STUDY PAPER

ON

SMART GRID SECURITY
INDEX:

1. Introduction.............................................................................................................3
2. Smart Grid...............................................................................................................4
3. Smart Grid Architecture..........................................................................................4
4. Smart Grid Threat landscape..................................................................................9
5. Real Security Incidents effecting Power System...................................................18
6. Challenges for New Security Solutions..................................................................18
7. Smart Grid Cyber Security Guidelines ...................................................................19
8. Conclusion...............................................................................................................21
9. Glossary..................................................................................................................22
10. References............................................................................................................23
1. INTRODUCTION:

In recent decades the application and use of Information and Communication Technologies (ICT) in Critical Infrastructures, like drinking water systems, energy grids, financial and communication infrastructures have increased enormously. These systems have opened an unforeseen amount of opportunities and have been beneficial for society.

The growing dependency on ICT also means that new threats have to be met. Threats to ICT, intentional and unintentional are a fact and are growing. The disruption or destruction of electricity grids would have a serious impact on economic and societal functions. In order to keep our infrastructures resilient, we have to invest in secure and resilient architectures.

In this paper introduction of Smart Grid architecture along with its functional domains and security of respective functional domains have been discussed.
2. SMART GRID:

A smart electrical grid is defined as an electrical grid, which can integrate the behaviour and actions of all connected users in a cost effective way including producer, consumer and actors, which are both producer and consumer to ensure a resource-saving and economically efficient electrical network with less losses, high quality, great security of supply and high technical safety.

Smart grids provide electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled and monitored using information and communications technologies (ICT). These technologies enable energy companies to seamlessly control the power demand and allow for an efficient and reliable power delivery at reduced cost via digital two-way communications between consumers and electric power companies, the smart grid system provides the most efficient electric network operations based on the received consumer’s information.

3. SMART GRID ARCHITECTURE:

Smart grid architecture is further explained on basis of domains based on service areas as per ITU-T and functional domains based on functions of individual components.

3.1 Smart Grid Domains:

As per ITU-T Smart Grid architecture consist of five domains 1 to 5 domains and are viewed in three service areas: smart grid service/applications, communications and physical equipment. (Fig 3)

i. Grid Domain:

The grid domain provides the bulk generation/transmission/distribution function. Components in the grid domain are classified as the 'smart meter infrastructure' and the 'distribution grid management' which are explained later in this paper.

ii. Customer Domain:

Customer Domain comprises of customer related equipment such as Smart Appliances, Plug in electric Vehicles, heating, ventilating & air conditioning (HVAC) etc.

iii. Service provider Domain:

This domain basically performs application functions & comprises of operators, service providers & governed by market scenarios.

iv. Smart Metering:

This mainly performs metering related functions such as meter reading function, meter control and maintenance function. This domain also deals with fault monitoring and protection.

v. Communication Network:

Mainly performs communication related functions between different domains either using telecommunication infrastructure including IP based infrastructure functions.
3.2 Functional Domain:

Smart grid architecture is mainly divided into 6 functional domains and subsequently failure scenarios, threats and vulnerabilities are identified on basis of functional domains as specified below:

3.2.1 Advanced Metering Infrastructure (AMI):

Smart metering infrastructure comprising smart meters at the customer’s premises, data concentrators, an AMI headend system and an MDM System.

The smart meter is typically located in the customer premises. It has multiple communication interfaces: the uplink employs a proprietary PLC system, which, according to the manufacturer, uses state-of-the-art encryption technologies. Besides the PLC communication interface, there is an optical interface for the configuration and maintenance of the smart meter. Access to the optical interface is protected with a strong password.

The utility uses the same service password for all smart meters. The smart meter firmware is proprietary and can be considered as a black box system to the utility. Additionally, the smart meter contains a remote controllable breaker unit. The data concentrator is the PLC endpoint for the smart meters. Apart from the PLC interface, it has an Ethernet uplink that is connected to the headend system over a fibre optic link secured via VPN. The data concentrators are all situated in physically secure locations such as substations or transformer stations operated by the utility. The headend system is located at the utility and comprises a proprietary manufacturer software implementation that is executed on an off-the-shelf server system. The system is connected to a metering VLAN to communicate with the data concentrators. Over a separate link, the system is connected to the MDM system, which is essentially a large proprietary database system supplied by the smart metering system manufacturer. It is executed on an off-the-shelf server system and has an uplink connection to a stand-alone SAP system used for billing purposes.

