DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4538

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

NOVEL RISK ASSESSMENT FRAMEWORK FOR SMART GRID

Dr. Ravinder Kumar
HMRITM Affiliated to GGSIP University,
Delhi Research,India

Anil Kumar
Scholar, USICT, GGSIPU,
Dwarka, Delhi,India

Abstract: Smart Grid is referred as next generation power system, and considered new revolutionary changes in existing traditional power system. Information Communication and Technologies (ICT) Integration in power grid enhance efficiency and reliability of future power systems. Power sector requires a secure distributed intelligence and customer demand based response along with an effective reusability of renewable energy resources. Despite, many silent features of Smart Grid, cyber attack risks are threatening the smart grid security. Malicious activities could be harm smart meters in distributed system and take out the power system in simulated attacks. Cyber attacks against Critical Infrastructures, like as Smart Grids, are especially dangerous, because they are tailored to disrupt assets, which are essential to the functioning of the society as whole. Critical Infrastructure sectors include Transportation, Communication and Technology utilities. Among these, the power system is possibly most critical, due to its strong dependency of all other Critical Infrastructures and involvement of Information Communication and Technology.

Keywords: Cyber Security; Smart Grid; Vulnerability; Risk Assessment.

I. INTRODUCTION

In past decade, the development of power grid has not been keeping pace with industrial growth and social advancements that drastically increase the demand of power supply. In India, total electricity generation is around 796 TWh to 1050 TWh during the period of 2008 to 2012 at the rate of 7.2 % per annum while country power consumption requirement is more than that. Despite, fourth largest electricity consumer, India's per capita electricity consumption is far below i.e. 875 kWh per head (at a population of 1.2 billion) while U.S average electricity consumption is 11900 kWh and 6600 kWh in German citizen, and global average consumption is 3000kWh. [1]. Overall generation of electricity in the country has been increased at the rate of 5.64 per cent between the period of 2014-15 to year 2015-16[2].Indian Government, Ministry of power has announced 14 smart grid pilot projects that will be implemented by state - owned distribution utilities. These projects will provide the functionalities of Advance Metering Infrastructure Residential (AMI R), Advance Metering Infrastructure Industrial (AMI I), Peak Load Management (PLM), Outage Management System (OMS), and Power Quality Management (PQM) [3].

In U.S energy production and consumption has been increased approximately three to four times, respectively. In order to cope up with power sector demand and supply unbalance in the world, one major challenge is to efficiently manage a variety of energy resources. In 30Th -3July, 2012 power system failure occurred due to lack of inadequate co ordination between demand and supply of transmission outages that affected that affected millions of people in India. Many major Power Grid transmission lines have been taken offline from last two three days. Same things happened in north India in the Middle of summer as demand exceeded local supply and this excessive demand tripped no transmission lines. Within fraction of second, ten additional transmission lines were also tripped in rest of India, which took overall blackout in the country and makes worsened conditions in the country. A review committee has been setup for finding this blackout reason in the country and submitted a report, which mentioned that lack of poor coordination of outages, inadequate infrastructures and lack of regional support [4,5].In U.S.A, according to federal databases available at the department of Energy (DOC) and North American Electric Reliability Corporation (NERC), electric power grid losses 285 percent more than in1984 and endures more blackouts than any other developed nation, led to approximate billions of dollars in economic losses in per blackout event. The root causes of increasing blackouts are aging infrastructure and lack of poor modernization in the power sectors. Apart from this now, new it based risk are involved such as cyber attacks are increasing drastically and extremely impacts on the power sectors [9].

National Institute of Standards and Technology (NIST) provides national efforts for development of power system referred to as the Smart Grid [5]. The IEEE has described smart grid as "a next generation electrical power system that is symbolized by the increased use of ICT technology in the generation, delivery and consumption of electrical energy". The success of smart grid is evaluated if it provides suitable, reliable electric power to its stakeholders [6].

