ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

Smart Grid: Power System Control and Security

Mag. Inż. Indrajeet Prasad

M.Sc., Control in Electrical Power Engineering, Politechnika Wrocławska, Wrocław, Poland

ABSTRACT: A Smart grid is expected to be a modernization of the legacy electricity network. It Provides monitoring, protecting and optimizing automatically to operation of interconnected element. It converts from traditional centre generator and/or emerging renewable distributed generator through transmission network and distributed system to 9industrial consumers and/or home users with their thermostats, Electric vehicles and intelligent appliances. This paper discusses on general aspects of smart grids and focuses on some smart grid features at distribution level like interconnection of distributed generation and active distribution management, using automated meter reading (AMR) systems in network management. In this paper, physical and cyber security issues for smart grid distribution systems are discussed, including vulnerabilities and security needs. An intelligent distributed control architecture is then presented to provide distribution systems with greater protection against threats and with the ability to quickly respond to attacks and disturbances. This vision is expected to be a critical part of the power system control of smart grid technology.

KEYWORDS: Smart Grid, Power system control, Power system security, Active distribution management, automated meter reading.

I.INTRODUCTION

Smart grid is a term referring to the next generation power grid in which the electricity distribution and management is upgraded by incorporating advanced two-way communications and pervasive computing capabilities for improved control, efficiency, reliability and safety. A Smart Grid delivers electricity between suppliers and consumers, home or buildings to save energy, reduce cost and increase reliability, efficiency and transparency [5].

The energy markets are in transition and there are many drivers for creating a new kind of power delivery system for the future. There are many drives and needs as follows [2]:
1. The penetration of distributed generation (DG), especially based on Renewable Energy Sources (RES), will continue due to environmental reasons.
2. The European and North American vision is to have common electricity market areas with a high penetration of distributed power generation.
3. Efficient use of energy at customer level and intelligent demand response has become an essential issue.
4. Power quality (supply reliability and voltage quality) requirements will increase due to public and regulatory actions and at the same time failure rates are expected increase due to the climate change.
5. There is a need, due to economical reasons, to increase the utilization rate of existing network. The traditional way of developing a distribution network would be the investment on passive wires which would lead to decrement of utilization rate.
6. The risk of major disturbances is increasing, both the probability and consequences. The reason for increased probability is the complexity of power network and the increased failure rate due to climate change. The consequences are increasing due to society's higher dependency on the power supply.
There are much research, and many visions and concepts for future power delivery system, like super grid, smart grid, micro grid, intelligent grid, active network, power cell etc.

A Smart grid is characterized by the bi-directional connection of electricity and and information flow to create and automated widely distributed delivery network. It incorporate the legacy electricity grid the benefits the modern communication to deliver real-time information and enable the real instantaneous balance of supply and de3mand management [5].

II. ASPECTS OF SMART GRID

Smart grid concept has different aspects as shown in Fig. 1. It includes novel solutions of infrastructure for future power distribution, e.g. use of power electronics and DC. Active resources (i.e. distributed generation, loads, storages and electricity vehicles) actually change the traditional passive distribution network to be an active one. New network solutions and active resources call for novel ICT solutions for network operation and asset management providing intelligence to active networks. Smart grids enable active market participation of customers and also have effect on changes in business environment. Smart grids are customer driven marketplaces for DG and consumers [2].

