Communication and Cyber Security issues in Smart Grid

M.M. Tripathi

Department of Electrical Engineering, Delhi Technological University, New Delhi, India

Abstract— *Smart Grid is an Information and Communication Technology (ICT) enabled Power grid. It is efficient, secure, reliable and self-healing power grid. Integration of micro grids, electric vehicles and other utilities make it more interesting. The deregulation of electricity sector has necessitated the use of many advanced software and embedded technologies to handle the size and complexity of power network. Smart grid needs to be supported by efficient and secure communication architecture design and implementation. At the same time it is necessary to ensure the security and privacy of data and information moving or stored in the smart grid system to have near 100% uptime of the power grid. This paper presents a comprehensive analysis of the various communication and cyber security issues involved with the successful operation of Smart Grid.*

Keywords— Smart grid, Cyber Security, Communication, Generation, Transmission, Distribution, Advance metering, restructuring.

I. INTRODUCTION

Smart Grid often called Intelligent Grid is a digitized electricity network which treats electricity unconventionally; not as a commodity but as a value added service. Its important features are deregulation, distributed generation, enhanced participation of consumers, generation and storage options, power quality, optimized asset utilization with high operational efficiency, self-healing and resiliency against attack and natural disaster. Integration of micro grids, electric vehicles and other utilities make it inspiring. The restructuring and deregulation of electricity market has necessitated the movement and analysis of large chunk of data in power network. The Smart grid is a new age transmission grid which is reliable, secure, affordable and efficient with improved power quality and low operational and maintenance cost. With the Advanced metering infrastructure, supported by bidirectional data flow, Demand side management with load and price forecasting and online bidding Smart Grid becomes most crucial to today's power system. The elements of the Smart Grid are (i) integrated communications (ii) advanced sensing and instrumentation technologies (iii) smart components (iv) advanced control strategies (v) improved interfaces.

Some of important features of Smart grid are:

- Distributed generation/ Micro-grids
- Enhanced customer participation
- Generation and storage options
- Better quality of power
- Bi-directional data flow
- Optimized utilization of Infrastructure with high operational system efficiency
- Self-healing and resiliency against cyber-attack and natural disaster
- Restructuring of Power system

A Smart grid is consisting of Power plus Energy Layers supported by the Communication Layer. Smart grid has better energy management, efficient and reliable network that integrates all energy supply and demand sources as well as smart devices. It also emphasizes the need of reliable and secure communications which pose biggest challenge of designing and deployment of appropriate communication architecture for smart grid which is interoperable, scalable, self-organizing, and secure against cyber-attacks.

The large scale introduction of distributed generation and non-conventional energy sources supports the institution of regional micro-grids. Making use of techniques like virtual power plants or virtual power systems they try for aggregating and autonomously deciding their own generation and demand side resources to balance production and consumption in as compact as feasible entities. Interaction with near-by distribution network and with the connected production, storage and consumption appliances would be the key to the economical and efficient management of such grids. Economical energy management in buildings needs in depth use of communication network infrastructure to and in buildings moreover because the provision of the mandatory interfaces to existing appliances, existing distributed generation and energy and service providers. The massive scale introduction of electrical vehicles would have an effect on the energy infrastructure. Providing sufficient charging points needs interaction between the energy infrastructures, the transport infrastructure, the vehicle data and information systems and also the communication network infrastructure so as to gather, process and deliver the required data.

The major software component in smart grid are the databases that collects demand orders from the customers

and keeps the record of the consumption and the decision making tool that determines generation and distribution scheme of the network. Artificial Intelligence tools may be utilized for forecasting of demand, price and other electricity parameters for better decision making, planning and operation. Various optimization techniques will be used for formulation of best optimized bids. Web technologies would be used for creating online systems for bidding, monitoring and management of smart grid, electricity market and consumer services. Smart meters provide communication (TCP/IP) between customer and supplier. Many smart devices using embedded technologies would become part of smart grid [1]. In the new system utility firms once consolidating the customer's orders will decide the optimum generation and distribution scheme to satisfy customer's demands. A virtual energy provisioning system might improve the stability and reliability of the electrical grid that is progressively integrated with distributed energy resources. The new system could permit customers to directly order the electricity via the web in terms of power needs and time of usage.