Critical Infrastructure (CIs) , such as power grid includes other major sectors like distribution and transmission of energy telecommunication networks, gas and water supply and distribution systems are complex in nature and made of different dependent and interacting components, provided an optimal, consistent and efficient and reliable services as whole to the society[17]. Infrastructure is known o be a a critical if its incapability, inadequacy and destruction have directly or indirectly impact in large scale to the health, safety, security, and economy of country and its social being[9]. Critical Infrastructure are complex, and its complexity drives from numbers of characteristics, in which heterogeneity of components, scalability, and dimensionality of connected components play the major role to make it complex[10,11,12,13]. Other, Critical Infrastructures complexity is self-organize and decomposability. Decompose means divide the complete system into sub system and related components. Smart power grids contain the structure decomposability of critical complex infrastructure. Self-organization feature means that any complex system has a capability to re-organization its isolated elements and subsystem into well coherent patterns without any intervention and involvement of central/ external authority [17, 18].

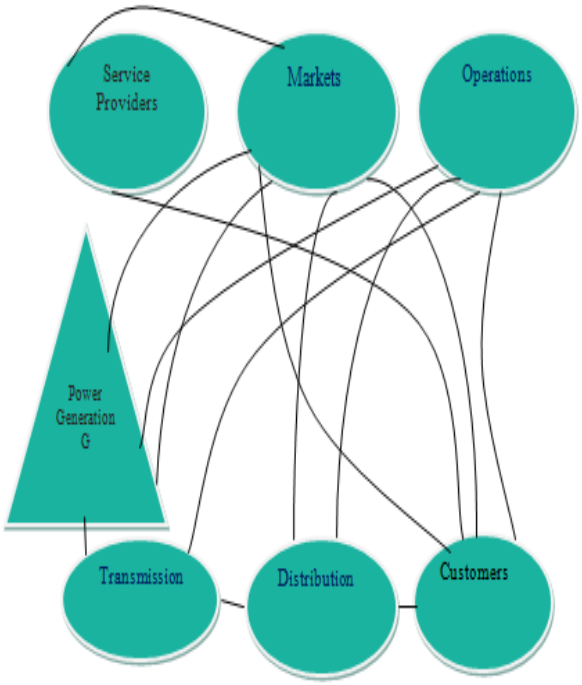

Figure 1. Smart Grid Architecture.

Disassemblies of a complex system into subsystem allow understanding every component but on the other hand it may also create more vulnerabilities and difficult to control and manage. Vulnerability situation due to decomposability arise stiffness and instability in Smart Grid. Smart grids, includes smart meters, provide the facilities of an efficient management of energy. Smart grid extends the capability of traditional power grid to make reliable, greens and cheaper electric power to the consumers. The Various subsystems of smart grid control by modern information and communication technology via internet. Smart grid, critical infrastructure are targeted by adversaries to disrupt the life and property that depend up it [18].The major aim of security is to provide confidentiality, integrity and availability of critical infrastructure and assets. Although, each asset requires different level of protection and smart grid is not an exception. In smart grid security control mechanisms implement one or more than one type of protection level and all risks, threats and vulnerability are measure their potential capability to compromise or all of CIA principles.

In many information security literature words vulnerability, threat, risk and exposure are interchanged, yet they have different meaning. Vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be a hardware or software or in both, procedural or human weakness that can be exploited in the smart grid system. A threat is any potential danger that is associated with the exploited of vulnerability. A risk is likelihood of a threat agent exploiting vulnerability and the corresponding business impact. The availability protection related to the availability and timely access of resources and data to an authorized network devices and individual. Integrity is implied when the assurance of the accuracy, reliability of information and system is provided and any authorized modification is prevented from the original data. Software and Communication network should work in such a way that data are processed and maintained correctly, without any alteration data can move from source to destination. System must be protected from outer interference and contamination. Confidentiality provides that the secrecy level is applied at each junction of data processing and unauthorized disclosure to anybody. These levels of confidentiality not only prevail while data resides on systems and devices part of that network but also the networks of destination machine/network. In this paper, we illustrate introduction of smart grid, cyber attack. Current smart grid scenario in India and other countries in section I section II includes related work of cyber security and standard for smart grid while section III illustrated risk assessment, section IV elaborated proposed risk assessment framework and in last we conclude and describe further scope in this field paper in section V.