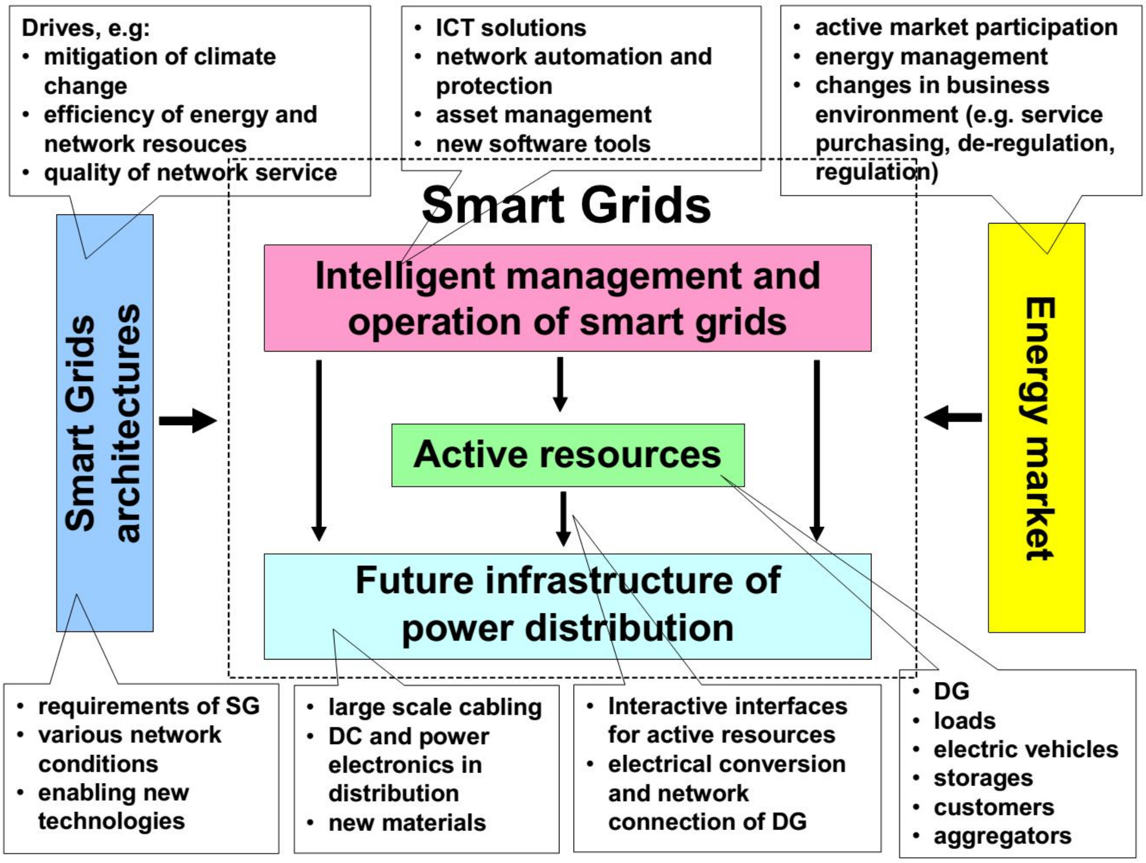
Drives, e.g:
• mitigation of climate change
• efficiency of energy and network resouces
• quality of network service
• ICT solutions
• network automation and protection
• asset management
• new software tools
• active market participation
• energy management
• changes in business environment (e.g. service purchasing, de-regulation, regulation)
Smart Grids
Smart Grids architectures
Intelligent management and operation of smart grids
Active resources
Future infrastructure of power distribution
Energy market
• requirements of SG
• various network conditions
• enabling new technologies
• large scale cabling
• DC and power electronics in distribution
• new materials
• Interactive interfaces for active resources
• electrical conversion and network connection of DG
• DG
• loads
• electric vehicles
• storages
• customers
• aggregators

Fig 1: Aspects of Smart grid [2]

The concept of smart grids may be characterized by words like flexible, intelligent, integration and co-operation. Grids are flexible because they utilize controllable resources throughout the network. Respectively the passive network has flexibility by network capacity i.e. network itself may handle all probable loading conditions. Intelligence is simply investments on protection, controllability and information and telecommunication technologies instead of pure passive lines, cables, transformers and switchgears [2].

III.SMART GRID TECHNOLOGY TRADES

Smart Grid enables two technologies that have a direct impact on the dynamic management of energy. These are; 1) microgrids and distributed energy generation and 2) transitive energy.

Micro grids are self-contained, grid-connected energy systems that generate and consume on-site power. These systems can either import power from, or export to, the grid as well as having the capability to disconnect (or island) from the grid. The decision making process required to determine the best mode of operation requires taking into consideration both local operations as well as grid operations [3].