3.2.2 Wide Area Monitoring, Protection, and Control (WAMPAC):

Systems that support wide area applications, related mainly to synchro phasor technology and the devices that generate, receive, and utilise synchro phasor data. WAMPAC is one of most critical component in smart grid landscape and hence few precautions have been taken by utility for preventing potential attacks. The solutions consist of various combinations of common design elements: Intelligent Electronic Devices (IEDs) capable of collecting samples of input waveforms and calculating phasors, sources for a high precision time synchronization reference, various phasor data concentrators, communications, applications, and visualization tools for data presentation

The redundant SCADA and NTP systems hosted at the utility can only be accessed by a small number of authorised employees. The system is physically separated from other communication networks. Maintenance operations can only be performed by temporarily enabling access to the maintenance functionalities. From the utility to the field, mostly fibre links are employed that are located at the top of high voltage power poles. Directional radio links are used for a small number of devices in rural areas. To secure both the fibre and any other communication media, state-of-the-art VPN tunnelling is employed. Various field units are generally deployed in physically protected areas. In addition, the utility has WAMPAC systems located in secondary substations as well as in medium- and low voltage generation stations. Secondary substations and low voltage generation stations are typically small and often situated in rural areas.
3.2.3 Distribution Grid Management (DGM):

A utility has a wide ranging DGM system in place that ranges from primary and secondary substations to plug-in electric vehicles (PEVs), low voltage generation, or smart buildings. In this utility leverage manufactures in device VPN implementation as mentioned above so that any communication outside the device is cryptographically protected. The configuration is thus comparable to the WAMPAC case study above, with the difference that the number of devices which are more easily accessible to attackers is higher.

3.2.4 Demand Response:

The primary focus on the Demand Response (DR) is to provide the customers with pricing information so that the customers or the energy-management and control system (EMCS) at the customer’s sites may respond based on the demands for electricity and electricity prices during some period of time. For instance, the customer may decrease demand (or shed load) during higher priced time periods or increase demand (or shift load) during lower priced time periods.

![Demand Response Use case](image1)

**Fig1. Demand Response Use case shows the interfaces between each component**

3.2.5 Supervisory Control and Data Acquisition (SCADA) System Security Issues:

SCADA systems are widely deployed in Critical Infrastructure industries where they provide remote supervisory and control. In the Smart Grid SCADA systems are used in automation.

SCADA is a collection of systems that measure, report, and change in real time both local and geographically remote distributed processes.

![SCADA general Layout](image2)

**Fig2. SCADA general Layout**
The fundamental components in the above figure are the control centre usually computer-based, referred to as MTU (Master Terminal Unit), RTU (Remote Terminal Unit) or also called as field site, and the communication link between them. The MTU issues commands to distant facilities and gathers data from them, interacts with other systems in the corporate intranet for administrative purposes and interfaces with human operators. In a SCADA system it is the MTU which has full control on distributed remote processes. An operator can interface with a MTU through an interface device consisting in a video display unit, a keyboard, etc. Control commands sent by a MTU to distant facilities are triggered by programs in that MTU which are executed either manually or through a programmable built-in scheduler.

The SCADA system is a control system which was originally designed to operate in an isolated environment. Today they are typically connected to the corporate network for business reasons.

3.3 Smart Grid Reference Points:

As explained above mainly 5 domains have been defined by ITU-T and reference points comprising of those domains is specified below:

![Fig 3. Reference Architecture of Smart Grid from ICT perspective](image)

3.3.1 Reference point 1:

i. This is a reference point between the grid domain and the communication network. It enables the exchange of information and control signals between devices in the grid domain and the service provider domain. Examples of information exchange taking place along with this point are listed below:

ii. A remote terminal unit (RTU) in transmission systems to enable SCADA operations;

iii. Intelligent electronic devices (IEDs) in transmission systems to interact with SCADA operations in the service provider domain;

iv. A plant control system interacts with SCADA and energy management system (EMS) in the service provider domain.
3.3.2 Reference point 2:

This is a reference point between the smart metering domain and the communication network. It enables the exchange of metering information and interactions through operators and service providers in the service provider domain towards customers in the customer domain. Some examples are listed below:

i. Management of meters, retrieval of aggregated meter readings from AMI head-end/controller in operations and the service provider in the service provider domain
ii. Interacting with customer EMS to exchange pricing, data related to demand response (DR), including the load shedding information, and relevant information enabling automation of tasks involved in a better use of energy
iii. Billing in the service provider domain that interacts with the meters in the customer domain; smart meters interact with billing in the service provider domain
iv. Smart meters form a metering infrastructure to ensure reliable communication to the meter head-end through this reference point.