Smart grid provides numerous opportunities for generators, market operators and customers to work and manage the sophisticated energy infrastructure. Customers will get cash discounts, marketers would be able to create a reliable dispatch scheme; and generators would maximize their asset utilization and profit. Customer would get opportunity to select energy supplier as and when he/she desires via web [2]. Power would be transmitted on the same distribution line for all service suppliers and calculation of power flow and revenue share are going to be determined based on software system applications. Massive amount of information from generators, distributors, customers and retailers, would need it to be stored and moved safely. Thus security and as privacy of information/ data is of utmost importance.

II. SMART GRID WORLD WIDE AND INDIA

Smart grid has been implemented in many countries worldwide and their status in different countries are shown below in table 1 [3], [4], [5], [6] and [7]. In 2003 the Electricity Act 2003 was passed in India. After this the traditional Indian Power System is transformed to restructured Power System paving the way for the automation of Power Grid. Indian power system is operated as five Regional grids viz. Southern Regional grid (SR), Western Regional grid (WR), Northern Regional grid (NR), Eastern Regional grid (ER), and North Eastern Regional grid (NER). In addition to this India have 31 state grids and more than 100 area-wise grids. To control the grid there is a hierarchical system as shown in fig. 1.

Market operation is coordinated by Market operators along with RLDCs [1]. Use of information, electronics & communication technology (IECT) paved the way for conceptualization of "Indian Smart Grid" by integration of large scale generation, distributed energy resources, transmission and distribution system to improve the operation and control of power grid [8]. Smart grid implementation in India includes followings [9]:

- Advance metering infrastructure (AMI)
- Smart meters and sensors
- Metered data transmission network system
- Metered data management
- SCADA applications and data transfer network.
- Intelligent electronic devices (IEDs) applications
- Peak demand reduction in distribution systems
- Voltage regulation system
- Demand response from Industry and home users

TABLE 1 SUMMARIZED R STATUS OF SMART GRID IMPLEMENTATION IN DIFFERENT COUNTRIES

Country	Smart grid status
Italy	Italy was the first country to adopt the smart grid technology. Most of the electricity customers are provided with smart metering system.
Denmark	Denmark has adopted smart metering by most of the electricity distribution system operators.
Finland	Finland has 100 percent installation of hourly metering and settlement system in the country.
France	France has already rolled out its nationwide implementation of smart meters.
Spain	In line with new regulations, Spain had planned to deploy 10 million smart meters in the country.
Ireland	A nationwide program has started for the deployment of smart meters from 2013.
The Netherland	A two-year trial period to roll out the smart metering was initiated as per the legislation adopted by the Dutch parliament in July 2008. The Country has already installed over100000 residential smart meters.
UK	The roll out of dual-fuel smart metering for 27 million households started in October 2008 which is likely to be completed by 2021.
Germany	The German power utility announced in February 2008 that it will install approx. one million smart electricity meters.
China	The China has announced to develop a national smart grid by the year 2020.

Indian power sector is one of the biggest in the world, with a capacity of 156,092.23 MW. It has 4th place in installed

capacity and 6th place in energy uses, globally. Energy demand for India has reached to 157,107 MW in the year 2012. India's rising population and growing economy need a rise in energy demand from 800,000 MW to 950,000 MW by the year 2030. India's huge energy supply-demand gap and its high losses have sought attention of the Government and other stakeholders in the smart grid. Indian stakeholders are required to take active interest in design and implementation of smart grid; they must acquire the required skills and invest in development of human resources in this area. At last but not least, Indian smart grid also requires standards and specifications for the smart grid. The priority areas should be:

- Advanced metering infrastructure
- Communication network Infrastructure
- Efficient electricity transportation system
- Energy storage systems
- Demand response
- Energy efficiency
- Distributed and hierarchical management of smart grid
- Setting up of cyber security policies, infrastructure and management system

