data from non-meter sources, including customer equipment, distribution automation devices, Home Area Networks, RE sources, Network components.
8. Support different pricing plans, including ToU.
9. Support import as well as export of energy from consumer premises
10. Enterprise class reporting engine.
11. Scalable to support chosen interval reads for million plus meters without performance degradation.
12. Load analysis / research for decision support.
14. Process and generate billing for customers of project area.
15. Required Security and Controls
16. Support consumer portal services.
17. Interface with other IT systems (applications).

4.4 Demand Side Management & Demand Response

The electricity is now an essential commodity and increasing the price may not result in reduction of demand. On the contrary the consumers may respond to time based pricing by judiciously shifting to lesser price periods of supply. This way of induced staggering in consumption is foreseen as potential demand moderation technique and can be expected to lessen the peak demand.

Demand Response Programs
1. Introducing Time of Use/Time of Day (TOD) tariffs.
2. Energy efficiency program – reduces energy requirement for same process
3. Mandatory usage schedules.
4. Disincentives for demanding more power
5. Incentives for shedding load.
6. Traditional Telescopic Pricing

The demand response in all its forms is easily implementable with smart grid AMI infrastructure.
5. Interoperability and Standards for Smart Grid

5.1 Background

The smart grid eco system embraces latest automation, information and communication technologies while rolling out this futuristic concept. For economical and successful deployments of new technologies, standard based solution is always recommended. The new technology would be required to co-exist with legacy systems. Hence there is need for interoperability standards.

Under the smart grid phase the present management practices will give way to data and information dependent procedures. The exchange of data and information among the various components of diverse technologies is a challenge. But can be overcome through adoption of open system design based on standard open communication protocols. This chapter discusses about the interoperability and standards for Smart Grid.

5.2 Interoperability

Interoperability can be defined as —the ability of two or more systems or components to exchange information and to use the information that has been exchanged. This emphasizes that not only information exchange taking place between two or more systems but also to interpret the information. Interoperability reduces installation and commissioning duration and protects investment. Unlike IT scenario type of interoperability like between printer and computer, in power system applications human interventions is required in many occasions like bilateral table configuration for ICCP etc. Energy meter reading is one example where a lot of proprietary standard existed that created hurdle in many of AMR / AMI implementations. Now there are standards for energy meter reading which simplifies the interoperability issues.

5.3 Standards Development

The Smart Grid represents a technical challenge that goes way beyond the simple addition of an Information Technology infrastructure on top of an electro technical infrastructure. Each device that is connected to a Smart Grid is, at the same time, an electrotechnical device and an intelligent node. Today's "connection" standards need to address both aspects concurrently. Standards development often takes through the standardizing bodies or Dominant Corporation or consortiums of interested vendors (de facto standards). In many cases, successful de facto standards become formalized in to real standards.

Another aspect of standards is that they cannot be too rigid, but must still leave flexibility for systems to add new functionality or select certain options. Many standards come with both mandatory requirements and optional selections, as well as with extension rules for expanding
the standards in a consistent manner for new functions. This is helps to address a few vendor-specific requirements or utility-specific requirements, as well as the flexibility to meet unforeseen requirements in the future.

While developing standards, it may be noted that a clear definition of the scope and purpose of the standard explicitly defined. Sometimes a standards effort is started with a vague scope, and either overlaps or even contradicts some existing, adequate standards, or fails to address enough of the area to be useful. It is also very essential to review existing standards to determine if they can meet the need with possibly only minor modifications or selection of options. The so developed draft shall include user’s requirements as well as the technology experience of the vendors. Sometimes it may be required to start with existing standard or propriety standard to build the open standard. The process requires testing and validation at field condition of system based on developed standard to ensure its robustness and interoperability. If required, standard can be amended based on the field experience.

5.4 IEC works in Smart Grid

Globally (except for a few countries), IEC standards are being followed in Power sector. IEC has various technical councils and working groups catering to the needs of entire power segment standardization requirements. IEC has representation from all countries which are following IEC standards. This helps adopting any localized requirements and harmonizing the national standards. In IES SG 3 (Strategic Group) on Smart Grid, set up by the IEC SMB (Standardization Management Board), provides advice on fast-moving ideas and technologies likely to form the basis for new International Standards or IEC TCs (Technical Committees) in the area of Smart Grid technologies [4]. It has developed the framework and provides strategic guidance to all Technical Committees involved in Smart Grid work and has developed the Smart Grid Roadmap which covers standards for interoperability, transmission, distribution, metering, connecting consumers and cyber security.

