M.Sc. Internetworking

Capstone

Project Report

On

5G solution

For

Future Utility Networks

Submitted by
Gaganpreet Singh

Project Supervisor
Mr. Juned Noonari

Abstract/Introduction:

A smart grid is the modernization of power grid for automation of energy, where transmission, distribution, power generation, utilization, and management are fully upgraded to ultra-high speed and low latency cellular network to improve efficiency, agility, eco-friendly, economy, security, and reliability. In future, the smart grids /intelligent network will be the golden key for making decisions and manage the energy consumption, breakdowns, and maintenance. In addition to that it will encompass energy storage, smart meters, IoT / IoE and the most importantly Cyber Security over large geographic areas.

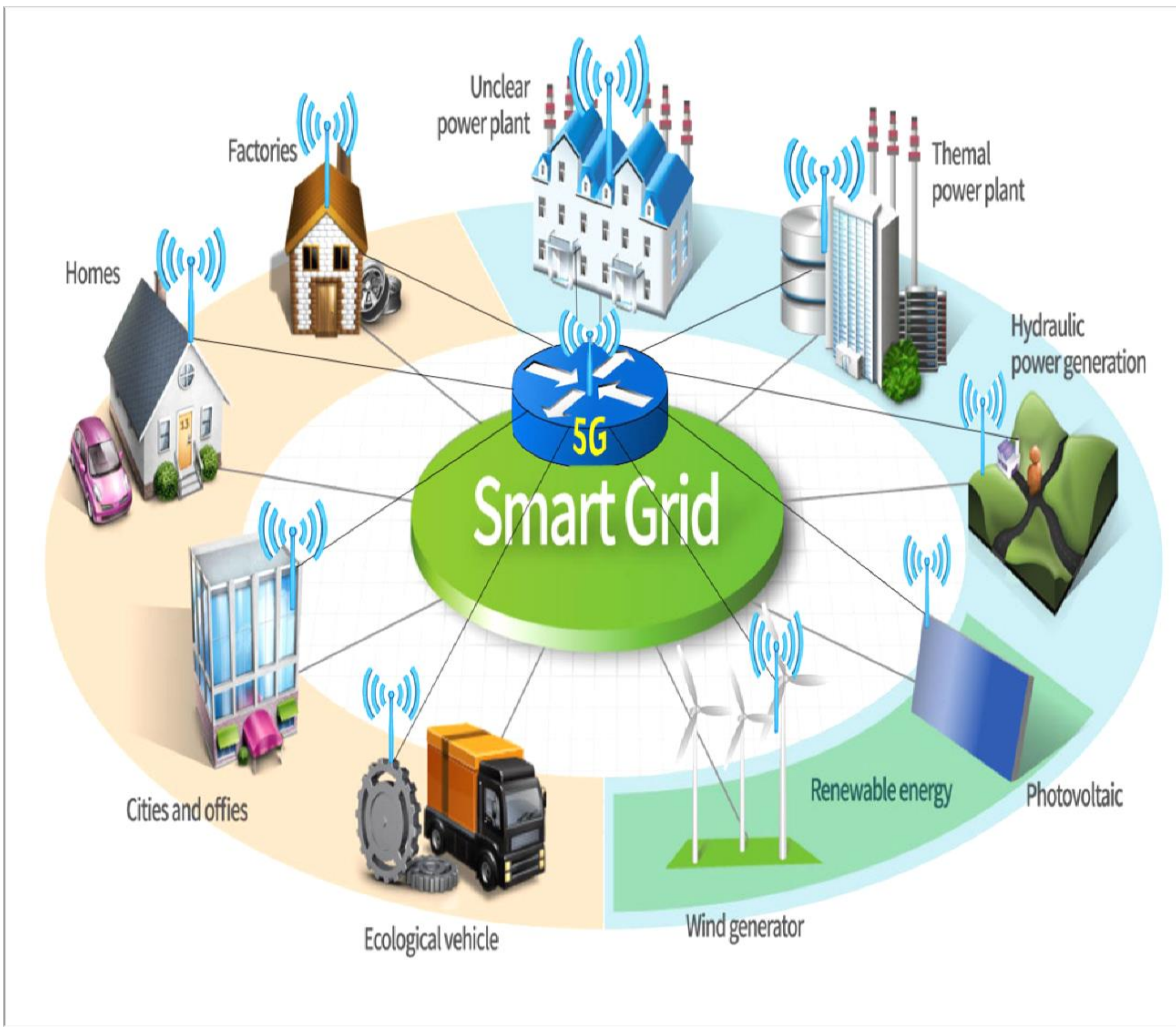


Figure – 1 Smart Grid Overview

Coexistence of technologies such as ZigBee, Wi-Fi, and Bluetooth and some domestic non-standardize appliances crowded the home area network (HAN) spectrum. Smart grid architecture requires high-speed data collection; real-time analysis of power transmission & consumption, fault detection & central alarm control system. Accomplishing this will require an essential move from the conventional unidirectional stream of communication and electricity to a bidirectional power stream known as a full duplex system.

The development in the IP based applications pushes the requirement for high bandwidth and all the more significant, high performance, efficiency and flexible bandwidth. Spectrum is the most critical component of a wireless network and the necessity of broad spectrum for smart grid network integration is there for a long time because the contemporary communication systems are designed for human communication and do not meet all the technical requirements of massive machines communication. The proposed spectrum for 5G is sub 1 GHz between 1-6 GHz and above 6 GHz (support IoTs, massive machines, wide spread coverage for high-speed data transfer). 5G networks will meet all these requirements, over a dedicated slice of the 5G network with the cost based on ongoing network usage. The consumers of this communication network will receive high data rate and ubiquitous connectivity, quality of service, low latency network and broadband access. Alongside their imagined benefits, these developing networks bring various challenges, for example, radio resources allocation and management, the concurrence of various networks, optimization of network slicing, software-defined core network architecture, dangerously expanded vitality utilization, edge computing for ultra-low latency, etc. It enables two-way transmission of data between sensors and monitoring systems; between control systems and energy generation, storage and transmission assets; and between control systems and end users' smart meters.

Machine-Type Communication (MTC) will be fundamental section of the fifth era cellular communication network in the Utility framework. Machine to Machine (M2M) correspondence of gadgets is independently or negligible human mediation. MTC has been additionally arranged into massive machine type communications (mMTC) and mission-critical machine type communications (uMTC). While mMTC is about the remote network to several billions of machine sort terminals, uMTC is about accessibility, low idleness, and high unwavering quality. mMTC means to meet requests for a further created computerized society and concentrates on administrations that incorporate high necessities for connection density.

Acknowledgement

To begin with, I am extremely indebted to the almighty for fostering immense strength in me to complete the project work. It was both challenging and interesting in my domain of study but with inner patience and support, I am able to present my work to you.

I express my sincerest gratitude to my project supervisor Mr. Juned Noonari, who rendered me with his invaluable guidance at each step. This project would not have been possible without his innumerable directions, contribution and mentoring skills. The stimulating suggestions and co-operation from him provided me a lot of confidence to take my work towards completion. His incredible knowledge in the subject gave me an impetus to present quality work.

I owe my deep gratitude to my program coordinator Mr. Shahnawaz Mir for encouraging and providing an opportunity to present the project for the partial fulfillment of the requirements for the degree of Master in Science in Internetworking. His guidance and help played a great part in choosing the project.

Finally, I would like to thank my family for their encouragement, quiet patience and unwavering love which acted as bedrock in this journey. Last but not the least I express my gratitude to the University of Alberta to give me this opportunity.

Table of Contents

Chapter II: 4G vs 5G

Chapter III: M2M Network Architecture for Smart Grids

List of Figures:

List of Abbreviations:

AMI	Advanced metering infrastructure
MTC	Machine-Type Communication
M2M	Machine to Machine
mMTC	Massive machine type communications
uMTC	Mission critical machine type communications
V	Volts
I	Current
P	Power
R	Resistance
J	Joules
A	Ampere
DC	Direct Current
AC	Alternate Current
HVDC	High Voltage Direct Current
IoT	Internet of things
IoE	Internet of everything
QoS	Quality of Service
UHV	Ultra-high Voltage
HV	High Voltage
MV	Medium Voltage
LV	Low Voltage
Emf	Electro motive force
NIST	National Institute of Standards and Technology
IT	Information technology
IED	Intelligent electronics devices
HAN	home area network
FAN	Field area network
NAN	Neighbor area network
WAN	Wide area network
PEV	Plug-in vehicles
SCADA	Supervisory control and data acquisition
MCU	Mater control unit
RTU	Remote terminal unit
UMC	Unattended monitoring and control
PLC	Programmable logic controller
AVR	Automatic voltage regulator
PMS	Power management system
HMI	Human Machine Interface
CB	Circuit Breaker
DNP	Distributed network protocols
IEC	International Electro-technical Commission

IETF	Internet Engineering Task Force
VT	Voltage transformer
CT	Current transformer
SV	Sampled Value
GOOSE	Generic Oriented Substation Event
MMS	Manufacturing Message
GCB	Goose Control Block
3GPP	3rd Generation partnership program
GPRS	General packet radio service
EDGE	Enhanced Data rates for GSM Evolution
CDMA	Code Division Multiple Access
WCDMA	Wideband Code Division Multiple Access
HSPA	High speed packet access
WiMAX	Worldwide Interoperability for Microwave Access
LTE-A	Long Term Evolution Advanced
TDD	Time Division Duplexing
FDD	Frequency Division Duplexing
MIMO	Multiple Input Multiple Outputs
HVAC	Heating Ventilation Air Conditioning
MAC	medium access control
VSAT	Very Small Aperture Terminal
GPS	Global Positioning System
GEO	Geostationary Earth Orbit
EMI	Electromagnetic interference
RFI	Radio frequency interference
OT	Operational technology
VPNs	virtual private networks
SONET	Synchronous Optical Networks
ICT	Information and Communication Technologies
3G	3rd Generation
4G	4th Generation
5G	5th Generation
GSM	Global System for Mobile Communications
NB- IoT	narrow band Internet of Things
EC-GSM- IoT	GSM/EDGE Internet of Things
CBS	Cell Broadcast Service
E-UTRA	Evolved UMTS Terrestrial Radio Access
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
EeNB	E-UTRAN Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
IP	Internet Protocol
P-GW	PDN Gateway

RAN	Radio Access Network
S-GW	Serving Gateway
NAS	Non-access stratum
UE	User Equipment
CRF	Charging rule functions
5G-CN	5G Core Network
NR	New Radio
SDN	Software Defined Network
ONF	Open Networking Foundation
API	Application programming interfaces
OF	Open flow
SDR	Software defined radio
SCR	Software Controlled Radio
NF	Network functions
PLMN	Public Land Mobile Network
SMF	Session Management Function
PCF	Policy Control function
NG	Next Generation
UDM	Unified Data Management
AUSF	Authentication Server Function
NSSF	Network Slice Selection Function
AF	Application Function
AMF	Access and Mobility Management Function
DN	Data Network
UPF	User plane Function
NEF	Network Exposure Function
SDSF	Structure data storage function
USDSF	Unstructured data storage function
PDU	Protocol Data Unit
WSAN	wireless sensor and actuator networks
LMR	Land mobile radio
TDMA	Time division multiple accesses
ETSI	European Telecommunications Standards Institute
IAN	Industrial Area Network
BAN	Building Area Network

Chapter – I

INVESTIGATION

- **Smart Grids**
- **Utility Communication Networks**
- **Utility Network Challenges**

1. Electrical Grid architecture :

The Electrical Grid architecture is consisting of Generation, Transmission, Distribution and Consumers and represented in Fig 2. The current grid infrastructure is a one-way flow of electricity and information from generation plant to consumers.

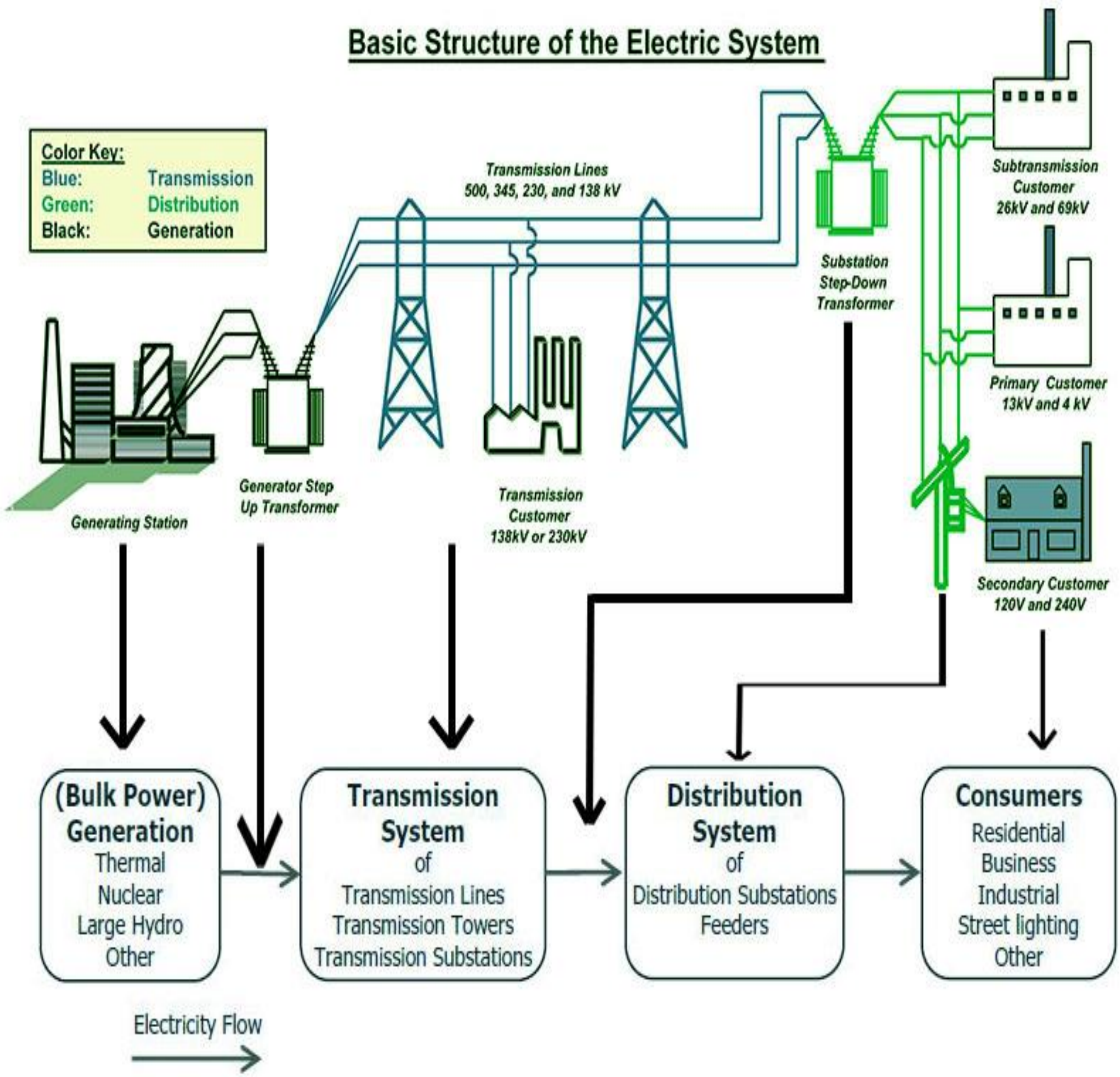


Figure 2 – Basic Structure of the Electric System

1.1 <u>Generation systems</u>: The demand of reliable electricity is increasing day by day. The legacy technique of generation of electricity is through fossil fuels (coal, oil and gas), but in contemporary times to reduce the GHG (greenhouse gases), carbon footprints, the electricity is also generate in nuclear power plants, modern wind farms, solar harvesting, fuel cells, biomass and biogas but they are limit to geographical areas. The major advantage is that the renewable energy sources convert the one form of clean energy into another form of clean energy.

<u>Electrical system is divided into DC and AC system and basics quantities are:</u>

1.1.1 <u>Voltage</u>: Voltage is a measurement of the electrical potential energy per unit charge. It is represented as 'V' and the metric unit is Volt (V).One volt is equal to one joule of electric potential energy per Coulomb of charge.

IV = I*J/C, where I = current, J = joules, C = Charge, V = Volt

For example: 12V, 24V, 110V, 220V, 440V

1.1.2 <u>Current</u>: It is basically flow of electrons from higher potential to lower potential and the rate of charge pass a given point in an electrical circuit. It is represented as '*I*' and the metric unit is Ampere, Amp (A).

One ampere is equal to one Coulomb of charge flowing past a point every second.

IA = I*C/S where I = current, S = Second, C = Charge, V = Volt

For example = 100mA, 1A

1.1.3 <u>Resistance</u>: Resistance is the hindrance to the flow of charge. The ratio of the voltage applied to the electric current that flows through the resistance. It also depends on temperature, resistivity, length, area of the conductor (R = *p**l/a). It is represented as R and the metric unit is Ohm (**Ω**).

R = V/I (by using Ohm's law), where I = current, V = Voltage, R = Resistance

For example = 10ohm or 10 **Ω**

1.1.4 **Power**: Power is the rate a t which energy is supplied. It is represented as P and metric unit is watt (1W = 1 joule/second).

P = V*I for DC system.

(Where P= Power, V = voltage, I = current)

For example, P = 12V* 1A = 12W

P = V*I*cosϕ for AC system

(Where cosϕ is power factor, ideally it is 1)

For example, P = 220V* 1A*0.8 = 176 W

1.1.5 **Ohm's law** V = I*R

It shows the relationship between voltage V and current *I* in a system, where positive and negative terminals of the battery or DC generator is connected with resistance. Basic principle is a flow of electron from high potential (positive terminal) to lower potential (negative terminal) via load (resistance).

1.1.6 **Direct current (DC) system**:

The voltage and current waveform remain constant over time and the frequency is zero. The flow of electric charge is unidirectional as shown in Fig 3.

The main source of generation of DC system are Batteries (chemical reaction) , Solar system, Fuel cells , converting AC into DC and DC generator (It converts mechanical energy into electrical energy , engine is rotated by steam, fuel, hydro, wind energy and it is couple with electrical windings (field and armature) , that generate DC voltage and current).

The main disadvantage of DC system is that the step up or step down of voltage level with transformer is not economical but High Voltage DC (HVDC) transmission over-sea is economical.

For example: 250 km of Baltic Cable Link between Sweden and Germany, 290 km of Basslink between Australian and Tasmania. [40]

Applications of DC systems in low voltage appliances are cell phones, IoT, smart-meters etc.

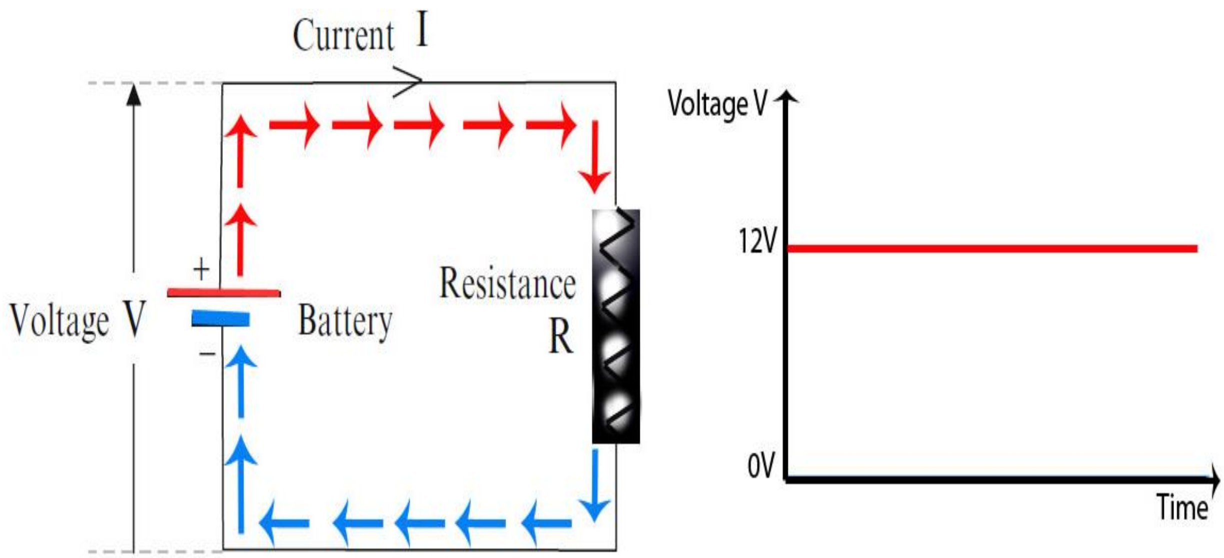


Fig 3 – A simple DC electrical Circuit

1.1.7 Alternating current (AC) system:

The voltage and current waveform reverse the polarity periodically over time. The magnitude and direction of voltage and current waveform change from positive cycle to negative and vice-versa over time. AC system is bidirectional. Standard frequencies of AC system are 50 Hertz and 60 Hertz. Most of the electrical grids are AC. Fig 4; depict the circuit diagram, phasor diagram, detailed components of the waveform to understand the AC system.

The AC voltage is generated through alternator (It convert mechanical energy into electrical energy , engine is rotated by steam, fuel, hydro, wind energy and engine is coupled with stator windings and rotor winding , rotor produce magnetic field and with a principle of electromagnetic induction ,rotating conductor cuts the magnetic field which generate AC voltage and current.)

The advantage of AC system is that the voltage level can be step up and step down with transformer but on the other side the distribution of high voltage AC require more insulation on wires to protect from leakage current.

Application of AC system is energy consumed in households, industries and other form of energy consumption.

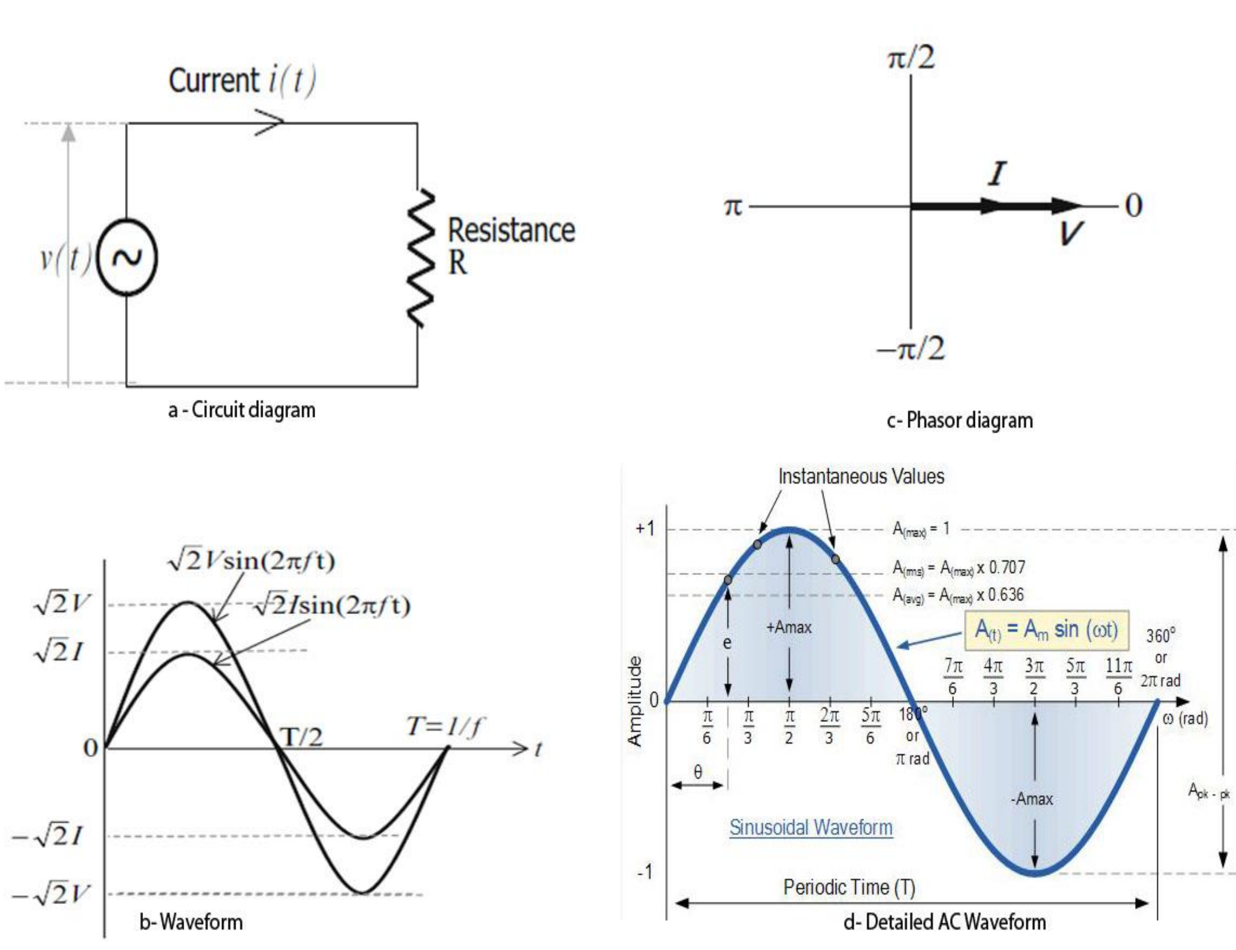


Fig 4 – [1] A simple AC electrical circuit and waveform

1.2 Transmission Systems:

The transmission system of electrical utility is to move bulk electrical power from generation plant to distribution grid and to wide range of consumers. Transmission system is critical to fulfill the continuously changing demand of energy over large geographical areas, a different type of generation plants supplies energy parallel with the interconnection of transmission system. The most important factor of transmission is to minimize the power losses, safe and reliable connectivity over long distances.

Fig 5 – [2] Transmission system

Transmission systems have a hierarchy of different voltage levels from UHV to LV.

- **Ultra-High Voltage** (UHV) > 230 kV ~ nearer to generation plants
- **High Voltage** (HV) > 35 kV < 230 kV ~ nearer to generation plants or in between distribution substations depending upon voltage transmission design.
- **Medium Voltage** (MV) > 1000 V < 35 kV ~ in between distribution substations.
- **Low Voltage** (LV) < 1000 V (450V, 440V, 220V, 110V) ~ supply to residential, small business and industries for different applications.

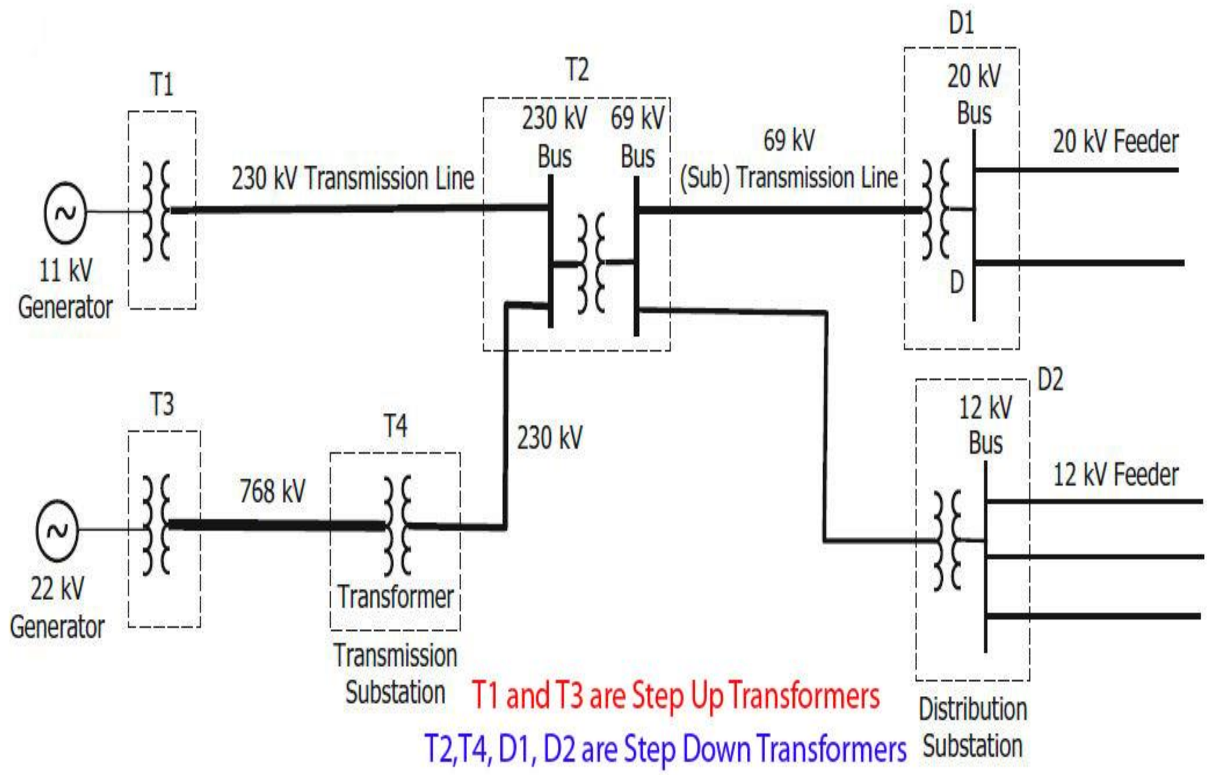


Fig 6 [3] Transmission system line diagram

Most common transmission system (often called High Tension Feeders) is AC system and the voltage level is step up (High voltage) or step down (Low voltage) with Transformer as shown in Fig 6. The working principle of transformer is electromagnetic induction, transformer consists to two coils (called primary and secondary windings), and core and windings are insulated from each other. Voltage is applied to primary winding of the transformer which induce emf (electro-motive force) on secondary winding and the voltage level is generated depends on ratio of primary to secondary windings.

Step up transformer (Low voltage to High voltage) have more turns of winding on secondary side than primary side and vice-versa for Step down transformer (High voltage to Low voltage). Step up transformer is used at generation plant, the main reason behind the extra high voltage transmission is to minimize or lower transmission power losses (I2R). At low voltage substation division step down transformer is deployed to convert back the voltage level to lower because the household appliances are designed at low voltages.

1.3 Distribution systems:

Distribution systems are taking power from overhead transmission systems (step-down transformer at substation) and safely distribution of uninterrupted power supply to residential, commercial and industrial consumers.

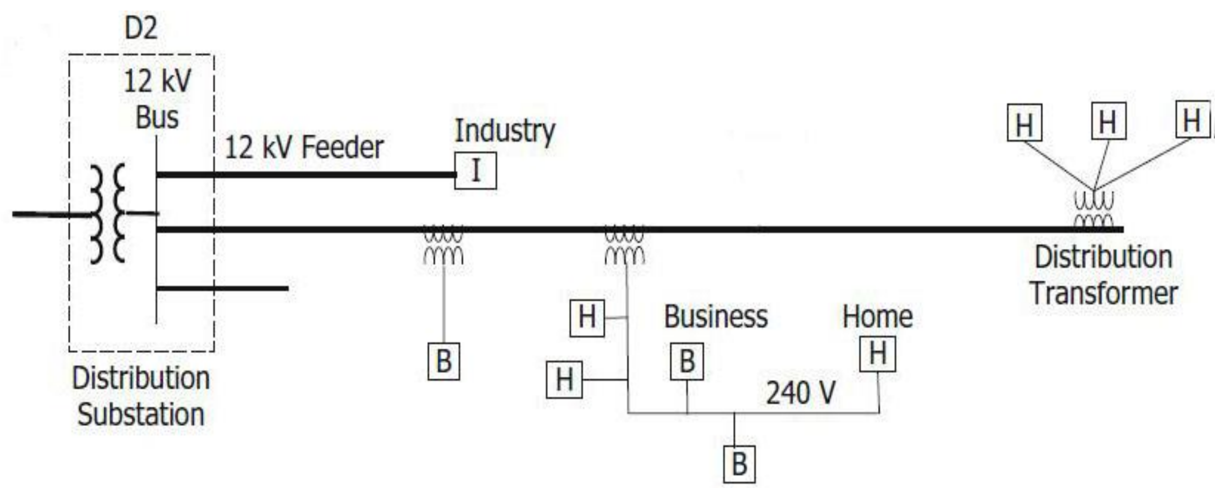


Fig 7 – [3] Distribution system

1.3.1 AC distribution systems are carrying different voltage levels.

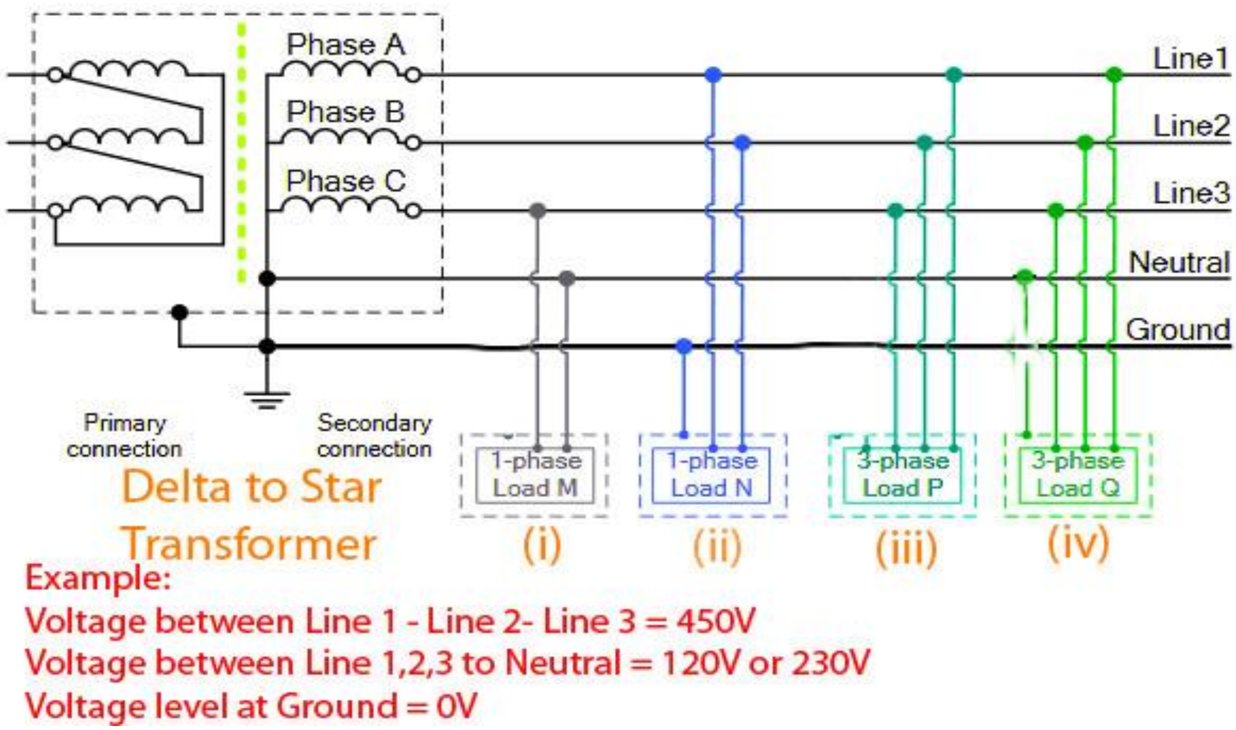


Fig 8 – [4] AC distribution system

(i) Single phase and two wires (live and neutral, usually l10V/220V)

(ii) Single phase and three wires (live, neutral and ground)

(iii) Three phase and three wires system (It is the most common system for 440V/450V connected star-connection or delta-connection (insulated neutral system), three R, Y, B wires with phase voltage is 440V/450V).