When external power cost is relatively high, a strategy based on exporting excess power generation and minimizing imported power would be the best course of action. If the cost of external power goes below the cost of self-generated power, then maximizing the power imported from the grid while decreasing on-site generation would be a suitable strategy. If an emergency or fault occurs on the external grid, the micro grid load can be curtailed or disconnected from the grid and reconnected when conditions permit [3].

DG and existing controllable resources like direct load control, reactive power compensation and demand side integration provide a good potential as a controllable resources for the smart grids. The integration of DG and flexible loads in distribution network will benefit the network when managed appropriately. The traditional passive network management or "fit & forget" principle in DG connection needs to be changed into active network management. The integration of DG and other active resources into a distribution system is a requirement in order to fully exploit the benefits of active resources in network management. With proper management of active resources the overall system performance may be improved from presently used practices [2].

One important control task in power systems is to maintain balance between power production and consumption which means keeping power system’s frequency at an appropriate level. This process is becoming more and more challenging due to increase of penetration level of intermittent power production, for example wind and solar power.

Today’s centralized control of the power grid will evolve toward distributed control with more localized, autonomous decision making. These decision-making “software agents” will interact with other agents to optimize the energy utilization of connected devices and systems. These interactions, known as transitive energy, will be in the form of transactions with other systems which will be based on local economics and context. Transitive energy does not change the requirement that the power grid must operate in a stable state of equilibrium with supply equal to demand. Autonomous market-driven behaviour creates system oscillations and instabilities through positive reinforcing feedback cycles. This behaviour can be very detrimental for grid-scale operations and must be managed proactively to avoid negative side effects [3].

IV. ACTIVE DISTRIBUTION MANAGEMENT

The production of electricity close to consumers will reduce the transfer of electricity. This will also affect network losses. Network losses may also increase when a large DG unit, e.g. wind farm, is located far from consumption and the electrical distance of transferred electricity increases compared to situation without a DG unit.

The intermittent (non-dispatchable, uncertain and uncontrolled) production into passive network does not benefit network rating. The load ability of distribution network is determined by voltage profile (decrease or rise), power quality and thermal ratings. The intermittent production in weak rural distribution network may cause voltage rise problems. The dimensioning of network becomes quite challenging when there are different size and type of DG units along the network. The worst case planning principle of DG interconnection in passive networks should be replaced with a statistical planning approach in active networks (Repo 2005). The increment of fault current level due to new DG units may cause investments in networks if the rating of components is exceeded. The voltage control or reactive power capability of DG units could also be utilized in network management [2].

Requirements for the protection of distribution networks are changing considerably (Mäki 2007). Protection schemes designed for unidirectional power flow may become ineffective. Unnecessary tripping as well as undetected faults or delayed relay operations may occur due to high DG penetration. DG may also disturb the automatic re-closing. The operation sequence of protection devices during a fault is thus important. Due to DG, the existing methods used in fault location could also become inappropriate.

The current operational practice of distribution network requires disconnection of DG units when a fault occurs. This will keep the operational conditions simple and clear, safe and suitable for auto-reclosing. The purpose of DG unit connection point protection (e.g. frequency and voltage relays) is to eliminate the feeding of fault arc from a DG unit and to prevent unintended island operation. When the penetration level of DG increases the consequences of immediate tripping of DG units may become adverse when short-circuit in transmission grid is seen by several DG units. Even during a fault at distribution network unnecessary disconnection of DG units may occur due to unwanted trips of feeder or DG unit protection relays, loss of synchronism of synchronous generators, sustained over-speed and over-current of asynchronous generators or over-current and DC over-voltage of power electronic converters. The current operational practice clearly creates a contradiction between network safety and stability. However the consequences of stability issues for the whole power system and also for DG owners and other distribution network customers are becoming more important when the disconnection of DG units may cause system wide stability or local power quality problems [2].

V.ADVANCED METERING INFRASTRUCTURE

The implementation of AMI represents the first step in the digitalization of the electric grid and it will provide two-way Communication between customers and utilities. Several countries including Italy, The Netherlands, Denmark, Sweden, and the United States have already taken initial steps toward the deployment of AMI by installing automated meter reading (AMR) systems, which can read measurement registers remotely.