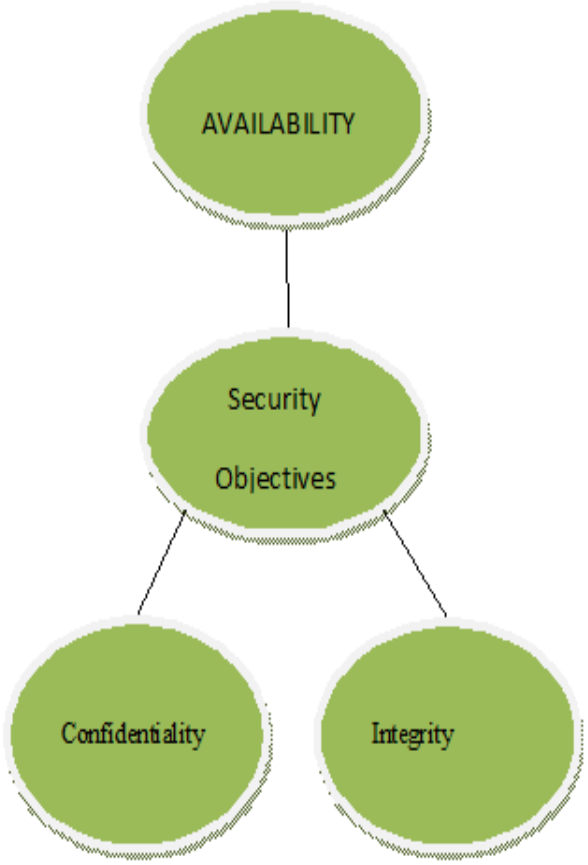

Figure 2. Security Basic Principle

II. RELATED WORK ON CYBER SECURITY AND STANDARDS

The IEEE defines electronic intrusions as an entry of unwanted elements into system via electronic devices or telephone lines or other electronic media for the manipulation or disturbance of electric devices in distributed system. These devices may include digitals relays, equipment diagnostic packages, fault recorders, programmable logic controllers, automation equipments and communicational interfaces [19]. Smart grid standard include draft guide, interoperability among the energy technology and ICT operation with End- User Applications and Electric Table 1: Security objectives of Smart Grid Communication Power System (EPS) [19]. IEEE also defines (SCADA) Supervisory Control and Data Acquisition system and cryptographic protocols for smart grid protection and Industrial Control. The National Institutions of Standards

and Technology (NIST) published the document titled System Protection Profile Industrial Control Systems which covers the risks and objective of SCADA systems (NIST, 2004) [21]. In 2005, the National infrastructure security coordination Centre (NISCC), previously known as Centre for Protection of National Infrastructure, published practical guideline to implement firewall deployment in SCADA [26]. In 2008

NIST, updates its new comprehensive guidelines on technical, operational and management security controls further these guidelines were updated in NIST, 2011. In 2013, European Union Agency released for Network and Information Security recommendation for Europe on SCADA Model. Although, Modern SCADA system is highly complex, sophisticated and totally based on advanced technology system, but faces the cyber threats due to its multi-components architecture. In last decades, several cyber attacks took place on Critical National Infrastructure (CNI) and SCADA. In [24] illustrated that hacker penetrated the operating system of power grid treatment facilities in USA. In [19] described global energy and oil firms were targeted by attacks including Trojans and window based exploits and number of cyber attacks on CNI increase in last few years in[20]. Presented that around 162 incidents were listed in RISI (Repository of Industrial Security Incidents) and around 10 new incidents were added in every quarter. In [21] described a larger number of experts had confirmed that cyber threats in SCADA system are escalating in last few years. In [22] illustrated that risk assessment must answers following questions:

What wrong with system?
What are affects of these risks?
How to manage these risks?
Which are the corrective and preventive actions has been taken?
What options are available to mitigate these risks?
What are the impacts of current management decision for future options?