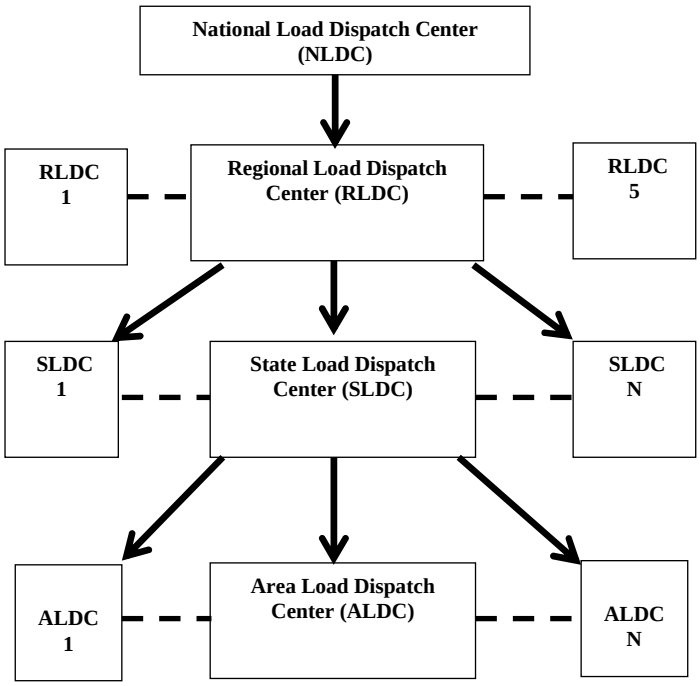

Fig.1: Hierarchical Grid Control System in India

III. COMMUNICATION ISSUES IN SMART GRID

Smart grid would allow the power producers, distributors and consumers to have real-time awareness of operating requirements and capabilities of one another hence smart grid would be able to generate, distribute, and use the electricity very efficiently. In smart grid several electrical devices, sensors, smart meters etc. would be connected to one another in a complex way, reporting back their status of power consumption, health condition and other signals via appropriate communication protocols. There would be many challenges in the design of the smart grid communications network where electrical devices and smart meters would be exchanging information related to continuously changing power requirements [10]. Various communication media which may be used in smart grids are:

- Optical Fiber network
- Wireless Radio network
- Zig-Bee network
- Cellular network (2G, 3G, 4G, WiMAX)
- Satellite network (GSM/ GPRS)
- Power line Communication (PLC)
- Advanced Digital Subscriber Lines (ADSLs)

The smart grid communication systems can be abstracted to four layers such as field layer, network layer, transport layer, and application layer. Field layer includes remote terminal unit, intelligent electronic device, information collection terminal, smart meters, and smart devices. Network layer would be consisting of wired or wireless network using low range media and switching devices used in LAN. Transport layer would include the wired or wireless network of long range communication such as optical fiber, power line communication, and mobile network and routing devices used in wide area network. Control and information system of master station of smart grid would be the application layer [11].

In smart grid communication network the transmission and distribution substations and control centers can be connected to one another in a meshed network, which can be built over optical fiber technology. The communication architecture for the lower distribution network may be divided into a number of networks arranged in hierarchical network architecture. Smart meters can be deployed in such architecture which is part of advanced metering infrastructure (AMI) for enabling automated two-way communication between various layers of network. These Smart meters would be equipped with power reading capability and would also work as communication gateway using Internet Protocol (IP) based communication [10].

A huge amount of raw data is collected by smart meters, sensors, phasor measurement units (PMUs) from different part of the smart grid and being send continuously to the central computation system. Subsequently, this considerably big amount of unstructured data must be processed, analyzed and stored in a cost effective ways. An enormous amount of computing, storage and software services must be provided to compute this vast amount of data and produce some valuable information in least possible time. Many technologies such as distributed and parallel computing,

Grid computing or cloud computing may be utilized for this purpose. Cloud computing and big data analysis looks very promising for the future of smart grid [12]. This allows distributed power generation such as local solar and wind generation and also promises higher efficiency in the power distribution system. Scalability and fast communication is crucial for practical deployment of smart grids into home and building automation. Communication in smart grid must be private and secure as many autonomic functions that would run over it might be critical to grid operations. It is very important to design and deploy the future communication architecture for smart grid which is interoperable, scalable, self-organizing, and secure against cyber-attacks [10], [13], [14], [15] and [16].

IV. CYBER SECURITY ISSUES IN SMART GRID

Increasing interconnection of smart grids additionally will increase the exposure of grid to potential attackers and/or unintentional errors. Networks that connect more often to totally different networks introduce most common vulnerabilities which will span multiple smart Grids and increase the possibilities of failures. Different variety of interconnections invites additional denial of service attacks, malicious code, compromised system and intrusions. Because the variety of nodes will increase within the network, the amount of entry points increase which can be used by potential adversaries for exploitation. Extensive information & data collection their flows might broaden the potential for compromises of information and data and breach of confidentiality and client privacy.