1. Description and Capabilities: AMI is widely considered to consist of several components. As specified in [7], these include:

i. Smart Meter
ii. Customer Gateway
iii. AMI Communication Network
iv. AMI Headend

A smart meter is the source of energy data and energy-related information. A customer gateway provides an interface between the AMI network and the customer systems and appliances such as a Home Area Network (HAN) or Building Management System (BMS), which may or may not be built into the smart meter. The AMI Communication Network provides a communication link from the smart meter to the AMI headend, and the AMI headend handles the informational exchange between external systems such as the Meter Data Management (MDM) system and the AMI network [1]. The diagram below depicts the input and output signal of a typical AMI.

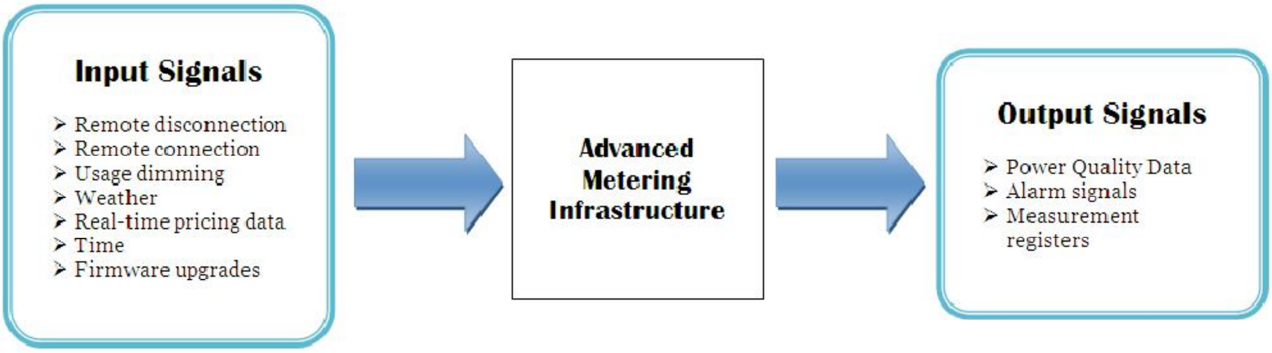

fig.2 : AMI Input and Output Signal

2. Vulnerabilities: Despite the increased interest in the utilization of AMI, there has been very little work done to identify the security needs for such devices. Smart meters, however, are extremely attractive targets for exploitation since vulnerabilities can be easily monetized through manipulated energy costs and measurement readings [8].
AMI will introduce earnest privacy concerns, as an immense amount of energy use information will be stored at the meter. Breaches into this data could expose customer habits and behaviors [8], [7]. Customers must also be prevented from viewing information sent over the network by other customers [7]. References [9] and [10] list several key privacy concerns that need to be addressed.

3. Security Needs: In order to defend against the preceding vulnerabilities, several security features need to be incorporated into the development of AMI, along with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague, and do not specifically address consumer energy usage [8].

One security feature alone, such as encryption, will not be able to cover all possible security threats [7]. Since it will be imperative that the industry maintain 100 percent uptime, both physical security of the AMI system hardware, and multiple standard IT security features such as encryption and authentication will be needed [11]. Furthermore, since it will be impossible to protect against all threats, smart meters must be able to detect even the most subtle unauthorized changes and precursors to tampering or intrusion [1].

VI.AUTOMATIC METER READING IN NETWORK MANAGEMENT

The primary role of AMR (Automatic Meter Reading) systems has been to provide energy consumption data to the utility, but the cost of retrofitting the existing energy metering system may not be justified without added value functions. At present many utilities in Europe level are installing large-scale AMR projects. So far the focus of the installations has been mainly on remote reading of energy measurements. Also some specific applications have been developed, e.g. for load control. The comprehensive concept of using AMR system and data in network and electricity market management is still rare [2].

One requirement for creating additional value functions is the open architecture in AMR systems to provide necessary integration possibilities. Standard integration ways e.g. OLE for Process Control (OPC) or open connectivity via open standards makes it possible to develop new types of intelligent system integrations [2].