(iv) Three phase and four wire system (It is same as three phase and three wire star-connection but 4th wire is taken from star point called neutral point.)

1.3.2 Distribution system design:

1.3.2.1 Radial Distribution systems: In early days of deployment, radial distribution system was a central point and independent feeder's branch supplies the energy to consumers. The primary disadvantage was lack of redundancy, if a fault occurs or scheduled maintenance performed on any of independent feeder or central distribution system, the consumer connected to respective feeder experienced the blackout.

The advantage of this system is less capital investment required.

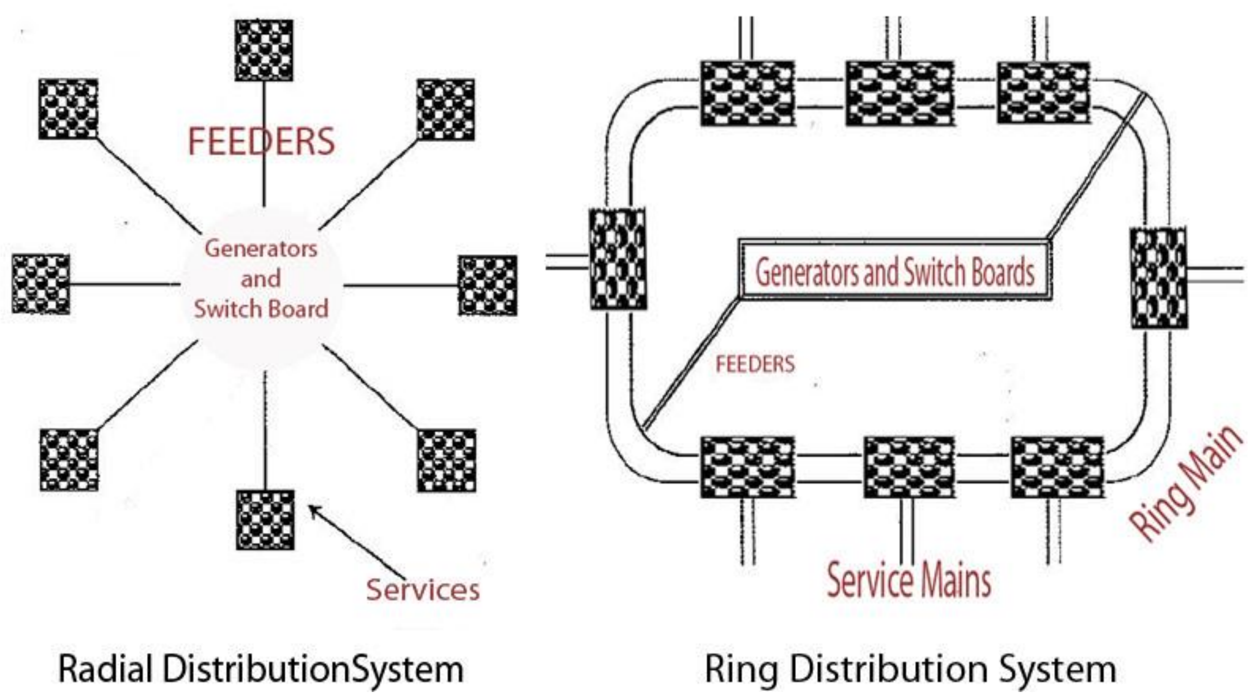


Fig 9 - Distribution system design

1.3.2.2 Ring Distribution systems: The distribution system design upgrade to ring distribution system for uninterrupted power supply to consumers. In this system, a number of power sub-distribution points are created in the form of the ring structure and central system is connected more than one point to the ring. The advantage of the ring system is that the sub-distribution system of the ring can perform scheduled maintenance with the continuous power supply to the consumer from other power sub-distributors.

1.4 Smart Grid:

Smart Grid consists of intelligent monitoring and control system that manages the demand, supply and quality of electrical energy throughout the Generation plants, Transmission system, and Distribution system and up to end users.

National Institute of Standards and Technology (NIST) defines that the smart grid is the integration of information technology (IT) network infrastructure for managing Generation plant, Transmission system, Distribution system and End-User with series of sensors, intelligent electronics devices, AMI (Advanced metering infrastructure) that exchange two-way real time communication. Smart Grid will lower the carbon footprints produced by generation plants running on fossil fuels by interconnecting with modern renewable energy sources. These renewable energy sources are inexhaustible, abundant as well as highly depends climate condition and geographical areas but the rising demand for energy consumption and prices can be efficiently managed with the integration of smart grid infrastructure.

1.4.1 NIST - Smart Grid Domains:

The conceptual model is meant for understanding the Smart Grid high- level operations, standards and protocols, identification of actors , communication paths, inter and intra domain interactions. Smart Grid conceptual model is divided into seven domains and each domain is including actors and applications. Actors may be systems, programs or devices that are responsible for making a decision and exchanging information (example, smart meter is “device”, power control system is “system”); and applications are the action carry out by actor within a specific domain.

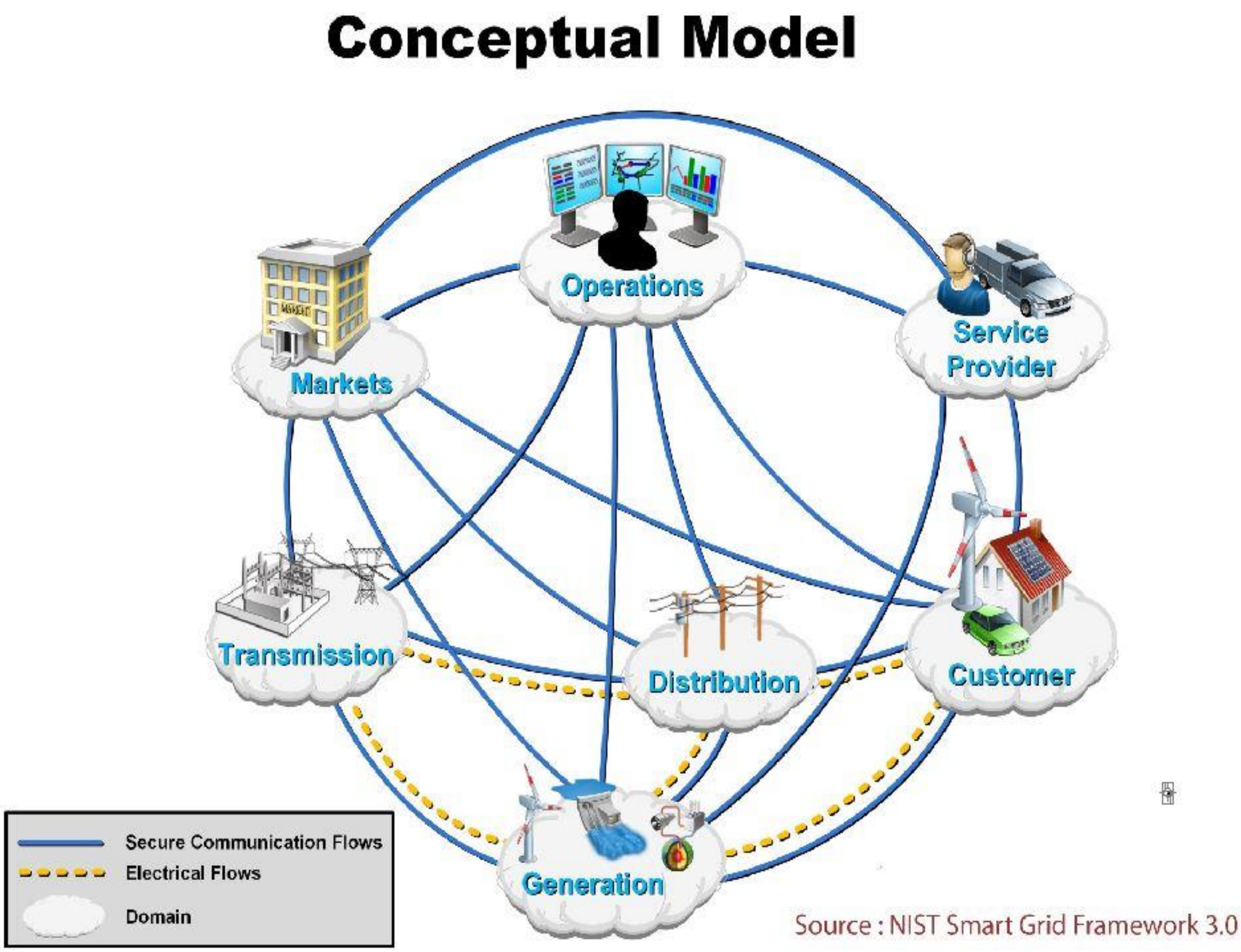


Fig 10- [5] Conceptual seven domains

- **Customers**: In smart grid infrastructure, the end users may also generate electrical energy (mainly from solar panels and wind turbines) and sell the energy to Grid.
- **Markets**: Energy market includes investors, stakeholders and operators for buying and selling energy, stock trades.
- **Service providers**: The different organizations are responsible for supplies and services to consumer and utility.
- **Operations**: Overall control center of each domain, which manage the communication, power supply and services.
- **Bulk Generations system.**
- **Transmission system.**
- **Distribution system.**

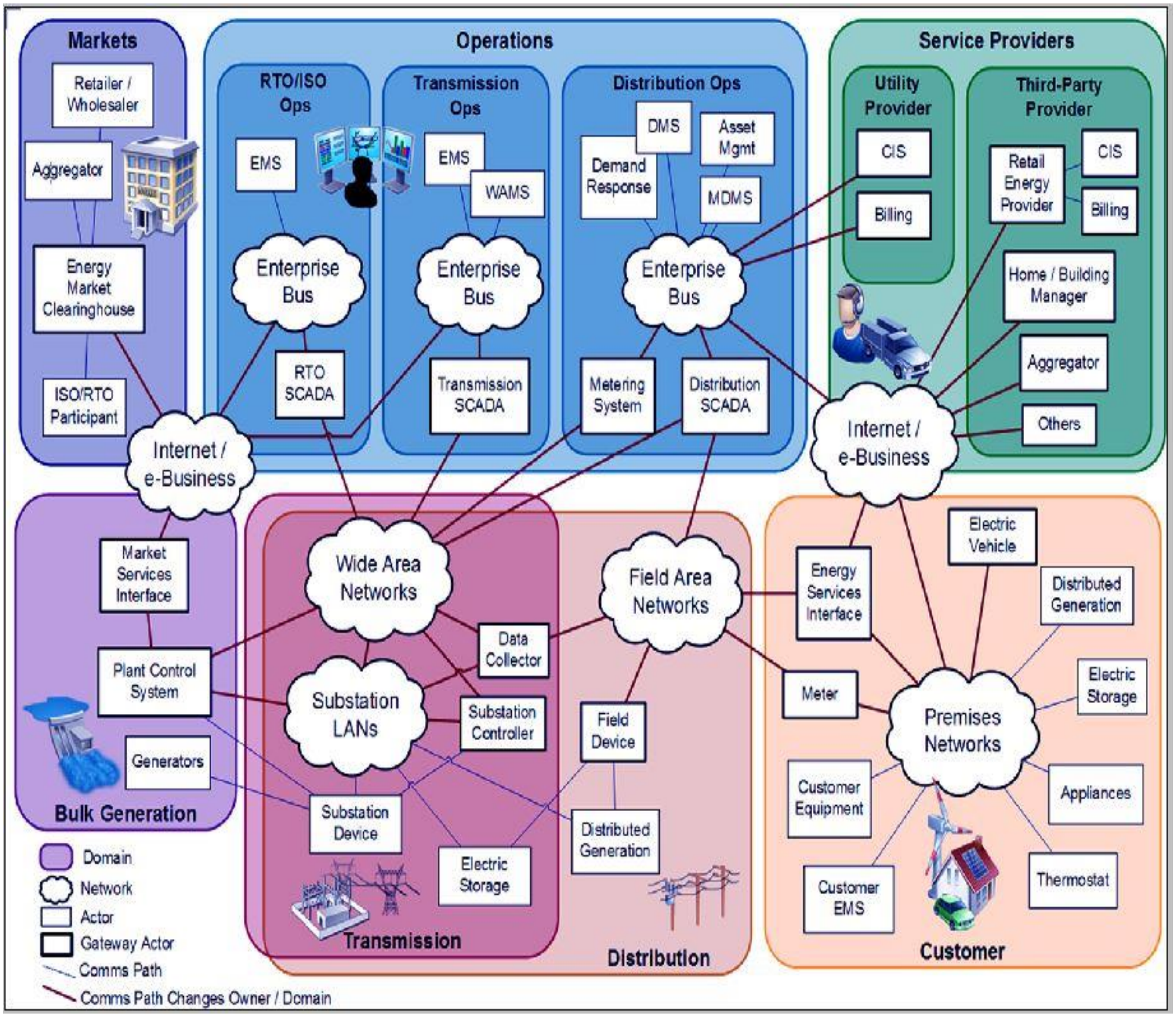


Fig 11 – [5] Smart Grid Information Network - (Logical Model of Legacy Systems Mapped onto Conceptual Domains)

- **Domain**: Smart Grid's seven domains are a classification of systems, buildings, organizations, devices or actors of common goals. Domains may divide into sub-domains, for example in Fig 11 Transmission domain is part of Distribution domain. Domains are interconnecting with each other for exchanging information with different communication networks which produce efficient operation of Grid.

- **Actor**: In the Smart Grid an actor may be individual, organization, software program, computer system or any device which is efficient in decision making as well as transfer information among actors.
- **Gateway Actor**: Gateway actor is communication interface between actors in different domains. Many communication protocols may be used by gateway actor within same domains. Gateway actor may use single or multiple protocols simultaneously.
- **Information Network**: Exchange of information is only possible between domains, actors, gateway actors with the planned deployment of different network technologies. It is aggregation of communication devices, servers and data centers are required to store massive data. For example : The connection between back office control center specialized application with other domains is Enterprise bus ; Wide area network connects the different sites of domain that are separated geographically for high speed data transfer ; Field area network connects IED devices which controls the circuit operation , voltage level, frequency level in generation , transmission and distribution system; home area network connects the Internet of things such as sensors, thermostat, smart appliances, home automation, security devices in consumer domain to operation domain. These networks may be implemented with a combination of public and private networks but cyber security is the big concern when communication is through the public network.

1.4.2 Smart Grid Functionalities:

1.4.2.1 Wide-area situational awareness: All the Smart Grid domains exchange real-time information over a wide area. It will optimize the power system, for example if any fault occurs in any part of the grid, it will self-notified to operation center domain. The service request will forward to the service provider for fixing the fault. In the meantime, the power supply of consumer will switch to battery reservoirs of photovoltaic cells and also called micro grid operation.

1.4.2.2 Demand response and consumer energy efficiency: The actors in the consumer domain will notify the operation domain about the power demand schedule. The power management system will control the load demand. During peak hours the entire required energy generation source will start to meet the demand, but it will stop automatically as the power demand reduces.

1.4.2.3 Electric transportation: As stated above, the smart grid will also reduce carbon footprints of transportation industry by integration of massive plug-in electric vehicles (PEVs).

1.4.2.4 Cyber-security: Actor in consumer domain provides the real time secure information of energy consumption, graphs as well as privacy to consumers. For example the information will be encrypted first then transmitted and authorize a user with decryption key can access the information. Multiple advanced protection protocols are required to prevent cyber-attacks.

1.4.2.5 Network Communication: The Smart Grid communication network will be public and private; the design is depending upon the networking requirement of actors, application, domain and subdomains. It is critical to implement standardize technology of wired or wireless network sensors for an end to end communication of all domains for reliability, resiliency and security. For example, Operation domain use the weather forecast information of hurricane from the internet and send proactive approach signal to the distribution grid management system to cut off or reroute the power supply and early notification of energy outage duration send to affected consumer domain.

1.4.2.6 **Advanced Metering Infrastructure (AMI)**: AMI is a bidirectional real-time communication system with intelligent hardware and software, smart meters, data management system for process data in the meter and only send encrypted information to the server. They are deployed in consumer domain to manage the automatic meter reading, demand response Management , real-time pricing of energy consumption, scheduling of smart appliance (such as electric boilers, dryers, AC and other smart appliances operates at off-peak hours), dynamic pricing rather than fixed price. AMI monitor two-way power flows by using micro grid technology.

1.4.2.7 **Distribution grid management**: Distribution grid management optimizes the automation control system, data collector, storage system of distribution domain and transmission sub-domain. The automation system of these domains is extremely important for the operation of mission-critical machines at different sites. It will increase reliability, energy efficiency, automatic reroute power path to the consumers via the complex distribution network, fault detection, linear demand response operation and most important constant voltage and frequency levels and other power parameters in case of sudden increase/decrease of load demand.

2 Utility Communication Networks:

The Electrical Grid has experienced the evolution in control and automation system time to time as the technology has evolved from the mechanical control system, electro-mechanical control system, hydraulic control system, pneumatic control system, electronic and instrumentation control system, intelligent automation and logical control system. On the other side grid communication networks are not revolutionized universally as cellular communication networks with a horizon of 5G communication technology.

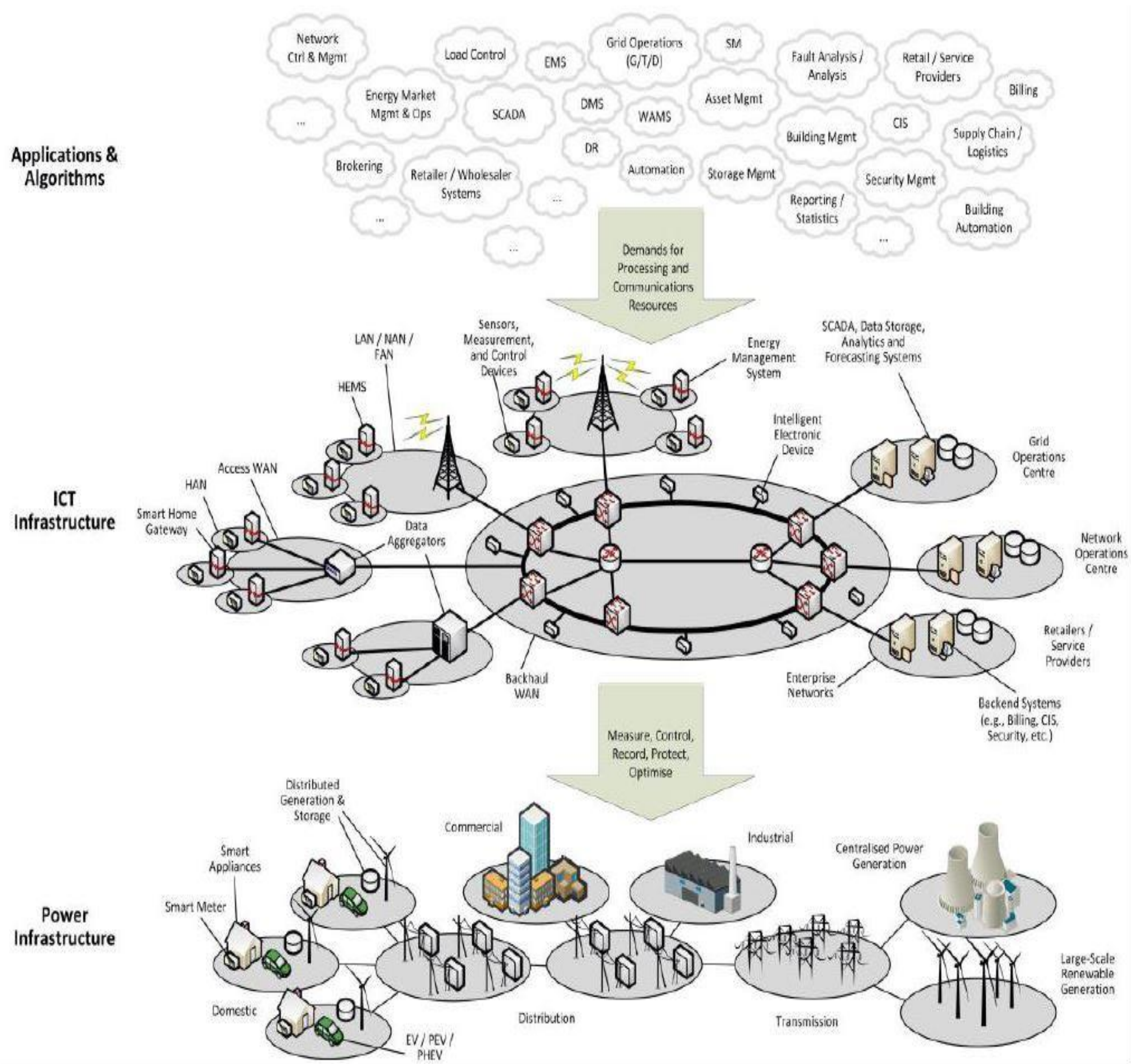
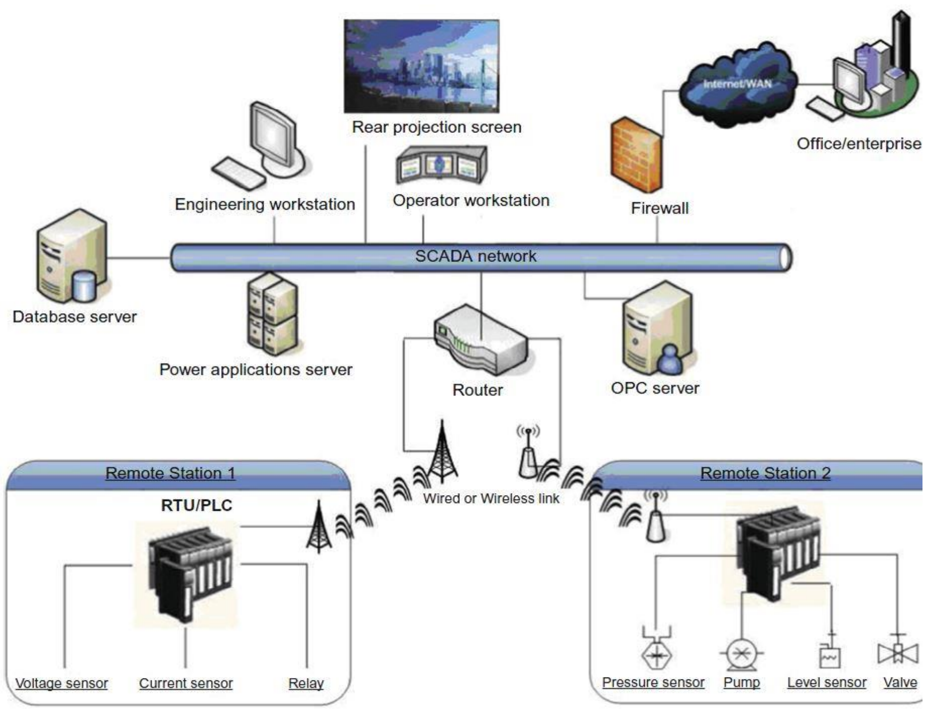


Fig 12 – [6] Utility Communication Networks

The hybrid communication network of Smart Grid will support multiple devices and its application such as Supervisory control and data acquisition (SCADA), Distributed control system, AMI, VoIP , video surveillance, mission-critical applications but in the conventional grid, the communication network infrastructure is limited to automation and control system widely known as Supervisory control and data acquisition and tele-protection applications. Usually, in the generation domain DCS system is used while in transmission and distribution domains over large geographical area SCADA is deployed for measurement, process, analyses and control the information. SCADA is one of the many critical application in the utility center developed by power system vendors and can be considered as brain of the grid. SCADA system is also used in various industries such as gas, water, transportation and utility for monitoring (measurement and reporting from electric substation measurable quantities voltage, current, frequency, power) and remote control of measurable real-time information for reliability, performance and security.

2.1 SCADA Control Components:

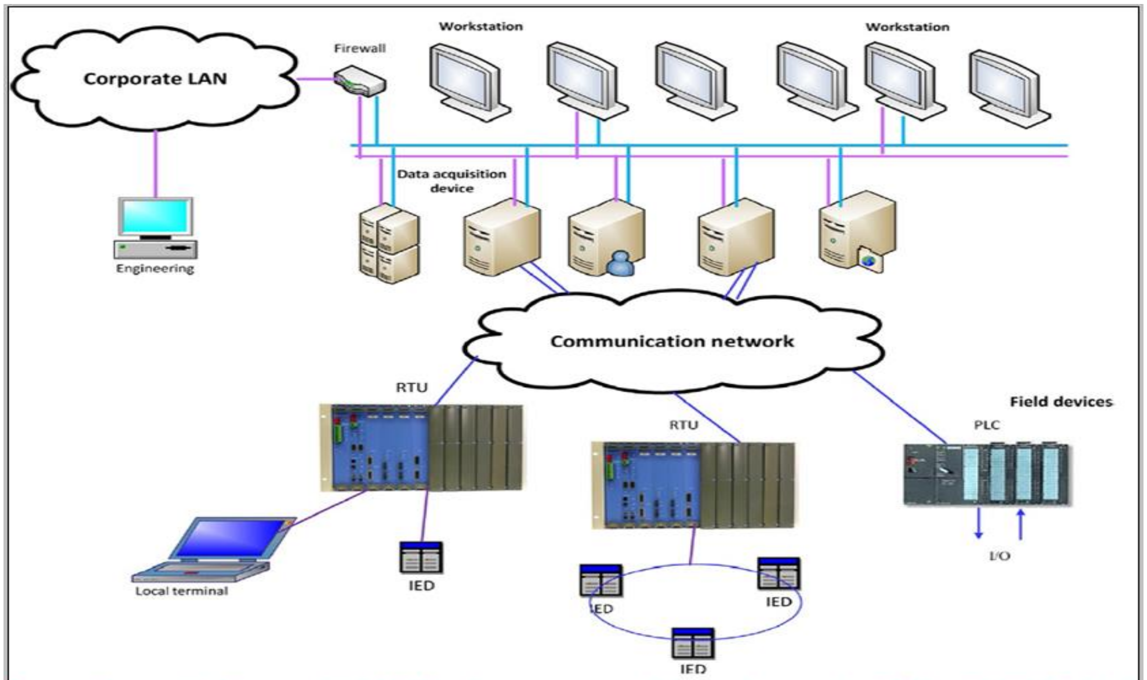


Source : Chapter 18 , Page no : 484, SCADA and smart energy grid control automation (K. Sayed*,†, H.A. Gabbar)

Fig 13 – [7] SCADA system network

2.1.1 SCADA control server: In the conventional grid, the problems of control system were to centralize control center, inflexible, and vendor specific. The need of decentralized, flexible and open standard evolved with the integration of intelligent software system. It hosts the supervisory control software on the high-performance server for communicate with input and output components of the system. It receives the input signal, processed in the controller (closed loop system) and send output signal according to deviation in the system. SCADA server act as master control unit which control the Remote terminal unit at remote sites and in case of malfunction the redundant server always operate in "live" backup mode for resiliency.

2.1.2 RTU (Remote terminal Unit): RTU is a microcontroller based modular device with data processing functions and remote telemetry functions that is the interface between field instrument devices and SCADA MCU (master control unit). The installation design is many different RTUs in a cabinet with a connection to different IEDs or one Master RTU connected with slave RTU at various locations of substation and communication via fiber optics. RTU is installed in small sites like a pole-mounted transformer to a very large power substation. The Modern RTU has expandable modules like analog/digital input/output cards, accumulated input units, and power supply and communication cards. It is usually used in unattended monitoring and control (UMC) remote stations and support wireless radio interface for transmitting and receiving telemetry data to master control system where wired communication is not feasible.



Source : Chapter 18 , Page no : 504, SCADA and smart energy grid control automation (K. Sayed*,†, H.A. Gabbar)

Fig 14 – [8] SCADA IED, RTU, PLC

2.1.3 PLC (Programmable Logic Controller): PLC is a solid state control system that controls the different parameter of electrical system based on the logical operation and these logics are programmable as per system requirement. In the input side of the PLC are the sensors and transducers which measure the quantities such as voltage, current, frequency and power. It processes the inputs signals in the controller according to program (logic) and the output signal is sent to the actuator, valves to control the parameters. If the human attention is required the audio visual alarm signal is sent to the display of the SCADA system. PLC replaced the hard wired electrical relays system to compact digital solid state control system.

For example : Generation plant is generating 440V and load is 500 KW, voltage sensor continuously sensing the output voltage via a step-down transformer (usually 5V) and send the input value to PLC , then PLC compares the input voltage with a reference voltage. If there will be a sudden increase in load, the voltage tends to decrease. PLC generates the deviation signal and sent to AVR (Automatic voltage regulator, device control the voltage of generator), the AVR increased the magnetic field in the rotor and voltage level will increase to 440V. If the load continues to increase, the PLC (PMS power management system) send a signal to start another generator to manage the load.

2.1.4 IED (Intelligent Electronic Devices): IEDs are advanced technology based micro-controller devices and are being deployed mostly in the mission critical application (tele-protection applications) of the power grid, in this the SCADA system process automatic control at the local level (edge). It supports IP enable two-way communication with all the smart sensing devices to gather the data for efficient operation of the grid. Then this gathered information processed locally in PLC controller and adjust the parameter of the power system. Additionally, IEDs are compact in size and immediately identify the faults, make an intelligent decision and achieve the self-healing methodologies by real-time communication with SCADA server through Ethernet port or serial port. The IEDs communicate with other IEDs (in series) and modern RTUs via RS-485 because it supports high speed, communication capabilities and long distance. IED device types: Protection relays, Auxiliary relays, Remote contactors, Load Tap changer, Solar Flare detectors, Revenue Meters.

2.1.5 HMI (Human Machine Interface): HMI is a full graphical representation of the human machine control system interface. The multi-display GUI shows the power system and networks along with electrical transmission and distribution system in a geographical perspective. It will allow humans to monitor all the parameters, change the control setting remotely, override the safety alarms but not critical safety alarms on mimic feeder and control diagrams on display. The HMI allows the easy configuration, backup and reset the set points of controllers, audio and visual fault detection alarms. Moreover, it displays the historical information, alarms and process logs, authorizes user login and change logs. The HMI display may be located in control room computer, remote laptops or on web browsers.

2.1.6 Input/output (I/O) servers: I/O server is the central point of collecting, buffering and access to process information of various inputs and output signals receiving from sensors, actuators and other field instruments. These I/O signals can access by different controllers concurrently, without having dedicated I/O unit to separate controllers. I/O server is also used by HMI to display the real time values of the smart grid components.

SCADA system is vital for the reliable operation of smart grid in daily operations, stormy weather conditions, fault isolation and service restorations. It can be integrated into the smart grid by electrical, electronics, automation and communication network that allows aggregation of information and centralize control of power supply chain from generation domain to consumer domain. SCADA application requires communication to exchange the periodic data packets between MCU and RTU in generation plants, storage system, distribution system, transmission system and other domains of the smart grid. SCADA and RTU communication network generally different in size and depends upon design and requirement of the system. For example the number of RTU, volume of traffic, latency requirement of the system, location and distance between RTU and field devices and location of control centers.

Smart Grid digital communication network exchange data over various diverse technology, protocols and intelligent devices over wired and wireless technologies such as Bluetooth , ZigBee, a cellular network, fiber optics, power line communications and satellite. SCADA system communicates with IED over a dedicated protocol that can be transmitted over Ethernet or serial port and from RTUs to SCADA system support different type of communication methods via local area networks and wide area networks such as analog modem networks, frame relay network, fiber optics, wireless radio and satellite communication networks.

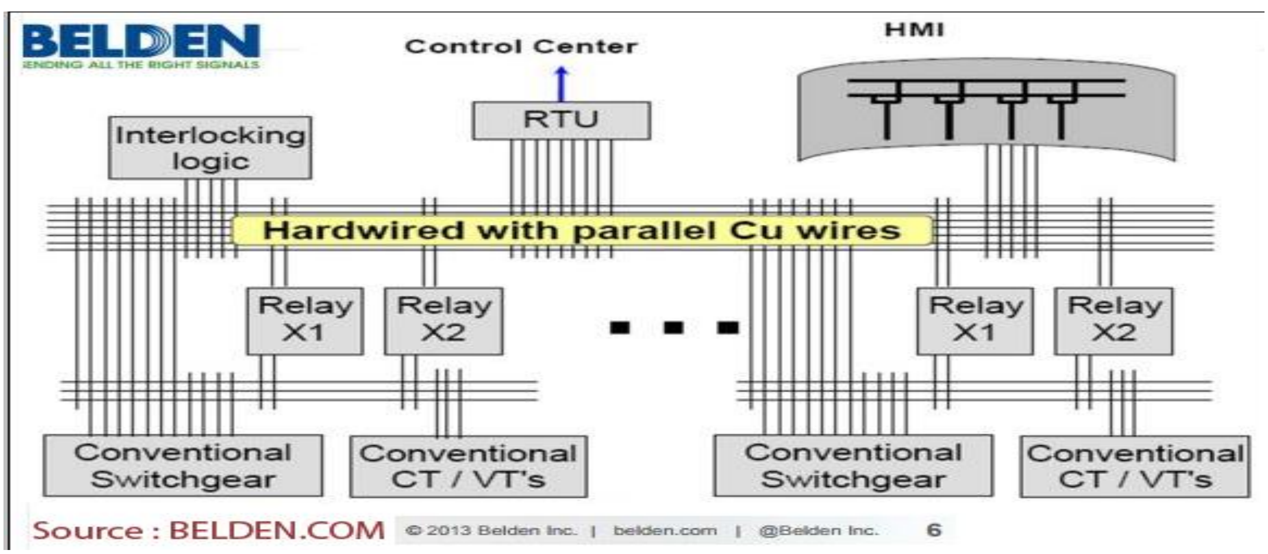


Fig 15 – [9] Hardwired conventional diagram

In early times the SCADA networking was implemented over circuit switching (dedicate path) thus variation and transmission delay was small. The technology is obsoleted which require hardwired status monitoring and control of RTUs for example circuit breaker (CB) auxiliary contacts are hardwire connected to RTUs for the status of CB (open or close) and also hard wire connected to a protective relay for initiating the closing and opening sequence. There are several emerging protocols available for implement of SCADA system such as Modbus, distributed network protocol (DNP), Fieldbus but modern substation automation, control and communication network system are designed under guidelines of International Electro-technical Commission (IEC) 61850 standards. The SCADA network can be designed based upon the different requirement of networks and transmission protocols (different TCP/IP suite but follow OSI model) of Ethernet and frame relay and the range of data rate is from 75 bits/sec to 2400 bits/sec.

SCADA is moving to connection-oriented TCP/IP standards with the advantages of worldwide adoption, simple application layer, strong network management, ensuring security, easy integration of hardware and software and migrate to single converged network. The problem arises will be the network congestion due to the business and nonbusiness applications traffic and latency requirement for different SCADA applications. The Internet Engineering Task Force (IETF) has ensured high Quality of Service over Multi-protocol label switching (MPLS) to classify the traffic that meets the requirements such as high availability, appropriate priority, secure and strong architecture. It improves the throughput and reduces the operational cost of Smart Grid by replacing the SDH/SONET network with IP/MPLS networks.

2.2 IEC 61850

2.2.1 **IEC 618560** is a standard for substation automation data and Ethernet-based communication network. It is used to deploy smart grid devices and communication network universally and provide interoperability (substation to substation, asset condition monitoring, substation to control center, synchro-phasor and also, communication within other domains). It is an architectural reference for communication between substation automation devices and in the beginning it is introduced for intra-device exchanges over local area network at substation level.