The IEC through SG 3 is working in close collaboration with Smart Grid projects around the globe, including NIST (US National Institute of Standards and Technology). IEC Standards are recognized as being crucial in the development of Smart Grids everywhere. IEC has classified the existing standards by relevance with reference to Smart Grid as Core, High, Low and Medium.

TC 57 of IEC

IEC TC 57 develops standards for electric power system control and associated telecommunications in the areas of generation, transmission and distribution real-time operations and planning. IEC has brought IEC TR 62357, Power system control and associated communications – Reference architecture for object models, services and protocols. The primary purpose of this Technical Report is to provide reference architecture to show how the various
standardization activities within TC 57 relate to each other and how they individually and collectively contribute to meeting the objectives of TC 57. A second objective is to develop a strategy to combine and harmonize the work of these various activities to help facilitate a single, comprehensive plan for deployment of these standards in product development and system implementations.

The need for this framework is motivated by at least two major factors:

- There are multiple independent standard initiatives that need to be coordinated and harmonized to minimize the need for data transformation to exchange data between systems using these various standards.
- There is a need to have a comprehensive vision of how to deploy these standards for actual system implementation and integration efforts.

There are several different initiatives within TC 57, each one dealing with a selected part of the real-time operations and planning. Each has a specific objective and may have sufficient breadth of scope to provide the bulk of the relevant standards needed for product vendors to develop products based on those standards.

IEC TR 62357 describes the reference architecture of the TC 57 standard series and describes the interdependencies between the different standards as shown in Fig.5.1 and 5.2

(Courtesy: IEC)  
Fig.1 TC 57 Reference Architecture
5.5 NIST, IEEE and NERC in smart grid

NIST

In cooperation with the DoE, NEMA, IEEE, GWAC, and other stakeholders, NIST has primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. NIST grouped Smart Grid standardization into three phase viz. phase – 1 Road Map & Smart Grid Release 1, Phase – 2 Public – Private Partnership for Longer Term Evolution and Phase – 3 Testing and Certification frame work.

NIST has brought out NIST Special publications 1108 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (January 2010) [5]. It describes a high-level conceptual reference model for the Smart Grid, identifies existing standards that are applicable (or likely to be applicable) to the ongoing development of the Smart Grid, specifies high-priority gaps and harmonization issues (in addition to cyber security) for which new or revised standards and requirements are needed, documents action plans with aggressive timelines by which designated standards-setting organizations (SSOs) will address these gaps, and describes the strategy to establish requirements and standards to help ensure Smart Grid cyber security.
NIST in its conceptual model divides Smart Grid into seven domains as shown Fig. 5.3. In general, actors in the same domain have similar objectives. To enable Smart Grid functionality, the actors in a particular domain often interact with actors in other domains, as shown in Figure 5.3. However, communications within the same domain may not necessarily have similar characteristics and requirements. Moreover, particular domains also may contain components of other domains.

Fig. 5.3 Interaction of actors in different Smart Grid domains

NIST also identified existing standards based on several guiding principles that led to the two lists. The major principles that NIST used to select the documents were:

1) they support interoperability of the Smart Grid as it evolves from the existing grid with new utility deployments, Smart Grid programs, and consumer investments in Smart Grid equipment and appliances; and

2) they have a demonstrably high level of consensus support. Since the Smart Grid is evolving from the existing power grid, NIST also included standards that support widely deployed legacy systems. The intent is for Priority Action Plans (PAPs) to be established with the goal of resolving interoperability issues between the standards for legacy equipment and those others identified for the Smart Grid.

NIST has developed Special Publications in the 800 series which provide documents of general interest to the computer security community. These are more guidelines than standards, but are very important for moving toward secure interoperability.
IEEE

IEEE is closely working with NIST and is also collaborating with other global standards bodies to effectively facilities standards coordination. IEEE has more than 100 standards and standards in development relevant to smart grid, including the over 20 IEEE standards named in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.