Components of good grid security includes physical elements and management applications, cyber infrastructures needed to support necessary designing, operational and market functions, cyber-attacks and its impact on the system, actions and measures to mitigate risks from cyber threats. Risk assessment to understand the potential of unwanted outcome ensuing from internal or external factors, as determined from the probability of occurrences and also the associated consequences is important to attenuate unacceptable risk levels by applying risk mitigation solutions. This might be performed through the preparation of a lot of sturdy supporting cyber security infrastructure or applications.

A. Cyber Security issues in Generation

Power generation management primarily involve managing the generator power output and terminal voltage by applying local automatic transformer (AVR) and governor control (GC) schemes. AVR and governor control don't rely on the supervisory control and data acquisition (SCADA) transmission infrastructure for its operations as each the terminal voltage and rotor speed are detected locally. Albeit these applications are susceptible to malware that would enter the station local area network (LAN) through different entry points like USB keys. Additionally associates working in company may compromise plant cyber security mechanisms to gain an entry point into the native local network and may disrupt normal operation by corrupting the logic or settings within the digital controllers. The automatic generation control (AGC) is a secondary frequency management that's involved with fine controlling the system frequency to its nominal value [17] and [18]. The AGC depends on tie-line and frequency measurements provided by the SCADA mensuration system. An attack on AGC may have direct impacts on system frequency, stability and operation. Denial of service (DoS) style of attacks might create a big impact on AGC operation once supplemented with another attack that needs AGC operation.

B. Cyber Security issues in Transmission

Power system state estimation [19] is used as a technique by that estimates of system variables like voltage magnitude, phase angle (state variables) and power flows on totally different sections are calculated based on likely faulty measurements from field devices. The control center application performs computations by making use of large no. of measurements it receives via wide-area network. False information injection attacks, that escape detection by existing faulty measurement identification algorithms, could also be dangerous.

The reactive (VAR) compensation with FACTS devices [17] is the method of controlling reactive power injection or absorption in a power grid to boost the performance of the transmission network. FACTS devices interact with each other to exchange operational data via communication link. It can face Denial of cooperative operation that may be a DoS attack. During such attack, the communication to some or all the FACTS devices might be stopped by flooding the network with unwanted packets. This may end in the loss of vital data and therefore have an effect on semi-permanent and dynamic management capabilities. De-synchronization (timing-based attacks) might disrupt steady operation of Cooperative FACTS devices (CFDs).

False data injection attacks [20] may well be utilized to send incorrect operational information like status and control data. This might lead to uncalled-for reactive power compensation and in unstable operational conditions. The phase angles of voltage phasors measured by PMUs directly facilitate the computation of real power flows within the network, and will therefore assist in decision making at the central control unit. Any attack on WAN backbone is going to be a danger to PMU.

C. Cyber security and distribution system

Modern relays are internet protocol (IP) capable and support various communication protocols [21]. Cyber-attack on the communication set up or malicious amendment to the control logic might end in unexpected tripping of distribution feeders, resulting in load segments not served.

Advance metering Infrastructure primarily depends on the deployment of good smart meters to supply real-time meter readings. Smart meters offer utilities with the flexibility to implement load management & control (LMC) to disable control devices once demand spikes. The capability to remotely disable smart meters through load management shift provides potential threats from attackers.

Embedded systems are used heavily in the grid to support observance and management functions. Intelligent electronic devices (IEDs) are placed to control relays throughout the grid [22]. Recent events have shown that IEDs are often maliciously reprogrammed to halt intended management functions. Deployments of embedded devices at large scale in smart grid additionally incentivize the employment of cheaper hardware leaving very little computing capability to support varied security functions like malware or intrusion observance. The deployment of secure computation within embedded platforms provides a key challenge to cyber security.

D. Cyber security in communication network of Smart grid

Cyber security [17] inside the communication network is known as protection of data and systems from unauthorized access, disclosure, modification, destruction or disruption. The objectives of Cyber security are confidentiality, integrity and availability. These 3 objectives need to be ensured altogether in various stages of data processing (i) storage state in storage media (ii) processing state in RAM and (iii) transmission state in communication media.