3.3.3 Reference point 3:

This is a reference point between the customer domain and the communication network domain. It enables the interactions between operators and service providers in the service provider domain and devices in the customer domain. Some examples are listed below:

i. HAN communicates over this reference point either through a secure energy service gateway or through a public network (e.g. Internet)
ii. Billing in the service provider domain interacts with customers in the customer domain
iii. Monitoring and controlling the information exchange for distributed generation and DER in the customer domain.

3.3.4 Reference point 4:

This is a reference point between the service provider domain and the communication network domain. It enables communications between services and applications in the service provider domain to actors in other domains to perform all smart grid functions illustrated above.

3.3.5 Reference point 5:

This is a reference point between the smart metering and the customer domain; it conducts services through ESI. Some examples are listed below:

i. Smart meter interacts with devices, including customer EMS, ESI in home, customer appliances and equipment;
ii. Devices in the customer domain, including customer EMS, ESI in home, customer appliances and equipment interact with smart meters

3.4 Smart Grid Component:

The Grid can be viewed as having two main components: System and Network component.

3.4.1 System Component:

The major system components in smart grid are Smart meter, Electrical household appliances, Renewable energy sources, Electric utility providers and Service Providers.

3.4.2 Network Component:

Smart grid incorporates two types of communication: Home Area Network (HAN) and Wide Area Network (WAN). A HAN connects the in-house smart devices across the home with the smart meter. The HAN can communicate using Zigbee, wired or wireless Ethernet, or Bluetooth. A WAN, on the
other hand, is a bigger network that connects the smart meters, service providers, and electric utility. The WAN can communicate using WiMAX, 3G/GSM/LTE, or fibre optics. The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information. The electric utility manages the power distribution within the smart grid, collects sub-hourly power usage from smart meters, and sends notifications to smart meters once required. The smart meter receives messages from devices within HAN and sends them to the appropriate service provider. Refer fig 2

**Fig. 4: Basic Network Architecture**

**4. SMART GRID THREAT LANDSCAPE:**

On basis of functional domains specified above, various threat scenarios are explained below:

**4.1 Advance Metering Infrastructure:**

From the above description of AMI, it is apparent that the smart meter is a critical device due to its physical location, the smart meter can be easily accessed by attackers and subject to physical attacks which are in general more powerful than typical network attacks. In comparison, physical access to the data concentrator becomes less likely for external attackers, whilst systems hosted at the utility (i.e. the headend and the MDM system) are very unlikely to be physically accessible to external attackers.

Considering external attackers following threat scenarios on a smart meter are conceivable:

**i. Unauthorised use of the optical communication interface:**

The attacker may able to break the configured password first (e.g. by utilising physical attacks, which are much more powerful than typical password brute force attacks), and might then be able to re-configure the smart meter or exploit a software vulnerability.
ii. Physical attacks on the smart meter device:

This would allow an attacker to deconstruct the smart meter device and potentially read out the firmware, the system configuration, as well as system credentials and key material. This information could be used to gain access to remote systems over the PLC network.

iii. Unauthorised communication over the PLC network:

As a consequence, an attacker could potentially control remote devices, although additional information on the PLC implementation or credentials and key material might be required first.

For PLC data concentrators possible threats are:

iv. Remote attacks over PLC:

If an attacker has figured out how the PLC communication works, remote attacks could be used against the data concentrator.

v. Remote attacks over the uplink connection:

Although more critical systems are available over the uplink connection, an attacker might still consider attacking the data concentrator due to the potential to control large amounts of smart meter devices.

vi. Physical attacks on the data concentrator:

This is the most powerful type of attack. Similar to smart meter devices, an attacker could use physical attacks to extract the firmware, key material, credentials, and other critical information from the data concentrator. Using the collected information, the potential to conduct remote attacks on other data concentrators, smart meters, or even headed system rises.