IEEE has brought IEEE P2030 Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads”. This standard provides guidelines in understanding and defining smart grid interoperability of the electric power system with end-use applications and loads. Integration of energy technology and information and communications technology is necessary to achieve seamless operation for electric generation, delivery, and end-use benefits to permit two way power flow with communication and control. Interconnection and intra-facing frameworks and strategies with design definitions are addressed in this standard, providing guidance in expanding the current knowledge base. This expanded knowledge base is needed as a key element in grid architectural designs and operation to promote a more reliable and flexible electric power system [6].

The draft report covers basic Smart Grid definitions, frame works, challenges and three different architectural perspectives viz. Power System, Communications Technology and Information technology. It also details about interoperability tables.

North American Electric Reliability Corporation (NERC)

NERC has recently issues security standards for the bulk power system. Although these security standards are explicitly for the bulk power system, it is clear that many of the requirements also apply to distribution and AMI systems, and may eventually become standards for these systems as well. The NERC CIP 002-009 Security Standards cover:

5.6 List of Standards

The standards and documents that is relevant for smart grid projects which involves interconnection of several technologically interdependent systems are listed in Table 5.1. The list includes both national and international references.

Adoption of standards reduces Cost and enables interoperability of Smart Grid technologies and future choices for companies that choose to install any particular type of technology independent
of vendor. It permits the integration of equipment and systems for controlling the electric power process into complete system solutions, necessary to support utilities' processes. Achieve cyber security objectives through digital signatures, authenticated access, preventing eavesdropping, playback and spoofing, and intrusion detection there by making risk management easy. Significantly reduces if not eliminates the vendor lock-in problem historically experienced in utility systems that use vendor specific proprietary information exchange technologies

### Table 5.1 List of Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS 13779</td>
<td>Indian standard for electricity meters, Class 1 &amp; 2</td>
</tr>
<tr>
<td>IS 14697</td>
<td>Indian standard for electricity meters, Class 0.5 &amp; 0.2</td>
</tr>
<tr>
<td>BIS ICS:DOC(6211)</td>
<td>Indian Companion specification for IEC 62056.</td>
</tr>
<tr>
<td>IEC 62056 series</td>
<td>Electricity metering : Data exchange for meter reading, tariff and load control</td>
</tr>
<tr>
<td>IEC 60870-6 / TASE.2</td>
<td>This standard defines the messages sent between control centers of different utilities. [ICCP]</td>
</tr>
<tr>
<td>IEC 61968/61970 Suites</td>
<td>These families of standards define information exchanged among control center systems using common information models. They define application-level energy management system interfaces and messaging for distribution grid management in the utility space.</td>
</tr>
<tr>
<td>IEEE 1547 Suite</td>
<td>This family of standards defines physical and electrical interconnections between utility and distributed generation (DG) and storage.</td>
</tr>
<tr>
<td>IEEE 1588</td>
<td>Standard for time management and clock synchronization across the Smart Grid for equipment needing consistent time management.</td>
</tr>
<tr>
<td>ZigBee/Home Plug Smart Energy Profile 2.0</td>
<td>Home Area Network (HAN) Device Communications and Information Model.</td>
</tr>
<tr>
<td>Open HAN</td>
<td>A specification for home area network (HAN) to connect to the utility advanced metering system including device communication, measurement, and control.</td>
</tr>
<tr>
<td>IEC 62351</td>
<td>This family of standards defines information security for power system control operations</td>
</tr>
<tr>
<td>NIST Special Publication (SP) 800-53, NIST SP 800-82</td>
<td>These standards cover cyber security standards and guidelines for federal information systems, including those for the bulk power system.</td>
</tr>
</tbody>
</table>

**Summary**

Interoperability is the key to the smart grid, and standards are the key to interoperability. Open standard based products/ solutions always ensure protection of investment over obsolescent.
6. Phasor Measurement Unit

A phasor measurement unit (PMU) is a device which measures the electrical waves on an electricity grid, using a common time source for synchronization. Time synchronization allows synchronized real-time measurements of multiple remote measurement points on the grid. In power engineering, these are also commonly referred to as synchrophasors and are considered one of the most important measuring devices in the future of power systems. A PMU can be a dedicated device, or the PMU function can be incorporated into a protective relay or other device.