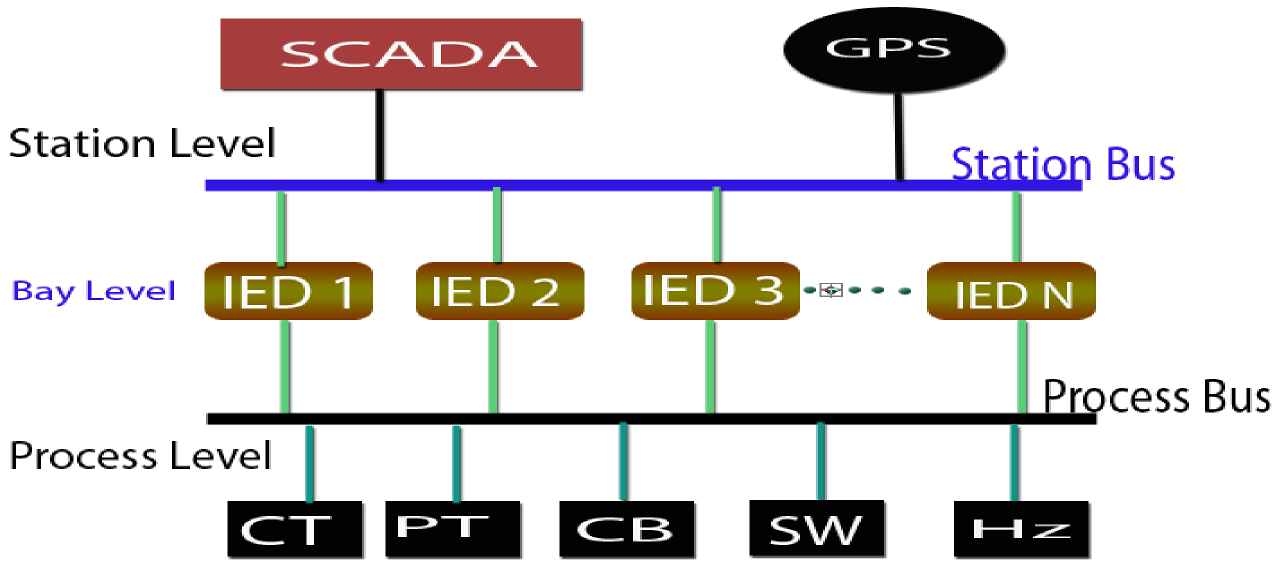


Fig 16 – 61850 Three level architecture

The three level of architecture consists of Station level, Bay level and Process level. In the station level the SCADA monitoring and control system, gateways are connected to station bus and the IED devices (protective relays, fault recorder) are connected with Station bus and Process bus at Bay level. The station bus is for polling the devices, controlling the opening and closing of the circuit breakers by reading the data from devices with Manufacturing Message Service. In the process level the end primary devices are connected such as voltage transformer (VT), current transformer (CT) and number of circuit breakers and Switch Gears.

In the traditional substation design the devices in the bay level and process level were connected via hardwired, but in this architecture hard wires are replaced with optical fiber for high speed and reliable communication. The process bus transmit and received the real time samples from various sensors with Sampled Values (SV) and Generic Oriented Substation Event (GOOSE) messages for example the voltage transformer measures the voltage of the generator and current transformer measures the current drawn by the load and IED send these values to SCADA.

The two types of data transfer methods are Client-Server architecture and Publisher-Subscriber architecture, the client server architecture is not having time critical reports and information's. The Publisher and Subscriber architecture are time critical information such as multicast GOOSE and SV messages for status of primary devices.

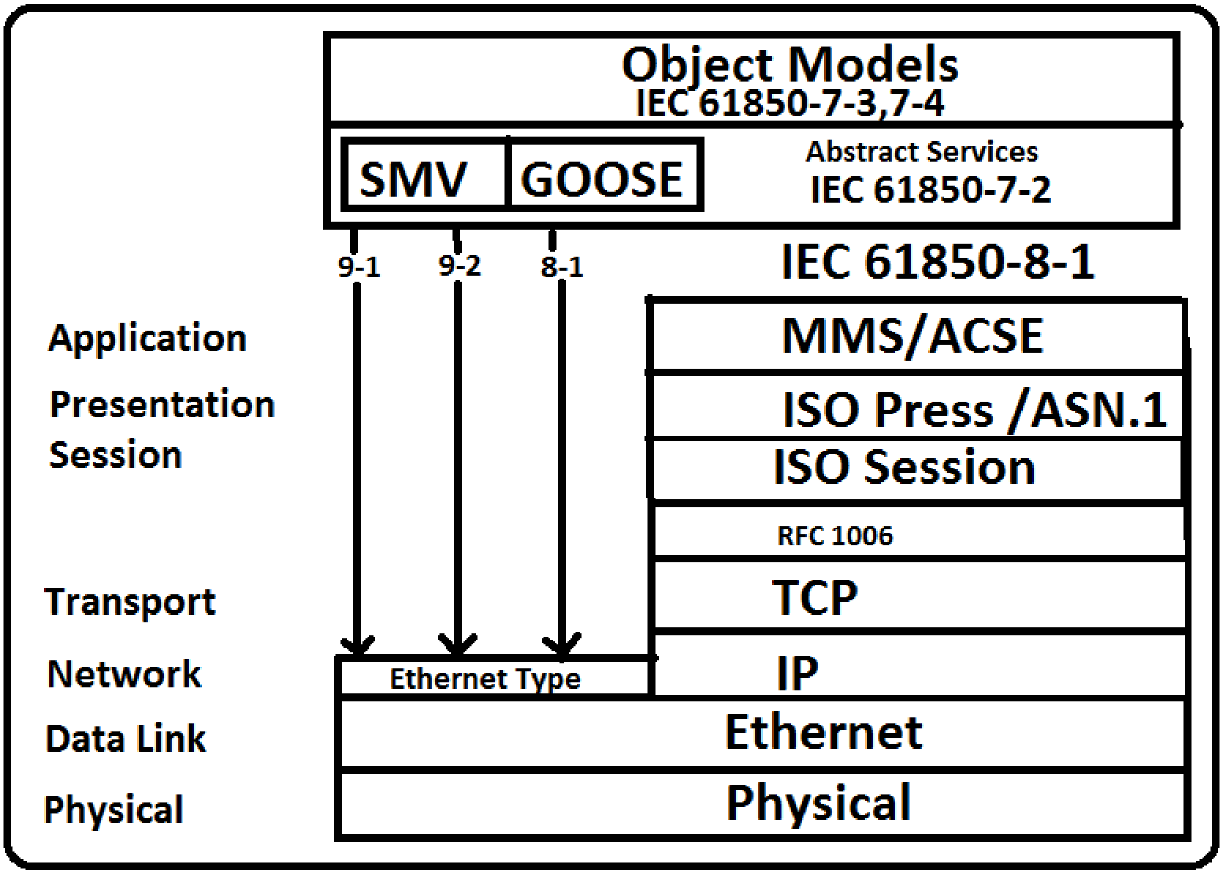


Fig 17 – [10] IEC 61850 Object Models

2.2.2 IEC 61850 Features: There are many features which make IEC 61850 different from all other previous standards:

- Self-Description: Standard names convention with standards units itself for example what units are represented the value of current A or mA.
- Structured Data from classes.
- LAN based time synchronization.
- Real-time transmitting samples of the waveform.
- XML based substation configuration language
- LAN based Interlocking and fast tripping for safety

2.2.3 The application focused architecture is categorized into various utility operations:

2.2.3.1 Substation to substation: The substation to substation applications can be considered as "mission-critical" for fastest response to automation, control and protection of smart grid. The electrical faults such as short circuit require millisecond response time (higher the intensity of current, shorter the time required for action to trip the circuit breakers). The low latency is required for the substation to substation applications and dedicated communication is needed for implementation of "mission- critical" applications.

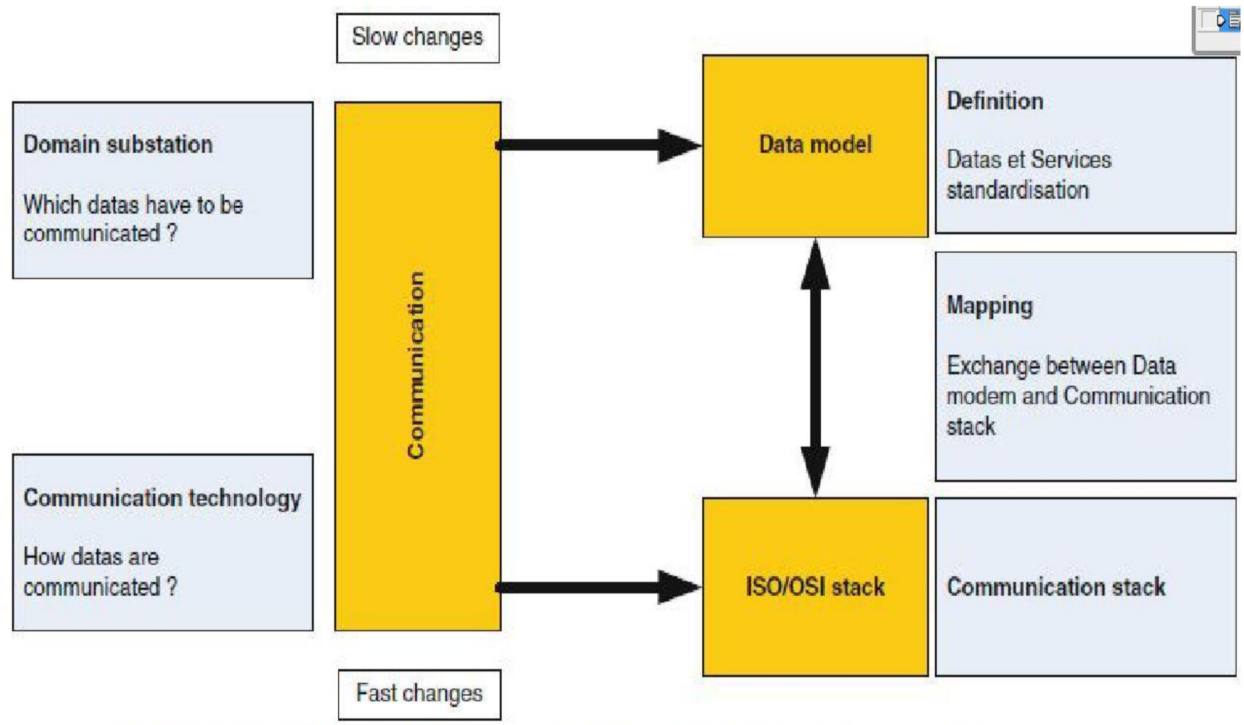
2.2.3.2 Field devices to central control unit: Application of field devices contains the status of device "active or passive", measurement data of the power parameters, commands signal for adjusting the settings and other internal signals of SCADA system. Addition to its Synchro-phasor measurement, alarms and monitoring, cyber security etc. are collecting data over short intervals of time and their latency requirements are different.

2.2.3.3 Inter-platform applications: In these applications the database is synchronized of various remote substations, distribution, service, consumer and market domains for redundancy and record keeping. The requirement of these applications will be the bulk amount of data as well as highly secure. The cyber security is necessary for the protection of sensitive information.

2.2.3.4 Service domain to field applications: The diverse services will be required from service domain for the operation of the smart grid such as application covers the requirement of remote configuration, set new parameter, and maintenance of existing or newly installed IED, AMI etc. A dispatch of the service team to maintenance area or for troubleshoots the site with information about all the events occur during the faults.

2.2.3.5 Consumer domain to market domain: A plethora of new application are being developed for smart metering, load analysis, revenue management, charging reports for electrical vehicles, micro grids etc. These will enhance the interaction of utility with consumers, generation and storage domains.

2.2.4 IEC 61850-90-4 "Network Engineering Guidelines" provides the guidelines of different traffic classes such as Sampled Values, Generic Object Oriented Substation Event, Manufacturing Message Service (MMS) for the Ethernet Network Architecture. It has also provided the analyses of performance and architecture for local area communication network and wide area communication network. The Ethernet architecture should meet the requirement such as high bandwidth, reliability, redundancy, low latency delay, maintainability, network convergence, scalability and expandability.



IEC 61850 model presenting data model and communication stack
Source : Page no 8, Book - Utility Communication Networks and Services

Fig 18 – [11] IEC 61850 model presenting data model and communication stack

2.2.4.1 Sampled Values: Traditional analog wiring is replaced with IED, the sample of current and voltage measurements are encapsulated and transmitted over Ethernet to multiple devices for the fast and accurate result. The IEDs send alarm signal and stop functioning if the time delay between two consecutive samples exceed 4ms. For example the voltage sample value of the generator is measured at 4000 per second and transmitted the sample values at 1 KHz to multiple users using MAC layer multicast address.

2.2.4.2 Generic Object Oriented Substation Event: In IEC 61850, GOOSE messages are multicast layer two (MAC) peer to peer non-routable messages. They move the information of primary devices such as status and event change at the process level. Devices can subscribe to messages and use the information. These are defined in fast messages class P2/P3, which means the time frame of mission critical information to send and receive from the device need to be less than 3ms, if the message not received within the time frame and failed message will show in Goose Control Block. GOOSE messages are mapped to Ethernet layer and based on critical events and with TTL mechanisms such as a trip, high-speed detection and isolation of faults, safety, and performance of substation.

Table 1 – [12] Latency Requirement for GOOSE messages:

TYPE	CLASS	TRANSMISSION TIME (ms) DEFINED BY TRIP TIME
TYPE1A	P1	10
	P2	3
	P3	3
TYPE1B	P1	100
	P2	20
	P3	20
TYPE 2		100
TYPE 3		500
TYPE 4	P1	10
	P2	3
	P3	3
TYPE 5		1000

2.2.4.2 Manufacturing Message Service: These types of messages are for download, upload configuration, file transfer messages, status update, changing parameter setting, auto-control functions, time-tag system data, transmission of event record and other control functions of devices that complies with IEC 61850 standards. These messages are stacked with TCP/IP over Ethernet layer and contain IP addresses. MMS messages can easily route over WAN but GOOSE and SVs required tunneling (IP/MPLS) or mapping over UDP/IP, TCP/IP protocols for transmission over WAN.

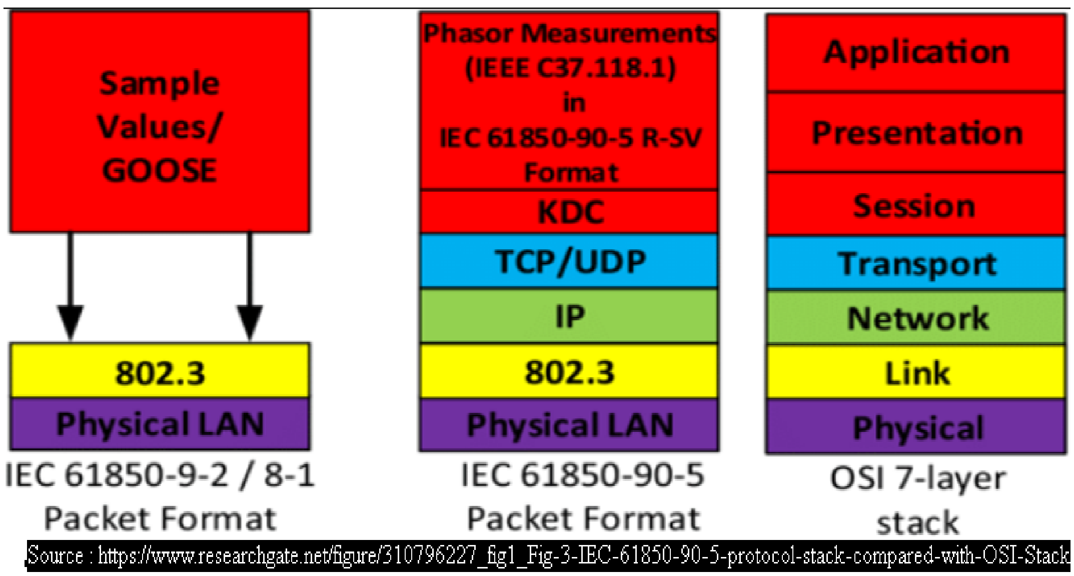
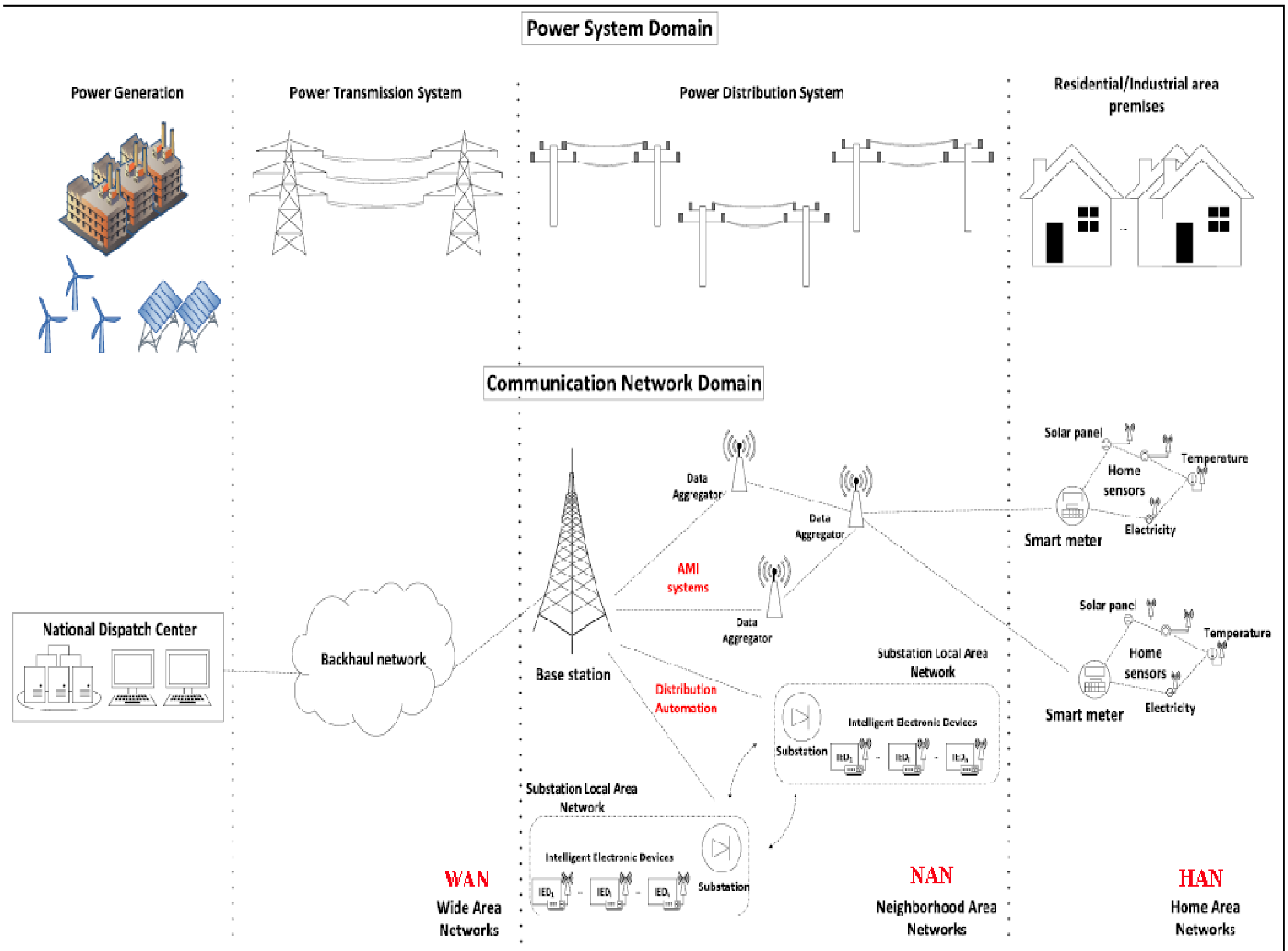


Fig 19 – [13] IEC 61850-90-5 protocol stack compared with OSI stack

The R-SV is routable sample value messages of IEDs and mapped over routable UDP protocol. The UDP with multicast addressing is selected as the transport protocol for Sampled Values. Similarly, R- GOOSE is routable GOOSE messages and mapped over TCP/IP protocols. Additionally, the security of R-GOOSE and R-SV messages is enhanced with authentication signature which is key-based. The IP/MPLS (MPLS-Transport profile) tunneling technique may introduce some end to end transmission delay due to encapsulation of GOOSE and SV messages but it also improves the latency because of end to end labeling (MPLS label switch router) technique rather than IP routing for forwarding the packets.

Fig 20 shows that the Smart Grid communication networks are generally divided into three segments Home Area Networks, Neighbor Area Network and Wide Area Network. These segments are responsible for the different type of traffic of the AMI system, SCADA system and Renewable energy sources.



Hierarchical smart grid architecture. Two parallel interdependent domains, the power system and the communication network, form the infrastructure of the smart grid. The power distribution grid along with the corresponding NAN constitute the heart of the new power system. In the figure, two fundamental grid applications within the NAN, the distribution automation and advanced metering infrastructure (AMI) systems are illustrated. Distribution automation information between substation Local Area Networks and aggregated metering data from spatially dispersed Home Area Networks, need to be transmitted through a reliable communication infrastructure.

Source : Cellular Communications for Smart Grid Neighborhood Area Networks: A Survey
CHARALAMPOS KALALAS1, (Student Member, IEEE), LINUS THRYBOM2, AND JESUS ALONSO-ZARATE1, (Senior Member, IEEE)

Fig 20 – [14] Power system network and communication system network of Grid

2.2.5 **HAN** : Home area network is deployed in consumer domain and it collects real time information from different smart energy devices, IoTs, smart appliances, electric vehicles within the residential/commercial consumers and transmits the information to control domain with AMI for energy management. Different applications will support the function of automatic start and stop of non-essential appliances during peak load and real time load consumption, automatic payment over a different communication network. The coverage range of HAN is 200 meter square with an approximate data rate of 10 to 100 kb/s. AMI works as a gateway between HANs and NANs. The short range communication technologies are used in this segment for frequent small sized data packets.

2.2.6 **NAN**: Neighbor area network is a communication network between generation domain (high voltage) and consumer domain (low voltage). It is an aggregate point for a large number of devices of SCADA system in the distribution domain (medium voltage) such as IEDs, sensors, CB (circuit breakers) and moreover, numerous HAN is incorporated in this segment. The different types of renewable energy sources will autonomous integration in the NAN at time of peak load demand. The different reliable, secure and real-time communication technologies are required with various protocols to support diverse application requirements of the devices in the NAN.

2.2.7 **WAN**: The Utility's backbone communication network aggregate the data traffic of multiple neighbor area networks to control domain. It is the ultra-high speed, low latency with high reliability optical fiber network for mission-critical and tele-protection applications of different substations with the control center for preventing cascading outages in the power grid. The coverage diameter of network is typically more than 1000km for control and monitoring for protection, wide area protection, optimize planning and fault proof operation in the smart grid. The communication of SCADA control and automation system will improve over higher bandwidth and shorter time response of mission-critical applications (example 60 samples per second).

The protection over wide-area gave an end to end protection to ensure power systems against across the cascade events of blackouts, transmission overload and focused on conditions, or sudden events. The protection applications mainly include different load shedding and versatile isolation techniques that are helpful to manage unpredictable faults over long distances in short response of time for example short circuit faults requires instantaneous isolation of equipment to minimize cascade hazards. The stability of power supply can be remotely monitored and managed by controlling the parameters such as voltage, frequency, active and reactive power in the various smart grid domains.

2.3 Wireless Communication:

The smart grid is a system of systems and a combination of multiple different technologies and layers, which requires an interface between these segments to be properly defined and harmonized with the existing standards. The goal is to create an end to end communication at the upper layer with all the sub-layers of all the domains of the smart grid.

There are many wireless communication technologies exist in smart grid infrastructures such as 802.11 and 802.15 (WLAN, ZigBee, Bluetooth) for short coverage and cellular network for wide coverage and they provided connectivity to massive devices of distribution domain and consumer domain. It is the cost-effective solution for exchanging the data traffic of (Neighbor area network and Field area network) field devices , IED, protective relays, sensors and AMI for reliable communication of automation and control system of the smart grid over wireless network.

Communication technologies applicable to smart grid and their characteristics.

Technology	Achievable data rate	Coverage range	Advantages	Disadvantages
Fiber optics	155 Mbps - 40 Gbps	100 km	• High capacity • High reliability • High availability • Enhanced security • Low latency • Noise immunity	• High cost • Low scalability • Deployment limitations • Regular maintenance
Ethernet	10 Mbps - 10 Gbps	100 m		
Narrowband PLC	10 - 500 Kbps	300 m - 1 km	• Existing infrastructure • Cost-effective • Wide availability	• Channel noise • Interference • Attenuation when signals cross transformers
IEEE 802.15.4	20 - 250 Kbps	10 m - 1.6 km	• Low cost • Low power consumption • Mesh connectivity	• Low data rate • Short range • Interference
IEEE 802.11	2 Mbps - 6.75 Gbps	20 m - 1 km	• Low cost • High data rate • Wide adoption	• Short range • Interference • Low security
LEO satellite	2.4 Kbps - 100 Mbps	3000 - 4500 km	• Wide-area coverage • High reliability • Low latency	• High cost • Non-private systems - shared bandwidth • Signal shadowing
WiMAX	63 Mbps DL 28 Mbps UL	48 km	• High data rate • QoS provisioning • Scalability • Low latency	• Not widespread use • Dedicated infrastructure • Limited access to licensed spectrum
Cellular	300 Mbps DL 75 Mbps UL	100 km	• Existing infrastructure and service models • Ubiquitous coverage • Low latency • High data rate • QoS provisioning	• Oriented for human broadband applications • Coexistence with HTC • Monthly recurring charges • No current support for mission-critical applications

Table 2- [15] Detail of Communication technologies

The reliability of wireless communication should be considered in case of power outage, the base station of SP (Service provider) on the limited power supply (battery banks or backup generators). The base station may experience longer power outages due to some severe faults or maintenance that can cause the loss of automation and control system communication of the grid. SP of the wireless communication system has licensed spectrum and utility companies can use the services without deploying their separate communication network.

Utility operation domain transmits and receives traffic with IP/MPLS technology from other domains of smart grid and these operation domains may be central for small utility or at multiple locations for large utilities. Eavesdropping can be possible over the wireless network, even the SP offers the security of the wireless connectivity but the utility will manage the security of the data.

3rd Generation partnership program, 3GPP+, IEEE are standard bodies for standardize the majority of wireless technology globally such as General packet radio service, Enhanced Data rates for GSM Evolution, Code Division Multiple Access, Wideband Code Division Multiple Access, High speed packet access, for higher data rates and end to end packet switch network two independent standards are available IEEE 802.16 Worldwide Interoperability for Microwave Access and Long Term Evolution Advanced (LTE-A). LTE (TDD) and WiMAX used Time Division Duplexing (TDD) scheme for uplink and downlink traffic shared one RF channel with different time slots. The Frequency Division Duplexing (FDD) used by all the other technologies except WiMAX, the data rate of the downlink is higher than the uplink data rate even the bandwidth of the channel is same. The data rate received by the users depends upon the location of the user relative to the base station, speed, cell sectors and other factors. Multiple input multiple outputs (MIMO) improved the spectrum use and increased the data rate of wireless transmission.

The low latency requirement (below 5ms) of backbone communication application partially acknowledge in WiMAX and LTE end to end packet-based architecture which eliminates the protocol translation of circuit switch to the packet in the core and improved the latency of the system. WiMAX technology has advantages of high data rate (up to 75Mbps) , easy scalability over wide area coverage, low deployment and maintenance cost and most important appropriate security protocols for control and automation applications.

Wireless broadband technology	Standard body	Channel bandwidth (MHz)	Typical peak data rate (Mbps) Downlink	Typical peak data rate (Mbps) Uplink	Typical one-way delay (ms)
GPRS	3GPP	0.2(x2)	>0.1	>0.01	<150
EDGE	3GPP	0.2(x2)	>0.4	>0.4	<150
CDMA 2000	3GPP+	1.5(x2)	>3	>1.8	<100
WCDMA	3GPP	5(x2)	>2	>0.4	<150
HSPA R6	3GPP	5(x2)	>10	>5	<50
HSPA R7/8	3GPP	5(x2)	>40	>10	<30
WiMAX	IEEE	5-10 (TDD)	40	10	<40
LTE (FDD)	3GPP	1.4,3,5,10,15,20 (each X 2)	>150	>50	<10
LTE (TDD)	3GPP	1.4,3,5,10,15,20 (TDD)	>70	>10	<10

Table 3- [16] Wireless technologies comparison

The advanced private LTE improve the productivity of the smart grid system by using unlicensed spectrum where licensed spectrum is not available or congested. It offers numerous advantages such as utility can set up their own small cell station for guaranteed coverage in the remote area, agriculture lands, and underground warehouses or along with setup of a new substation. The setup of uplink and downlink capacity, usage policy changes in RAN part are exclusive decision of utility and make full utilization of spectrum. Moreover the radio parameters can be customized, fully controlled and managed by the organization as per their needs and requirement to optimize reliability and latency. Sensitive information and data protection protocols are designed as per business needs.

2.3.1 Advantages:

- **Cost**: In wireless network installation the high capital expense of cable deployment will eliminate. The utility can utilize existing cellular infrastructure for wide area wireless coverage between various domains. Cost effective, fast installation and wide coverage of cellular communication make its first preference for smart grid applications (AMI, demand response, outage management).
- **Rapid Installation**: The setting up time of wireless communication is much less than the wired communication networks, especially if the renovation is required in existing infrastructure. In consumer domain, the customer can use plug and play smart meter devices for AMI applications.

2.3.2 Disadvantages:

- **Redundancy**: Mission critical application requires high bandwidth and ultra-low latency for quickest response to situation in case of emergency, for example the high voltage short circuit occurs at distribution domain and signal send to control center for open the breaker or disconnect the power supply, due to congestion in the cellular network (assume no QoS) or service outage the signal may get delay and that short circuit lead to initiate the fire in that area. Hence, the solution to the similar situation is private communication network or dedicated cellular network slice for mission critical application.

- **Security**: The security is a big challenge in a wireless network as the RF signal can be captured and decoded with devices. The AMI application may contain some personal information that wills the concern to address. Therefore, for securing the wireless network the encryption and efficient authentication technique should consider.

2.4 <u>ZigBee</u>:

The ZigBee Alliance built a wireless communication standard for Home Area Network and according to IEEE 802.15.4; it operates worldwide in the 2.4GHz frequency spectrum (16 separate 5MHz channels) and 868MHz/915 MHz (Europe and Americas). NIST realized that the ZigBee and ZigBee Smart Energy Profile (SEP) are emerging smart grid standards for the residential network. It offers very low power usage, low cost, simple and supports massive devices up to 64000 over the single standardized network. ZigBee integrates the home automation, and industrial control system, building automation, medical sensor applications, consumer electronics (toys and games), and PC peripherals. The applications of ZigBee are energy management of smart appliances with sensors, Heating Ventilation Air Conditioning (HVAC) which can be controlled with programmable thermostat, temperature, air flow, a valve actuator and humidity sensors, home security sensors. Utilities can send real-time information of energy consumption to consumers by using ZigBee SEP (Smart Energy Profile) with integration of AMI.

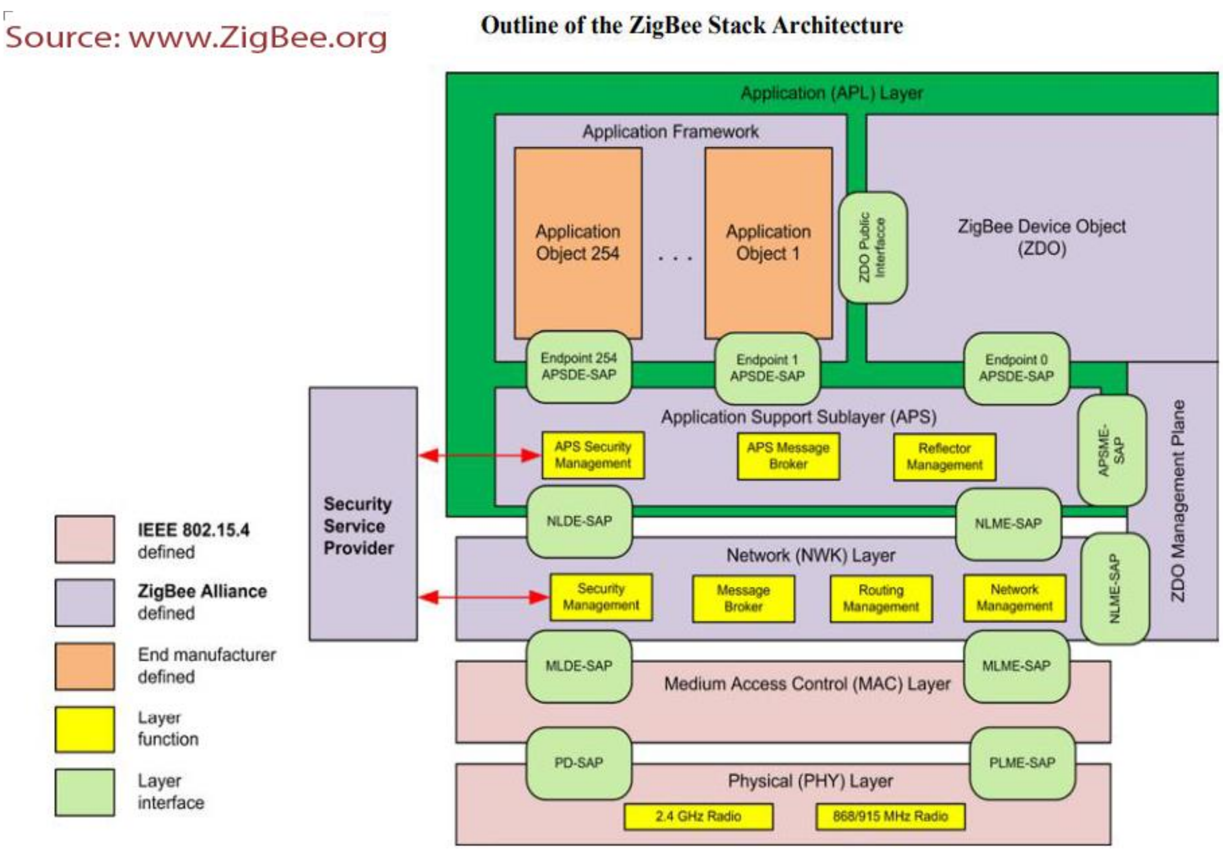


Fig 21 – [17] Zigbee architecture

ZigBee stack architecture consists of layers and each lower layer services are defined for above layer. A data transmission services are offered by data entity and all other services provided by the management entity. Service access point is an interface of each service entity for the upper layer and support many services for required functionality. The two lower layers physical layer and medium access control (MAC) sub layer are defined by IEE802.15.4 standards. The CSMA-CA (carrier sense multiple access with collision avoidance) mechanisms are used to control the access of radio channels. The Physical and MAC sub-layer are the foundation of the ZigBee Alliance and provide network layer and application layer framework which include the ZigBee device objects (ZDO) and application support sub-layer (APS). The network layer entities provide data service and management service. The network layer data entity (NLDE) provide Network layer PDU (NPDU), Security and Topology specific routing. Network layer management entity (NLME) offer management services of configuring a new device, starting a network, allocation of IP addressing, joining and leaving a network, routing ,reception control, route and neighbor discovery.