Traditionally AMR and Distribution Management System (DMS) have been separate systems without any integration with each other as illustrated in Figure 3. The primary role of AMR has been to provide energy consumption data to the utility for billing and balance settlement purposes. AMR system has also been used for load control in some installations. So far automatic monitoring and control center measures by the DMS have been used mostly for operating 20 kV medium voltage networks. A fault in low voltage network is cleared automatically by blown fuse, but no information about that is received to the control center [2].

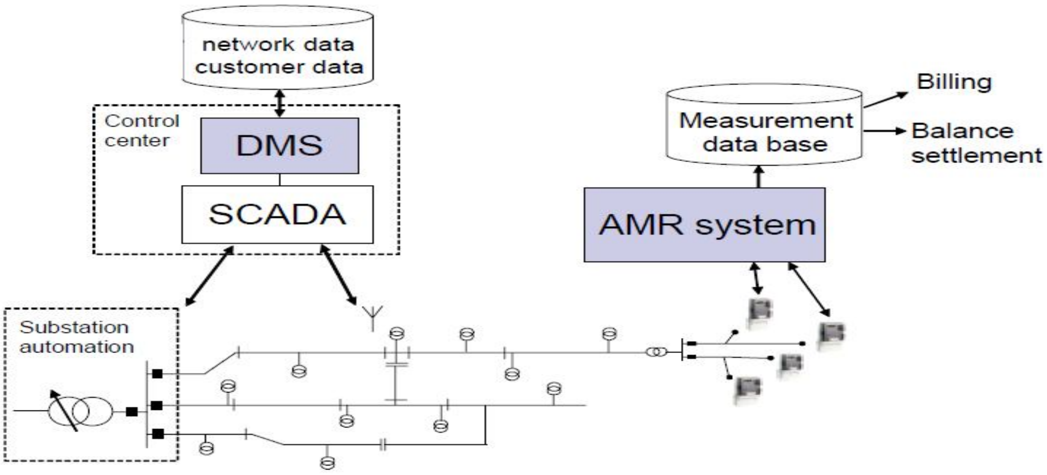

Fig.3: Traditional way for network management

The present AMR meters offer the platform (i.e the infrastructure and communication) to determine and develop new upper-level functions (see Figure 4). These will be used in developing the network asset management, market enhancement as well as the customer service. First implementations of advanced AMR systems have already changed the function of basic energy meter to be a smart terminal unit and gateway to enable real time two-way communication between customers and utilities. In advanced meters alarms based by exceptional events i.e. network faults and voltage violations are enabled. Meters may also have some protective functions adding the safety [2]. The use and integration of AMR in network operation can be seen as an extension of SCADA and distribution automation to the low-voltage level. As Figure 4 illustrates, AMR system can be utilised in many functions of distribution company

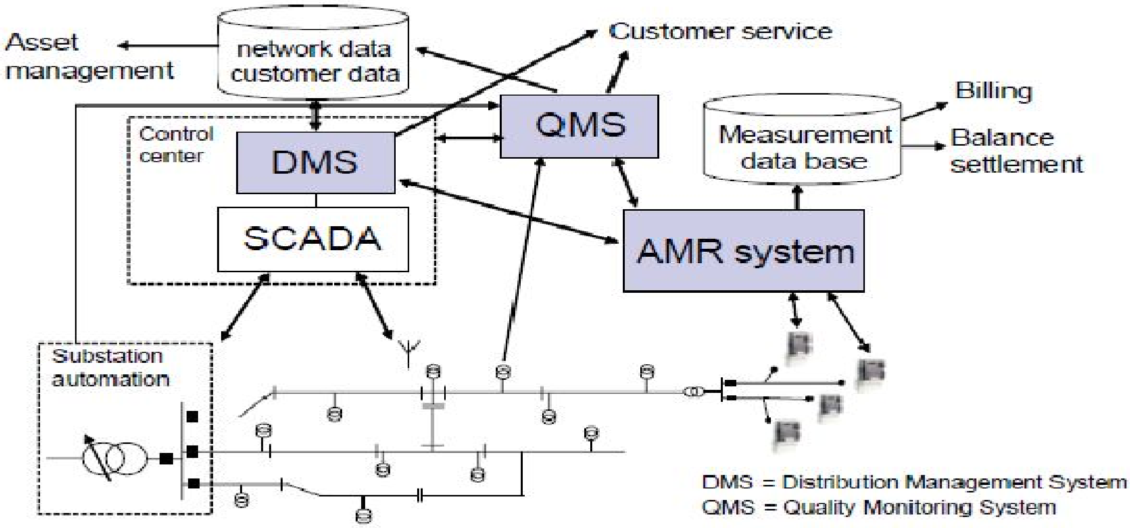

Fig 4 : Integrated information systems for comprehensive network management.