6.1 Technical overview

A phasor is a complex number that represents both the magnitude and phase angle of the sine waves found in electricity. Phasor measurements that occur at the same time are called "Synchrophasors", as are the PMU devices that allow their measurement. In typical applications phasor measurement units are sampled from widely dispersed locations in the power system network and synchronized from the common time source of a global positioning system (GPS) radio clock. Synchrophasor technology provides a tool for system operators and planners to measure the state of the electrical system and manage power quality. Synchrophasors measure voltages and currents at diverse locations on a power grid and can output accurately time-stamped voltage and current phasors. Because these phasors are truly synchronized, synchronized comparison of two quantities is possible, in real time. These comparisons can be used to assess system conditions.

The technology is relevant in the smart grid regime which also looks at reliability improvement under optimum power delivery. The PMU technology would allow increased power flow over existing lines. Synchrophasor data could be used to allow power flow up to a line's dynamic limit instead of to its worst-case limit.

6.2 Wide Area Monitoring, Protection and Control (WAMPAC);
Wide Area Monitoring Systems are essentially based on a new data acquisition technology. In contrast to conventional control systems, where e.g. RTUs are used for acquisition of RMS values of currents and voltages, a Wide Area Monitoring System acquires GPS-synchronized current, voltage and frequency phasor measurements, which are measured by Phasor Measurement Units (PMUs), from selected locations in the power system. The measured quantities include both magnitudes and phase angles, and are time-synchronized via Global Positioning System (GPS) receivers with an accuracy of one microsecond. Critical nodes in today's transmission grids are usually monitored using static or quasi-dynamic data based on RMS measurements. Phasors measured at the same time instantly allow snapshots of the status in the monitored nodes to be made. By comparing the snapshots with each other, not only the steady-state, but also the dynamic state of critical nodes in transmission and sub-transmission networks can be observed. Thereby, a dynamic monitoring of critical nodes in power systems is achieved.

6.3 Applications

i. Power system automation, as in smart grids.

ii. Load shedding and other load control techniques such as demand response mechanisms to manage a power system. (i.e. Directing power where it is needed in real-time)

iii. Increase the reliability of the power grid by detecting faults early, allowing for isolation of operative system, and the prevention of power outages.

iv. Increase power quality by precise analysis and automated correction of sources of system degradation.

v. Wide Area measurement and control, in very wide area super grids, regional transmission networks, and local distribution grids.

6.4 Standards

i. The IEEE 1344 standard for synchrophasors was completed in 1995, and reaffirmed in 2001.

ii. In 2005, it was replaced by IEEE Standard C37.118-2005, which was a complete revision and dealt with issues concerning use of PMUs in electric power systems. The specification describes standards for measurement, the method of quantifying the
measurements, testing & certification requirements for verifying accuracy, and data transmission format and protocol for real-time data communication

iii. IEC 61850 a standard for electrical substation automation
7. Technologies for distributed generation

7.1 Background

The smart grid philosophy advocates adoption of DG in all possible forms and capacity to tide over the energy needs. These small sized DG units when deployed in large numbers will contribute a sizeable power in the LV or MV grid. The utility can leverage these DGs at times of peak to tide over the situation without load curtailment if possible.

7.2 Introduction

Centralized power concept is suitable for high density power pockets like towns and cities. But with growing concern about energy security any form of energy resource will be welcome. The present technology for harvesting renewable energy and the declining cost has given impetus to adopt for widespread deployment and bring in additional capacity. Distributed packages have many advantages over traditional grid connected distribution systems such as:

- Decentralized power
- Better control over the source because of the nearness
- Better source-load matching and consequently control over the load curve
- Boosting of sagging voltage in rural feeders
- Demand side management is possible
- The energy source can be directly used for end tasks without the necessity of converting to energy carriers like AC

The concept of rural micro grids are emerging in weakly powered areas based on distribution level injection of power from solar PV, Biomass or Wind.