2.4.1 Advantages :

- The battery life of devices are longer if they operated in beacon mode, the devices are in sleep mode and only wakes up when there is a beacon to transmit. The duty cycle is lower and lower power consumption. The maximum power output is 1mW and the data rate is 250 Kb/s with Offset quadrature phase-shift keying (OQPSK) modulation. ZigBee is easy to implement and ideal for smart grid requirement of AMI such as demand response and load control, real-time pricing and system monitoring.

2.4.2 Disadvantages:

- There are some limitations in the practical implementation of ZigBee over large scales such as small delay, small memory size, low processing capacity and limitation to install for outdoor applications due to lower coverage area and less penetration power. It may cause high interference if other appliances share same license free spectrum such as Wi-Fi, Bluetooth and Microwave.

2.5 <u>Satellite Communication</u>: Satellite communication is an innovative way for communication between remote sites and central substations where public communication infrastructure is not present. Very Small Aperture Terminal (VSAT) satellite service is installed in oil fields, rig fields (some countries have constructed offshore large wind turbine farms for generation of clean electricity) and rural area. Furthermore, Global Positioning System (GPS) is used for micro second accuracy in time synchronization. It is used in some of the application of smart grid where critical communication between remote stations requires microsecond accuracy for disconnection of electrical power in case of a fault.

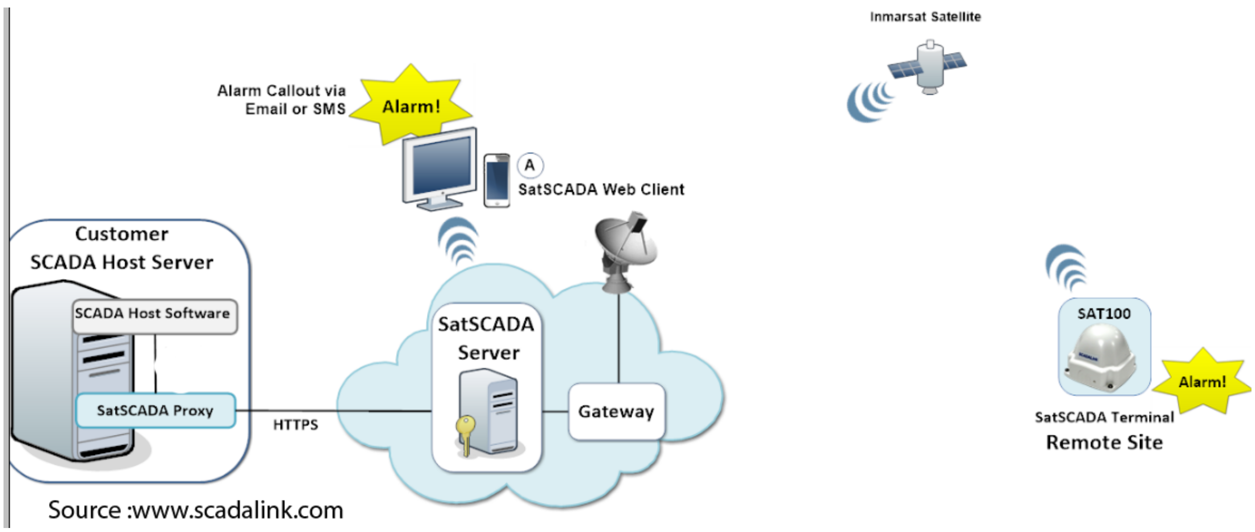


Fig 22 [18] SCADA communication via Satellite

2.5.1 Advantages:

- **Global Coverage**: The higher bandwidth, reliability and large geographical area (urban, rural, and remote) are covered with satellite communication. It is a cost effective solution where the new communication system deployment is required.
- **Rapid Installation**: Satellite communication support easy wireless network setup for remote sites rather than wired network installation. Some utilities are currently using VSAT services for monitoring remote substation sites.

2.5.2 Disadvantages:

- **Long delay**: The distance between remote sites and substation via satellite is very long, so the round trip delay is higher in Geostationary Earth Orbit (GEO) satellites than terrestrial communication. The different protocols are required to support satellite communication for reducing the delay in commonly used Low Earth Orbit (LEO) satellite.
- **Satellite channel characteristics**: The performances of communication system depend upon the fading effects, atmospheric conditions which can degrade the satellite channel characteristics. These challenges are an inevitable and most considerable factor for using satellite communication in the utility system.
- **Cost**: The investment is higher for the initial installation of satellite services (transceiver), infrastructure cost, monthly fees and it is recommended that these services are cost-effective for remote sites and offshore communication, where another mean of communication is not yet available.

2.6 Optical Fiber Communication:

In mid-1960, the optical fiber communication was introduced with speed 45 Mb/sec but in contemporary times the speed of single strand of fiber has exceeded the 100 Gb/sec. In an electrical grid system, the optical fiber communication offered high advantages than copper-based communication system for wide area control and automation applications. It is almost ideal for high voltage environment because of its resisting properties such as Electromagnetic interference (EMI) and Radio frequency interference (RFI) has no effects on optical fiber communications. In addition to that, it has a large capacity signal over a longer distance with the intermediate repeater requirement is much less than in optical fiber (usually require about 100-1000 km) than the traditional coaxial cables (require every 2 km) for long distance communication. Due to high bandwidth and reliable communication, it is best suited for backhaul communication between generation domain, operation domain, and distribution domain.

2.6.1 Advantages:

- **Capacity**: The demand of smart grid is the interconnection between all the seven domains (refer smart grid section) requires extremely high bandwidth for a large number of applications and their data. The single mode fiber offers transmission rate about 10Gbps with less dispersion and attenuation (most common wavelength in SM are 820 nm, 1300 nm and 1550 nm) but in multimode the wavelength division multiplexing (WDM) technique offers the transmission rate from 40Gbps to 1600Gbps and also low bit error rate in transmission system. The MM fiber is usually deployed for inside the substation communication.

- **Immunity characteristics**: This property made it unique, optical fiber communication is immune from electromagnetic interference and radio frequency interference because the EMI is noise generated when current is flowing through the conductor as the current flows in the coaxial cable, but light signal is transmitted inside the optical fiber which does not produce any EMI.

- **Security**: Optical fiber is a highly secure way to transmitting critical information because of its immune characteristics. The optical fiber does not generate EMI or RFI, so the information cannot decode with a radio receiver and the only way to get information is cut or taps the fiber.

2.6.2 Disadvantages:

- **Cost**: The initial cost is much higher than the copper cables for installation between remote sites and central substations. The experts or trained personals are required due to its splicing, bending and fragile property. It will be cost-effective solution for high speed backhaul communications.

2.7 **PLC (Power Line Communication):** PLC technology is used for low data rate signals since 1950 as an alternative to build utilities dedicate communication infrastructure. The transmission of electrical power as well as data over high voltage power lines (10 kV or above) and low voltage power lines with different frequencies for remote meter reading. With the advancement in technology, the high speed (2-3 Mbps) data communication is possible over power lines of low voltage and medium voltage (110V/220V and 15 kV/50 kV) for protective relaying for distribution domain, remote tripping for transformer protection, remote breaker failure relaying and shunt reactor protection. Countries like China, France, and Italian have launched projects for smart meter data collection using PLC technology.

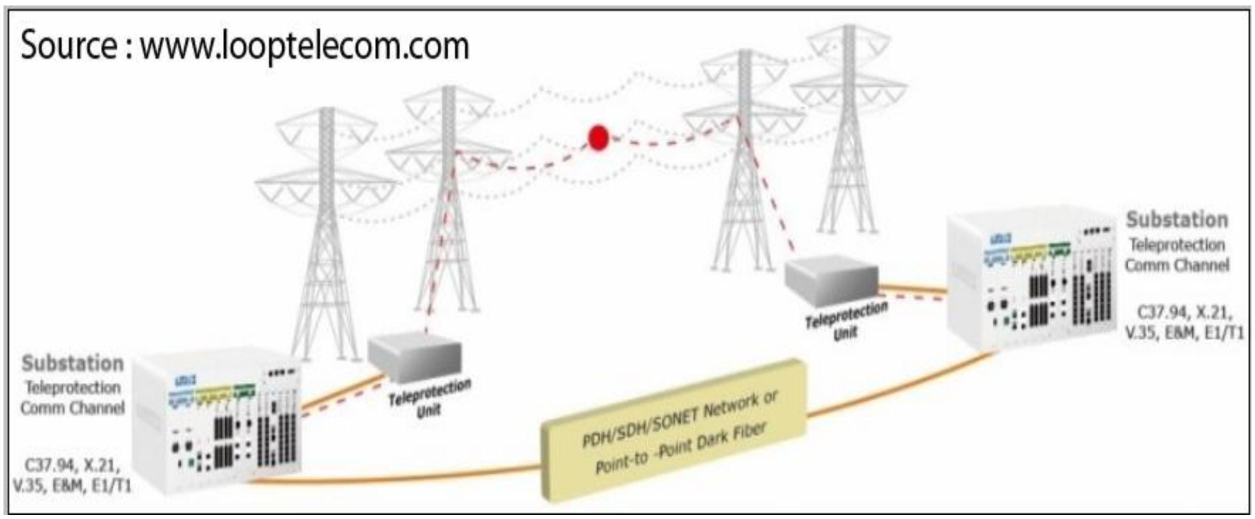


Fig 23 – [19] Power Line Communication

2.7.1 Advantages:

- **Coverage**: The power line infrastructure is in place for electricity and spread over the large geographical area. The PLC is highly beneficial for the rural area of some countries where public communication network is not possible. It is suited for smart grid applications, smart meters, utility control and automation.
- **Cost**: PLC ultimate solution for eliminating capital investment in dedicated communication network because it can be deployed quickly over existing power lines for transmitting communication signals.

2.7.2 Disadvantages:

- **Open circuit problem**: This will be the one of the main disadvantages of PLC, as the control signal is also transmitted via power lines, in case of power line disconnect from another end, it may result in a short circuit or serious fatality as well as failure in automation and control system.
- **Noise**: The signal quality will depend upon various interferences caused by load impedance of radio signals, electrical motor, fluorescent lights, and power supplies. This noise will cause high bit errors which decrease the signal to noise ratio and affect the performance of PLC.
- **Capacity** : The capacity of PLC depends upon a number of users, as it is shared the medium and data rate will less than the capacity due to high attenuation and distortion of signals.
- **Security**: Electrical power cause electromagnetic interference over power lines, which means that information security concern, arises. This radio receiver can decode the information in the EMI. Therefore, the data should be encrypted before transmitting for eliminating security concerns.

3 Utility Network Challenges :

Today, the demand of energy is growing around the world but instead of large capital investment to build new generation plants for managing the growing demand, the requirement of modernizing the communication network infrastructure is critically important. The flow of valuable information in modern smart grid network domains will increase the competitiveness, enhanced the business requirements which improved the operational methods for the reliability of energy system. This will be one of the challenges for the efficient design of communication network in all the seven domains of the smart grid.

The fluctuation in the demand and capacity of electricity can be met by increasing the overall capacity with the integration of micro grids into the smart grids. The challenge of utility communication network interoperability with other utilities communication network will standardize the architecture of interoperable system globally for the reliability of the system. The interconnection of local, regional and national utilities will be cost effective solution to use the existing infrastructure and curb the demand-supply difference.

The deregulation in the competitive market of utilities has clearly defined the need of unified standard for exchanging the high amount of information and it also points out the concerns of reliability and security of information at local, regional and national level. The current network infrastructure of some utilities are at end of life or having limited lifespan and these infrastructure are not able to support the large amount of modern traffic such as two-way communication of smart grid and micro grid, smart metering, power management system, operational system for outage and flow management, transmission interconnectivity and network security with rigorous safety standards. These clarify the requirement of a modern communication system in the smart grid.

3.1 Aging Infrastructure: In some countries the electric grids are mostly very old infrastructure and it has spread over a large geographical area. It has a central generation plant and the flow of electrical power via reliable transmission grid and distribution substation to different industrial, business and household consumers. These different domains have old electro-mechanical devices and periodic maintenance is vital for their proper functioning but occasionally these devices required replacement for continuous supply in peak demands or in extreme environments. Sometimes, the replacement of one device requires the upgrade of the full system because of the technology incompatibility and these electro-mechanical devices are replacing with digital for high reliability and adequately connect to the rich source of renewable generation latest technology. Large capital investment is required to replace the traditional devices with modern digital devices and designed the modern smart grid infrastructure.

3.2 **Environment-friendly:** The non-renewable generation plants produced greenhouse gases (GHG) and the direct impact on the environment is an overall increase in global temperature and climate change. The recent studies show that the up to 40% of carbon dioxide emission is due to fossil-fuel generation plants and these are unsustainable for long-term production. The transition of the existing way of electricity generation to renewable energy sources has begun in developed countries. The integration of climate dependable renewable sources into the smart grid will require intelligent communication network for management of the generation and distribution according to weather conditions. The consumer will use energy efficiently with smart energy appliances and manage them over home area network.

3.3 **Regulations and Standards**: The objective of building the Smart Grid in the 2007 Energy Independence and Security Act was assigned to National Institute of Standards and Technology and Federal Energy Regulatory Commission for crafting standards of Smart Grid devices and systems as per the recognized needs and requirement of interoperability. NIST will replace the manual operation of the substation with the highly synchronized automatic operation and divide the SCADA system into groups of responsibility for developing IT information technology units and operational technology units and even more sub groups for developing standards with fine granularity. The standardized protocols and architecture of telecommunication are fundamental for utilities to adapt the IEC

61850, 61970, 61968 (substation automation and communication, data exchange standards). These standards are also necessary for standardize SCADA control system to mitigate the risk of proprietary protocols and deployment of different network technologies for backhaul. The risk involved in the vendor-specific system is high cost of replacing unavailable equipment in case of emergency, aging equipment due to system or model incompatible with newer models and knowledgeable utility work force retirement.

3.4 Communication Network: Utilities have different areas where it is important to evaluate the accessible alternatives of communication technology deliberately before deciding. Seller connections, innovation decisions, and accessible administrations, are on the whole illustrations. There are a few choices for utilities with respect to communications network management. A few utilities favor overseeing what's more, constructing their own particular networks with assistance from vendors for supplemental staffing, outline mastery, and hardware. These vendors can enable utilities to fragment networks, give virtual private networks (VPNs), expand or isolate data transmission, and give extra value for dollars as of now put resources into networks.

On the other hand, some utilities are giving these projects to companies that have some expertise in communications networks, enabling them to outsource the greater part of the network modernization exertion. A few utilities utilize a hybrid of the two methodologies, in these cases, utilizing outer carriers in certain geographic areas however keeping up the vast majority of the utility network under interior control for high performance and overall control. Utilities that set up their private networks should mean to limit the interruption of core operations and keep operational staff concentrated on the conveyance of communications operations. The best answer for a business case for improvement is frequently to utilize existing networks with more current gear to use what's more, expand the operational life of legacy utility equipment.

The substations are installing modern intelligent electronic devices to process various inputs from sensors to perform control and automation operations, load balancing and outage management. The utility need to build up a standardize communication network architecture to support communication between standardize (based on NIST, IEC 61850) new device, equipment and packet-centric applications for collecting, processing and managing the operation of power system over wide area, i.e. similar to Synchronous Optical Networks (SONET) that have served them for decades and giving most astounding network reliability.

The Metro Ethernet Forum has standardized the Carrier Ethernet for high-performance networking capabilities with non-Ethernet transport technologies like SONET, OTN, WDM or T1 over packet-based network architecture. The importance of Ethernet based network infrastructure made by packet optical networks is that the utilities can implement a legacy application with emerging packet-centric applications over legacy SONET network in the inter domains and intra domains communication of Smart Grid. This empowers utilities to move step-by-step to guarantee reliability and implement Ethernet-based communication network in progressive stages, while expanding efficient use of the new hardware equipment for quick fault isolation over network, guaranteed bandwidth for critical applications, network protection within 50ms and real-time monitoring of system performance

The professional communication companies can offer their expertise to utilities such as designing of the communication architecture and optimization, engineering, testing, installation and maintenance of networks, 24x7 support centers for emergency operations. They also assist in challenging integration of various developing information technology units and operational technology units groups, existing communication infrastructure and modern technologies, improving the security of the overall system for reliable power supply to customers. Moreover, the competitive and dynamic pricing of power supply applications requires bi-directional communication networks with the highest availability. It is important for Smart Grid market domain and customer domain to analyze and manage the load in peak and off-peak time frames. The Smart Grid require unified communication network in the all the seven domains (generation, transmission, distribution, operations, customers, market and service provider) for interoperability, control and automation as well as two way power flow for demand response, AMI , Electric vehicles, mission-critical applications, mission critical applications and last but not least security and privacy.

3.5 Reliable and time-critical NAN operations: First and foremost requirement is to deliver the reliable power supply to consumers and it depends on many factors such as a number of outages, outages durations, restoration time, planned outages notifications and the power quality during peak hours. It is required to minimize these factors to improve the reliability of power system. There are many Smart Grid applications which are emerging in the distribution domain and the requirement of high-performance communication between IEDs in NANs; and the development of reliable cellular communication infrastructure is a necessity. One of the challenge in the current cellular communication network is the transmission of GOOSE messages over wide area network and the current wireless network is not designed to control time-critical applications of Smart Grid communications over wide area network for example the instantaneous trip circuit is placed in local control panel for immediate isolate the faulty device from the system. The solution to that problem will be dedicated low latency and high bandwidth network which guarantee the synchronized convergence of Smart Grid domain devices to respective networks in case of power outage or failure. Moreover, it exchanges real-time data of time-critical applications between different domains with ultra-low latency to detect and mitigate the faults.

A wide range of Information and Communication Technologies (ICT) are included with various levels of investment and at various levels of development for support mission-critical applications. In the Release 13, 3GPP has begun to examine low latency system with a specific end goal to keep cellular network latency requirement nearer to the prerequisites that will originate from the future mission-critical application of Smart Grid. The solutions will include less time for processing, LTE shorter scheduling timing and high speed uplink access.

Release 14 will standardize some portion of the latency-reduction method which will depend if data packets are available and then only transmit them (Semi-persistent scheduling constitutes). The size of Long Term Evolution sub frame Orthogonal Frequency Division Multiplexing symbols needs to be adjusted for a smaller time interval of transmission which impacts the scheduling decision. The alarm signals required high-speed transmission but the 1ms scheduling time granularity is not sufficient in LTE network. This may require the draft of novel multi-carrier modulation methods in the physical layer that permit fast channel estimation.

The 5th Generation cellular heterogeneous network will integrate the Smart Grid communication network and the network slice capability provide a dedicated network for various applications with different bandwidth and latency requirement. The simultaneous radio will improve the availability, reliability and integrity for the same reason empowering the misuse of diversity in transmission for example, distribution domain IEDs send GOOSE message to Generation domain IEDs for starting another generator to regulate the power supply demand.

The utilization of simultaneous radio interfaces for the transmission of the mission critical message could augment the likelihood of successful delivery. Further communication challenge includes integration of renewable energy sources, micro grids, distribution generations, self-healing grid and storage of power. The requirements and architectures are developing by standardizing bodies. It is difficult to trial on an extensive scale because power grid is a critical infrastructure.

3.6 Quality of Service (QoS) Requirement: The challenge of differentiating the real-time and non-real-time traffic classes of various applications in smart grid modern communication network. Quality of service is required to fulfill the end to end bandwidth and latency requirement of various applications.

3.6.1 End-Users: In-home applications the traffic of electricity usage of the appliance, smart metering, load analysis, revenue management, charging reports of electrical vehicles will consume few kbps of bandwidth. The latency requirement is not critical and will be in the range of 2 to 15s for home applications.

3.6.2 Connection and Disconnections: The long latency requirement can be accepted if end users can connect and disconnect the smart appliances without physically turn ON and OFF the switch but can be through the application. In case the response to grid operations, the connection and disconnection latency requirement will drop too few milliseconds and require quick response to the action.

3.6.3 DR (Demand Response): DR is direct communication between utility companies and devices of the smart home. During peak load time the automatic shift or reduce the power usage of pre-configured devices. The bandwidth requirement is small because it simply sends the turn-off command to the appliance with energy management system. Even the micro-grid controller disconnects the grid supply and switches over to internal renewable energy sources to control the demand response situation.

3.6.4 Outage Management: Smart grid enables the automatic detection of an outage at end-user. Usually end users have to notify the utility office in case of outage occur. The smart meter will detect and send the real-time data signal to control domain and it will reduce recovery time. A smart meter can early detect the fault location and provide the valuable information to service domain.

3.6.5 Synchro phasor: It measures the real-time electrical waveforms samples at various points in the distribution domain and provides high precision of information to control domain. This improves the overall power quality with a high degree of precision. There are different latency requirements for synchro phasor data traffic with a range of 20 to 200ms and bandwidth of 600 to 1500 kbps.

3.6.6 SCADA system : One of the SCADA application for polling and send the data from IEDs to Master control unit in the substation required low latency usually from 100 to 200ms.The IEDs will transmit data (approximately 2-5 Mbps) of different measurable parameters of electrical quantity to control domain for optimization and required high bandwidth and latency requirement are 25-100ms.

3.6.7 Inter-substation Communication: This is communication between various substations for integration of distributed energy resources and different application of automation and control. 12 to 20ms are the latency requirement for application in the inter-substation communications.

3.6.8 Fault Location, Isolation, and Restoration for distribution domain: The mission-critical applications are categorized for communication between SCADA systems for finding fault, isolation of faulty circuit and reroute the power supply to the consumer with in few milliseconds. These applications require ultra-low latency for detection and isolation of faults in distribution domain. The complexities of the circuit require inputs from different sensors to analyses the parameters and give output to trip circuit of the particular section to isolate the fault. The mission-critical applications required dedicate communication network with high bandwidth and low latency.

3.6.9 Site Surveillance: The application of video site surveillance needs high bandwidth for data transfers and the volume of data depend upon the resolution of the video. These applications are required in the remote substation and real-time monitoring of critical infrastructure. Few second latency delays are acceptable.

3.7 **Security and Privacy**: The widespread deployment of communication and information technology infrastructures in the smart grid have turn out to be more vital to guarantee the security and reliability of power system and it is a wide scale network that stretches out from a power generation domain to every single power consuming gadget, for example, smart appliances, electric vehicles, IoTs, smartphones. This expansive scale nature has expanded the potential outcomes of remote operation and control of power management and distribution system. The prime concern of energy applications in smart grid are security from abuse, theft and malicious activities.

The new applications and communication technologies such as broadband capabilities and distributed intelligence can incredibly improve effectiveness and unwavering quality, however they may likewise make numerous new vulnerabilities if not deploy with the fitting security controls. The contests of guaranteeing cybersecurity in a smart grid are many different ways because of the decent variety of the modules and area of deployment. Un-detection of advanced cyber-attacks and without implement diligent and preserving security measures can compromise the entire smart grid system. The grid can expose to utility fraud, loss of classified client data and vitality utilization information by not taking adequate security measures. Reliability of smart grid network communication cannot be determined without security and privacy of user information.

Security of information is mainly divided into three categories:

- **Integrity**: Smart grid security protocols will give protection of misusing and modification the critical information of consumers; otherwise mishandling of these data can access the mismanagement of power supply tier.
- **Confidentially**: AMI applications will automatically transmit the billing payment which can contains the confidential information of consumers (Industrial, small business and household). Emerging security protocols will the private and confidential data to get tempered.

- **Availability**: The confidential information should be securely available and accessed timely for reliable delivery of power supply.

However, the attacker can easily access the information of demand management, load shedding, integration of renewable energy source and real-time pricing tiers because all the seven domains of smart grid are interacting with real time two way communication and it is highly important to consider security objectives include integrity, availability and confidentiality of the whole system such as AMI, data centers, communication network, SCADA control and automation system. There are many interfaces and access points especially in consumer domain (HAN) where the attacker can penetrate the network and take control of software by altering the codes and commands. Smart grid communication network will mostly mesh configuration and end to end connected the manipulation of data in the smart meter of the customer can affect the entire architecture if adequate security is not in wireless architecture. This can directly target the control and automation system which will make outage or destabilize the power system.

Cyber security must provide protection against deliberate attacks for example from displeased employees, secret information of the device and psychological militants. Moreover, unintentional infrastructure attacks in case of equipment failure, user errors and natural disasters. NIST address the potential vulnerabilities, which may enable an attacker to enter into a smart grid network, access the SCADA control system, and modify stack conditions to destabilize the grid in erratic ways. Smart Grid need to identify the privacy concerns such as real-time surveillance, identity theft, personal usage information of appliances and extracting the information from residual data

Additional security threats:

- Customer privacy breach and compromise of sensitive data because Smart Grid can relate to always "online" multidirectional network and energy management system.

- Different communication technologies increased the complexity of the smart grid could increase the vulnerabilities and increment unintentional errors and potential attackers.
- Internetwork of HAN, NAN and WAN can expand the common vulnerabilities and presentation of pernicious software could bring about denial of service or trade off the integrity of software and networks.

Therefore, the need of advanced cellular communication network which can deploy end to end in all domains of smart grid and provide flexibility in terms of bandwidth and latency requirement can also address the security of the diverse electrical infrastructure. The testing and integration of security protocols should be incorporate at the various phases of Smart Grid communication system architecture to ensure the security and safety of the system.

Chapter II

4G vs. 5G

4 4G standard investigation :

4th cellular Generation is a compilation of technologies that create fully end to end packet-switched (IP base) networks to communicate the data at faster speed. 4G technologies are aimed to provide speed of 1Gbps while stationary and 100Mbps while moving. Therefore, 4G is a network that utilizes the Internet technology and also work with other technologies such as Wi-Fi and applications, and runs at speeds ranging from 100 Mbps to 1Gbps. It is a fourth-generation (4G) cellular communication system.

The aim of **4G** systems is to include and integrate different mobile network architectures and wireless access technologies to achieve a seamless wireless access infrastructure.

The main advantages of 4G are:

1. Multi-standard wireless system.

   Wireless (802.11x), wired, Bluetooth
2. Faster and more reliable than previous generations.
3. Lower cost than previous generations
4. IPv6 Core.
5. Ad Hoc Networking.
6. OFDM used instead of CDMA.
7. Potentially IEEE standard 802.11n

4.1 3GPP Standards:

The 3rd Generation Partnership Project is an integration of seven groups for development of telecommunication standards. The primary benefit of 3GPP was to develop a worldwide applicable third-generation (3G) mobile data networks using Global System for Mobile Communications (GSM) specifications.

The scope was then improved to contain the progress of: GSM and related "2G" and "2.5G" networks, including GPRS and EDGE, UMTS and related "3G" networks, including HSPA, LTE and related "4G" standards, containing LTE Advanced and LTE Advanced Pro etc.

3GPP standards are structured as *Releases* and these are discussed as follows:

4.1.1 Release 8: For the first time, LTE has been developed by Release 8 with improved core network and radio interface, enabling significantly enhanced data performance than available technologies. It provides data up to75Mbit/s uplink and 300Mbit/s downlink with lower latency to 10ms, multiple input multiple output antennas, single-carrier frequency domain multiple access (SC-FDMA) uplink and OFDMA downlink.

4.1.2 Release9: The initial improvement was comprised to LTE in release 9. These enhancements are:

- **i.** PWS (Public Warning System) which states users always receive services timely and got good results even in case of disasters or peak traffic situations.
- **ii.** Femto Cell is utilized in commercial buildings and associated to providers' networks using landline broadband. These cells are deployed around world and in order for LTE clients to take gain of this cell.
- **iii.** MIMO Beam forming is utilized to improve cell edge by directing beam towards specific UE by position estimation.
- **iv.** Self-Organizing Networks (SON) reduce manual work and cost associated with technical support.
- **v.** The Multimedia broadcast Multicast Services (MBMS), operators have ability to multicast applications over LTE network.

4.1.3 Release10: Release 10 improves the capability and data delivery of LTE and also took phases to enhance capability of system for mobile devices placed at various distances from a base station. The key features of this release are as follows:

4.1.3.1 Carrier Aggregation

i. The bandwidth is extended up to 100 MHz

ii. Enhancement of maximum data rate and facilitate the compatibility with LTE Release 8.

iii. Common physical layer constraints between LTE Rel-8 carrier and component carrier

4.1.3.2 Advancement in MIMO techniques

i. Extension up to 4-layer transmission in uplink

ii. Extension up to 8-layer transmission in downlink

iii. Enhancement of capacity and peak data rate

iv. Improvements of multi-user MIMO

4.1.3.3 Enhanced Inter-Cell Interference Coordination (eICIC)

i. Improvement of cell-edge throughput and coverage.

ii. Deferent transmission power cells Interference coordination.

4.1.3.4 Synchronised Multi-Point broadcast and response.

i. Improvement of cell-edge throughput and coverage.

ii. Support of multi-cell transmission and reception.

4.1.3 Release11

Release 11 was enhancement of Release 10 with a several improvements to standard capabilities by improving the eICIC, relay nodes, MIMO and Carrier Aggregation. Motivation for LTE-Advanced is as follows:

i. 3GPP aligned to ITU-R IMT process

ii. Allows Coordinated approach to WRC

iii. 3GPP Releases evolve to meet:

- Future end user and operators requirements
- Future Requirements for IMT

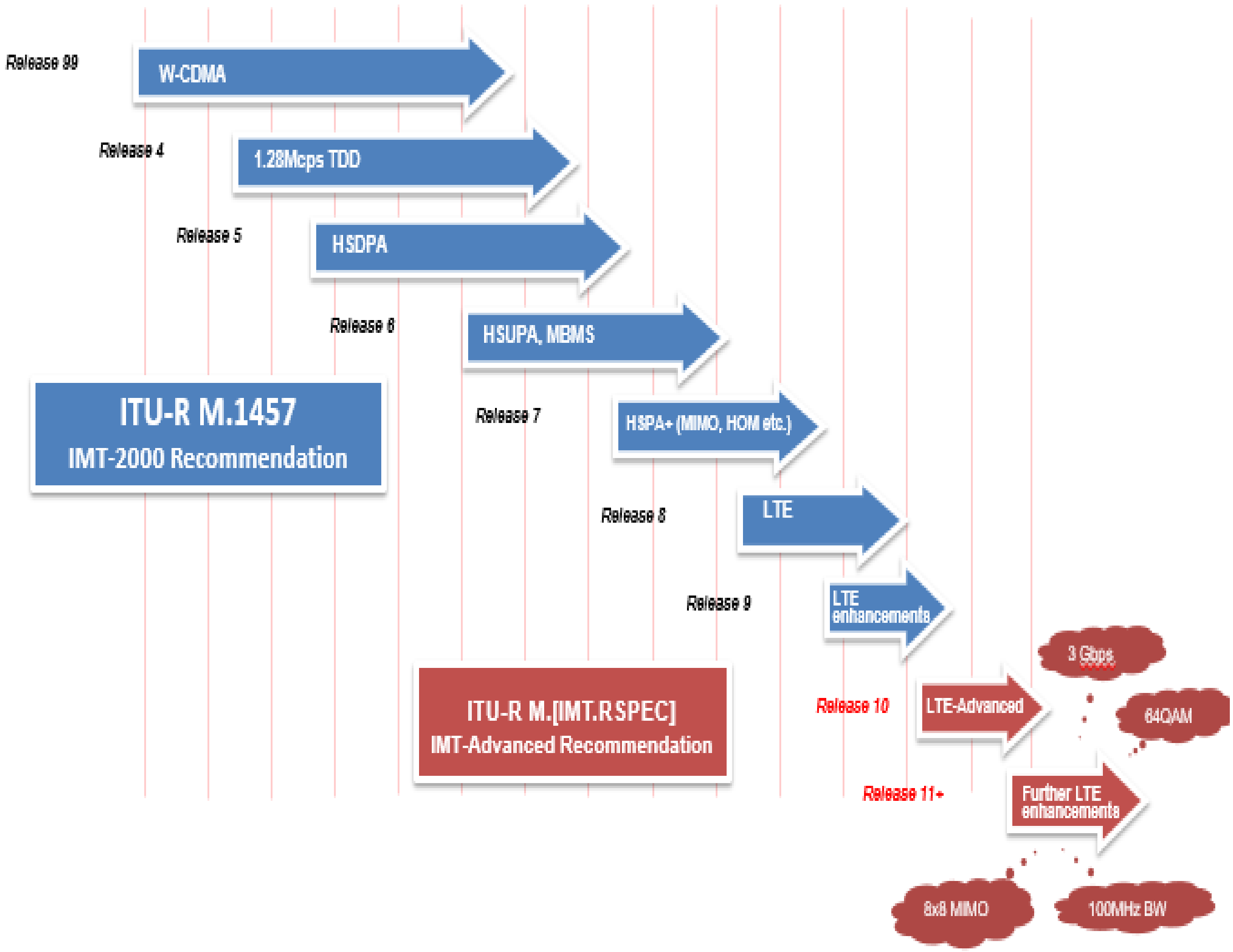


Fig 24 – [20] 3GPP Releases

4.1.4 Release 12: This release has improved cells for LTE by using the inter-site carrier aggregation, to combine and match the features of adjacent cells. New antenna technologies have been used with improved receivers to enhance the significant of large cells. It utilizes interworking among LTE and HSPDA.

4.1.5 Release13: The primary objective of this release is to support carrier aggregation up to 32 component carriers (CC). It has also improved that Machine-Type communication (eMTC), GSM/EDGE Internet of Things (EC-GSM- IoT) and narrow band Internet of Things (NB- IoT) market. Also, in release 13 integrates primary cells from licensed and secondary cells from unlicensed spectrum to handle the peak time traffic. It has also improved the multi-user transmission techniques. Support has been increased up to 64 MIMO antennas.

Rel-13 eMTC, NB-IOT and EC-GSM-IoT

	eMTC (LTE Cat M1)	NB-IOT	EC-GSM-IoT
Deployment	In-band LTE	In-band & Guard-band LTE, standalone	In-band GSM
Coverage*	155.7 dB	164 dB for standalone, FFS others	164 dB, with 33dBm power class 154 dB, with 23dBm power class
Downlink	OFDMA, 15 KHz tone spacing, Turbo Code, 16 QAM, 1 Rx	OFDMA, 15 KHz tone spacing, TBCC, 1 Rx	TDMA/FDMA, GMSK and 8PSK (optional), 1 Rx
Uplink	SC-FDMA, 15 KHz tone spacing Turbo code, 16 QAM	Single tone, 15 KHz and 3.75 KHz spacing SC-FDMA, 15 KHz tone spacing, Turbo code	TDMA/FDMA, GMSK and 8PSK (optional)
Bandwidth	1.08 MHz	180 KHz	200kHz per channel. Typical system bandwidth of 2.4MHz. 600 kHz considered feasible for static, small data applications
Peak rate (DL/UL)	1 Mbps for DL and UL	DL: ~60 kbps UL: ~50kpbs (multi-tone), ~20 kbps (single tone)	For DL and UL (using 4 timeslots): ~70 kbps (GMSK), ~240kbps (8PSK)
Duplexing	FD & HD (type B), FDD & TDD	HD (type B), FDD	HD, FDD
Power saving	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX
Power class	23 dBm, 20 dBm	23 dBm, others TBD	33 dBm, 23 dBm

** In terms of MCL target. Targets for different technologies are based on somewhat different link budget assumptions (see TR 36.888/45.820 for more information).*

Fig 25 – [21] Release 13 eMTC, NB-IoT and EC-GSM-IoT

4.1.6 Release14: Release 14 contains Cell Broadcast Service (CBS), massive Internet of Things, Flexible Mobile Service Steering (FMSS), and mission critical video over LTE, mission critical data over LTE, Location Services (LCS), energy efficiency, enhancement for TV service, Multimedia Broadcast Supplement for Public Warning System (MBSP), etc. It also supports the direct and network communication application, safety application of V2X communion.

i. **eMTC –** Voice support (VoLTE) and enhancement in the speed of data rate for Machine Type Communication.
ii. **eMTC, NB-IOT** - Enhancement in features like mobility and multicast.
iii. **eMTC, EC-GSM-IoT, NB-IoT –** Enchantment in the position of massive machine type communication**.**
iv. **NB-IoT –** Enhancements of features access/paging and different power classes.