The integrated AMR, DMS and power quality monitoring systems offer information to be used in overall asset management and network planning. At present advanced network calculation applications of network information systems and DMS use hourly-load curves as load information. AMR system offers mass of measurement data to determine more detailed load models for different purposes in network management and load prediction. Real-time AMR data can be used in state-estimation, but for network planning purposes load models are still needed. For network operation purposes more accurate real-time state estimation of the whole network gives information on voltages, loads, losses, and stressing of components, and also make it possible to optimize e.g. network topology, voltage control, and load control actions. In network planning more accurate load models (e.g. more accurate division of customer groups, regional models, etc.) for network calculations and information on realization of power quality (i.e. interruptions, voltage dips, voltage levels) can be used to allocate measures and investments [2].

VII.SMART GRID SECURITY

Upgrading the power grid will present many new security challenges that must be dealt with before extensive deployment of smart grid technologies can begin. The digitalization of the electric grid may enable remote attacks to grow rapidly, potentially spanning countries or even continents [8]. Moreover, it is rapidly becoming easier to compromise computer systems due to the increased availability of hacker tools on the Internet and the decrease in technical knowledge required to use them to impose significant damage [12].

1. Vulnerabilities: In order to defend the smart grid, [1] emphasizes three types of vulnerabilities that must be considered – physical, cyber, and open-source information.

Physical and cyber: While physical attacks – facility break-ins, weapon attacks, or explosives – are real and frightening possibilities, cyber attacks have the potential to be just as destructive and carry the added threats of stealth and long-distance control [13]. Attackers have the potential to initiate attacks from nearly any location in the world. Furthermore, currently more than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices [14]. In addition, the types of protocols and equipment used in the communication and control of power systems are numerous. The diversity and lack of interoperability in the communication protocols causes problems for anyone who tries to establish secure communication to and from a substation (or among substations in a network of heterogeneous protocols and devices). Within a substation control network, it is common to find media including commercial telephone lines, wireless, microwave, private fiber, and Internet connections [1].

2. Security Needs: In order to protect electric infrastructure from the threats outlined above, several defense mechanisms are needed to minimize disruptions to system operations.
i. Layered Security: Layered security (or defense-in-depth as the Department of Defense (DOD) refers to it) involves strategically combining multiple security technologies at each layer of a computing system in order to reduce the risk of unauthorized access due to the failure of any single security technology. It exponentially increases the cost and difficulty for an attacker to compromise a system by creating a much stronger defense than the use of any individual component alone, thus, reducing the likelihood of an attack. Security features to be employed at each layer include examination, detection, prevention, and encryption [1].
ii. Deception: Deception consists of two possible techniques, dissimulation, hiding the real, and simulation, showing the false. McQueen and Boyer describe potential dissimulation and simulation techniques that can be used for control systems in [15]. Deception defense mechanisms can greatly increase the difficulty of planning and conducting successful attacks upon the system, and can alert operators to possible threats before any systems are harmed.

VIII. INTELLIGENT DISTRIBUTED SECURE CONTROL

In For deeper and layered protection, intelligent distributed secure control is required, which would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failure. With distributed intelligence and the components acting as independent agents, those in each island have the ability to reorganize themselves and make efficient use of whatever local resources remain to them in ways consonant with the established global goals to minimize adverse impact on the overall network. Local controllers will guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition [1].