7.3 Technology Options

The deterministic technologies where the energy storage in the form of fuels are as follows:

- Fossil fuel power : fuel oil based
- Bio-diesel
- Biogas
- Biomass gasifiers

The stochastic technologies are as follows:

- Solar thermal and photovoltaic
- Wind electric generators (WEG)
7.4 The technology options are as follows:

i. Solar photovoltaic
Solar photovoltaic panels have both stochastic and deterministic components. The advantages are clean and free energy.
Disadvantages are:
- High capital cost
- Stochastic nature of solar energy necessitating storage/back up

ii. Solar thermal
The possibilities are Solar Stirling engine & Solar Rankine engine

iii. Wind
While the advantages of wind are clean, free energy and capacity addition is in increments of MWs. The disadvantages are:
- Winds are not spread all over the year. Major winds occur during the rainy season.
- Stochastic nature of wind energy

iv. Biogas plants
Biogas generated from biological matter can be used for power generation through internal combustion engines. The advantages local and pollution free energy while the disadvantages are:
- Gas generation rates are low
- Smell of feed during retention period
- Gas needs to be cleaned of moisture
- High CO₂ content in gas

v. Biomass gasifiers
Downdraft gasifier technology through internal combustion engines is useful for small power applications of 5-100 kW. The advantages are local availability of fuel while the disadvantages are:
- Size reduction requirements
- Availability of biomass
- Price fluctuations of biomass

7.5. Integration of Distributed Generation

i. Mini-grids
Mini grids have evolved on the basis of:
- DC bus (because many renewable sources generate DC power).
AC bus
AC & DC bus

The DGs with current technology can be directly connected to grid.

The issues with grid connected systems are as follows:

i. **Reactive power management:**
Wind electric generators absorb reactive power but do not generate reactive power. The solution to this is to go for fixed/variable capacitor banks. However it must be mentioned that the response time of the variable compensators must be adequate to handle varying wind environments.

ii. **Over voltage:**
When penetration of WEG is higher or in other words when conventional generators (thermal and hydro) are under maintenance, over voltages up to 20 % of the rated voltages are experienced. Transient surges or voltage fluctuations lead to electronic components. The solution of this could be improvement in the short circuit levels of the system cards around the wind area, static variable compensators at a few locations, etc. Over 70 % of the failures on electronic cards, transient voltage surge suppressors are to be installed on electronic equipment sensitive to voltage variations.

iii. **Wind integration into the grid:**
According to a study wind capabilities up to 50 MW can be integrated into the grid without any modifications to the transmissions and above 100 MW systems re-engineering or re-configuration is required.

Spinning reserve requirements for WEG spread over different geographical areas are low and the regulation margins are more. Every unscheduled movement of power from the WEG must be offset through another deterministic resource (coal/hydro/nuclear). This problem is overcome by aggregating wind with other resources and considering this as a bonus resource, every MW movement of wind power need not be offset. Rather additional generation is to managed effectively. The capacity addition from wind must not be added to the grid capacity as this is not a fixed capacity and will not be available when the source is not generating.

iv. **Wheeling and banking:**
While banking works well wheeling of power between different locations in the same grid is difficult to implement in real time as the movement of power generated and drawn should match.
v. **Penetration of distributed generation:**

While penetration of up to 20% is smooth and trouble free penetration of above 20% present grid management problems. Injection of over 40% of power through distributed generation poses the question of feasibility. If distributed generation is sufficiently generated, unidirectional power flows are reversed. Bi-directional power flows improve the utilization factor the network. But above 40%, real time power flow management without affecting the regulating margin becomes a challenging task. The feasibility of the same has not been established till date.

Multi-source integrated packages are possible through integration of solar, wind with fossil fuels and grid. Integrated systems through AC grid, DC grid, AC & DC grids are useful for integration of multi-source integration with diesel engines and grid power. The advantages are that there saving in non-renewable fuels. Disadvantages are:

- High capital cost
- Reliability level is low because of multi-component systems

### 7.6. Pricing trends

The pricing trends for renewable power are much higher than the energy from conventional generation. Conventional power is priced at Rs. 2.5-4.5/kWh whereas biomass and wind are priced at around Rs. 6.5-7.5/kWh and solar pv is priced at Rs. 15-17/kWh. The markets for renewables are being presently driven by the renewable energy obligations of each utility and power entity.
7. References

[4] SMB Smart Grid Strategic Group (SG3), (June 2010) IEC Standardization Road Map; available online http://www.iec.ch/smartgrid
[8] Demand Side Management & Time of Use Billing in Indian Utilities, Ashish Sethia, Business Manager, New Carbon Finance
[13] Smart Grid – Train the Trainers Workshop Conducted by USAID