4.2 Key components of 4G Architecture :

The advanced-LTE network architecture so called architecture of 4G network is an overall flat architecture. It consists of SAE gateway and e-Node B. The 4G network is based on a TCP/IP protocol with advanced features such as messaging, video, voice, etc. Based on this, 3GPP had started the achievability studies related to all IP networks (AIPNs) in 2004.

The telecommunications industry has been changing the trend from circuit switched networks to packet data services. The data services firstly have been brought by GPRS to GSM networks. UMTS with HSPA persistent the same trend with much privileged data speeds. To deploy all 3GPP and non-3GPP technologies, Advanced LTE provides an evolutionary path for operators. It means that there is not only one specific path to LTE. Each up-gradation case will be different based on the existing technology and network architecture.

The general architecture is depicted in technical specification 36.401 and 36.300. X2 interfaces are used to connect the E-Node Bs. E-Node Bs are joined to the evolved packet core network (EPC) network through S1 interfaces.

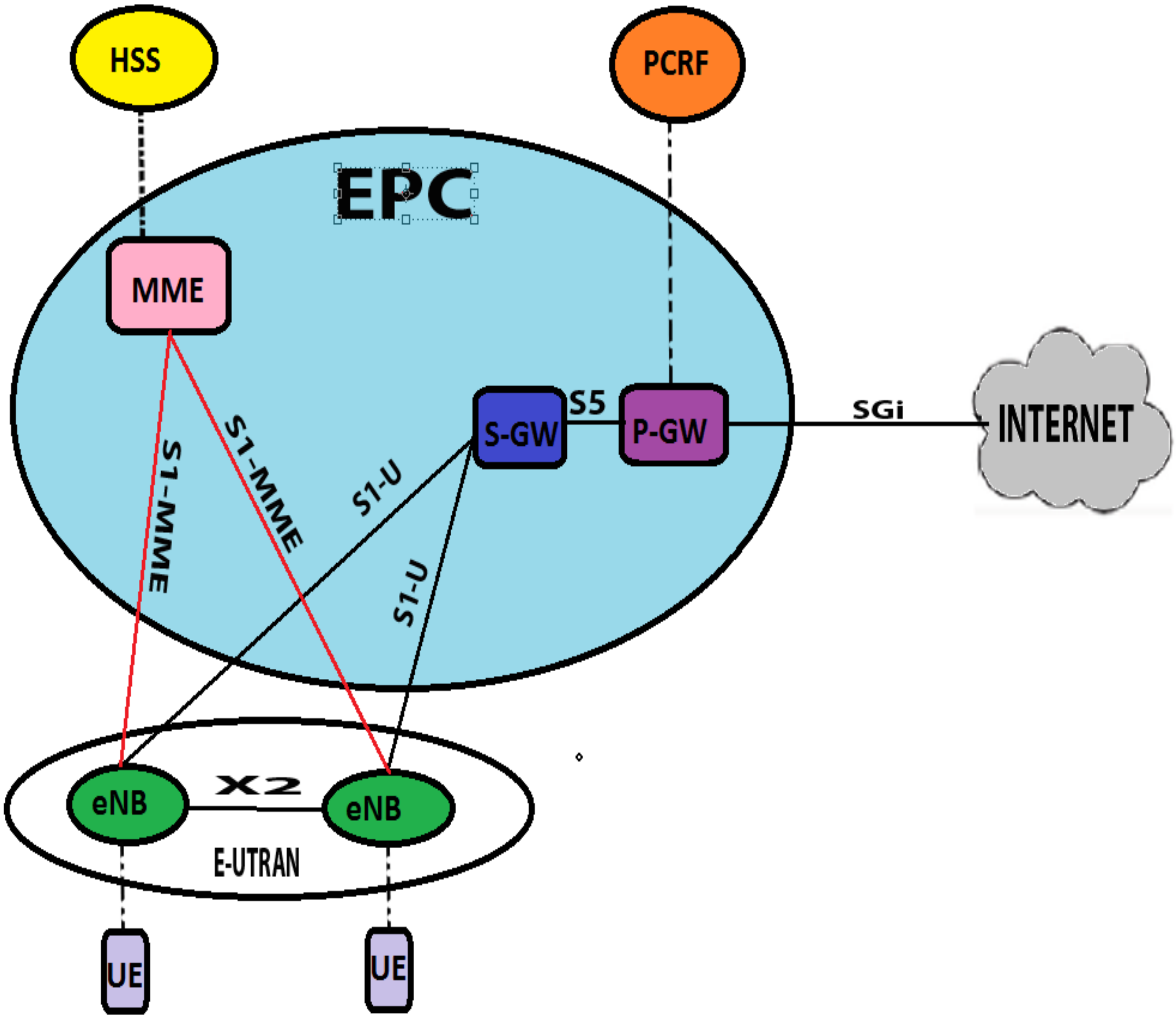


Figure 26: 4G architecture

3GPP evolution for 3G mobile systems defined the System Architecture Evolution (SAE) network (LTE Core Network) and the UTRAN Long Term Evolution. LTE/SAE network involves many new network components such as SAE GW and MME. Only remaining component in radio access network is eNode B. The LTE structure relies upon IP and thus is intended to adequately supporting the two essential parts of the LTE architecture; Evolved Packet Core (EPC) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN). eNodeBs are part of E-UTRAN and is responsible for managing control plane and radio access of UE (User Equipment's). Moreover the data transmission is handling by user plane protocols and connection management between UE and the system is control by control plane protocols.

Mobility management entity (MME), Packet gateway (P-GW), Serving Gateway(S-GW) is components of Evolved packet core (EPC) and provide lower latency because of reduced nodes. S1 and X2 are main communication interfaces, X2 interface is between different eNodeBs in the E-UTRAN and provide functions like client data forwarding, links coordination messaging reports, handover information, and design setups. The communication between EPC and E-UTRAN is with S1 interface where as S1-MME is for control-plane communication between eNodeBs and MME and S1-U is for user-plane communication.

4.2.1 **UE (User Equipment)**: Uu is the communication interface between UE and eNodB and the connection setup is based on the specification in the 3GPP 25/36 and ETSI 125/136. UE is an end user and responsible for initiate the calling; it can be mobile broadband modem enable smart phone, computer/laptop or other equipment.

The NAS (non-access stratum) protocols are transparent to eNodBs and the data sent by UE to EPC cannot use or understand by eNode Bs in the E-UTRAN. Main functions of UE are Identity management, Call control, Session management, mobility management.

4.2.2 **eNode B**: Evolved Node B is a base station in LTE/SAE network. Its primary functions are routing of user plane data towards SAE gateway, selection of an MME at UE attachment, IP header compression and encrypting of user data stream, radio resource management, and reporting configuration for mobility and scheduling. The RNC (radio network controller) functions are enabled in eNodeBs and which faster the response time and improve the overall architecture.

Functions:

- MME pool support
- Mobility control
- User plane and Control plane Security
- Shared channel handling
- HARQ
- Scheduling
- Multiplexing and Mapping of channels
- Physical layer functionality
- Measurement and reporting

4.2.3 **Mobility Management Entity (MME):** MME is handling the signaling among the EPC and UE via E-UTRAN and it is a key node of LTE core network. The EPS bearers are initiating and maintain by Non-access stratum (NAS) between UE and EPC. The main functions done by MME are authentication, security, paging, mobility and registration but out of that connection management and bearer management in the network. S1-MME interface connects MME to eNode B and is ending point of NAS protocol system.

4.2.4 **Serving Gateway (S-GW):** S-GW is used in the user plane of LTE Core network. It is used to routes and forwards data packets of users and has all the charging information of the traffic load on the link by UE. When UE is moving between eNodeBs during the handover, S-GW is a mobility anchor for user plane, all the IP packets are flow through it and also known as central point for moving IP traffic from UE and outside networks. S-GW interfaces with P-GW through S5 interface and in addition, 3GPP (UMTS and GPRS) also internetworking with S-GW for mobility. It may interface with SGSN also for handover support. It acts as a buffer while reestablishment of the bearer by MME to UE and moreover, the all the bearer information is store when UE is idle (Idle mode buffering).

4.2.5 **P-GW (PDN Gateway)** – Packet data network gateway worked as entry and exit gateway which enables the communication and transfer the data from UE (User Equipment) to outer packet data networks. It behaves like a mobility anchor during handover communication between LTE and non-3GPP technologies (HRPD – high rate packet data and Wi-Fi). The main responsibilities are IP address allocation, Quality of service to the user equipment and as per TFTs (Traffic Flow Templates), it control the flow of IP packets using standard QoS . P-GW is also screen and restricts the interception of unlawful packets as default gateway.

4.2.6 **HSS (Home Subscriber Server):** HSS is a similar to HLR +AuC in the earlier infrastructures and known as central permanent database for each UE which record and store all the information such as confidential data, IMS numbers related to each user equipment. In addition, it manages and authenticates the data of the subscriber and the system architecture evolution (SAE) subscription such as QoS and roaming access limitation.

4.2.7 **Policy and Charging Rules Function (PCRF):** The service policy is managed by the PCRF server and for each session of the users it determines the QoS setting, accounting rule and policy rule. During session establishment the Policy Decision function (PDF) make decision on the receive media requirements (SIP signaling) of terminal and P-CSCF according to the network operator. The P-CSCF send the type of application information (audio, video, identifier, data rate etc) to the charging rule functions (CRF) and it choose the charging rules as per service data flow.

4.3 Advantages of 4G Technology:

1. It provides the end-to-end IP connection. As 4G technology can provide mobility, the cellular providers can offer data access to a broad variety of devices. It is more flexible, reliable and easy to standardize and can be afford.
2. Using this technology one can easily access video calling, streaming media, social networks, IM, Internet and other broadband services. It is very steady during the connectivity to the internet without any disruption.
3. The 4G technologies are HSPA+, LTE and WiMAX. HSPA+ is used by AT&T and TMobile, LTE is used by Verizon and AT&T, and WiMAX is used by Sprint. It allows IP based mobile technology that has high speed and significant capacity.
4. It also improves the voice quality and provides ten times faster download speed than the 3rd generation network. It provides high quality streaming for watching online TV, online music, watching online videos, and the others streaming applications
5. 4G mobile network provides very fast speed. 4G has a higher bandwidth that means data transfer can be transferred at a much higher speed which is especially fruitful for mobile devices.
6. 4G networks provide complete safety, security and privacy. It is specifically advantageous for those who operate their businesses from mobile devices.

4.4 Disadvantages of 4G Technology:

1. 4G technology can be attacked using jamming frequencies and the important information can be leaked.
2. To support 4G, the consumer is needed to buy a new device. New technology means new frequencies and it means consumer needs new components to use those frequencies that are expensive and hard to implement.
3. Data prices are higher for 4G LTE network and consume more energy when data is used by the device for a long time.
4. This technology is limited in specific areas though it is increasing day by day. Because it needs complex hardware.
5. The mobile operators are charging the mobile user according to 4G plan but as it is present in only some specified areas, the user facing problems as they are offered 3G in reality. This issue can be solved only when operators increase their coverage areas.

5 5G standard investigation:

Release 13 has defined the LTE-Advanced Pro and further improvements have been introduced in Release 14. Recently, further standardization has also been planned in Release15. Both releases 14 and 15 have started the study of items towards 5G. While release 14 has focused only on study items of 5G, the release 15 will work for the initial (first) phase of the 5G system specification. Release 15 will provide the enhancements in LTE-Advanced Pro which includes 1024 QAM for LTE, LAA/eLAA for CBRS at 3.5GHz, enhancing LTE operation in unlicensed spectrum, enhancements to V2X, and enhancements to NB-IoT. Rel-15 include various 5G related features such as 5G system phase-1 , New Radio (NR) access technology, EPC enhancements to support 5G NR via Dual connectivity, and LTE Connectivity to 5G Core Network (5G-CN).

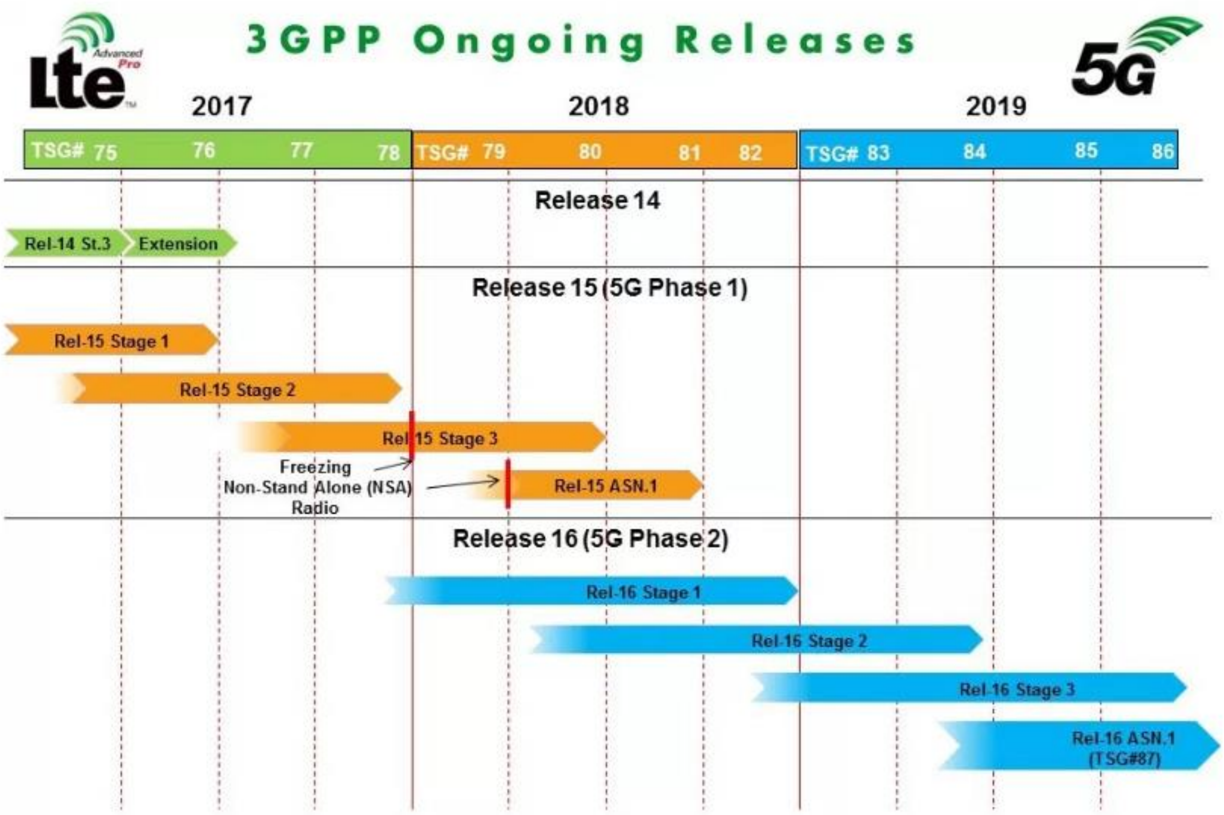


Fig 27 – [22] 3GPP ongoing Releases 14,15 and 16

5G promises mobile internet speeds that far outstrip the fastest home broadband network speed currently available in the majority of countries. Therefore, 5G will provide speed around 100 to 150 Gigabits per second. It will be as approximately 1000 times better than standard 4G technologies. The advances carried by 4G are already being felt by industries whose professionals are frequently on the move. As known previously, 3G networks unable to provide data speed demanded by modern mobile users. Users in urban areas frequently feel the effects the most, with poor internet speed also sometimes unavailability of internet connections common in peak working hours.

As 4G networks have significant base internet speeds, therefore it provides good internet speed and connection during the peak-hour load. However, during the travelling time it provides not significant speed as per user’s requirements. Therefore, the need of the 5G technology comes in the mind of internet service providers to provide high availability of internet during the traveling time. 5G will have the ability to provide high-speed internet speed almost real-time, putting mobile internet data speeds on par compared to speed provided by office broadband.

Table 4 compares the three well known internet technologies i.e., 3G, 4G and 5G. For comparison purpose, deployment, bandwidth, technology and service features have been considered. It has been clearly observed from the table that the 5G technology has quite more speed compared to 4G and 5G technology. Also, it provides additional services than 3G and 5G technologies.

3G VS 4G VS 5G

	3G	4G	5G
DEPLOYMENT	2004-05	2006-10	BY 2020
BANDWIDTH	2mbps	200mbps	>1gbps
TECHNOLOGY	Broadband with/CDMA/IP technology	Unified IP and seamless combination of LAN/WAN/WLAN/PAN	4G + WWWW
SERVICE	Integrated high-quality audio, video and data	Dynamic information access, variable devices	Dynamic information access, variable devices with all capabilities

Table 4 - **[**23] Comparison between 3G, 4G and 5G technologies

5.1 Advantages of 5G technologies:

1. 5G will provide approximately 1000 times faster internet bandwidth compared to standard 4G technologies.
2. It will have the ability to save up to 90% of energy compared to energy consumed by existing 4G service providers. Also. It will allow mobile users to save their energy by providing internet speed at a quit higher rate. Therefore, one may call 5G technology as green internet technology.
3. It will also have the ability to minimize the mean service development time cycle from hours to minutes.
4. It will develop a protected, highly reliable, efficient and fastest internet service with a “zero perceived” downtime for services delivery.
5. It will provide wide deployments of wireless communication connections to link the various wireless devices to connect the world.
6. It will ensure that every user at every location has the access to an extensive range of internet applications at lower cost.

5.2 Disadvantages of 5G technologies:

The 5G technology is still in development and facing many challenges to resolve the existing technologies shortcomings for examples issues in the radio signals, security issues, and overall technology advancement problems of the mobile world.

1. Some parts of the world are using 3G technologies and to achieve such a fast speed seems to be difficult.
2. New hardware (UE) equipment is required to support 5G services.
3. Security and privacy still need new protocols to work effectively.
4. Infrastructure needs a high cost of supporting new radios.

6 Applications of 5G technology :

Fig 28 – [24] 5G Applications

5G communication technologies will expect to support the applications with high variety of utilizations and fluctuation of their performance attributes. These applications may have extreme diverse requirements such as low latency, delay-sensitive videos, vehicle to mobility high speed connections and services, health and safety ultra-reliable applications. Furthermore, heterogeneous communication environment with massive devices will be work smoothly even with different network requirements. The application is divided into eight groups with twenty-five use cases tool to capture the level of flexibility required in the 5G system.

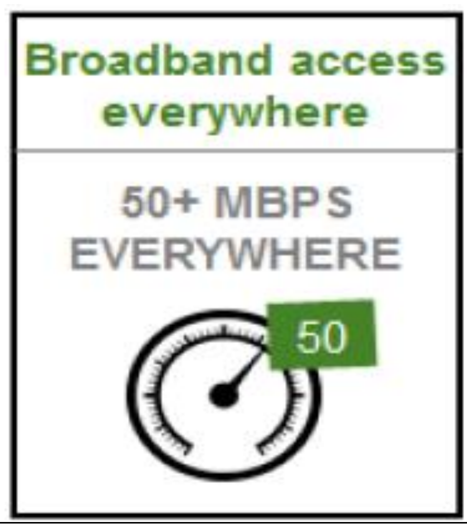
6.1 Broadband access in the dense area:

5G network will provide broadband access can be given in dense area, crowded area and ultra-high access in indoor. This will help to serve dense urban society, cloud operators, smart offices, and sharing of HD videos in the open-air gathering.

- Broadband access per square kilometer (km2).
- Augmented reality.
- 3D video streaming services.
- HD video communication from person to person or group.
- Several concurrent connections with high data rate and low latency.

6.2 Broadband access everywhere:

The target of 5G technology is to provide the access of network everywhere which means that minimum 50+ Mbps speed should be available to every user and the cost of the network should be minimized. There will be high infrastructure cost to the less populated area to provide high-speed services, but 5G is expected to be flexible in offering these services at manageable cost.



6.3 Higher user mobility:

It includes mobile broadband in vehicles and Airplane connectivity. The mobile broadband means provide good speed in high speed trains, moving hotspot and remote computing. The airplane connectivity includes 3-D connectivity to aircrafts. Moreover, the demand of autonomous driving, entertainment, internet streaming and high –speed navigation features, safety and diagnostic reports while mobility is expected in 5G network.

6.4 Massive Internet of Things (IoT):

5G can provide a wide range of massive device connection and IoT services which includes smart wearable clothes, the connection between the wide range of sensor networks, and mobile video surveillance. The massive devices include low-cost, low-power and broadband machine to machine communication, and machine to human communication.

Examples: Massive ultra-light water ingress sensors embedded in smart wearables for measure health attributes and around environment. In sensor networks, it have high density of smart low power devices for measuring (temperature, noise, humidity, pollution, utility measurements, light management, etc.), services. The major problem of massive devices will be overall efficient management. Moreover, 5G will provide secure and reliable network for security monitoring massive devices such as drones, video surveillance cameras and other safety equipment.

6.5 Extreme real time communication:

Rea-time virtual With 5G the realization of Tactile Internet is possible. Tactile Internet is an internet network that can combine ultra-low latency with extremely high security, reliability and availability. It believes that it represents a "revolutionary level of development for culture, economics and society".
For example: Connected cars application required high speed as well as ultra-low latency network for quick response to prevent collisions. Moreover, these applications will useful in smart medical care, manufacturing, mission critical applications.

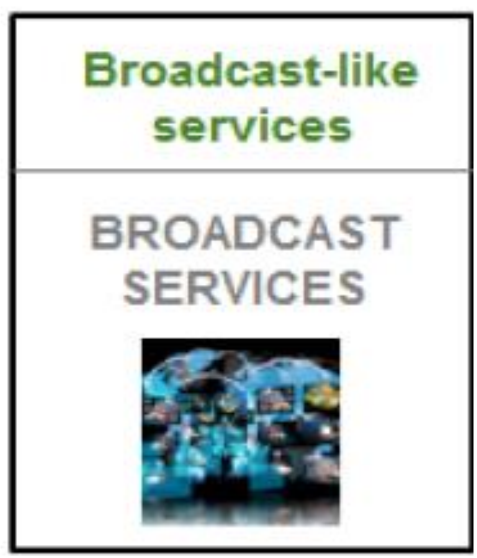
6.6 Lifeline Communications:

The dedicated 5G network slice has been expected to improve the public safety system by providing high availability and robust communications in case of emergencies like natural disasters, total power loss, terrorist attacks, etc.
The several applications are emerging for improving public safety, disaster relief, prediction of emergency, public to authority communication channel, separate network for alerts and support.
In addition to that, 5G network will be highly available first lifeline approach and provide basic communication services like voice and text message for life safety.

6.7 Ultra-reliable communication:

The ultra-reliable communications can also vision in the 5G mission-critical applications for industrial communication especially in the Smart Grid. It will modernize the diverse traditional communication network and provide the unified low latency connectivity between SCADA control system and IED equipment for early fault detection and troubleshooting of Smart Grid electrical architecture. This communication will be also beneficial for autonomous driving cars, robotics industry, eHealth services, 3D connectivity and Public Safety.	

6.8 Broadcast like services:

In contemporary times, the broadcast service is mostly downlink dominated for example, linear TV, single source to multiple destinations. The 5G technology will include uplink channel in the real time or non-real time broadcast services for feedback and provide an interactive experience. It includes news and information, and services related to local, regional, and national. The broadcast services are also important for vertical industries for firmware distribution and upgrade, software patches and these services can be documented with feedback via uplink channel.	

.

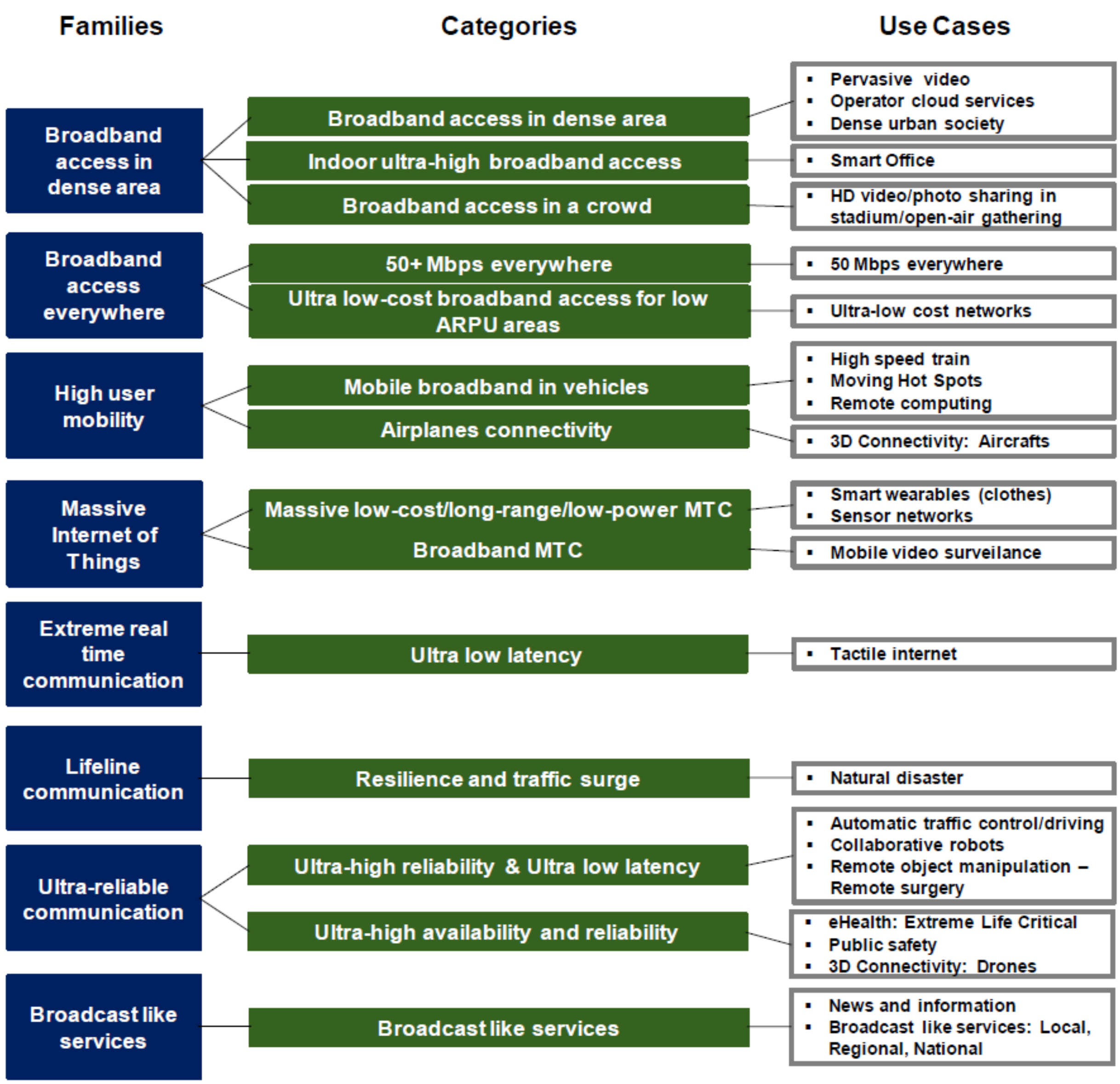


Fig 29: [25] 5G application categories.

7 Software Defined Network (SDN):

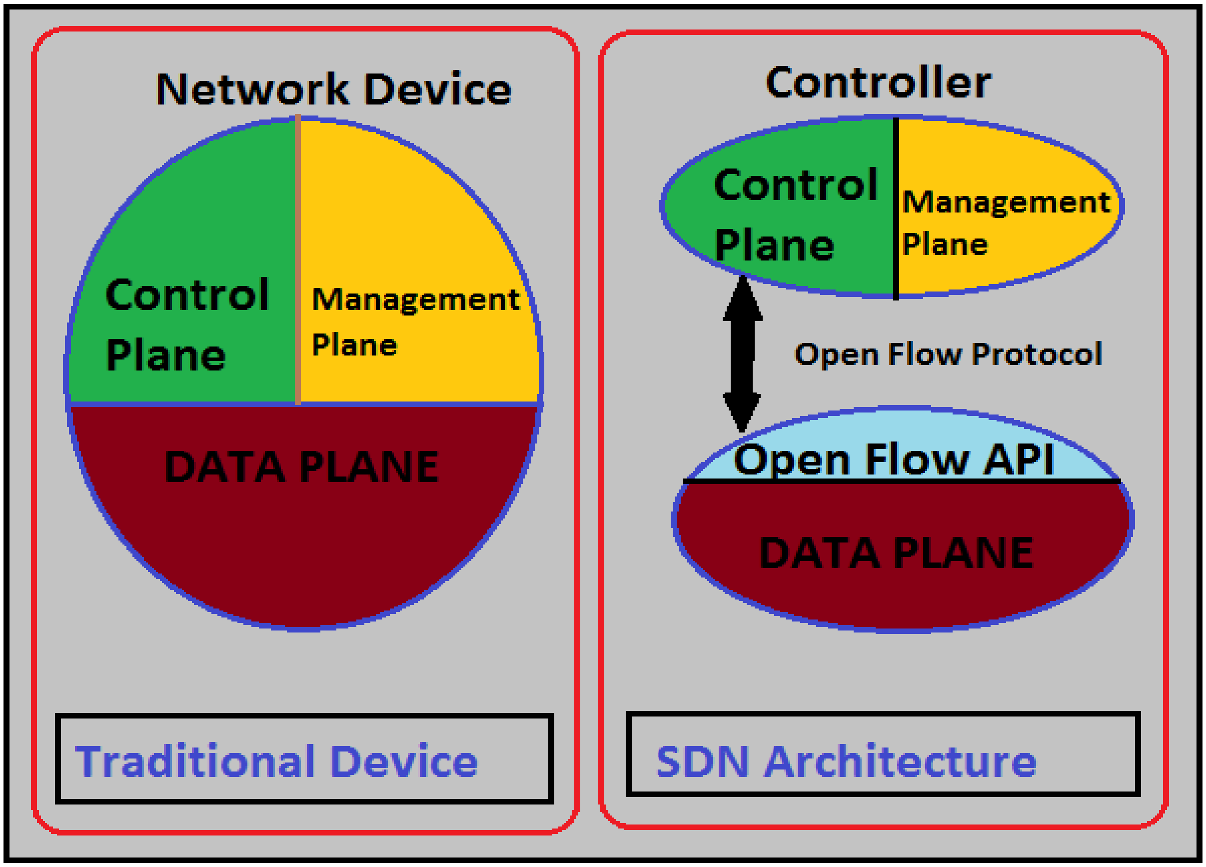


Fig 30 - Traditional vs SDN Architecture

Software Defined Network (SDN) is the system which separates the network control from forwarding hardware (that can be access point, router, switch etc.) and is integrated into a software that is a logically centralized controller. The open interfaces such as Open Flow developed by Open Networking Foundation (ONF), For CES (Forwarding & Control Element Separation) developed by IETF, or any other proprietary protocol can be used to program the forwarding hardware.

SDN architecture mainly involves following two points:

- Decupled the control plane and data plane and move the control plane to external hardware named as a controller.
- A set of Open APIs (application programming interfaces) are used for control plane and data plane. Control plane use the programmed interfaces that empower the controller to operate the switches.

7.1 SDN architecture:

In SDN architecture, the forwarding hardware is remains separated from the network control. The rules in the forwarding hardware are defined by the network control program which resides in the controller. Traffic in the network proceeds according to these rules. SDN can be demonstrated as three layer architecture (can see from Figure 31):

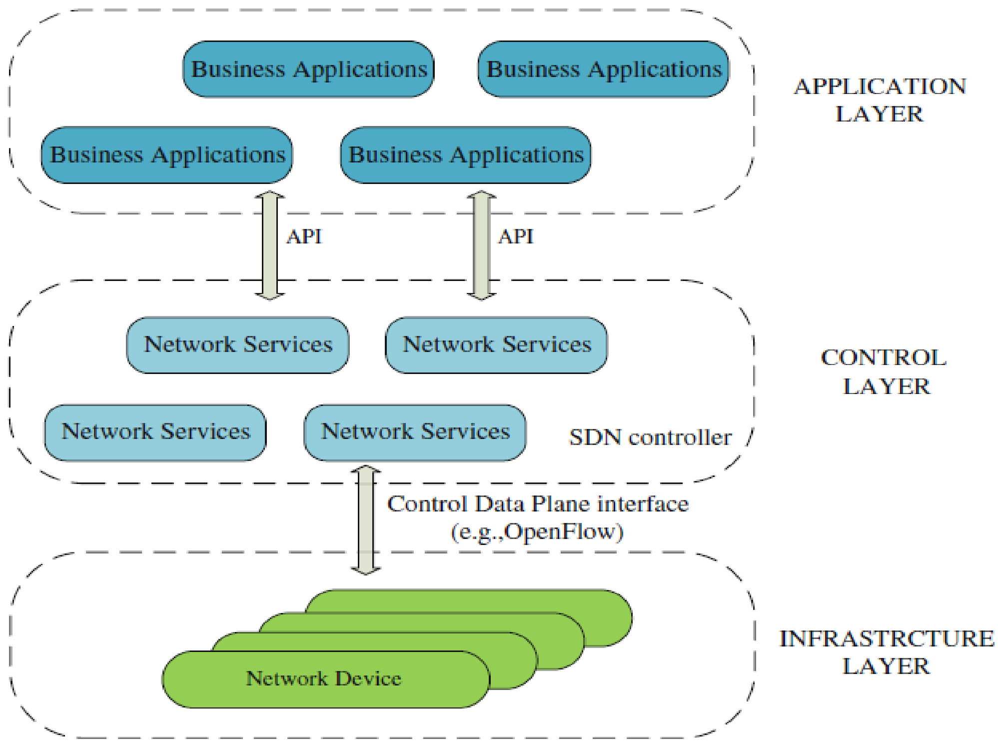


Fig 31- [26] SDN architecture

7.1.1 Infrastructure Layer:

It includes forwarding hardware such as switches and routers. It also includes all hardware components and software interfaces required in forwarding hardware.

7.1.2 Control Layer :

It includes SDN controller which regulate and manage the forwarding hardware. SDN controller considered as an intelligent network, which logically controls the devices and provides network services between application and infrastructure layers.

7.1.3 Application Layer :

This layer takes benefit of infrastructure and control layer. Conceptually, this layer is the topmost layer. These applications help in regulating the traffic in the network so the user requirements can easily meet. Figure 31, shows the architecture of Open flow (OF) protocol of SDN.

7.1.4 Open Flow :

The Open Flow is an open source routing protocol for SDN and which offers standard interfaces that allow data plane to communicate with the control plane. Subsequently, the forwarding hardware is directly controlled by the control plane to regulate the packets movement in the network. Therefore, many forwarding devices are managed by a single controller. OF is based on flow mechanism that means it handles flows not only one flow at a time. The open flow switches have an internal flow-table and the open flow controller updates the entries of flows in flow-table. Open flow has developed numerous specifications but 1.0.0 is usually used.

7.1.5 Control Plane :

This is an approach to centralize the decision making capacity of all the switches from individual ones in the SDN controller. The application programming interfaces are linked the application and the control plane which simplify the development of the new network applications. These applications have logics which easily manage the new flow rules. APIs provide communications between controller, applications and switches. Moreover, APIs also offers communication to the different layers in SDN stack and these are divided as:

- **Northbound APIs**: It is a communication interface between application and controller which allows programming the network. The advantages are open standard; customize control and easy modification of applications according to needs.
- **Southbound APIs**: It is a communication interface between forwarding nodes and controller which is also low level components. The advantages are easy user control and improve the efficiency of the controller.