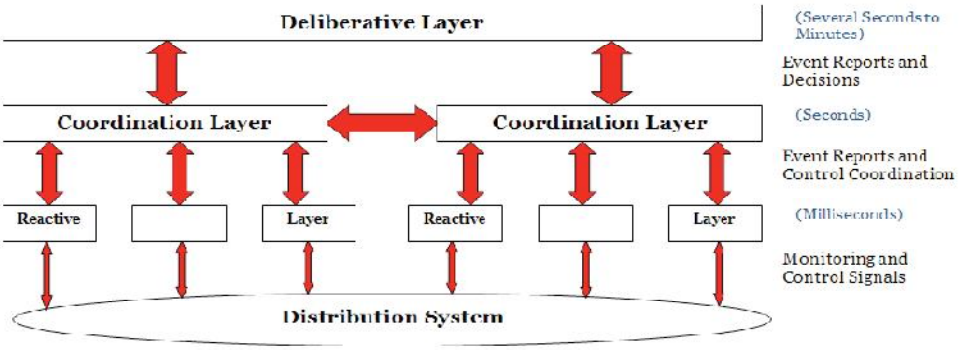
Deliberative Layer
(Several Seconds to Minutes)
Event Reports and Decisions
Coordination Layer
Coordination Layer
(Seconds)
Event Reports and Control Coordination
Reactive
Layer
Reactive
Layer
(Milliseconds)
Monitoring and Control Signals
Distribution System

Fig. 5: Intelligent secure distribution system control architecture

To achieve the desired goals stated above for distribution systems, a distributed intelligent secure control was developed. The model was based on the Strategic Power Infrastructure Defense (SPID) system control architecture developed by the EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI) for systems with intelligent wide-area protection and reconfiguration capabilities [1]. Using several concepts central to the SPID model, an architecture specific to distribution systems was formed. A diagram of the resulting control architecture is shown in Fig. 5.

IX.INTERACTIVE CUSTOMER GATEWAY

For developing distribution management and functionality of electricity market one essential objective is to make the customer, or at least customer connection point, active for improving e.g. interconnection of distributed generation, efficient use of energy, market-based demand response, quality of supply, and management of active distribution networks. Remote readable energy meter is being developed to be an intelligent equipment (i.e. interactive customer gateway) including in addition to traditional energy metering also different kind of advanced functions based on local intelligence and power electronic applications as a part of active distribution networks. The interactive customer gateway will be based on the use of modern power electronics, advanced AMR technology and two-way communication between date bases and applications of the distribution system operator (DSO), transmission system operator (TSO), service providers and electricity energy market players (e.g. aggregators), as illustrated in Figure 6 [2].

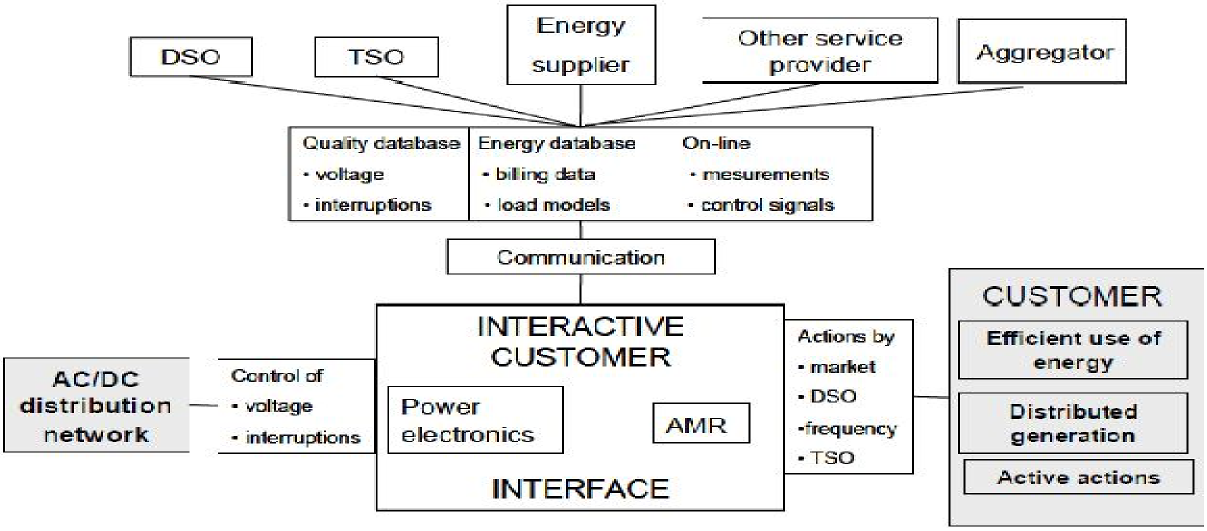

Fig. 6: The concept of Interactive Customer Gateway (INCA)