For the heade, MDM and other utility hosted systems, potential threats are:

vii. Remote attacks over the data concentrator uplink

viii. Remote attacks over the Internet or other public networks that, due to inadequate security controls, enable access to critical headend systems. For instance, this could be caused by a malware infection through a targeted attack on a utility employee, which spreads over the internal network until it reaches critical headend systems.

ix. Exposure of weak encryption in the PLC uplink:

Either by analysing the PLC communication or by disassembling the hardware and software implementation of a smart meter device, the attacker discovers that the encryption protecting the PLC traffic is easy to break, and is thus able to decrypt any communication within the PLC network.

x. Exposure of smart meter vulnerabilities:

By analysing the smart meter hardware and software implementation, an attacker discovers and publicly discloses smart meter vulnerabilities, which can be exploited by the attacker and by other, potentially less experienced individuals to conduct remote attacks over the PLC network.

xi. Exposure of credentials and key material:

Either by analysing the PLC communication, by utilising the optical configuration interface, or by reverse engineering the hard- and software implementation of the smart meter, an attacker gains access to the configured credentials and key material within the smart meter device. As a result, this information could be publicly disclosed and widely used for remote attacks on the AMI infrastructure.
xii. Access to headend systems through malware infection or targeted attacks on publicly available systems of the utility.

4.2 Wide Area Monitoring, Protection, and Control (WAMPAC):

Since WAMPAC systems can be easily physically accessed by attackers, the utility employs components that have the full VPN functionality built into the devices by the manufacturer. As a result, any communication to or from these devices is VPN protected.

4.2.1 For the **physically well protected systems** at the utility’s premises, the following threats are conceivable from the perspective of an external attacker:

i. Denial of Service (DoS) attacks on the network, VPN and NTP infrastructure:

To mount this attack, the attacker needs to have access to the WAN. The VPN tunnel effectively protects the inner systems if credentials and key material are not available to the attacker.

ii. DoS attacks on the wireless infrastructure:

Due to easy accessibility, an attacker manages to jam or flood wireless links with erroneous messages.

iii. Software vulnerabilities:

The systems at the utility contain software Vulnerabilities that are exploited by an attacker. However, the VPN tunnel provides protection unless the attacker gains knowledge of credentials and key material.

4.2.2 For the **physically less protected systems** in secondary substations or low voltage generation stations, the attack vectors from the perspective of an external attacker are:

i. Physical attacks on WAMPAC devices:

An attacker utilises powerful physical attacks on accessible devices allowing him, for instance, to read out the firmware, configuration, credentials, or key material, potentially providing the attacker with the information necessary to access the VPN network.

ii. Injection of bogus measurement data:

An attacker compromises the local authentication at a WAMPAC device and injects bogus measurement data to destabilise the grid.

4.2.3 Considering the **present attack vectors** from the perspective of external attackers, viable attack scenarios could be:

i. Physical attacks on WAMPAC devices in secondary substations:

An attacker mounts a physical attack on a less protected WAMPAC device in a secondary substation and manages to extract the device’s configuration data, including credentials and key material to access the VPN network.

ii. DDoS attack on wireless WAMPAC communication links:

Although all traffic is encrypted by the VPN tunnel, the attacker is able to inject large amounts of wireless signalling traffic that causes the wireless modems to massively slow down the VPN traffic.
4.3. Distribution Grid Management (DGM):

Considering physically more easily accessible systems, viable threats considering external attackers are:

i. Physical attacks on in-field DGM devices:

An attacker could utilise powerful physical attacks on accessible devices allowing him, for instance, to read out the firmware, the configuration, the credentials or the key material from those devices. These attacks could provide the attacker with the necessary information to access the VPN network. Subsequently, the attacker might leverage this information to compromise the DMS system through the VPN uplink channel.

ii. Attacks on the wireless infrastructure:

As wireless links are physically easy to access, an attacker might jam these links, flood the wireless links with messages, or target the implementation of the wireless routers. Access to the DMS traffic is however protected by the VPN.

iii. DoS attacks on the DMS uplink

By levering these attack vectors, the attacker can potentially impact the physically well protected DGM systems in the utility’s premises

4.4. Demand Response:

4.4.1 Demand Response at Residential Sites and Security issues

Demand response events arrive at the residential site from the utility to adjust the electricity price. During peak hours the price of the electricity rises; through demand response the customers can adjust their residential temperature on the basis of the demand response event received. During normal conditions the broadcast messages consisting of price signals are sent to residential whereas during emergency control signals are issued. The Programmable Communicating Thermostat (PCT) would be used in order to reduce the electric power at the residential site. Broadcast messages which will be sent out to the thermostat which causes the thermostat to update the power consumption. The PCT will communicate with the utility through a meter. The connection is done through a wide area network. The PCT allows the customer to set the temperature for heating as well as cooling.