7.1.6 Forwarding Devices :

In SDN the forwarding devices are also called dumb devices for example access points, routers and switches and can be classified as

- Application and Control layer processing is not required normally in dedicated OF switches.
- A secured channel, OF protocol and a flow table are the main components of the OF switch and these interfaces are added to the OF-enable routers and switches.

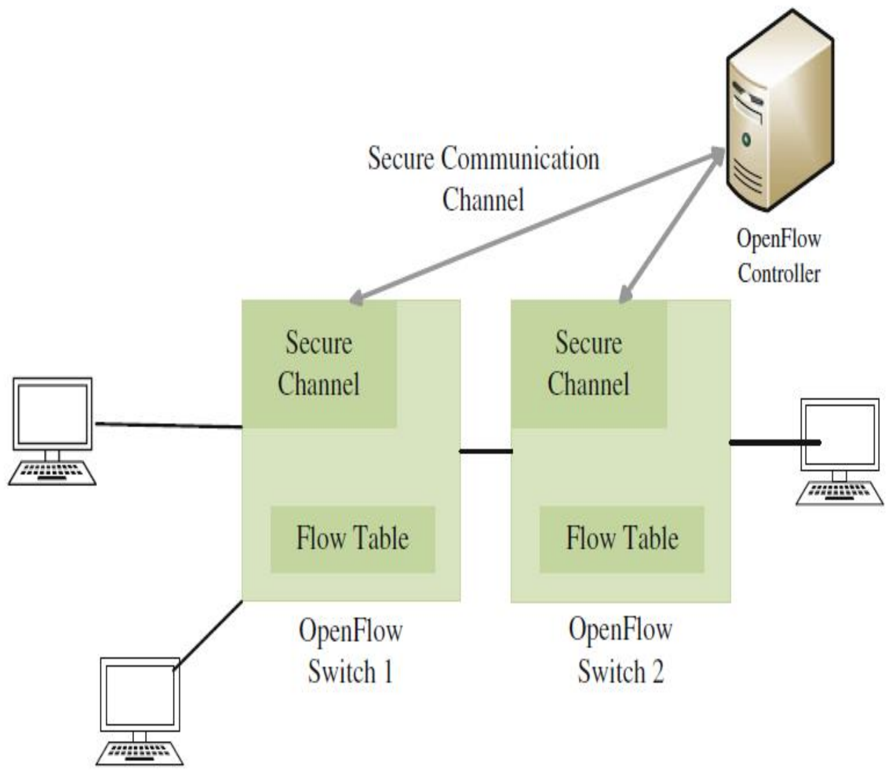


Figure 32 – [26] Open Flow architecture

7.1.7 SDN and 5G: In the 5G network technology, the UE will latch to the high quality signal network and there will be continuous connectivity with the 5G network for high mobility devices even in the diverse the situation. Additionally, there will be dynamic RAN and the UE will likewise remain alert and searching for a connection to the best signal network.

SDN will provide the dynamic service to UE and will be the foundation of the wireless network infrastructure. It wills correspondence the service between SDN applications and innovation, regarding the dynamic changes at the present access technology. Therefore, the network designs can be changed in the program rather than replacing the expensive hardware and it will provide overall real-time management, session management, and resource virtualization. SDN and 5G technology is undergoing in research phase to mitigate the limitation of overhead (user send a request to the controller), mobile resources and computing capabilities.

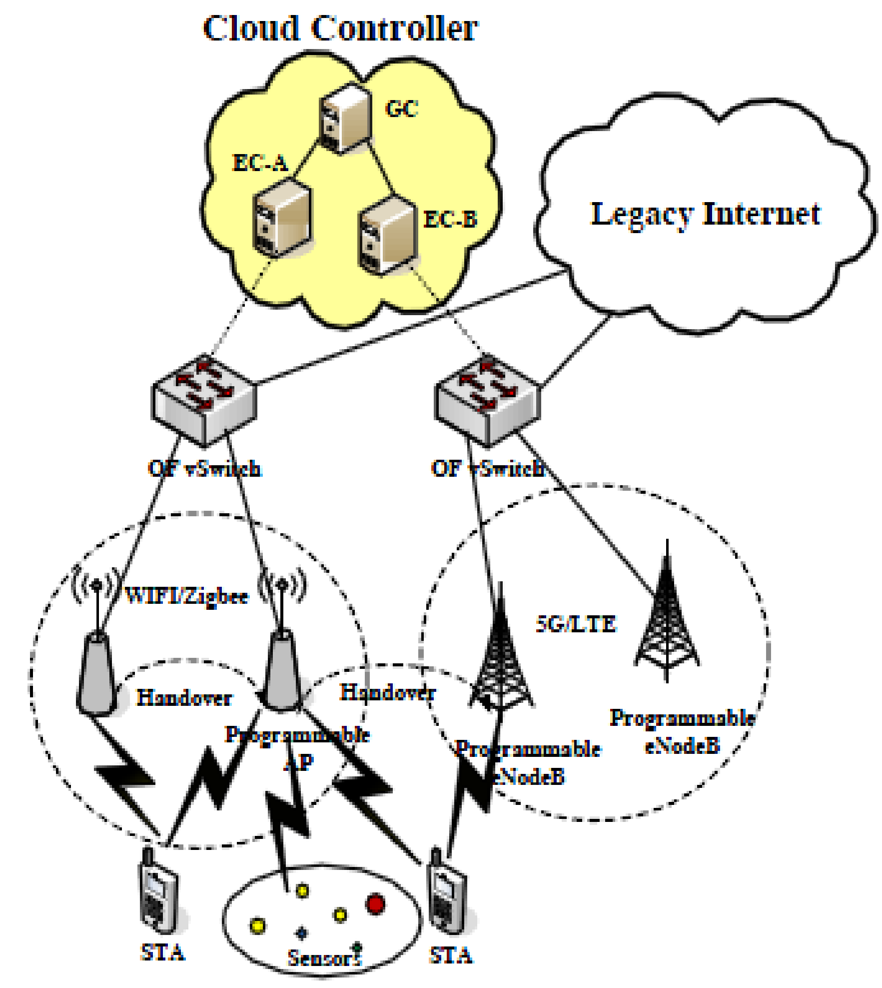


Fig 33: [27] SDN and 5G network

SDN has high significances due to its flexibility to optimize the network performance with programmable interface. The telecom industries have moved to IP based networks and in the 5G technology, the numerous applications like vehicle to vehicle (V2V), massive machine type communication, mission-critical applications, high speed videos and mobile broadband have different network requirements for example latency, throughput, massive devices, robustness, unique air interface, high reliability because of these requirement the SDN based architecture will offer many benefits of instantiating, lower costs as well as high performance in the virtualized environment. Accordingly SDN has involved significant interests from academic community and industries.

7.1.8 Software Defined IXP (SDX)

SDX tries to bring the features of SDN into inter-domain routing. In today's networks, traffic is forwarded only based on destination IP prefixes and the routes are selected according to routes that offered by their immediate neighbors. The programmable defined rules of packet- processing are control and managed by the SDN controller. The programmable rule performs several actions by matching the header files of the protocols. This will interconnect different networks and may also perform the content base routing, which has a significant role in bringing the popular content closer to end user.

For example, the routing of Border Gateway protocol packets on Internet is inflexible, unreliable as well as difficult to manage. It also has limitation of direct neighbors influence, IP prefix based routing, and forwarding paths are controlled indirectly. The SDN provides the solution of these limitations by separating the control and data plane, which enables the flexible forwarding policies; controller will receive control messages and forward path can be controlled in data plane by applying the packet –processing rules.

7.1.9 Software defined radio (SDR):

The software-defined radio has been the objective of numerous radio advancements for various years. Introduction of software within radios and radio technology gave origin to software-defined radio.

Radio can be completely defined and managed by the software is the basic and primary concept of SDR. It will not only give a common platform that can be utilized in various areas but also is used for changing the configuration of radio at a given time for the specific function. Reconfiguration of the software-defined radio can provide the solutions in many ways, for example when upgrades to the new standards are available; if there are some changes in scope of its operation and if some other role is to be met.

Although, it is necessary to produce a concrete definition of SDR for many reasons such as standard issues, regulatory applications and this will facilitate the SDR technology to advance rapidly. There are numerous definitions that might appear similar to the definition of SDR. There are two main types of radio containing software as defined by SDR Forum.

- **Software Controlled Radio**: Radio in which software controls some or all of the physical layer functions fixed within it.
- **Software Defined Radio**: Radio in which its specification and what it does is determined by the software. Changing of the software may alter its performance and its function.

Another definition of the Software Defined radio is that the controller has programs to build functions like filter, modulate and demodulate as well as some related to frequency selector that runs on generic hardware forwarding. The radio signal performance changes when software reconfigured those function. Software modules are used to attain this software defined radio. A generic hardware platform, used to run software modules that are consists of general processors and digital signal processing (DSP) processors, which execute radio functions to transmit and receive signals.

Levels of SDR

The radio network that has all the features of a software defined radio is not always achievable. Some radios may be fully SDR whereas some only support few features associated with SDR. The Wireless Innovation Forum (SDR Forum) has classified tiers in order to differentiate levels at which radio may be seated.

Configurable tiers are described below:

- ***Tier 0:*** It cannot be changed by software and is known as a non-configurable hardware radio.
- ***Tier 1:*** In this type of SDR limited functions, like power levels, interconnection etc. are controllable by software. But it does not control mode or frequency.
- ***Tier 2:*** The considerable proportion of the radio under this tier is software configurable. It is sometimes called Software Controlled Radio (SCR). The parameters such as frequency, wide/narrow band operation, modulation and generation and detection of the waveform, security, etc. are controlled by software. The RF signals are not configurable and rest hardware based.

- ***Tier 3:*** It is also called ideal software radio (ISR). In this type of SDR the edge among non- configurable and configurable elements subsists precisely close to the antenna. In addition to it the "front end" is configurable.

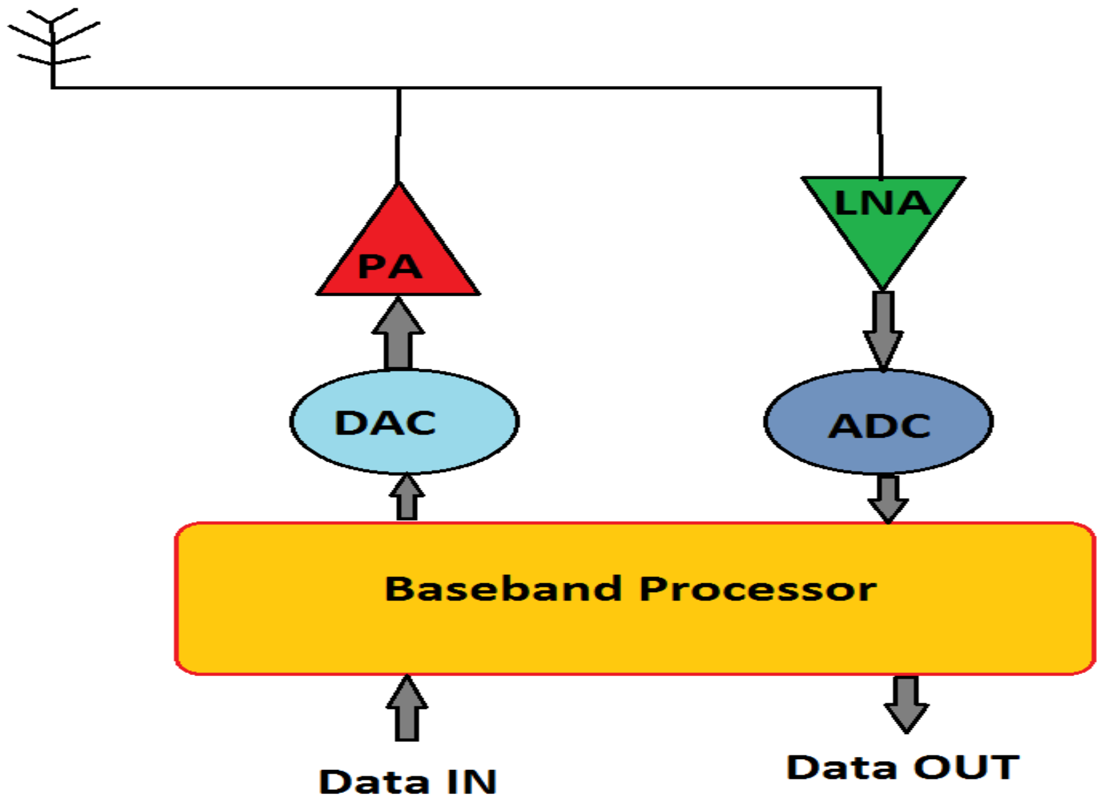


Fig 34 – Block diagram of an 'Ideal' Software Defined Radio

- ***Tier 4:*** The further advancement of the Ideal Software Radio is also known as ultimate software radio (USR). USR is a broad range of functions and frequencies is supported by this type of SDR and have full programmability. Some of the devices falling under these categories are electronic items such as a software definable multifunction phone and the cellphones those are having many different radios and standards.

These SDR tiers do not seem to be attached but they effectively provide a way of summarizing the existence of the diverse software defined radios' level. Waveform portability and self-configurable are major advantages of the software defined radio. Waveform portability reasons:

- ***Cost savings:*** Huge amount of money is invested by military and commercial to develop these waveforms for transmission. So, it is important we can reuse waveform on different projects that involve different platform there is a real need to be able to re-use waveforms on different projects and this is likely to compromise of very different platforms
- ***Obsolescence mitigation:*** It is also necessary to transfer waveform, which already exists on newer platform when there is an update in hardware.
- ***Interoperability*** A customer can request the use of a specific waveform across equipment from various manufacturers. These provide complete interoperability to a customer.

8 Network slicing:

Everything Mobile (+) Everything Connected (+) Everything Virtualized

Fig 35 – [28] Everything is 5G network

The evolution of cellular communication has been reached to a point where the concept of collecting real-time information "Everything to Internet" is become possible to support day to day life. The advent of 5th generation will not only be the ultra-speed cellular network but also target the technologies which require low latency (0.1~1ms) services and high reliability for end to end communication , massive machine to machine connections (mMTC & uMTC), new era of services with longer battery span, virtual & augmented reality. Network function virtualization/ Software defined network are the foundation blocks of 5G sliced-architecture and will have numerous advantages such as automate service deployment, simplified network design, increase network utilization and multi-layer protection. 5G network will consist of multiple networks and multiple air interface technologies for different applications. NFV/SDN will provide the solution of the biggest integration challenge of different networks.

Network slicing concept is already sometimes ago in the cellular network but due to the hardware or physical designs of the network only certain aspects are used in the current network technology. The network slicing is running multiple virtual network infrastructures on the physical network infrastructures and create slice instances of those virtual network which perfectly match the 5G eight class heterogeneous services requirement for example, broadband access in dense area, broadcast like services, ultra-reliable communication, Massive IoT, Extreme real-time communication, Broadband access everywhere, Life line communication and higher user mobility. These network instances are basically network functions and all the required resources which are needed to perform the required function to fulfill the business needs. The current research is ongoing to decide how many network slices are there to improve the overall efficiency of the physical network and provide cost-effective solution.

8.1 Network slicing concept by NGMN (Next Generation Mobile Network Alliance):

According to NGMN, the network slicing can be divided into three components and shown in below figure 36.

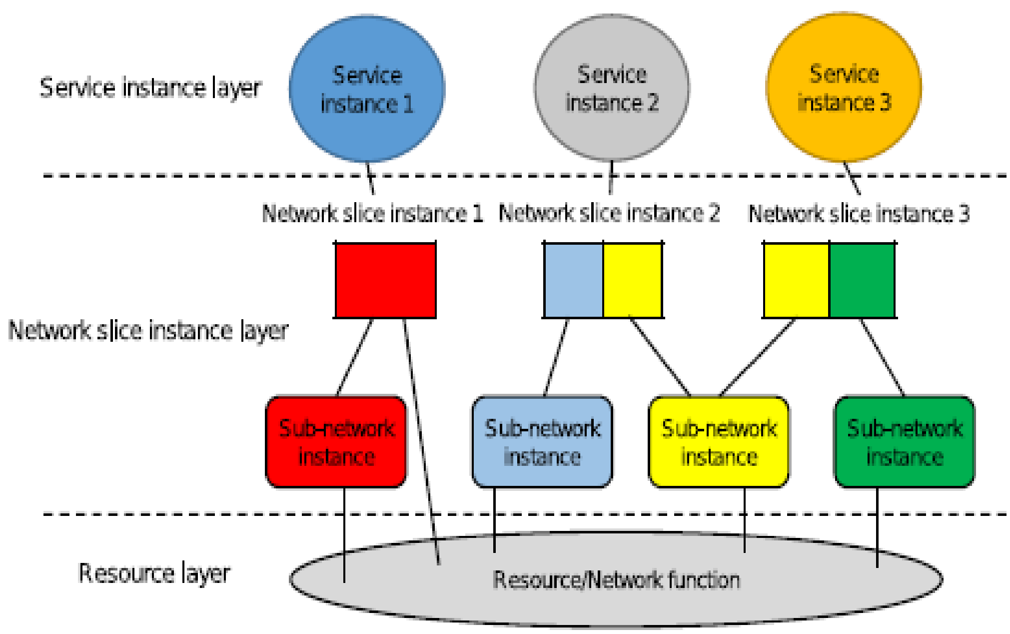


Fig 36- [29] Component of network slicing

- **Service instance layer**
- **Network instance layer**
- **Resource layer**

The 5G network operator will provide different services (xMBB, mMTC, uMTC) and these are representing by the service instance layer. It basically created one single instance of each offered service. Network slice instance offers network features and multiple service instances can be mapped to single network slice. Service instances have particular network characteristics requirement because each instance is different and these network slices may share or combine with other sub-network instances. A group of network Functions (NF) is dynamically built the sub network instances on logical/physical resources. Network slices are different network and telecommunication functions and running on virtual or logical network which dynamically built the instances and provides the services as per service level agreement (SLA) of the business.

8.2 NextGen Network Slicing: High level network slice architecture has developed by the SA2 to customize the services of 5G network. The particular services can be offered by selecting the required number of user and control plane network functions which will ensure the optimization and stability of independent network slices.

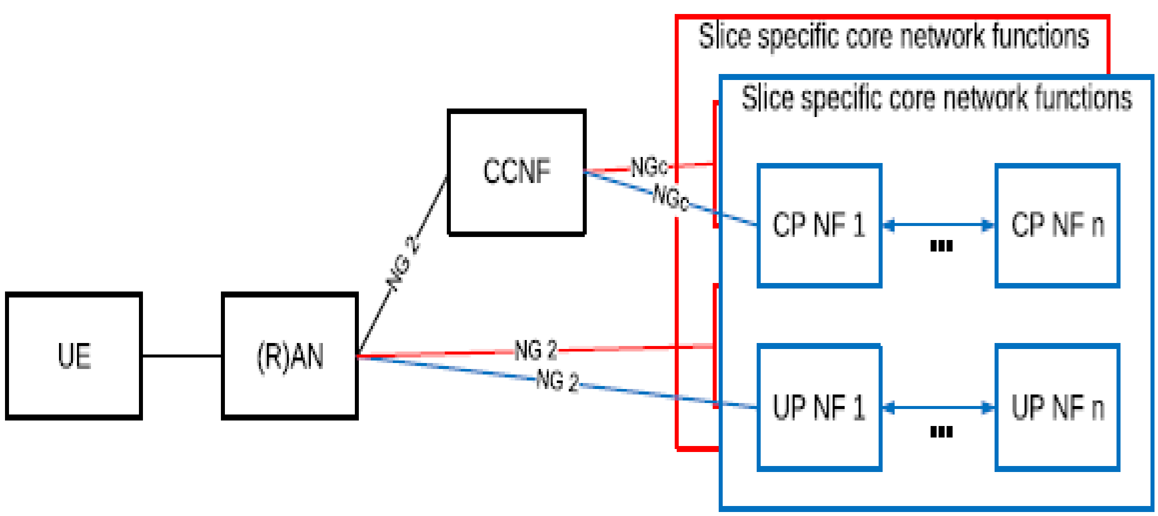


Fig 37 – [29] NextGen network slicing

Slice Selection: The fig 37, depict the group of network functions (NFs) such as Network slice selection functions (NSSF), Access and Mobility Management Function (AMF) is included in the Common Control Network Functions (CCNF). The particular UE (user equipment) sessions are supported by NFs. Single CCNF provide numerous functions to UE such as slice selection, mobility management and authentication during the time of connection. However, various instances of network slices served the multiple PDU sessions. UE provides the NSSAI (Network slice selection assistance information) information during network slice deployment. Before any interaction of Public Land Mobile Network (PLMN) and UE, each Public Land Mobile Network has NSSAI stored and configured in a UE. UE used the accepted NSSAI, once it accepted by the network. Mobility management (MM) updates the Network slice selection assistance information and it included in the message of the UE attach accept. Initially, when the procedure of UE attachment begins, Common Control Network Functions is selected using NSSAI by RAN. The final network slice instance is selected by the Network slice selection functions which are the network function in the CCNF.

Various vertical industries have their own network requirements and the one option is to have separate physical communication network and the second option is divides the single physical network into virtual network slices for dedicated application requirement. In the below simplified network slice figure 38, we have divided the physical network into three slices consists of Utility, Health and Automotive industry. These industries have unique dedicated needs in terms of high and low latency, battery life, data rate, cost and narrow-wide range of the network. For example Utility requires low data rate as well as high latency for some of its smart meter applications but on the other hand autonomous driving require reliable, low latency and high data rate in the automotive industry.

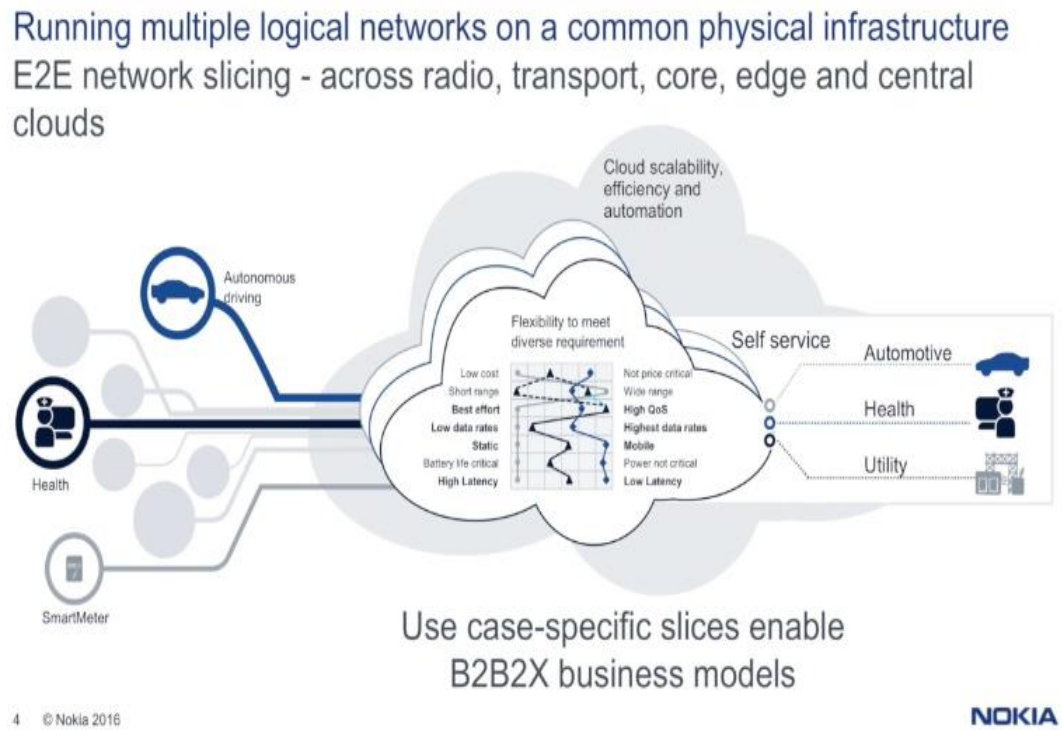


Fig 38 – [30] Network Slicing

This diversity in the business models will increase in the 5G cellular network and to address these changes the telecom operators are transformting the business model from best efforts delivery to customer oriented (network slicing on demand) servies delivery. These all changes will happen with implementing the technologies like SDN, cloudifcation, virtualization, network slicing to use flexible elements of network functions. Ouality of Service is a another method to sperate the bulk data traffic into classes (class maps) and assign the rules (priorities or allocate more bandwidth) to critical traffic classes. The QoS is inefficent to provide a solution to this requirement because QoS can differetiate and control it as per the type (class) of traffic but it is insufficnet to control same class (type) of traffic streaming from different sources and have different priority in case of emergency, mission critical or life line communication.

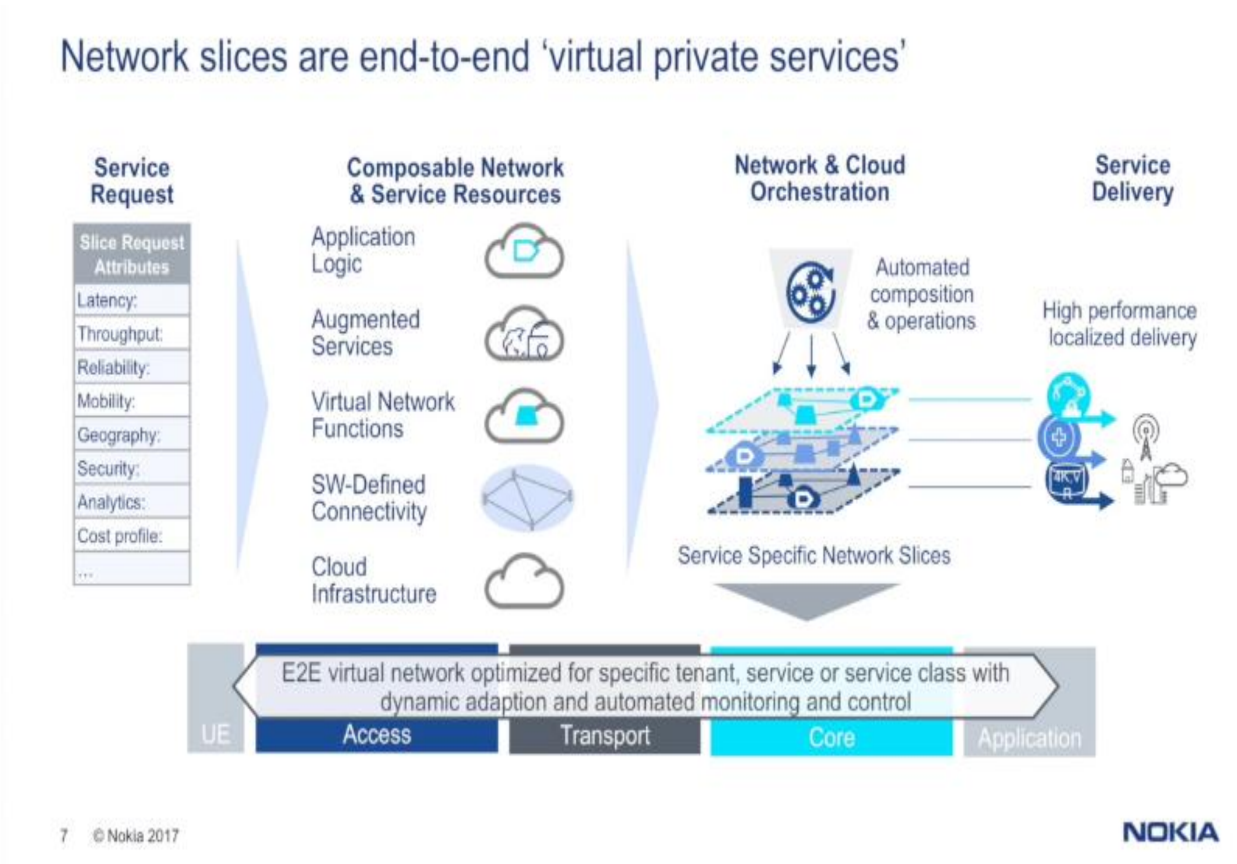


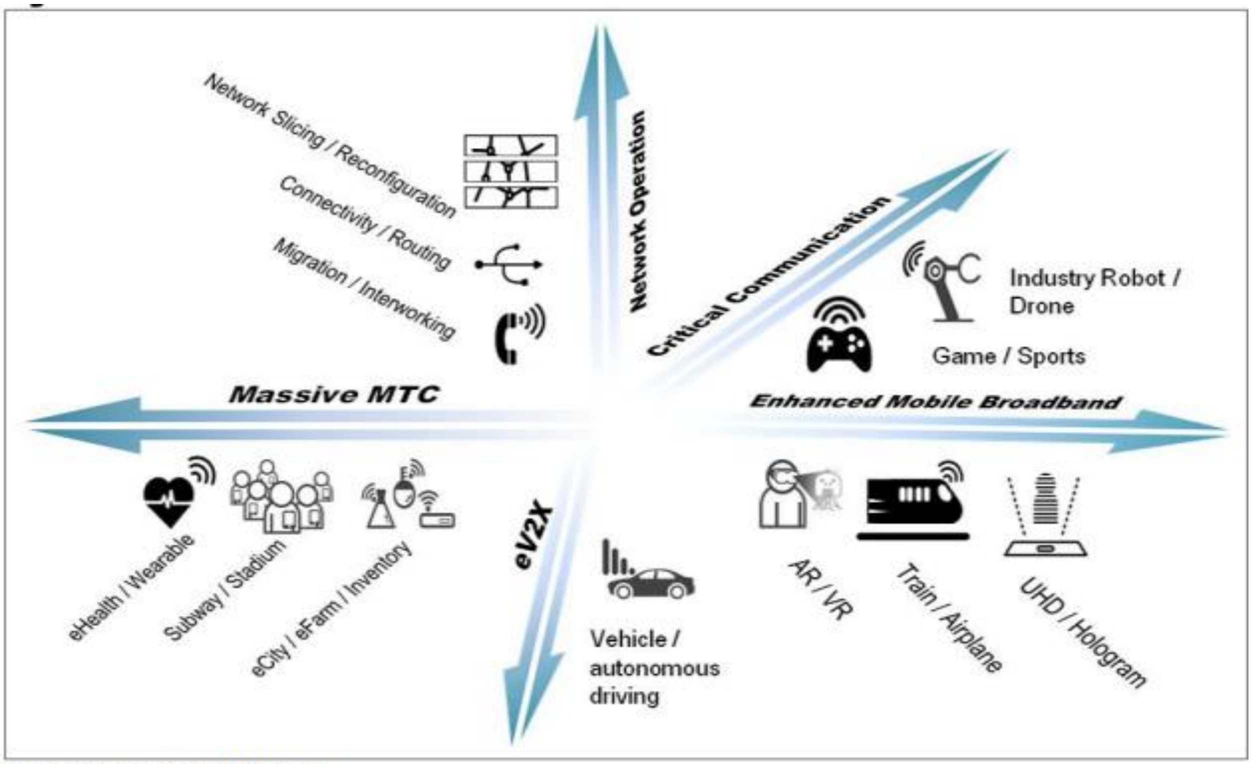
Fig 39 – [30] Network Slicing Components

First and foremost , network slicing implentation can not be possible on the existing cellular network hardwares infrastructure and require network function enable hardware infrastructure which allows to running the network function virtualisation (NFV) which dynamically built the slicing instances (virtual network instance over physical) as per service requirement in Fig 39 , latency (application and network), throughput (uplink & downlink), reliablity, mobility, cost effecitvess etc, in the software defined applications (ablity to program the network) to create communication services. The creation of network slicing solution can be manual and automoted , but it will be diffuclt to manage numerous manual sophisticated slicing (may underprovision or overprovision the avaliable resources for high performance) than the automted ones which requires minimal human intervention or zero touch network and service automation.

9 5G System Architecture:

9.1 The general idea in the 3GPP Release 15.0:

In phase 1, 3GPP (3rd generation partnership project) will mainly focus on enhancement of mobile broadband whereas network automation is the key design and cloudifcation, NFV, SDN, virtual data center are the foundation technologies. The 4G LTE network was better alternative to 3G network because in the 4G, Evolved packet core was a designed to support cellular user demands such as wide network coverage, best utilization of spectrum, high speed data rate, and faster mobility.



Source: 3GPP SMARTER

Fig 40 – [31] 5G service dimensions

The 5G system is beyond the just cellular network by introducing the next generation core also called 5G NG core. This core network is essential for fulfillment the extreme different demands of the users and vertical industries such as enhanced mobile broadband , massive machine to machine communication, eV2X, critical machine communication Software defined networking and Network function virtualization technique are used to provide various services and data connectivity in the 5G system architecture. These are based on flexible, scalable, automated, cloud native software centric, dynamic network slicing of 5G architecture.

In the 5G system, the need to adopt cloud native technologies is for moving to IoT/MTC/Verticals. These cloud natives will foundation to move toward 5G NGC. 5G is moving forward from one designated core architecture to flexible core architecture that adopts these diverse services and applications. It is an evolution of expanding the services and capabilities. Moreover, cloud native architecture to deliver massive scalability, performance, flexibility, and reliability to meet the economics of IoT/mMTC and broadband evolution and a foundation of 5G system architecture. It is expected that the 5G network will be commercially available in 2020.

9.2 Main concepts and principles:

- Flexible distribution and independent scalability by separating the control plane and user plane functions.
- Enhancement in slicing capabilities such as End to End slicing, Core slicing, RAN slicing, efficient and modular networking slicing design.
- Direct interaction and re-use the services of network functions by defining the proper procedures.
- Core network and Access Network are mostly independent functions and offer easy integration of 3GPP and non-3GPP access technologies. Concurrent multiple connections over same/multiple access technologies.
- The network functions are stateless and decoupling of storage and computing resources.
- Deployment of user pane function nearer to Access network which support edge computing and low latency services.
- Structure of authentication is unified.
- Support roaming traffic of Public Land Mobile Network (PLMN) (local and home routed traffic).
- Even on radio side, there will be evolution in RAN architecture, licensed spectrum, unlicensed spectrum and shared spectrum.

9.3 5G architecture is shows in two type of representation:

9.3.1 Service-based representation: It is point to point reference, which shows the services accessibility between NF (one network function allows other network functions to use their services) with in control plane.