In ISO/ IEC 27005, 'Risk Assessment' includes both 'Risk Analysis' and 'Risk Evaluation'. Risk Analysis is then further divided into Risk Identification' and 'Risk Estimation'. In SP 800-30 by NIST, ' Risk Management is said to encompass of three processes, namely 'Risk Assessment', 'Risk Mitigation' and 'Risk Evaluation'. European Network Working Group(WG) define Risk Management includes 'Definition of Scope' 'Risk Assessment', 'Risk Treatment, 'Monitoring' and Communication while Society of Risk Analysis defines Risk Analysis consist of ' Risk Assessment' , Risk features', Risk Communication' , 'Risk Policies' and Risk Management. So in one definition risk assessment encompasses risk analysis while in another it is reverse. In [25] Expert Group of European Commissions' Smart Grid Task Force collected data Protection and Impact Assessment Template for Smart Grid and Smart Metering and working group emphasized that attack and threat are not clearly defined As elaborated in table1, Communication in Smart Grid flow is mainly device in two parts: Command Control and Market. Command control is deals with related devices and services plus command data while market is deals with meter data, information privacy and price of unites.

In above state of arts showed that risk assessment on smart grid system must be solved on priority bases because it can be affected in large scale, as smart grid is also part Critical Infrastructure Assets.

Table 1: Security objectives of Smart Grid Communication

Security	***Communication***					
	Command Control			***Market Attributes***		
	Device Data	***Service Data***	***Command Data***	***Meter Data***	***Privacy***	***Price***
Integrity	L	L	H	L	L	L
Confidentiality	M	L	M	M	H	H
Availability	L	H	M	L	L	M

III. RISK ASSESSMENT

One of the popular ways to estimate the impact of cyber attack on the smart grid is developing risk assessment. A new methodology should be matched as defined in NISTIR and SCADA Standards for smart grid. In NISTIR risk can be calculated as product of Vulnerability, threat, and consequences. [15]

Risk = Vulnerability * Threat* Consequences.

Or

Risk = Uncertainty of variables * Consequences.

In smart grid domain above equation can be formulated as given below:

$$R=P_A (1-P_E)*C \quad (1)$$

Where R represent level of risk and PA represents uncertainty of variables and consequences are dented by C. It range must be within 0 and 1. Total probability of the smart grid is attacked can be evaluated as if probability of attack is 100% than P_A value is 1. P_E is probable effectiveness of security system and (1- P_E) measures lack of security mitigation. C is a value between 0 and 1 that rates the consequences of successful attacks. PE may be expanded to

$$P_E = P_I * P_N \quad (2)$$

PI denotes the probability of interception and P_N is probability of neutralization of given threats.

IV. PROPOSED RISK ASSESSMENT MODEL OF SMART GRID

Till now , the quality of cyber security risk assessment on smart grid projects has generally not as sufficient [17].This new proposed framework of cyber security provides an efficient risk assessment conduct of risk assessment efficiently for smart grid consumers and all its stakeholders. Proposed framework comprises no of steps includes: risk identification; risk analysis; risk planning; risk evaluation; risk management; risk monitoring. These steps are elaborated in as below:

4.1 Risk Identified: In risk identification step is used to identify all related threats, vulnerability and unwanted incidents. Using this identification of threats ensure stakeholder that risk might be extracted.

4.2 Risk Analysis: Risk analysis includes analysis of vulnerability.

4.3 Risk Evaluation: In risk evaluation steps involves assigning like hood level to the identified unwanted incidents; assigning severity level of the identified harm; assigning risk value and arranges the risk according to priority levels. In risk evaluation steps the harmful impact incident are evaluated on bases of risk severity and likelihood. Severity and likelihood lists assigned numeric values.

4.4 Risk Planning: Risk planning steps of risk assessment framework of smart grid includes level of risk acceptance while allowing for uncertainties; identification and evolution of existing risk controls; review and select other suitable controls; identified new risk and evolution of residual risk; Risk planning further measures transferring risk and acceptance risk and identification of contingency measures.