Possible attacks in PCT:

i. An attacker may attempt to shut down the A/C, prevent the load reduction, and manipulate the scheduling of events received.

ii. An attacker tries to tamper with the incoming signals or PCT system. The attacker carries out the attacks by carrying out masquerading and man in the middle attack by shutting or turning down the A/C units in order to cause the grid instability.

iii. An attacker blocks the incoming broadcast signal by carrying out denial of service attack. Replay attacks can be carried out in order to manipulate the incoming demand response signal.

iv. An attacker could manipulate the system by disabling the PCT antenna or changing the PCT local time.
4.5. Supervisory Control and Data Acquisition (SCADA) System Security Issues:

Security issues of SCADA is mentioned below:

4.5.1 Platform configuration vulnerabilities:

i. OS and application security patches are not maintained.

ii. Inadequate Access controls: Poorly specified access controls can result in giving an SCADA user too many or too few privileges. The following exemplify each case: System configured with default access control settings gives operator administrative privileges, system improperly configured, results in an operator being unable to take corrective actions in an emergency situation.

4.5.2. Platform Software Vulnerabilities:

i. Denial of service (DoS):
SCADA software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control centre networks, SCADA systems, interconnections, and access links.

ii. Intrusion detection/prevention software not installed:
Incidents can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms.

iii. Malware protection software not installed definitions not current, implemented without exhaustive testing:
Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software.

4.5.3. Network parameter vulnerabilities:

i. Network leak vulnerabilities:
TCP/IP networks by their very nature promote open communications between systems and networks, unless network security measures are implemented. Improper network configuration often leads to inbound and outbound network leaks between SCADA networks, corporate networks, business partners, regulators and outsourcers and even the Internet which pose a significant threat to network reliability. Network leaks can allow worms, viruses or hackers direct visibility to vulnerable SCADA systems.

ii. Insecure connections exacerbate Vulnerabilities:
Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access link such as dial-up modems to equipment and control information open for remote diagnostic SCADA, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure
connections to break into remotely controlled systems. Control system often use wireless communications systems, which are vulnerable to attack or leased lines that pass through commercial telecommunications facilities.

**iii. Firewalls non-existent or improperly configured:**

A lack of properly configured firewalls could permit unnecessary data to pass between networks such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

4.5.4 Network Communication Vulnerabilities:

The SCADA systems are built using public or proprietary communication protocols which are used for communicating between an MTU and one or more RTUs. The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The most common protocol is DNP3 (Distributed Network Protocol Version 3.3). It was developed to achieve interoperability among systems in the electric utility.

i. **Destination Address Alteration:**

By changing the destination address field, an attacker can reroute requests or replies to other devices causing unexpected results. An attacker can also use the broadcast address 0xFFFF to send erroneous requests to all the outstation devices; this attack is difficult to detect because (by default) no result messages are returned to a broadcast request.

ii. **Rogue Interloper:**

An attacker installs a “man-in-the-middle” device between the master and outstations that can read modify and fabricate DNP3 messages and/or network traffic.

4.5.5 Securing Serial SCADA Communications:

Many substations and distribution communication systems still employ slow serial links for various purposes including SCADA communications with control centres and distribution field equipment. Furthermore, many of the serial protocols currently in use does not offer any mechanism to protect the integrity or confidentiality of messages, i.e., messages are transmitted in clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over PPP will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

4.6. Generic Security Issues in Smart GRID:

These Security issues are not uniquely associated with specific smart grid “logical” component but are critical and affect any smart grid component.

4.6.1 Authenticating and Authorizing Users (People) to Substation IEDs:

IEDs stand for Intelligent Electronic devices. This device may be accessed locally i.e. user may be physically present in substation & access the IED from front panel or access remotely from different physical connection. Hence the problem to authenticate and authorize different users arises so as to access is granted specifically to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally
managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

4.6.2 Authenticating and Authorizing Maintenance Personnel to Smart Meters:

The Security problem in Smart meters is similar to IEDs. Access to these is may be local through the optical port of meter or through the AMI infrastructure, or remote through the HAN gateway. In this, password is shared between users and the same passwords is used across entire meter deployment and hence problem arises for authenticating and authorizing Smart meters.