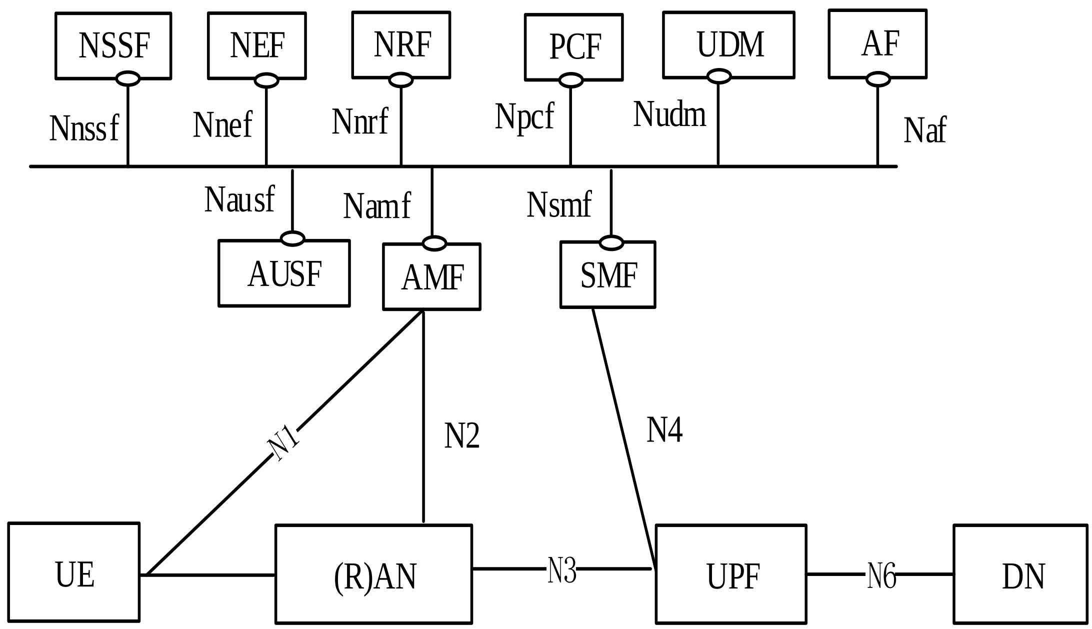


Fig 41– [32] Service based interfaces 5G system architecture (non-roaming)

9.3.1.1 Interfaces of Service based 5G system architecture :

Service based Interfaces	Service Name	Function	Example Consumer(s)
Namf	Namf_Communication	This service enables an NF to communicate with the UE and/or the AN through the AMF	SMF, SMSF, PCF, NEF, Peer AMF
	Namf_EventExposure	This service enables other NFs to subscribe or get notified of the mobility related events and statistics.	SMF, NEF, PCF, UDM
	Namf_MT	This service enables an NF to make sure UE is reachable.	SMSF
Nsmf	Nsmf_PDUSession	This service manages the PDU sessions and uses the policy and charging rules received from the PCF. The service operations exposed by this NF service allow the consumer NFs to handle the PDU sessions.	V-SMF, H-SMF, AMF
	Nsmf_EventExposure	This service exposes the events happening on the PDU sessions to the consumer NFs.	PCF, NEF, AMF
Npcf	Npcf_AMPolicyControl	This PCF service provides access control, network selection and mobility management related policies, UE Route Selection Policies to the NF consumers.	AMF
	Npcf_SMPolicyControl	This PCF service provides session related policies to the NF consumers.	SMF
	Npcf_Policy Authorization	This PCF service authorises an AF request and creates policies as requested by the authorised AF for the PDU session to which the AF session is bound to. This service allows the NF consumer to subscribe/unsubscribe to the notification of Access Type and RAT type, PLMN identifier, access network information, usage report etc.	AF, NEF
Nudm	Nudm_UE Context Management	1. Provide the NF consumer of the information related to UE's transaction information, e.g. UE's serving NF identifier, UE status, etc. 2. Allow the NF consumer to register, remove its information for the serving UE in the UDM 3. Allow the NF consumer to register, remove its information for the serving UE in the UDM	AMF, SMF, SMSF, NEF

Service based Interfaces	Service Name	Function	Example Consumer(s)
	Nudm_Subscriber Data Management	1. Allow NF consumer to retrieve user subscription data when necessary 2. Provide updated user subscriber data to the subscribed NF consumer;	AMF, SMF, SMSF
	Nudm_UEAuthentication	1. Provide updated authentication related subscriber data to the subscribed NF consumer.	AUSF
	Nudm_EventExposure	1. Allow NF consumer to subscribe to receive an event. 2. Provide monitoring indication of the event to the subscribed NF consumer.	NEF
Nnrf	NF_management	Provides support for Discovery of NF, NF services.	AMF, SMF, PCF, NEF, NRF, SMSF, AUSF, UDM
Nausf	Nausf UEauthentication	The AUSF provides UE authentication service to requester NF	AMF
Nef	Nnef_EventExposure	Provides support for event exposure	External application /Internal NFs
Nsmf	Nsmsf_ SMService	This service allows AMF to authorize SMS and activate SMS for the served user on SMSF.	AMF
Nudr	Nudr_Unified Data Management	This service allows NF service consumers to retrieve, update, modify and delete data stored in the UDR. This service allows the NF service consumers to be notified of the data modification.	UDM FE, PCF, NEF, Provisioning FE
N5g-eir	N5g-eir_Equipment Identity Check	This service enables the 5G-EIR to check the PEI and check whether the PEI is in the black list or not.	AMF

Table 5: [32] Service based Interfaces

9.3.2 Reference point representation: It is point to point reference, which shows the connections between network functions services (for example, N7 is the p2p connection between Session Management Function (SMF) and Policy Control function (PCF). Regulative standardized call flow can be developed by using reference point representation.

The signaling between UE and AMF are defined in the Next Generation (NG) N1 and in addition to that N2 defined the connection between AMF and (R) AN; and N3 defined the connection between (R) AN and UPF. AMF controlled the SMF with reference point N11. SMF generate the control signals to manage the states of UPF by using N4. Different UPFs can be connecting by using the reference point N9 and same way N14 is for different AMFs. The policies are applied by the PCF to AMF and SMF with defined reference point N15 and N7 respectively. The UE subscription data is necessary for SMF and AMF and the defined reference points are N8 and N10.

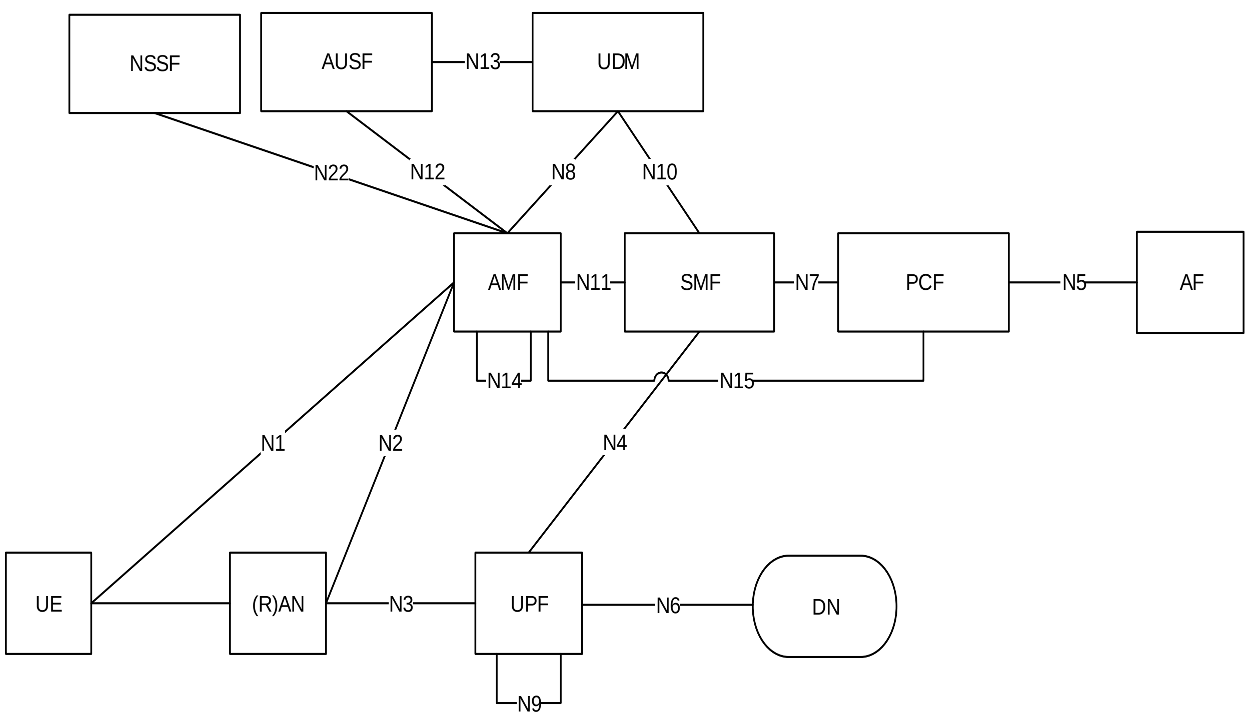


Fig 42– [32] 3GPP 5G system architecture (non-roaming)

UE (User Equipment) is connected to RAN (Radio Access Network) and AMF (Access and Mobility Management Function), the core network consists of many network functions such as:

(i) **UE** (User Equipment)

(ii) **RAN** (Radio Access Network)

(iii) **UPF** (User plane Function)

(iv) **DN** (Data Network)

(v) **AMF** (Access and Mobility Management Function)

(vi) **SMF** (Session Management Function)

(vii) **PCF** (Policy Control function)

(viii) **AF** (Application Function)

(ix) **NSSF** (Network Slice Selection Function)

(x) **AUSF** (Authentication Server Function)

(xi) **UDM** (Unified Data Management)

9.3.2.1 Description: In standalone architecture, the 5G radio cells are used by the UE directly. The basic principle of design is a separation of responsibility among the functions and the goal is to achieve orthogonal system as much as possible. The functions supported by AMF are Radio Access Network control plane (RAN CP) interface termination with N2 connection between them and it is an evolution of S1-MME interface in LTE architecture with the same functionality. N1 is connection with UE for NAS termination, Mobility Management, Connection, Reachability and Registration management. It also includes authorization, authentication and security functions. AMF is an independent function and single AMF can be connected to UE with several access technologies.

The session management function is explicitly handled by the session management function and assigned IP addresses to user equipment. SMF also it handles the UPF for data transfer over N4 interface and it is an evolution of the S6 interface that had in Evolved packet core), the difference is that UPF is a flexible single entity and embrace the function as required by the user. The concept of functions is eliminating the strict rules or rigid structures of LTE core architecture (packet core, P-GW, SGW etc).

In addition to that separate SMF may be establishing for each UE sessions and it may offer different functionalities to each session. The policy control function framework is extended to support QoS , and handles another type of polices as well , for example slicing policies, mobility management policies and policies related to user end point, which are transfer to user end point over N1 interface. The placket flow data is provided by the application function to PCF and according to that information, policy should map to application session and service continuity mode for proper operation of SMF and AMF sessions.

The Authentication Server Function becomes an independent entity to facilitate the universal authentication of UE end points and independent access to authenticate the stored data that is used to connect to the core. The Unified Data Management holds the subscriber information of the UE. The network function's capabilities and services are securely exposed to other non-3GGPP network by the Network Exposure Function (NEF) such as edge computing, application functions and moreover, it do vice-versa. The structure data storage function (SDSF) is used by NEF and AMF (expose its structured information like location information to NEF and NEF stored this information to SDSF). The unstructured data storage functions (UDSF) is optionally used by the control plane NFs, in order to store appropriately OPEC session data. The UDSF can be common to control plane NFs or each NF have their own USDF in order to achieve low latency and high performance.

9.3.2.2 User Plane Function and Control Plane Function: The NFs in the 5G architecture are modular and this design approach has several advantages. The decoupling of control plane and user plane provide the independent scalability of each plane resources. Different type of traffic is handled by the user plane function such as user plane function and control signals are managed by control plane (such as UDM, AUSF, PCF, AMF, SMF and AF are control plane network functions) in the network. Even in the control plane, these functions are modular and can be scale independently. In the 5G system there will be many user plane functions (UPFs) and setup separate from control plane with a customized approach, for example in the mission critical applications, the

UE and UPF are deployed in a nearer proximity to reduce the round trip time (RTT) for fulfilling the low latency requirement.

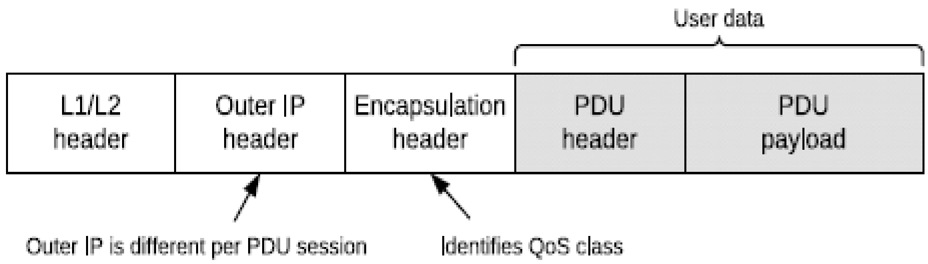


Fig 43: [29] Packet format

The service base representation shows the direct interaction of NFs with each other's and these interactions are defined as services, so the network functions able to route messages to another network function. The logical connection between the data network and UE known as Protocol Data Unit (PDU) and these connections can be established when services are required as per the UE attachment procedure. The default PDU session is always required in the 4G architecture but in the 5G network, no PDU session is needed for UE attachment. Ethernet, IPv4, IPv6 etc. are various types of Protocol Data Unit sessions in this architecture.

The user end points might be connected to more than one Protocol Data Unit sessions, each session might have its own SMF and UPF. There is no S-GW convergence point as we have in the EPC. UPF may be chained between home and visited network in case of roaming and each PDU session in the RRC- IDLE state of UE have separate buffering node. The packet format of user plane is shown in Fig 43 and it support tunneling of PDU session. QoS marking is different for each encapsulated header but the outer IP header is same for all quality of service classes.

The summarization of 4G EPS and 5G NextGen key functions are shown in Table 6, there are two states of mobility management in 4G EPS (RRC- CONNECTED and RRC-IDLE) but in addition to that 5G NextGen have third state called RRC INACTIVE CONNECTED state, which also defined the RAN paging, location tracking level and cell switch method but these are also similar in 4G EPS except RAN paging. In the session management, the UE attachment procedure is followed to establish the session in the 4G

EPS but UE can attach in idle mode but when the services are required, then the session is established in the 5G NextGen. The session continuity is not guaranteed and is also be determined by service and UE type.

System	Mobility management				Session management		QoS framework
	RRC state	Cell switch	Location tracking level	Paging	Session establishing time	Session continuity	QoS granularity
EPS	RRC-CONNECTED RRC-IDLE	Handover Cell reselection	Cell Tracking area	No Yes	Attachment procedure	Guaranteed in the whole area	EPS bearer
NextGen	RRC-CONNECTED RRC-INACTIVE CONNECTED RRC-IDLE	Handover Cell reselection Cell reselection	RAN CN location area	No RAN paging CN paging	Service request procedure	Depending on the type of UE and type of service (SSC mode)	QoS flow

Table 6 – [29] 4G EPS and 5G NextGen Comparison

Chapter III

M2M

Network Architecture for Smart Grids

10 Smart grid communication requirements:

The communications need of smart grid and other entities included in generation, transmission, and distribution of power will tell the progress of nation's 5G policies. A number of new applications offered by the smart grid to utilities, suppliers, consumers, and others, and these can be offered through many vast and interrelated systems. The integrated two-way communication is one of the key technology areas of 5G that can allow for automated scheduling of electricity use and dynamic monitoring of power use.

To support the smart grid applications, different communication and networking technologies can be used including power line carrier , broadband over power line , traditional twisted-copper phone lines, WiMAX, microwave, satellite, cellular, fiber optic cable, cable lines and wireless technologies like ZigBee, Bluetooth and Wi-Fi. The 5G applications can use many communications technologies for example, Wide area network, neighbor area network, and home area networks charging systems for SCADA control system, smart electric transport system (plug-in electric), dynamic pricing for utility system, and demand response and mission critical fault detection , monitoring and control system.

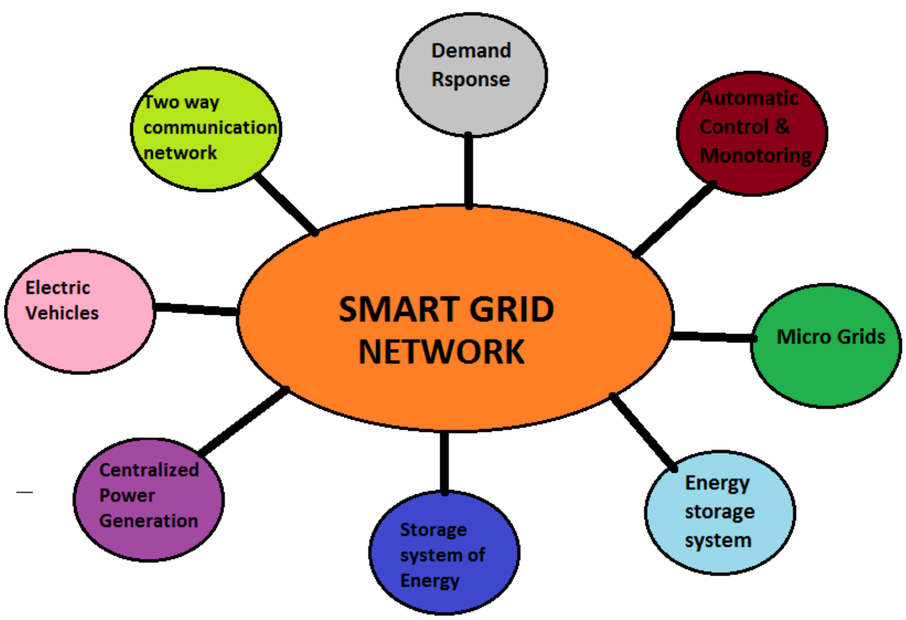


Figure 44 – Requirements of smart grid system

10.1 Smart energy demand: It shows the energy consumer in the all the seven domains of the smart grid and represents the overall energy demand by smart devices based upon their demand and requirements. It contains any kind of energy-user task to:

- Increase the reliability
- Decrease the peak demand of energy
- Movable usage to off-peak hours
- Minimize the total consumption of energy
- Dynamical electric vehicle management.
- Micro grid management of additional utilization to respond to renewable energy resources such as wind, solar, etc.
- Purchase significant smart devices in time with high power efficiency and low energy consumption.

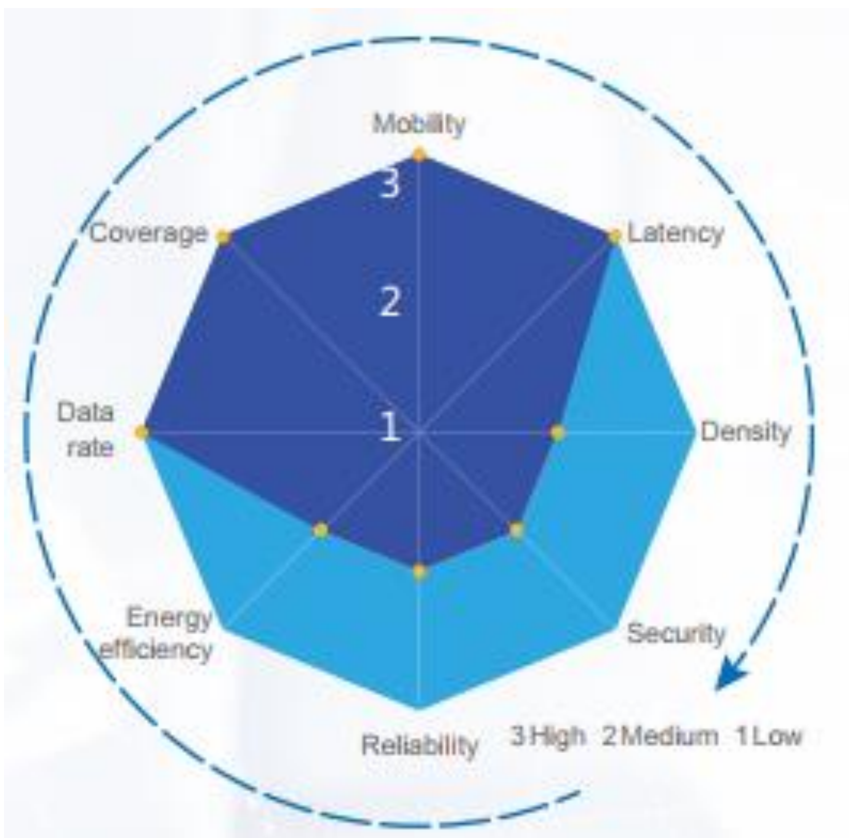


Figure 45 – [33] Smart energy demands

The above stated actions will minimize the adverse impacts on energy grids and will increase the savings of consumers. The following mechanisms are needed for smart energy demand:

- Smart equipment or devices in the house active and sleep as per scheduling of overall load and lower energy price at off peak hours.
- Usage by device data
- Real-time power information feedback to electricity consumers.
- Automated control of devices
- Smart thermostats and appliances
- Dynamic pricing
- Smart meters

Machine-to-Machine communication is also considered as foundation block in the deployment of the 5G network, which facilitates massive device connection in dense area, wide-area control and monitoring infrastructures. This brings a big opportunity for industries that based on information and communication technology. The flexible demand management can be provided by smart metering in M2M where a smart meter has a capability of real time two-way communication that measures utilization of electricity and send that consumption information back to the local utilities.

When the real-time information of power utilization is available in the 5G network and this information can separate into different tariff levels by the software and access by the consumers. Then, consumers can use the consumption information online anywhere to made smart decisions. Therefore, the data compiled by smart meters turns like “glue” that permit the different components of smart grid to work together efficiently. In order to perform monitoring task in the smart grid system numerous wireless sensor and actuator networks (WSAN) (such as home applications and energy system generation) can be deployed. WSANs play a vital role in recognizing several faults and troubleshooting mechanism because of self-healing properties which are essential in the smart grids. 5G cellular M2M network slice will provide a dedicated network connection, QoS, higher availability and data rate wide area coverage and continuous development.

The various standardization activities are going in M2M communications to bring a synchronize set of telecom standards with a conscious effort. Therefore, smart grid network and AMI present the challenges and opportunities to communications networks. These are home networking with a various number of devices and appliances, a scalable overlay network, scalability of internetworking, and interoperability. At the same time security and privacy of digital data are also extremely important because data given by smart meters can be compromised.

10.2 Machine to Machine Communication:

Around the world, humans are communicated with each other with the invention of mobile phones and moreover these communications has been extended with the connection of multiple short range devices with each other.

M2M is an embedded communication technology that enables information exchange between human to machine and machine to machine with low human interface (autonomously), low cost and little efforts. The machine to machine also known as Machine type communication (MTC) has the built-in intelligence itself for specific operations requirement, which results the impact on the humans life positively in the various sectors such as smart home, smart health care, security and surveillance, smart transport, smart industry operations and smart grid, etc.

M2M communication are based on different short range such as Bluetooth, RFID, MICS (Medical Implant Communication Services), Transport and Traffic Telematics (TTT), Wireless alarm system, Wi-Fi and ZigBee as well as Long range such as GPRS, HSPA, LTE, CDMA , smart metering technologies, open standard Weightless technologies, Sigfox, OnRamp and Wireless Mesh

Network but the fastest emerging M2M industry will be **5G cellular network** which is expected billions of connected devices in the form of IoT.

10.3 The main characteristics of M2M communication are:

- Low complexity
- Low mobility
- Longer battery life and low power consumption
- Low traffic per volume
- Wide communication between devices
- Use different communication technologies
- Packet Switched
- Monitoring
- Location Specific Trigger

10.3.1 Summary of M2M frequency bands (current and potential)

Band	Regulatory Status	Applications / Technologies	Pros	Cons
LF (125-134 kHz)	Licence Exempt (harmonised)	Passive RFID tags (typically used for inventory / asset control and low cost animal tags)	Low cost, good penetration through non-metals	Very short range, slow speed
HF (13.56 MHz)	Licence Exempt (harmonised)	Passive RFID tags (typically used for smart cards, item identification or access control)	Medium range and speed	Can be relatively expensive
169.4-169.475 MHz	Licence Exempt (harmonised) for specific application	Remote meter reading	Harmonised European band	Power and bandwidth limitation – range limited
412–414/422-424 MHz	National licence (acquired at auction – indefinite duration)	Arqiva is deploying smart meter technology (Sensus Flexnet) in the northern part of the UK	Licensed band, long range, good building penetration	Requires rollout of dedicated wide area network
433.05-434.79 MHz	Licence Exempt (harmonised)	General purpose short range device band	Low cost, internationally harmonised	Prone to congestion and interference
450 – 470 MHz	Mix of licensed, licence exempt and Government services in UK	CDMA450 being promoted in some countries. Possibility of LTE450 in longer term	Established relatively low cost technology for wide area use (CDMA)	Band is not harmonised in the UK and would require major re-planning. Uncertain availability of low cost LTE450 hardware
Band	**Regulatory Status**	**Applications / Technologies**	**Pros**	**Cons**
458.5 - 458.95 MHz	Licence Exempt (UK only)	Telemetry and Telecontrol	Higher powers permitted than in other licence exempt telemetry bands	UK – specific allocation (non-harmonised)
470 – 694 MHz	Harmonised band, primary use digital TV broadcasting based on GE-06 plan	TV White Spaces – has been under consideration for deployment of Weightless technology but interest appears to be waning currently	Wide bandwidth available. Claimed to provide cellular-like coverage in a licence exempt band	Would require wide tuning range to cover full band. Requires geodatabase to facilitate sharing. Prone to periodic interference from distant TV transmitters
733-736/ 788-791 MHz	The possibility of a 2 x 3 MHz dedicated cellular M2M sub-band in this range has been mooted within CEPT and ITU	LTE	Ideal for wide area communication if internationally harmonised	Would depend on level of industry support – additional band may add cost and complexity to networks and devices
863 – 870 MHz	Licence exempt (harmonised)	General purpose short range device band (excludes alarm sub bands, see below), including ZigBee	Internationally harmonised, technical standards include interference mitigation techniques (power / duty cycle constraints and/or listen-before-talk)	Limited capacity for ZigBee (one 20 kbps channel). Potential interference, e.g. from wireless audio devices below 865 MHz
865 - 868 MHz	Licence exempt (harmonised) for specific application	Active and passive RFID (typically used for vehicle ID, logistics or entry control)	Long range (higher powers permitted than for other in-band applications), high data	Relatively expensive, requires line of sight

Band	Regulatory Status	Applications / Technologies	Pros	Cons
			speeds	
869.4 - 869.65 MHz	Licence exempt (harmonised)	Sigfox LPWA band (assumed); Mesh networks for smart metering (e.g. Connode technology used by Telefonica UK)	Higher powers permitted than in other parts of the 863-870 MHz band. Technology claimed to provide cellular-like coverage in a licence exempt band	Limited bandwidth and duty cycle. Unclear whether current EC definition of short range device encompasses wide area technologies.
868.6 – 869.7 MHz	Licence exempt (harmonised) for specific application	Alarm systems (fire, intruder and social	Various sub-bands with differing power and duty cycle constraints support enhanced quality of service	
870 - 875.6 MHz.	Licence exempt (harmonised) subject to national adoption of CEPT Recommendation. Also scope for individual licensing of wide area networks	Transport and Traffic Telematics, Tracking, tracing and data acquisition (recently adopted harmonised European band). Suitable for wide area wireless mesh networks.	Low frequency and wide bandwidth. Higher powers permitted for tracking, tracing and data acquisition (500 mW)	Constraints on power and duty cycle to protect other services
875.6-876 and 915-915.2 MHz	Proposed sub-bands for low duty cycle, low latency systems	Alarms	Provides additional spectrum to support volume and traffic growth	Potential interference from adjacent band mobile transmissions at 915 MHz
915 – 921 MHz	Licence exempt (harmonised) subject to national adoption of CEPT Recommendation	Active and passive RFID; also recently identified by CEPT as a general purpose SRD band.	Low frequency and wide bandwidth	May be subject to interference from cellular terminals in adjacent band

Band	Regulatory Status	Applications / Technologies	Pros	Cons
2.4 GHz (2400-2483.5 MHz	Licence exempt (harmonised)	Bluetooth, Wi-Fi and ZigBee widely deployed. Also used by some active and passive RFID systems	Globally harmonised, large bandwidth available	Heavily congested in many locations due to intensive use of Wi-Fi and other wireless consumer devices
2483.5 – 2500 MHz	Licence exempt (harmonised)	Medical Body Area Networks	Large bandwidth available	Potential interference from Wi-Fi or LTE in neighbouring bands
5.8 GHz (5725-5875	Licence exempt (harmonised)	Used by some active and passive RFID systems (e.g. road tolls)	Wide bandwidth available	Expensive, requires line of sight. May suffer interference from other services (e.g. fixed wireless access)
5795 – 5815 MHz	Licence exempt (harmonised, but limited implementation of CEPT Recommendation in UK)	Transport and Traffic Telematics (e.g. car to car or in-car communications)	Established European band	High frequency, limited range / mobility

Table 7: [34] Summary of M2M frequency bands (current and potential)

10.4 Machine to Machine mission critical Communication :

Services mostly depend on the narrowband spectrum for mission critical Land Mobile Radio (LMR) voice methods to deliver intercommunications between their respective employees. The devises have transformed from analog to digital, the capability to support M2M services turn out to be feasible. An improvement in digital era enhances the capacity of data links on LMR methods. Significant data link capacity allows the support of progressive information methods such as M2M services without impacting voice procedures on LMR methods. By designing an advanced mission critical LMR methods, inter communication industries can now have the provision to provide both voice and data applications including M2M services on a reliable network.

For decades, communication industries have utilized numerous types of intercommunication methodologies in some particular form or another for distribution automation, supervisory control and data acquisition, grid-based applications, demand side management etc. However, they were never positioned in an extensive class like M2M nor were they interconnected with each other to develop a smart grid. Coupled with the lack of commercial registered broadband spectrum opportunities, intercommunication to these services have been inadequate and place only at significant positions on a cost-effective basis. With the improvements in digital technology, the cost of intercommunication devices has been minimized, that allow their utilization across additional infrastructure and services.

The secure and efficient exchange of data is of principal significant to utility procedures and client service. The electric utilities depend upon intercommunication data links to secure lives and guarantee the protection of their employees throughout critical service restoration stages and also throughout daily actions, keeping power flowing. M2M communication is a significant differentiator in producing the smart grids.

10.5 Key features: Following are the significant features of M2M communication systems:

10.5.1 Low Mobility: M2M devices are either stationary in nature or can move within a given radius.

10.5.2 Application Independent: M2M devices allow intercommunications to significant services which do not have intercommunication in these days and are completely transparent to the services.

10.5.3 IP-based: The cellular networks transform to end to end IP base, these new digital networks support IP bearer applications and have an ability to transfer both IP and serial-based protocols by utilizing the IP-based network.

10.5.4 Small Data Transmissions: M2M devices usually transmit or receive small amounts of data, leveraging the additional capability enabled by moving to an improved time division multiple accesses (TDMA)-based LMR network.

10.5.5 High Reliability: It states that whenever and wherever M2M communication is demanded, the secure and efficient communication among M2M device and M2M server shall be available. High reliability is required in M2M applications that involve either the prospect of an emergency or highly sensitive data.

10.5.6 Network Priority: It states that with network slicing and quality of service, there is a way for delivering a hierarchical prioritization of clients within the solution when services, voice or information, are competing for network access. It becomes more significant as utilities have long considered their voice communications to be mission critical because they focus on them for both protection and reliability.

10.5.7 Security: It contains the end to end protection of M2M data, authentication of clients to access M2M devices, and encryption of data communicated across M2M networks. Utilities demands private deployment of networks for their higher levels of security delivers a strong platform that can be leveraged when utilizing the identical security for M2M services.

11 Machine-to-Machine Architecture :

The European Telecommunications Standards Institute (ETSI) specifies the general architecture of M2M networks which can be shown in Figure 46. M2M network considers a five-part structure. Firstly, it includes devices that reply to requests or sends data. Secondly, it includes gateway which provides a connection between different networks. Thirdly, M2M area network provides a connection between all kinds of gateways and smart devices. Fourthly, communication networks attain links between applications and gateways. Fifthly, the application assigns datum using several services and is utilized by particular business-processing engines. It acts as application agent which monitors information then triggers action and acknowledges data. The five elements structure of M2M communication is decomposed into three domains. The first domain is M2M area developed by an M2M area network and its gateways. The second domain is communication network which contains different types of networks like xDSL and cellular network. The third domain is designed to provide application services.

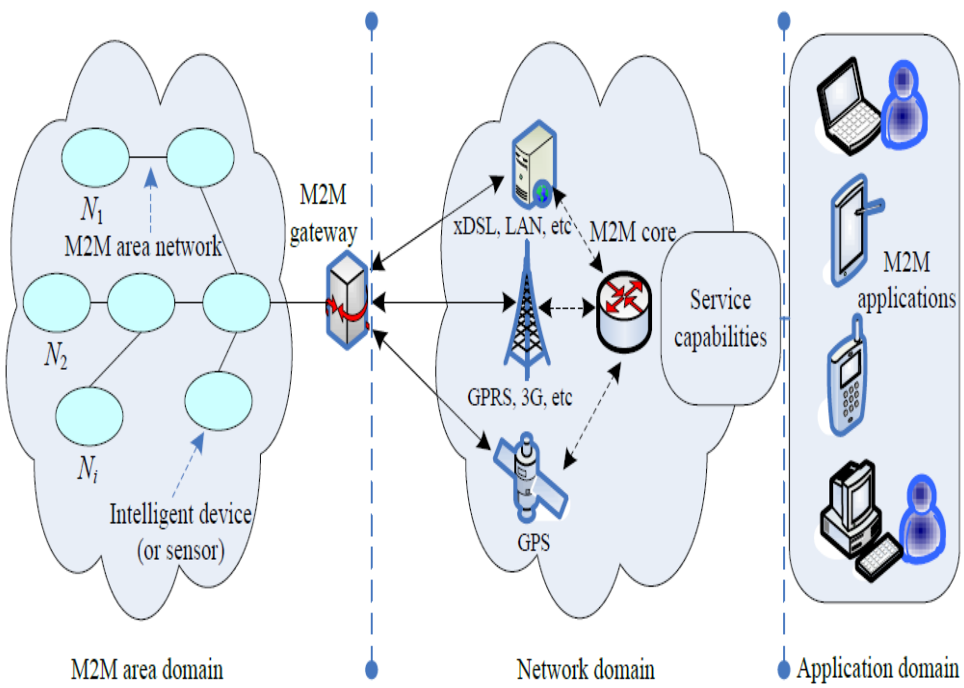


Figure 46: [35] Architecture of M2M networks

11.1 M2M in Smart Grid:

The numerous functionalities offer by M2M system that can be used to realize 5G and various foundations are working in this direction to carry out M2M in 5G. We already discussed the basic architecture of 5G and needed requirements in the previous sections (Chapter II). In this section, we study how M2M framework can relate to 5G. For this two important M2M scenarios will be discussed and various applications related to this will also be explored using WSAN. It is essential to understand when more detailed technical and functional requirements need to be accomplished. WSAN play an important role in delivering M2M applications in a smart grid context.

ETSI board of director architecture for 5G is shown in Figure 47. This architecture is comprised of three main planes or layers such as energy layer, control layer and service layer. The transmission, distribution, generation and consumption of energy handle by the energy plane also considered as first layer. Therefore, this layer includes a large number of distribution and transmission systems, storage systems and sensors. This layer also includes the M2M area networks such as Industrial Area Network (IAN), Building Area Network (BAN) and Home Area Network. The second layer is controlled layer that control and links the energy layer to service layer. This is interrelated to the network layer of M2M communications. The 5G services related to M2M communication are offered by the last layer also known as service layers such as building and home management, installation and maintenance, billing, customer services and marketing etc.