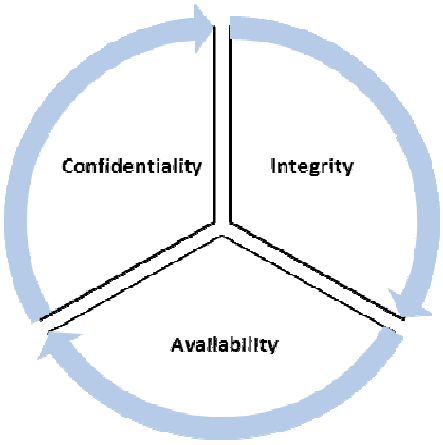

Fig. 2: Three Objetives of Cyber-security in Smart Grid

Confidentiality is outlined in literature as protection of data from unauthorized access or revelation. The authorized users only ought to get access to data and un-authorized ones ought to be prevented from doing this. Integrity is defined as protection of data from unauthorized modification or destruction. It's necessary to make sure that the data and information and system containing information is correct, non-corrupted and complete. Availability refers to the protection of data and information systems from unauthorized disruption. It is important to make sure the timely and reliable access to and use of data and information systems. The graphical representation of the 3 objectives of the cyber-security in smart grid is shown in fig. 2 above.

Other cyber-security concerns are authentication, identification authorization, access control, non-repudiation and privacy of data and user's information. Other than this auditability and reliability of data and information is also very important. Some of the important cyber-security features are shown graphically below in fig. 3. It is must to implement the features listed in fig. 3 in the smart grid for secure and reliable operation of the grid.

There are several threats to the ICT infrastructure of smart grid and it regularly faces many types of attacks. Some of the Security threats and attacks to ICT infrastructure of Smart grid is shown in fig. 4 and fig. 5 respectively. Other than the tools and techniques mentioned in table 2, many management, audit, measurement, monitoring, and detection tools are used for better management of cyber-security in the communication network of smart grid as shown in the fig. 6 below. It is difficult to respond these attacks as the ICT system is designed for trust and without authentication. Also it is evolving as it is being employed for uses beyond design. Some cyber security features and tools/ techniques for their implementation as listed below in table 2 can be practiced based on the risk assessment of the system [23].