X. Conclusion

The paper presents some smart grid features at distribution level dealing with interconnection of distributed generation and active distribution management, using automated meter reading (AMR) systems in network management and power quality monitoring. Remote readable energy meter is being developed to be an intelligent equipment (i.e. interactive customer gateway) including in addition to traditional energy metering also different kind of advanced functions based on local intelligence and power electronic applications as a part of active distribution networks.

Before wide-scale deployment and implementation of smart grid technologies can begin, security of cyber and communications networks must be addressed. In this paper, several security issues for the smart grid and its dependent systems are discussed. In addition, an intelligent distributed secure control architecture is presented to provide distribution systems with greater protection against disturbances, both intentional and unintentional.

References

[1] Anthony M, Giacomoni, "A Control and communications model for a secure and reconfigurable distribution system" national science foundation grant, report University of minnesota, USA.

[2] Pertti Jarventausta, Sami repo, Antti Rautiainen, ""Smart grid Power System Control in distributed generation environment". TUT, Tampere.

[3] Dave Hardin, Smart Grid and dynamic power management, enerNOC,Inc. USA, www.interchopen.com 2011.

[4] Apostolos N. Milioudis, Georgios T. Andreo, Dimitrios P. Labridis, "Enhanced Protection scheme for smart grids using power line communication techniques-Part 1: Detection of high Impedance fault occurrence" IEEE, volume 3, issue 4, Dec. 2012.

[5] Ye Yan, Yi Qian, Hamid Sharif, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges", IEEE communications surveys and tutorials, 2012

[6] Fangxing Li, Pei Zhang, Navin Bhatt, "Next generation monitoring and control for future control centers" www.ieeecss.org. (eds), 2011.

[7] Maryam Sadeghi, F. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure," in IEEE T&D Conference , April 2008.

[8] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security and Privacy, vol. 7, no. 3, pp. 75-77, May/June 2009.

[9] NIST, "Smart Grid Cyber Security Strategy and Requirements," The Smart Grid Interoperability Panel– Cyber Security Working Group, DRAFT NISTIR 7628, February 2010.

[10] J. Cline, "Opinion: will the smart grid protect consumer privacy?," Computerworld, November 2009

[11] M. Amin, "Scoping Study and Survey of Electric UtilityIndustry Chief Information Officiers (CIOs): Trends, challenges, opportunities, and plans regarding future Information Technology Needs for the Electric Power Industry," Electric Power Research Institute, Palo Alto, White Paper, Nov. 2007.

[12] T. Kropp, "System threats and vulnearabilities," IEEE Power & Energy Magazine , vol. 4, no. 2, pp. 46-50, March/April 2006

[13] R. Schainker, J. Douglas, and T. Kropp, "Electric utility responses to grid security issues," IEEE Power and Energy Magazine, vol. 4, no. 2, pp. 30-37, March/April 2006.

[14] D. Watts, "Security & vulnerability in electric power systems," in 35th North American Power Syposium, Rolla, 2003, pp. 559-566.

[15] M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in 2nd Conference on Human System Interactions, Catania, 2009.

BIOGRAPHY

Indrajeet Prasad received the M.Sc. degree in Control in Electrical Power Engineering from Politechnika Wroclawska, Poland in 2013. He received the B.Tech. degree in Electronics and Instrumentation Engineering from West Bengal University of Technology,India in 2011.

He have done an apprenticeship with ABB and worked on his master degree project "Adaptation of Gas and Steam flow correction function to the SIL-3 requirements" in 2012-'13. He was the vice-President of an International scientific Circle "WINDMILL" at Politechnika Wroclawska for 2012-'13. His main interests of research are Control in Electrical Engineering, Smart Grid and E. & I. Engineering.