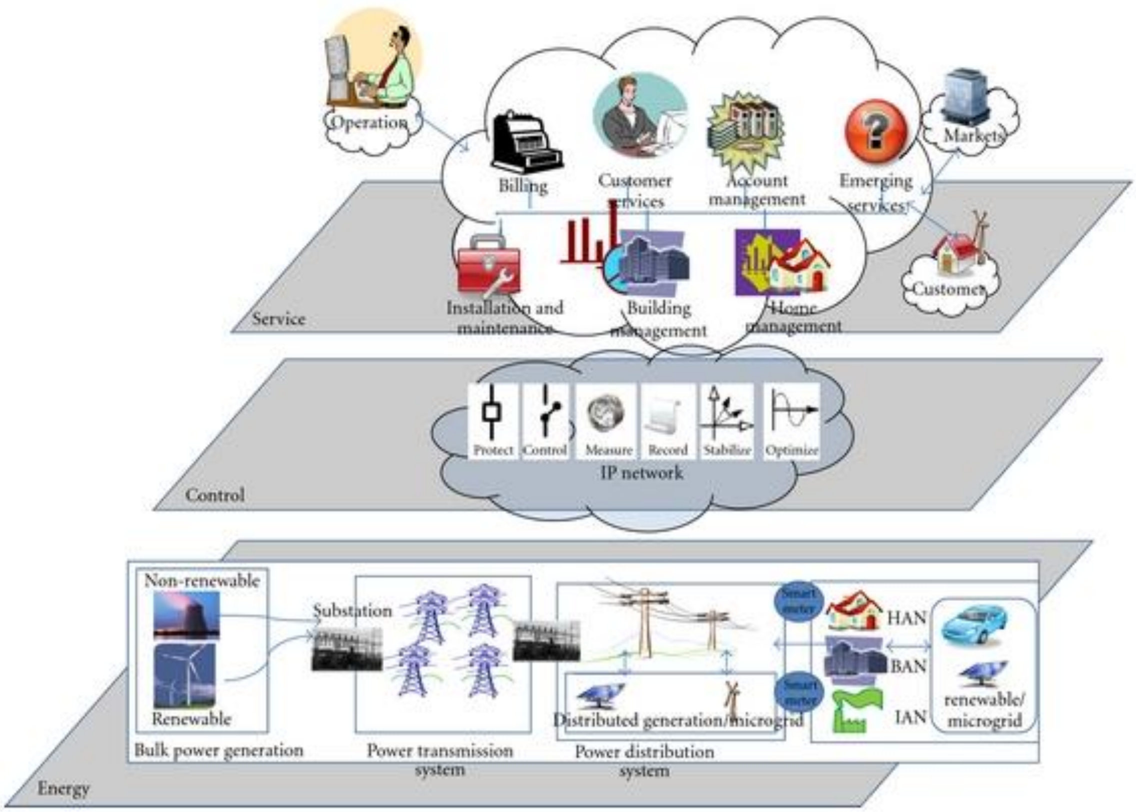


Figure 47- [36] ETSI board of director architecture for Smart Grid

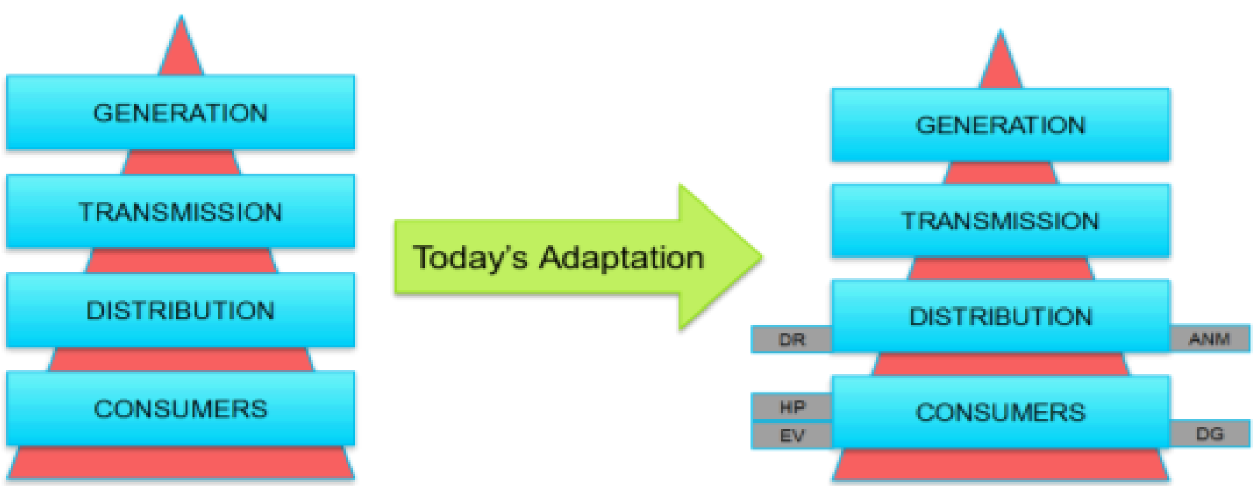
In recent times, wireless sensor and actuator network has been gaining recognition because of their remarkable work in energy systems that include generation, transmission and consumption of energy. It becomes possible due to low-cost combination of multiple networks. Therefore, the high end cost and complex network infrastructure is not required. In spite of that, wireless sensor and actuator network also has few important benefits over former traditional communication networks like adaptability to changing network conditions and wide area coverage. Therefore, diverse environments cause dissimilar challenges for wireless sensor and actuator network; for instance, energy system environment is insensitive and complex, it faces fault tolerance, robustness and reliability challenges to deliver 5G applications.

11.2 5G in Smart Grids:

Digital transformation is challenging existing electricity generation facilities in terms of their types and scales, as well as energy management and control of the power system. At the same time, the conventional unidirectional energy transmission from power generators to consumers is changing. With the development of the sharing economy, power users can also serve as energy suppliers by sharing off-peak energy. This achieves bidirectional energy transmission and use. These transformations require real-time, safe, and stable smart grids with large capacity and high speed.

- **Diversified technical requirements**:

  A smart grid has different requirements for security and reliability, network bandwidth, latency, and coverage on its four stages (power generation, transmission, distribution, and consumption). These four stages can be seen from Figure 48. Existing communication systems do not meet all the technical requirements.



DR=Distributed Resources, ANM=Active Network Management, HP=Heat Pumps, DG=Distributed Generation

Figure 48: [37] Stages of smart grid

- **Cross-regional coordinated control :**

  Energy and power distribution in China is extremely unbalanced. China is taking measures such as South-to-North energy transfer to schedule and manage resources across grids. Taking the automatic control of substations in smart grids as an example, replacing the single-site-level transmission with grid level transmission increases requirements for the transmission and security of the backbone transmission network in terms of distance, efficiency, and safety.

  Standardize protocols and equipment-s are essentials for inter – region control in all the seven domains of the smart grid (refer Chapter I) and moreover it will also fill the energy demand gap in the different regions.

- **Sustainable, efficient, and sharing economy :**

  A standardized grid will help realize sustainable development of smart grids over the next two decades. Another advanced technology, remote intelligent metering and scheduling, not only reduces labor requirements, but also comprehensively reflects the power consumption and operating status. The sharing economy mode allows UEs to sell off-peak energy, saving energy and reducing problems of regional power shortage.

  The United States government surveyed 38 electricity companies and found that the popularization of intelligent metering and bidirectional energy transmission makes it easy to obtain overall energy consumption information. Users can then limit their consumption or avoid using power at peak hours, reducing power consumption by 11%. The over-the-air connectivity on the 5G network eliminates the need for grid construction.

  With strong anti-disaster abilities, 5G networks are easier to construct and recover in mountainous areas or over water than fiber optic cable networks or other short distance networks. In addition, featuring ultra-large bandwidth, non-line-of-sight transmission, wide seamless coverage, and roaming, 5G network slicing technologies will fulfill the diversified necessities of future smart grids and ensure the robustness of intelligent networks with high reliability and high bandwidth.

11.3 Applications :

In the seven domain of the smart grid, wireless communication technologies can mainly be applied in the scenarios in Figure 49, which are explained as follows:

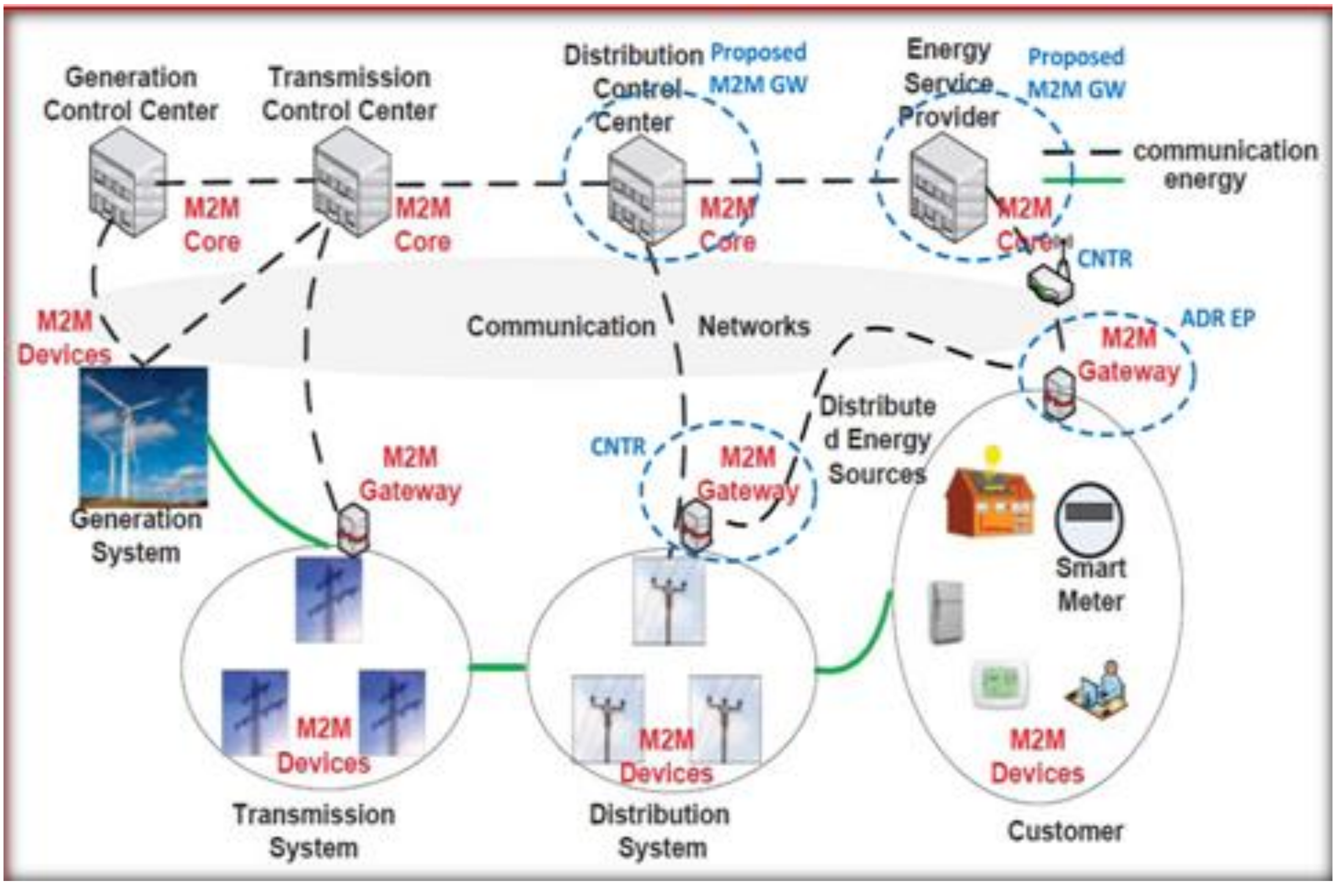


Figure 49 – [38] 5G applications of smart grid

- **Distributed grid-tied management of new energy:**

  Featuring wide coverage, large capacity, real-time performance, reliability, and scalability, 5G networks allow grid-tied management of new energy such as hydraulic, wind, and solar power. 5G networks also address challenges to grid-tied management, such as random and intermittent new energy supply, unbalanced peak load regulation capability, and bidirectional transmission.

- **Intelligent management of the power transmission and transformation network:**

  To promptly handle abnormal disturbance, the transmission network, voltage transformers, and other power devices are monitored real-time online. Furthermore, onsite operations and outdoor facilities are under video surveillance.

- **Intelligent management of power distribution network:**

  Online real-time monitoring and automated management of power distribution facilities improve device efficiency and provide timely dispatching and scheduling of power to different consumption areas.

- **Remote smart meter :**

  This technology collects and analyzes power consumption and quality, based on which other value-added services are provided, including remote control of home appliances, home security, and power sharing during off-peak hours. According to the UK government, installing intelligent meters in 26 million houses nationwide would save consumers and energy companies some 3 billion pounds over the next two decades. Energy consumption would be reduced by 3% to 15% relative to the base case. The measure will bring both social and environmental benefits. By allowing many unconnected, energy consuming devices to be integrated into the grid through low-cost connections, 5G enables these devices to be more accurately monitored to support better forecasting of energy needs.

11.4 Wireless Network Requirements:

11.4.1 Wide coverage, high bandwidth, and massive connections:

The communication network provides long-distance consecutive communications across the country, and the data center implements real-time data processing. Both of them require high bandwidth and enormous data volume. In addition, the access and communication of massive user data recorded on intelligent or gateway meters raise high requirements on the coverage, bandwidth, and a number of connections. For example, millions of intelligent meters are installed in large cities, and massive measurement data is transmitted from each meter to the concentrators and data center every day.

11.4.2 Milliseconds- to second-level latency :

Smart grids raise high requirements on the real-time performance of the power transmission and scheduling and the monitoring of power devices. On the 4G network, less than 20ms latency can hardly be ensured when there are a huge number of concurrent connections. 5G networks, therefore, must be able to monitor the grid operating status in real time, isolate faults, and implement self-recovery, avoiding large-scale power failures.

11.4.3 Gbit/s bandwidth :

Remote high definition (HD) video control, virtual reality (VR), and augmented reality (AR) provide visualized communications to identify faults in the electric power system, give warnings, and help rectify the faults. The backbone power supply network now delivers transmission bandwidths of Gbit/s or even higher, meeting the bandwidth requirements of substations and control centers on the transmission network. Generally, the bandwidth required by each intelligent substation is 0.2–1 Mbit/s, that required by every one million digital meters is 1.85–2 Mbit/s, and that required by every 10 thousand intelligent sensors is 0.5–4.75 Gbit/s.

11.4.4 **Flexibility, compatibility, and scalability:** In response to the expansion and increased access to distributed energy, smart grids now support access to both traditional centralized and distributed energy sources.

11.4.5 **Carrier-class security**:

Eavesdropping or attacks on the power system would have significant societal and economic consequences. To ensure quick and accurate response to power system exceptions, more emphasis must be put on carrier-class data confidentiality and security

11.4.6 **5G networks** can free utilities from the need to deploy their own communications systems.

- By using 5G networks utilities can avoid building and maintaining their telecommunications systems. 5G networks will meet all their requirements, over a dedicated slice of the 5G network, with the cost based on ongoing network usage.
- 5G networks will match smart grid requirements for decades. They can also support backward compatibility as smart meters are already being deployed now. 5G operators will need to demonstrate progress on power consumption and battery life issues for user side components.
- Running smart grid communications networks require expert knowledge. Network operators are ideally placed to provide this expertise and experience. Meanwhile, energy companies could be important anchor tenants for mobile operators' 5G networks.

12 **IoT for Smart homes and smart grids:**

The 5G has made remarkable progress in information processing, transmission and sensing, and it is widely adopted by various utilities. Now, IoT technology shows a significant part in the construction of the smart grid. To enhance the efficiency of 5G technology, IoT offers an interactive real-time network connection to consumers and appliances through using different communication technologies. And also provide required cooperation to realize real-time applications using energy equipment and two-way communication through various IoT smart devices which enhance the data sharing speed between distributors and various consumers.

There are three ways to apply IoT in 5Gs. Firstly; to monitor the state of equipment, various IoT smart devices can be deployed by IoT technology. Secondly, IoT can be applied to collection information from various equipment's with the assistance of connected IoT smart devices by using different communication technologies. Thirdly, IoT can be applied to control the 5G using application interfaces.

The sensing devices of IoT are generally include GPSs, laser scanners, infrared sensors, cameras, M2M devices, RFIDs, wireless sensors and various data collection systems. IoT technology can easily support and enhance the information sensing in the 5G. There are many other features of IoT that plays an important role in 5G such as the deployment of information sensing and transmission infrastructure, user interaction, measurement, information collection, security monitoring, maintenance, safety management, operation, assistance in network construction, etc.

Moreover, the existing architectures of cellular technology primarily focus on the requirements of energy distributors to manage the entire electric grid. The consumers are connected to AMI network using mobile networks. Although, the consumers have other smart home infrastructures like Wi-Fi but the reality is that these have not been incorporated in existing communication networks or architectures. There is some architecture which considers the existing smart home infrastructures but they are not scalable in large deployments. Therefore, the protocols specific to IoT and 5G systems cannot be directly posed to integrated IoT-aided 5G systems. As the protocols only consider the individual features of either IoT or 5G systems that is not adequate for an integrated IoT-aided 5G system. Figure 50, shows the existing and potential applications of IoT aided 5G systems.

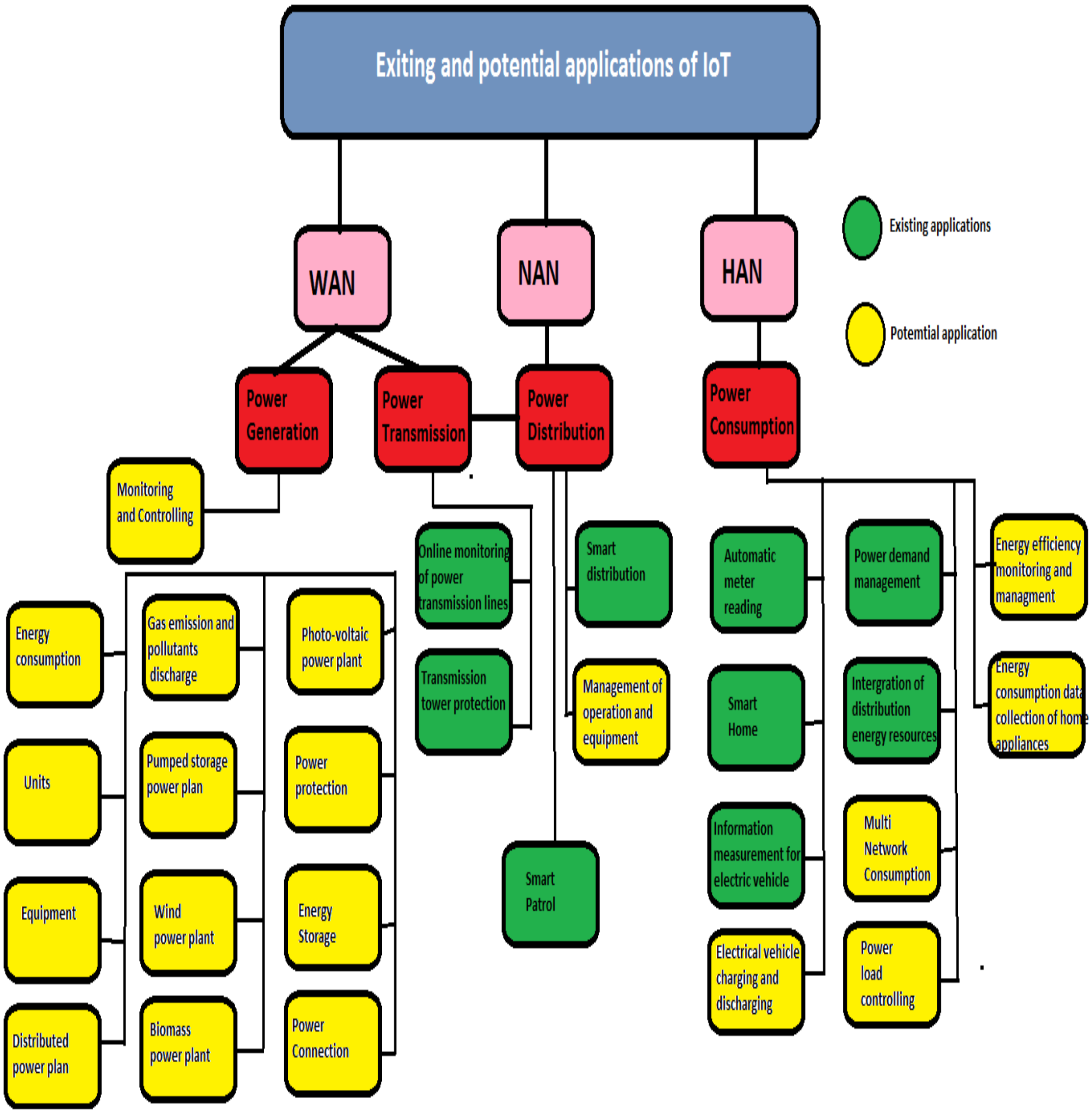


Figure 50- [39] Applications of IoT aided Smart Grid systems

As discussed in earlier sections, 5G has four main subsystems such as energy generation, energy transmission, energy distribution and energy utilization. IoT provides a promising solution to enhance these subsystems through the application of IoT technology to these subsystems. So, the IoT becomes a key element in 5G infrastructure. In the case of energy generation, IoT can be utilized for photo-voltaic power plants, biomass power, wind power, pumped storage, energy storage and power connection, power use/production prediction, gas emissions and pollutants discharge, monitoring and controlling of energy consumption, and management of distributed systems.

In the case of energy measurement, IoT can be utilized for automatic measurement, control and management of equipment and operations. In the case of energy consumption, the IoT can be utilized for multi network consumption, power demand management, monitoring of energy efficiency and management, controlling of power load, gathering the data about the energy consumption of home appliances, vehicle charging and discharging, automatic reading of smart meters, and smart homes.

12.1 Three layered architecture for IoT-aided 5G systems:

Three layer Internet of things and 5G system architecture as shown in Figure 51. These layers are perception layer, network layer and application layer. These are discussed as follows:

12.1.1 Perception Layer: This layer uses various smart devices to sense and collect data in IoT-aided 5G systems. It uses various IoT sensing devices, such as M2M devices, GPS, WSN, cameras, and RFID tags to gather the information in 5G. It can be divided into two sub-layers, a perception control sub-layer and a communication extension sub-layer. In perception control sub-layer, the perception of the physical world is realized by processing IoT devices, monitoring and control, and information acquisition. In communication extension sub-layer, the connection is made between IoT devices and the network layer through communication modules.

12.1.2 Network Layer: It is formed by the combination of various telecommunication networks and the Internet. This layer uses mature technologies which are widely accepted by utilities. It maps the information from perception layer to telecommunication protocols that collected through IoT devices. Consequently, it transfers the mapped data to application layer using appropriate telecommunication network. For information transmission, routing, and control, the core network that is Internet is responsible. Other telecommunication networks are also be used to access the data. The management of IoT and information centers is also part of the network layer.

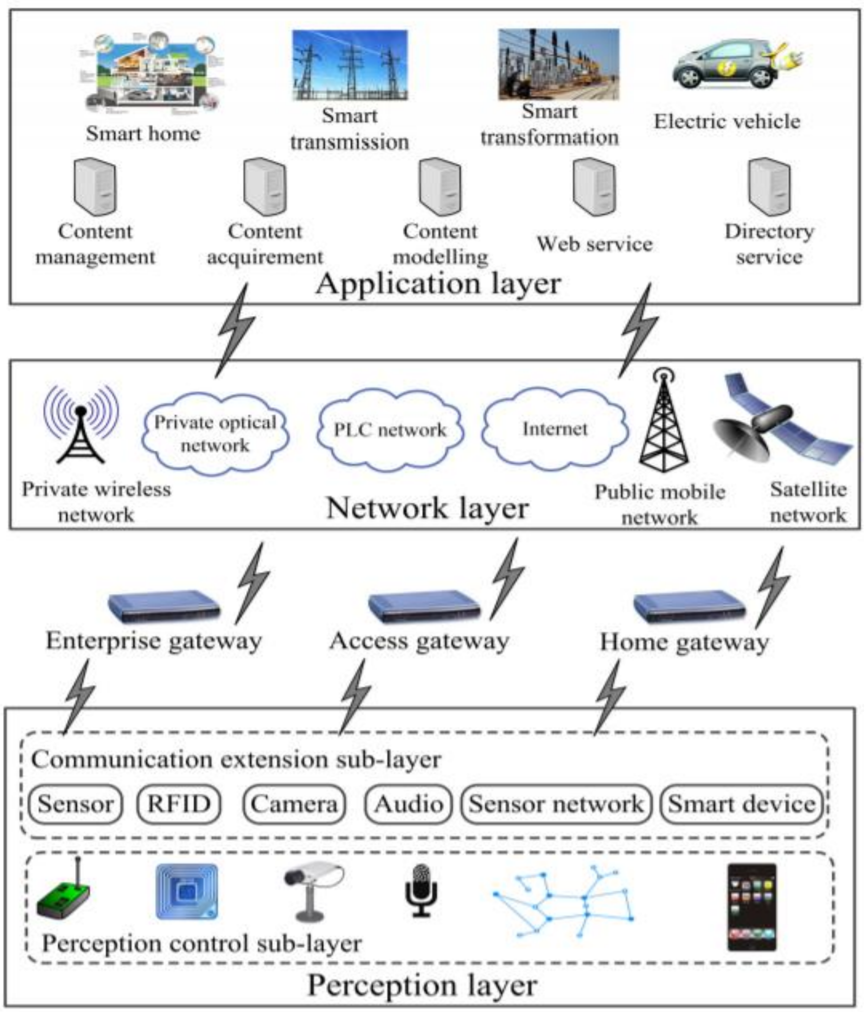


Figure 51 – [39] Three layered architecture for IoT-aided 5G systems

12.1.3 Application Layer: For the realization of IoT-aided 5G applications, application layer combines the IoT technology and industry expertise. The main function of this layer is to process the information that given by network layer. Then, it use the received information for monitoring and troubleshooting the IoT devices and 5G infrastructure in real-time. It also contains different types of servers related to directory services, web services and content services. The infrastructure of application layer also provides resources, processing and computing for IoT technology. Information sharing and security are the key aspects provided by the application layer. The application layer can extend to 5Gs that have the ability to provide much richer information.

12.2 Smart Home:

IoT has a significant part to play in the 5G technology for the accomplishment of smart homes and its appliances such as smart televisions, washing machines, home fire sensors control and security systems, etc. For monitoring the environment and its communication of the surveillance information to the control units, sensor devices are used. These applications can be remotely monitored and managed with the specialized controller that connects to the 5G network IoT slice. Therefore, smart home (IoT system) is a significant issue of 5G cellular IoT network slicing technologies to implement real-time communication among users and the smart grid; moreover it enhances the application features and expands the capability of emerging smart grid applications, which will satisfy users' energy requirements in an utmost significant way.

Broad utilization of smart home applications also improves daily energy usage. For example, the consumer can remotely turn ON and OFF the devices to enjoy their favorite atmosphere while on the way to home or setup for family and friends. Adding to it, users can schedule the timer in the application to turn ON their smart appliances, like dish washer, dryer, washing machine during the peak hours when electricity price is low. The control unit helps the user to perform appropriate action during suspicious activities because of 5G dedicated network slicing for IoT technology; everyone can enjoy all these functions.

12.3 IoT for Smart Energy:

Smart energy systems will take time to acquire the cognitive intelligence needed to monitor for energy disturbances. There are challenges to interconnecting various energy systems. IoT protocols are being positioned for use in smart energy systems. eXtensible Messaging and Presence Protocol (XMPP) can provide a common transport to harmonize sensor information among different protocols.

XMPP utilizes a metadata approach using eXtensible Messaging Language (XML), which is a description language by the World Wide Web Consortium (W3C) that can be used effectively for many purposes including sensor networks. Security is built-in with the use of Transport Layer Security (TLS) encryption, which has been accepted by the **Smart Grid Interoperability Panel (SGIP)** as a standard for the smart grid. It has demonstrated its IoT scalability in use by billions of users around the world.

12.3.1 XMPP provides following features in IoT:

- **Request/response** is the capacity of a client to request something from a device and has a response returned (momentarily or somewhat delayed).
- **Publish/subscribe** allows publishers to publish items to a message broker, which in turn forwards the item to registered subscribers.
- **Multicast** is the ability of multiple parties to communicate together, that is messages are broadcast to all members of certain groups.
- **Events or push notification** is the capacity of a device to send data to an interested party without a previous request for each delivery.
- **Bypass firewall** means that messages can be sent and received even if the sender and final receiver lie behind different firewalls.

- **Federation** means that different islands can be interconnected using a federation of message brokers, and that messages can be forwarded between brokers, enabling devices on one island to communicate with devices on the other island.
- **Authentication** refers to user authentication, that is, validation of user credentials in networks. This security mechanism is where messages are only allowed to be sent between approved parties, known as "friendships."
- **Network identity** means participants in communication are aware of each other's authenticated network identity when they communicate.
- **Encryption signifies** that encrypted communication is possible.
- **End-to-end encryption** refers to encrypting the communication in such a way that not even message brokers can eavesdrop on messages being transmitted.
- **Compression** is the capacity to compress transmitted data to reduce the number of bytes transmitted over the network.
- **Streaming** is the ability to send unending streams of data bytes over a channel.
- **Reliable messaging** means that the protocol has a mechanism to assure the delivery of messages and that the sender has the option to be informed of the successful receipt of the messages.
- **Message queues** are popular in back-end protocols, but are generally not supported in the available IoT protocols. It allows the ability for multiple publishers to queue items in a queue. These items are then consumed on a first in, first out basis by multiple consumers (or workers). Items are sent using reliable messaging to ensure that each item is processed exactly once.

Conclusion:

To epitomize, 5G ecosystem is on its peak of launch in the market to gift this world a fully mobile and connected society. The diversity of use cases requires improvement in the capabilities of the network and develops it as flexible as possible to incorporate a variety of features. The time and service footprint is essential to give consistent customer experience. To interactively include all use-cases and business models requires design flexibility so as to have real time allocation of resources. Moreover, the traffic growth needs to be expected beforehand so as to ensure efficiency. Thus, 5G network is entirely open to new innovations to leverage the Smart Grid industry with completely new experience.

References:

[1]	www.electronics-tutorials.ws/accircuits/sinusoidal-waveform.html
[2]	www.engineering.electrical-equipment.org/power-quality/flexible-ac-transmission-system-facts.html
[3]	(1) Marine Electrical Technology by Fernandez, (2) Chapter 2, Communication Networks for Smart Grids (Kenneth C. Budka • Jayant G. Deshpande Marina Thottan)
[4]	White paper from APC data center
[5]	NIST Smart Grid Framework
[6]	www.hubnet.org.uk/filebyid/613/SmartGridComms.pdf
[7]	Chapter 18, Page no : 484, Scada and smart energy grid control automation (K.Sayed, H.A.Gabbar)
[8]	Chapter 18, Page no : 504, Scada and smart energy grid control automation (K.Sayed, H.A.Gabbar)
[9]	www.Belden.com – IEC 61850 substation communication presentation – 2013, Donny Sia
[10]	www.EnerNex.com
[11]	Chaper 2, page no . 8, Book June 2016- Utility Communication Network and Services – Editor – Carlos Samitier
[12]	Baigent, D., Adamiak, M. and Mackiewicz, R. (2003) IEC 61850-5, Communication Networks and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models.
[13]	www.researchgate.net/figure/310796227_fig1_Fig-3-IEC-61850-90-5-protocol-stack-compared-with-OSI-Stack
[14]	Cellular Communications for Smart Grid Neighborhood Area Networks: A Survey CHARALAMPOS KALALAS1, (Student Member, IEEE), LINUS THRYBOM2, AND JESUS ALONSO-ZARATE1, (Senior Member, IEEE)
[15]	Cellular Communications for Smart Grid Neighborhood Area Networks: A SurveyC. Kalalas et al.: Cellular Communications for Smart Grid NANs

[16]	Page no. 250 , Book Communication network for smart grid , Kenneth C. Budka • Jayant G. Deshpande Marina Thottan
[17]	www.zigbeeg.org
[18]	www.scadalink.com
[19]	www.looptelecom.com
[20]	www.slideshare.net/hamdani2/day-one-09-november-2012
[21]	Broadband world forum 3GPP 2016
[22]	www.4g-lte.net/lte/how-fast-4g-5g-lte/
[23]	www.raconteur.net/technology/4g-vs-5g-mobile-technology
[24]	www.4gltemall.com/blog/wp-content/uploads/2017/11/what-is-5g.jpg
[25]	Page no 25 /NGMN_ 5G_ Initiative_White_paper_17_February_2015
[26]	Chapter 2, Page no 22/ SDN technology overview/ Springer_Book_5G Heterogeneous Network (Bo Rong.Xuesong Qiu.Michel Kadoch.Songlin Sun.Wenjing Li
[27]	Guolin Sun, Feng Liu, Junyu Lai, and Guisong Liu, "Software De_ned Wireless Network Architecture for the Next Generation Mobile Commu- nication: Proposal and Initial Prototype", Journal of Communications , December 2014.
[28]	Fujitsu Network Communication
[29]	Junseok Kima, Dongmyoung Kimb, Sunghyun Choi , 3GPP SA2 architecture and functions for 5G mobile communication system.
[30]	Network slicing nokia, http://telecomsradar.com/2017/12/network-slicing-5g-e2e-network-architecture/?webiStatus=webi
[31]	3GPP Smarter
[32]	3GPP TS 23.501 (www.3GPP.org)
[33]	http://www.huawei.com/minisite/hwmbbf16/insights/5g_opening_up_new_business_opportunities_en.pdf
[34]	www.ofcom.org.uk/__data/assets/pdf_file/0040/68989/m2m_finalreportapril2014.pdf

[35]	Machine-to-Machine Communications: Architectures, Standards and Applications, Min Chen, Jiafu Wan and fang Li, published February 28, 2012
[36]	M2M Communications in the Smart Grid: Applications, Standards, Enabling Technologies, and Research Challenges, Siok Kheng Tan,Mahesh Sooriyabandara, and Zhong Fan, Academic Editor: Chi Zhou
[37]	5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White_Paper-on-Energy-Vertical-Sector.pdf
[38]	omnet-manual.com/wp-content/uploads/2015/12/Architecture-of-smart-Grid.png
[39]	arxiv.org/ftp/arxiv/papers/1704/1704.08977.pdf
[40]	www.sinovoltaics.com/learning-center/basics/direct-current-dc-power-definition-and-applications
1	Utility Communication Network and Services – Editor – Carlos Samitier
2	Scada and smart energy grid control automation (K.Sayed, H.A.Gabbar)
3	Utility Communication Network and Services – Editor – Carlos Samitier
4	Baigent, D., Adamiak, M. and Mackiewicz, R. (2003) IEC 61850-5, Communication Networks and Systems in Substations
5	Slice Architecture for 5G Core Network, Young-il Choi and Noik Park
6	www.radio-electronics.com
7	Nishtha, , and Manu Sood. "Software definednetwork — Architectures", 2014 International Conference on Parallel Distributed and Grid Computing, 2014.
8	www.unwiredinsight.com
9	Kim, Yu-Doo, and Il-Young Moon. "Zigbee And Ieee 802.15.4 Standards", ZigBee® Network Protocols and Applications, 2014.
10	www.ngmn.org
11	5g-ppp.eu

12	Junseok Kim, Dongmyoung Kim, Sunghyun Choi. "3GPP SA2 architecture and functions for 5G mobile communication system", ICT Express, 2017
13	Ahmadi, Sassan. "Network Architecture", LTEAdvanced, 2014.
14	Ferrari, Paolo, Alessandra Flammini, Stefano Rinaldi, and Gunnar Prytz. "Mixing Real Time Ethernet traffic on the IEC 61850 Process bus", 2012 9th IEEE International Workshop on Factory Communication Systems, 2012
15	Sato, "Frontmatter", Smart Grid Standards, 2015