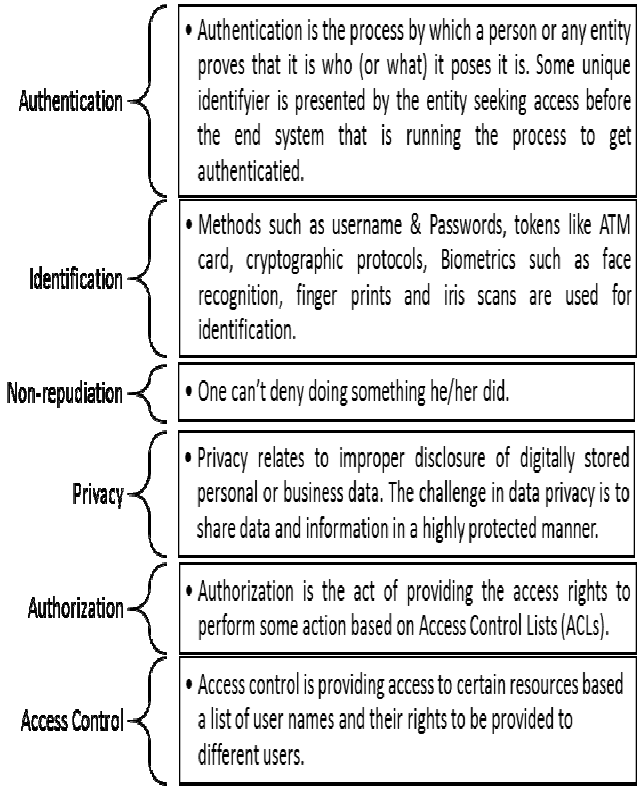

Fig. 3: Features of secure Smart grid

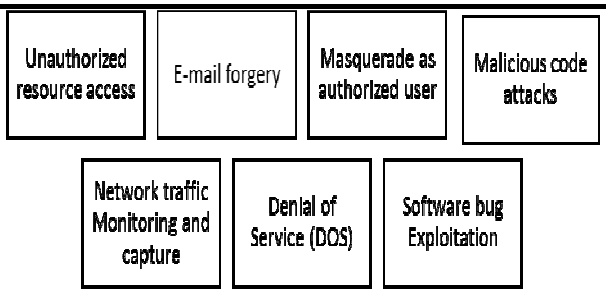

Fig. 4: Security threats to ICT Infrastructure

Fig. 5: Cyber-attacks on ICT infrastructure

TABLE II CYBER SECURITY FEATURES AND METHOD OF IMPLEMENTATION IN SMART GRID

Cyber-security feature	**Cyber-security techniques/ tools**
Confidentiality	Encryption Data Separation Symmetric Key Encryption Public Key Encryption Virtual Private Networks (VPNs)
Integrity	Digital Signatures Message Integrity Safeguards Time Stamping
Availability	Protection from attack Protection from unauthorized users Resistance to routine failures
Identification	User ID and passwords PIN number Biometric
Authentication	Secure Tokens Smart Cards Single Sign-on Password Authentication Challenge/Response Authentication Physical/Token Authentication Smart Card Authentication Biometric Authentication Location-Based Authentication Device-to-Device Authentication
Authorization	Certificates Attribute use Role-Based Authorization Tools
Access Control	Role-based Access Control Passwords Network Firewalls Host-based Firewalls Virtual Networks Physical Protection Personnel Security
Non-repudiation	Digital Signatures Time Stamping Certificate Authority

The development of a secure and reliable smart grid requires a clear understanding of potential risks and impacts resulting from cyber-attack on smart grid [24]. Estimation of risk and impact requires an evaluation of the dependency of smart grid system on the Information and Communication Technology (ICT) infrastructure and its ability to continue the operations in presence of potential cyber-attacks [25]. Regular evaluation of the cyber–physical relationships of smart grid with its ICT infrastructure and specific review of possible attack vectors is important to determine the effectiveness and reliability of the cyber security system in place.

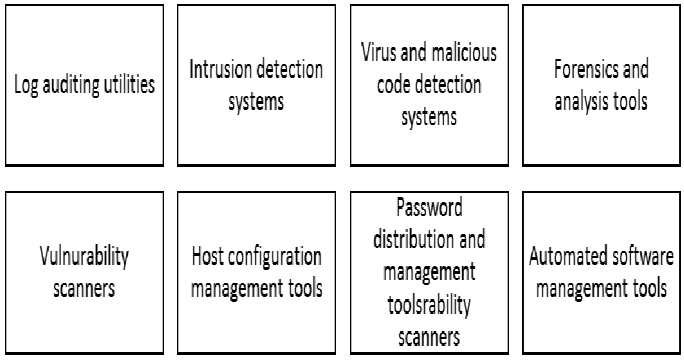

Fig. 6: Cyber-security management tools in Smart grid

V. CONCLUSION

Many countries in the world have moved towards making their power grid smarter and others are in the process. With increasing integration of many regional grids across the globe would make it possible to form power cloud where power can be drawn from the cloud in any amount at any time and place. This would necessitate storage and movement of large chunk of data, high speed network connectivity of various systems in power grid, use of smart devices and high speed computing techniques to handle the complexity and size of the smart grid.

Many new scalable communication architecture, protocols and software need to be designed and developed to handle the real time requirements of operation and control of smart grid. It would also require that policy, procedures and technologies are identified and implemented to operate the smart grid in a secure and reliable manner.

Estimation of potential risk and its impact assessment on the business continuity of smart grid system would decide the appropriate tools and technologies to be put in place for mitigation of potential cyber-attacks on the smart grid. By making correct choices it is possible to run the future smart grid in an efficient, secure and reliable manner as it is important for sustainable growth.

REFERENCES

[1] Xiang Lu, Zhuo Lu, Wenye Wang and Jianfeng Ma," On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP", 978-1-4244-9268-8/11/$26.00 ©2011 IEEE

[2] Tongdan Jin, Mechehoul M., "Ordering Electricity via Internet and its Potentials for Smart Grid Systems, " Smart Grid, IEEE Transactions on, vol.1, no.3, pp.302-310, Dec. 2010

[3] Jingjing Lu, Da Xie,and Qian Ai," Research on Smart Grid in China ",IEEE T&D Asia 2009

[4] V S K Murthy Balijepalli, S A Khaparde, R P Gupta," Towards Indian Smart Grid", 978–1–4244–4547–9/09/$26.00 ©2009 IEEE

[5] Arup Sinha, S.Neogi , R.N.Lahiri, S.Chowdhury, S.P.Chowdhury , N.Chakraborty, "Smart Grid Initiative for Power Distribution Utility in India ",978-1-4577-1002-5/11/$26.00 ©2011 IEEE

[6] Mohsen Fadaee Nejad, AminMohammad Saberian, Hashim Hizam, Mohd Amran Mohd Radzi, Mohd Zainal Abidin Ab Kadir ,"Application of Smart Power Grid in Developing Countries", 978-1-4673-5074-7/13/$31.00 ©2013 IEEE