4.6.3 Side Channel Attacks on Smart Grid Field Equipment:

These attacks are based on physical accessibility (Substation, Pole-Top, Smart Meters, Collectors, etc.). A side-channel attack is based on information gained from the physical implementation of a cryptosystem. Tempest attacks similarly can extract data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle as a probe to tap extremely fine wire traces on printed circuit boards. Smart grid devices that are deployed in the field, such as substation equipment, pole-top equipment, smart meters and collectors, and in-home devices, are at risk of side channel attack due to their accessibility. Extraction of encryption keys by side channel attacks from smart grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side channel attacks could allow an attacker to impersonate smart grid devices and/or personnel, and potentially gain administrative access to smart grid systems.

4.6.4 Patch Management:

Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake because of how distributed and isolated equipment can be. Also there are many unforeseen consequences that can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware needs to be managed.

4.6.5 Home Area Network and Neighbourhood Area Network Security Issues:

As per Network component explained in fig4 above security issues are specified below:

4.6.5.1 Home Area Network:

Smart Grid provides two-way communications between home owner’s premises and utility companies back end IT infrastructure. This is done by deploying Advanced Metering Infrastructure (AMI) systems that combine Home Area Networks (HANs) and Neighbourhood Area Networks (NANs). A HAN typically connects home devices together whereas a NAN connects the home for the Utility Network. The key enabling technology for energy management products in the home are protocols such as Zigbee, Z-Wave etc.
i. Zigbee:
Zigbee focuses on low cost, low speed ubiquitous communication between devices with little or negligible use of underlying infrastructure. It makes practical to embed wireless communications into virtually any home/building automation/metering product without the prohibitive cost and disruption if installing hard wiring. Security Issues are involving with Zigbee are:

a. Fast denial of service Attack on AES-CTR (Advance Encryption standard CTR mode)
b. Acknowledges Forgery since the ACK frame returns only the DNS (Domain Name Server) value. If the attacker knows the DNS value, he/she can send a false acknowledgement to the sender saying that the receiver has received the message when in fact it hasn’t.

ii. Z-Wave:
Z-Wave is a wireless communications proprietary standard designed for home automation, specifically to remote control applications in residential and light commercial environments. Security risks involved with Z wave is:
Unsecure connection while establishment of networks and distribution of network key which increases the possibility of sniffer attacks.

4.6.5.2 Residential Gateway:
Residential Gateway (RG) is a device that interconnects various home electronic devices to one another as well as connects these private home network devices to exterior public network. In the smart grid architecture, the current assumption is that there is an identifiable unit performing the gateway function.
Gateway consists of Wi-Fi module, a Zigbee Microcontroller and a power supply. There are two implementation techniques for the gateway:

- Its implementation technique involves hardware component which integrates Zigbee based home automation system with an external IP based network.
- The gateway is part of the PCT (Programmable Communicating Thermostat), one such example is the U-SNAP (Utility Smart Network Access Port). This is a hardware solution to the interoperability issues between the native AMI network and the home area network. U-SNAP card brings a Serial interface between the module that communicates with the Utility AMI network and the HAN control unit.

The gateway provides two functionalities:

- Data translation between the IP based network and the Zigbee network.
- To provide a secure environment for processing command received from the external network.

Security risks with Gateway are:

i. MAC Address spoofing: When the U-SNAP card is plugged in for the first time it registers on the network. Since the network operates in an unlicensed frequency band any eavesdropper can listen to on-going traffic and spoof the MAC address, this MAC address the U-SNAP card uses as an ID to uniquely recognize a card. The second scenario occurs when pricing information is sent by the utility to the consumer, but as the MAC address of the card has been spoofed. In this case the utility would be sending sensitive data to an unauthorized person which is breach of confidentiality of highest security level.
ii. **Public Key Infrastructure Security Issues**: The U-SNAP card uses Public Key infrastructure as a security feature. With the use of PKI emerges the problem of distribution of public keys and the added responsibility of choosing a certifying authority to sign the keys.