4.5 Risk Management: In risk assessment framework involves risk management process for taking decision. Risk management step includes detailed planning and implementation and testing of risk in smart grid.

4.6 Risk Monitoring: In risk assessment framework for smart grid required to update and monitoring the system.

Figure3. Risk assessment Framework for Smart Grid

V. CONCLUSION

The most important elements in smart grid security are detection of threats and vulnerabilities. In this paper, we proposed a risk assessment smart grid framework which includes many steps for improving smart grid security. Framework start with risk identification and its characterization then detect impact of risk on smart grid. On the bases of risk identification, framework suggests a suitable risk analysis and relative impact. Risk management takes decision to rectify the risk and monitor it continuously. In next paper, we will analysis the smart grid cyber attacks data using machine learning

REFERENCES

[1] http://www.bridgetoindia.com/blog/how-much-power-will-india-need-in- 2035 dated on 24.08.2016

[2] http://powermin.nic.in/en/content/overviewdatedon24.08.2016

[3] http://www.indiasmartgrid.org/pilot.php dated on 24.08.2016

[22] Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk analysis, 1(1), 11-27.

[23] Chittester, C. G., & Haimes, Y. Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. Journal of Homeland Security and Emergency Management, 1(4).

[24] Guan, Y., & Kezunovic, M. (2011). Grid monitoring and market risk management. IEEE Intelligent Systems, 26(2), 18-21.

[4] http://blog.ucsusa.org/mike-jacobs/2003-northeast-blackout-and-13-of-the-Largest-power-outages-in-history-199, date on 25.08.2016

[5] www.cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf

[6] http://www.ibtimes.com/aging-us-power-grid-blacks-out-more-any- other- developed-nation-1631086, date on 25.08.2016

[7] Rouse WB (2003) Engineering complex systems: implications for research in systems engineering. System Cybern Part C Appl Rev IEEE Trans 3(2):154–156

[8] Ottino JM (2004) Engineering complex systems. Nature 427(6973):399

[9] Kro¨ger W (2008) Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools reliab Eng Syst Saf 93(12):1781–1787

[10] Gheorghe AV, Schlapfer M (2006) Ubiquity of digitalization and risks of interdependent critical infrastructures. In: Systems, Man and Cybernetics, 2006.

[11] SMC'06. IEEE International Conference on, 1: 580–584

[12] Rinaldi SA, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21(6):11–25

[13] Chou CC, Tseng SM (2010) Collection and analysis of critical infrastructure interdependency relationships. J Comput Civil Eng 24(6):539–547

[14] D'Agostino G, Bologna S, Fioriti V, Casalicchio E, Brasca L Ciapessoni E, Buschi S (2010) Methodologies for inter-dependency assessment. Critical Infrastructure (CRIS), 2010 5th International Conference on, pp 1–7

[15] Granic I, Lamey AV (2000) The self-organization of the Internet and changing modes of thought. New Ideas Psychol 18(1):93–107

[16] Billinton, R., G. Tollefson, and G. Wacker. Assessment of Electric service reliability worth. in Probabilistic Methods Applied to Electric Power Systems, 1991., Third International Conference on.1991.

[17] Lockstep Consulting, Privacy Impact Assessment Report – Advanced Metering Infrastructure (AMI), Victoria, Australia (2011).

[18] NRECA, Guide to Developing a Cyber Security and Risk Mitigation Plan, National RuralElectric Cooperative Association/Cooperative Research Network,

[19] Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents.In Proceedings of the 1st Annual conference on Research in information technology (pp.51-56). ACM.

[20] Tudor, Z., & Fabro, M. (2010). What went wrong. In A study of actual industrial cyber security incidents. Industrial Control Systems Joint Working Group (ICSJWG) spring conference.

[21] Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. Engineering Management Journal, 25(2), 38-45.

[25] Yesudas, R., & Clarke, R. (2013, September). A framework for risk analysis in smart grid. In International Workshop on Critical Information Infrastructures Security (pp. 84-95). Springer,

[26] Cham.Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. computers & security, 56, 1-27. Arlington, VA (2011)