[7] The Smart Grid Vision for India's Power Sector: A White Paper

[8] Yong Wang, Da Raun, Dawn Gu, Jason Gao, Daming Liu, Jianping Xu and Fang Chen," Analysis Of Smart Grid Security Standards", 978-1-4244-8728/11/$26.00©2011 IEEE

[9] Arup Sinha, S.Neogi, R.N.Lahiri, S.Chowdhury, S.P.Chowdhury, N. Chakraborty, "Smart Grid Initiative for Power Distribution Utility in India ",978-1-4577-1002-5/11/$26.00 ©2011 IEEE

[10] Zubair Md. Fadlullah, Mostafa M. Fouda, and Nei Kato, Akira Takeuchi, Noboru Iwasaki, and Yousuke Nozaki,"Toward Intelligent Machine-to-Machine Communications in Smart Grid" IEEE Communications Magazine, April 2011, 0163-6804/11/$25.00 © 2011 IEEE

[11] International Telecommunication Union, "ITU Internet Reports 2005: The Internet of Things", 2005

[12] Berthold Bitzer, Enyew Sileshi Gebretsadik, "Cloud Computing Framework for Smart Grid Applications", 978-1-4799-3254-2/13/$31.00 ©IEEE

[13] Xudong Wang and Ping Yi",Security Framework for Wireless Communications in Smart Distribution Grid", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011

[14] Vehbi C. Güngör, Dilan Sahin, Taskin Kocak, Salih Ergüt,Concettina Buccella, Carlo Cecati and Gerhard P. Hancke," Smart Grid Technologies: Communication Technologies and Standards", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 7, NO. 4, NOVEMBER 2011 529

[15] Fariba Aalamifar, Hossam S. Hassanein and Glen Takahara," Viability of Powerline Communication for the Smart Grid," 978-1-4673-1114-4/12/$31.00 ©2012 IEEE

[16] Yi Xu and Wenye Wang "Wireless Mesh Network in Smart Grid: Modeling and Analysis for Time Critical Communications", IEEE Transaction on Wireless Communications, Vol. 12, No. 7, July

[17] Siddharth Sridhar, Adam Hahn and Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid" Proceedings of the IEEE | Vol. 100,No. 1, January 2012

[18] Siddharth Sridhar, and Manimaran Govindarasu," Model-Based Attack Detection and Mitigation for Automatic Generation Control" IEEE Transaction on Smart Grid, Vol. 5, No. 2, March 2014

[19] Saman Zonouz, Katherine M. Rogers, Robin Berthier, Rakesh B. Bobba, William H. Sanders, Thomas J. Overbye" SCPSE: Security-Oriented Cyber-Physical State Estimation For Power Grid Critical Infrastructure"IEEE Transactions on Smart Grid

[20] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A. Emesih, and Zhu Han, "Detecting False Data Injection Attacks on Power Grid by Sparse Optimization" IEEE Transaction on Smart Grid, Vol. 5, No. 2, March 2014

[21] Higgins, N.; Vyatkin, V.; Nair, N.-K.C.; Schwarz, K.; "Distributed Power System Automation with IEC 61850, IEC 61499, and Intelligent Control," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on , vol.41, no.1, pp.81-92, Jan. 2011

[22] A. M. Gaouda, Ahmed Abd-Rabou and Abdul Rahman Dahir, "Developing Educational Smart Grid LaboratorY", 978-1-4673-6355-6/13/$31.00©2013 IEEE

[23]]Vehbi C. Güngör, Dilan Sahin, Taskin Kocak, Salih Ergüt, Concettina Buccella, Carlo Cecati and Gerhard P. Hancke, ," Smart Grid Technologies: Communication Technologies and Standards", IEEE Transactions on Industrial Informatics, Vol. 7, No. 4, November 2011, pp 529-539

[24] Tosin Daniel Oyetoyan, Reidar Conradi and Kjell Sand," Initial Survey of Smart Grid Activities in the Norwegian Energy Sector – Use Cases, Industrial Challenges and Implications for Research", 978-1-4673-1864-8/12/$31.00c 2012 IEEE

[25] Boban Panajotovic, Milan Jankovic, Borislav Odadzic," ICT and Smart Grid", 978-1-4577-2019-2/11/$26.00 ©2011 IEEE.