### 4.6.5.3 Wireless Neighbourhood Area Network (WNAN):

Wireless neighbourhood area networks (WNAN) are a type of packet switched wireless mobile data networks. Wireless NANs are flexible packet switched networks whose geographical coverage area could be anywhere from the coverage are of a Wireless Local Area Network (WLAN), to wireless metropolitan area network (WMAN), to Wireless Wide Area Network (WWAN). In Smart Grid, WNAN has a role to play in the HOME to HOME or HOME to GRID communication. The communication protocols that are used for WNAN for Smart Grid are IEEE 802.11, IEEE 802.16. Security issues with these two communications protocols is mentioned below:

**IEEE 802.11**: Wireless LAN which subsequently become basis of Wi-Fi.

i. **Rogue Access Points**: Rogue AP is easy to set up and does not even require authorization.

ii. **MAC Spoofing**: The management frames are not authenticated in 802.11. Every frame has a source address. The attackers take advantage of the spoofed frame to redirect the traffic and corrupt the ARP tables.

iii. **Denial of Service attacks**:

a. **Physical Attacks**: Simple devices that operate in 2.4 GHz frequency band like cordless phones that support 802.11b can be used to take the network offline. This is done by reducing the signal to noise ratio of the channel to an unusable range, by inducing noise into the network.

b. **Data-link Attacks**: For devices manufactured before 2003 with wired equivalent privacy (WEP) turned on, the attacker can perform DoS attacks by accessing the user information on the link layer. Data link attacks are difficult for post 2003 devices that support WPA2.

iv. **Network Attacks**:

An attacker can flood ICMP packets to the gateway, thereby creating a difficult time for clients associated to the same AP to send and receive packet.

v. **Man-in-the-Middle (MITM) Attacks**

**IEEE 802.16 (WiMAX)**:

i. **Authentication**: The drawback with WiMAX is that it does not have Base Station authentication which makes it prone to Man-in-the-middle attacks exposing subscribers to confidentiality and availability attacks. Since BS does not authenticate itself, the SS cannot be protected from rouge BS.

ii. **Encryption**: 802.16e supports for Advanced Encryption Standard (AES) cipher providing strong confidentiality on user data. Again the drawback is with encryption not applied on the management frames thereby sufficing the attacker to gather information about the subscribers in the area and also about the network characteristics.
iii. Availability: Even though WiMAX uses a licensed RF spectrum, attackers can use easily available gadgets to jam the network. This is an example for physical layer denial of service attacks whereas attackers can send legacy management frames to disconnect legitimate station, this is nothing but de-authenticate flood attacks.

iv. Water Torture Attack: This is a form of physical layer attack wherein the attacker sends a series of frames to any node to drain the battery life of the victim node.

5. Real Security incidents affecting Power Systems:

5.1 Considering power generation, in March 2008 the Edwin I nuclear power plant in Georgia (USA), was forced to make an emergency shutdown for 48 h due to a software update. This software update was applied to the computer system in charge of monitoring chemical and diagnosis data of one of the plant’s primary control systems. After applying the update, the computer was rebooted and this lead to a lack of monitoring information. Safety systems misinterpreted this and signalled that the water level in the cooling systems for the nuclear fuel rods had dropped, which caused an automatic shutdown. There was no danger to the public, but the power company lost millions of dollars in revenue and had to incur the substantial expense of getting the plant back on-line.

5.2 In distribution and transmission domain one of the most relevant incidents was the attack suffered by the US electrical grid in 2009. Officials from the US public administration recognised that cyber spies from other countries had hacked into the US electricity grid and hidden software that could be used to disrupt power supplies. Later on it was confirmed that attackers could use this software backdoor to cut electricity at will.

5.3 Night Dragon was the name given to a number of targeted attacks. Their main objective was to compromise the industrial control system of several energy companies in the United States, including oil, gas and petrochemical companies. These attacks relied on a combination of several techniques, tools and vulnerabilities (i.e. spear-phishing, social engineering, Windows bugs and remote administration tools). Although the attacks were not very sophisticated and did not exploit any zero-day vulnerability, the information such as financial information, related to oil and gas field exploration and big negotiations, as well as operational details of production supervisory control and data acquisition systems was very valuable for competitors.

5.4 Duqu is a computer worm that was discovered in September 2011. Its main objective was to collect information such as keystrokes and system information to prepare future attacks against industrial control systems. Duqu executables have been found in a limited number of organisations, including those involved in the manufacturing of industrial control systems. Experts are still analysing the code but they consider that Duqu may be used to enable a future Stuxnet like attack or might already have been used as a basis for the Stuxnet attack.

6. Challenges for New Security Solutions:
Security solutions developed for traditional IT networks are not effective in grid networks because of the major differences between them. Their security objectives are different in the sense that security in IT networks aims to enforce the three security principles (confidentiality, integrity and availability), while the security in automation (grid) networks aims to provide human safety, equipment and power lines protection, and system operation. Moreover, the security architecture of IT networks is different than that of the Grid network since security in IT networks is achieved by providing more protection at the centre of the network (where the data resides), while the protection in automation networks is done at the network centre and edge. Their underlying topology is also different where IT networks use a
well-defined set of operating systems (OSs) and protocols, while automation networks use multiple propriety OSs and protocols specific to vendors. Finally, their Quality of Service (QoS) metrics are different in the sense that it is acceptable in IT networks to reboot devices in case of failure or upgrade, while this is not acceptable in automation networks since services must be available at all times. These major differences between the IT and grid network security objectives necessitate the need for new security solutions specific for the smart grid network.

7. Smart Grid Cyber Security Guidelines:

Considerable efforts have been done across the world and policy to support the modernization of Nations electricity transmission and distribution system to maintain a reliable and secure infrastructure that can meet future demand growth by using digital information and control technology and principle of dynamic optimization of grid operations and resources with full Cyber Security is adopted.

Hence Guidelines for Smart Grid Cyber Security was developed by NIST. This initial version of Guidelines for Smart Grid Cyber Security was developed as a consensus document by the Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by NIST in January 2010. The CSWG now numbers more than 500 participants from the private sector (including utilities, vendors, manufacturers, and electric service providers), various standards organizations, academia, regulatory organizations, and federal agencies. A number of these members are from outside of the United States.

The three volume report NISTIR 7628 Guidelines for smart grid Cyber Security presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.

The first instalment of guidelines is:

i. An overview of cyber Security Strategy used by the CSWG to develop the high-level Cyber Security Smart Grid requirements.

ii. A tool for organizations that are researching designing, developing, implementing and integrating Smart Grid technologies established and emerging.

iii. A evaluative framework for assessing risks to Smart Grid components and systems during design, implementation, operation and maintenance.

iv. A guide to assist organizations as they craft a Smart Grid Cyber Security strategy that included requirements to mitigate risks and privacy issues.

For development of Security Architecture, NIST identifies seven domains within the smart Grid-Transmission, Distribution, Operation, Bulk Generation, Markets, Customer, and Service Provider.
It then identified 46 actors distributed across 7 domains. One output of this analysis is a logical reference model that shows logical interface linking actors and suggests the type of information exchanged.

Over 130 possible logical interfaces were identified. These interfaces (shown in Figure 5) were assigned to one of 22 categories on the basis of shared or similar security characteristics. For instance, category 13 covers the logical interfaces between systems that use the Advanced Metering Infrastructure (AMI) network.
NIST specifies that security must be applied in layers, with one or more Security measures and controls implemented at each layer. This layered approach to security should leverage existing power system design and capabilities that have been successful in assuring reliable supplies of power to consumers.

The logical reference model does not imply any specific implementation but its work is in progress.

8. CONCLUSION

Smart Grid is identified as one of main components of Critical Infrastructure group. Smart grid integrates the traditional electrical power grid with information and communication technologies (ICT). Such integration empowers the electrical utilities providers and consumers, improves the efficiency and the availability of the power system while constantly monitoring, controlling and managing the demands of customers. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber-attacks. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level.

Several pilot projects are for implementation of Smart Grid is under progress in India and hence Security issues and concerns should be addressed in priority so as not to cause any major incidents in future.
9. GLOSSARY:

i. AMI-Advance Metering Infrastructure

ii. CSWG-Cyber Security Working Group

iii. DER-Distributed Energy Resources

iv. DOS-Denial of Service

v. EMS-Energy Management Systems

vi. ESI –Energy Service Interface

vii. HAN-Home Area Network

viii. ICT- Information & Communication Technology

ix. IED- Intelligent Electronic devices

x. ISO-Independent System Operators

xi. PCT-Programmable Communication Thermostat

xii. PLC-Programmable Logic controller

xiii. RTU- Remote Terminal Units

xiv. SCADA-Supervisory Control and Data Acquisition Systems
9. REFERENCES:

[i] ITU Smart-O-33Rev.6: Deliverable on Smart Grid Architecture


   Potential Threats, Vulnerabilities & Risks

[iii] NISTIR 7628 Guidelines for Smart Grid Cyber Security

[iv] Book on Smart Grid Security – Innovative solutions for a modernized Grid by Florian Skopik

[v] ENISA_Annex II Security aspects of the smart grid