A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges

Ye Yan, Yi Qian, Hamid Sharif, and David Tipper

***Abstract*—A communication infrastructure is an essential part to the success of the emerging smart grid. A scalable and pervasive communication infrastructure is crucial in both construction and operation of a smart grid. In this paper, we present the background and motivation of communication infrastructures in smart grid systems. We also summarize major requirements that smart grid communications must meet. From the experience of several industrial trials on smart grid with communication infrastructures, we expect that the traditional carbon fuel based power plants can cooperate with emerging distributed renewable energy such as wind, solar, etc, to reduce the carbon fuel consumption and consequent green house gas such as carbon dioxide emission. The consumers can minimize their expense on energy by adjusting their intelligent home appliance operations to avoid the peak hours and utilize the renewable energy instead. We further explore the challenges for a communication infrastructure as the part of a complex smart grid system. Since a smart grid system might have over millions of consumers and devices, the demand of its reliability and security is extremely critical. Through a communication infrastructure, a smart grid can improve power reliability and quality to eliminate electricity blackout. Security is a challenging issue since the on-going smart grid systems facing increasing vulnerabilities as more and more automation, remote monitoring/controlling and supervision entities are interconnected.**

***Index Terms*—Smart grid, communication infrastructure, intelligent network, interconnected power system, monitoring, sensing, cyber security**

I. Background

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 using two-way digital technologies. It controls intelligent appliances at consumers' home or building to save energy, reduce cost and increase reliability, efficiency and transparency [1]. A smart grid is expected to be a modernization of the legacy electricity network. It provides monitoring, protecting and optimizing automatically to operation of the interconnected elements. It covers from traditional central generator and/or emerging renewal distributed generator through transmission network and distribution system to industrial consumer and/or home users with their thermostats, electric vehicles, intelligent appliances [2]. A smart grid is characterized by the bi-directional connection of electricity and information flows to create an automated, widely distributed delivery network. It incorporates the legacy electricity grid the benefits of modern communications to deliver real-time information and enable the near-instantaneous balance of supply and demand management [3].

Many technologies to be adopted by smart grid have already been used in other industrial applications, such as sensor networks in manufacturing and wireless networks in telecommunications, and are being adapted for use in new intelligent and interconnected paradigm. In general, smart grid communication technologies can be grouped into five key areas: advanced components, sensing and measurement, improved interfaces and decision support, standards and groups, and integrated communications.

Figure 1 illustrates a general architecture for smart grid communication infrastructures, which includes home area networks (HANs), business area networks (BANs), neighborhood area networks (NANs), data centers, and substation automation integration systems [4]. Smart grids distribute electricity between generators (both traditional power generation and distributed generation sources) and end users (industrial, commercial, residential consumers) using bi-directional information flow to control intelligent appliances at consumers' side saving energy consumption and reducing the consequent expense, meanwhile increasing system reliability and operation transparency. With a communication infrastructure, the smart metering/monitoring techniques can provide the real-time energy consumption as a feedback and correspond to the demand to/from utilities. Network operation center can retrieve those customer power usage data and the on-line market pricing from data centers to optimize the electricity generation, distribution according to the energy consumption.

In a complex smart grid system, through wide deployment of new smart grid components and the convergence of existing information and control technologies applied in the legacy power grid, it can offer sustainable operations to both utilities and customers [5]. It can also enhance the efficiency of legacy power generation, transmission and distribution systems and penetrate the usage of clean renewable energy by introducing modern communication systems into smart grids.

Manuscript received 25 April 2011; revised 23 January 2012.

Y. Yan, Y. Qian, and H. Sharif are with the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln (e-mail: yqian@ieee.org).

D. Tipper is with the Graduate Telecommunications and Networking Program, University of Pittsburgh.

Digital Object Identifier 10.1109/SURV.2012.021312.00034

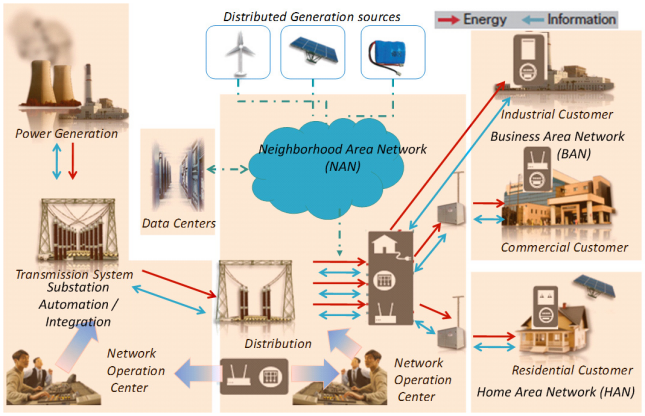


Fig. 1. Smart Grid Communication Infrastructures [4]

The cornerstone of a smart grid is the ability for multiple entities (e.g. intelligent devices, dedicated software, processes, control center, etc) to interact via a communication infrastructure. It follows that the development of a reliable and pervasive communication infrastructure represents crucial issues in both structure and operation of smart grid communication systems [6], [7]. In this connection, a strategic requirement in supporting this process is the development of a reliable communication infrastructure for establishing robust real-time data transportation through Wide Area Networks (WANs) to the distribution feeder and customer level [8].

Existing electrical utility WANs are based on a hybrid of communication technologies including wired technologies such as fiber optics, power line communication (PLC) systems, copper-wire line, and a variety of wireless technologies (i.e. data communications in cellular networks such as GSM/GPRS/WiMax/WLAN and Cognitive Radio [9]). They are designed to support some monitoring/controlling applications as Supervisory Control and Data Acquisition (SCADA)/Energy Management Systems (EMS), Distribution Management Systems (DMS), Enterprise Resource Planning (ERP) systems, generation plant automation, distribution feeder automation and physical security for facilities in wide range areas with very limited bandwidth and capacity in closed networks.

Many applications such as energy metering on the smart grid, have emerged from a decade of research in wireless sensor networks. However, the lack of an IP-based network architecture precluded sensor networks from interoperating with the Internet, limiting their real-world impact. The IETF chartered the 6LoWPAN and RoLL working groups to specify standards at various layers of the protocol stack with the goal of connecting low-power devices to the Internet. In [10] the authors present the standards proposed by these working groups, and describe how the research community actively participates in this process by influencing their design and providing open source implementations.

The new communication infrastructures should evolve toward nearly ubiquitous data transport networks able to handle power delivery applications along with vast amount of new data coming from the smart grid applications. These networks should be scalable, in order to support the present and the future set of functions characterizing the emerging smart grid communication technological platform, and highly pervasive in order to support the deployment of last-mile communications (i.e. from a backbone to the terminal customers locations) [11]. In the rest of this section, we discuss several key factors for smart grid systems including power line communications, distributed energy resources, smart metering, and monitoring and controlling.

A. Power Line Communications

Power line communications (PLCs) uses the power feeder line as communication media. First generation ripple control systems provide one-way communications, in which centralized load control and peak shaving have been performed for many years. The European standards body CENELEC restricted the use of frequencies between 3 kHz and 95 kHz for two-way communications for electricity distributor use. A number of second generation PLC systems with low data rates were proposed in the 1990's, and Automatic Meter Reading systems have been deployed based on this technology. Third generation systems based on OFDM with much higher data rates are currently being developed and deployed for Smart Grids, Distribution Automation and Advanced Metering Management [12].

With the development of smart grids, the PLC on the power transmission and distribution networks have become one of the potential technologies to exchange the information between the end users and the utilities. In order to provide communication services with different priorities under the smart grid environment, it is a must to design a PLC system with variable data rates supported, which means understanding of the PLC physical channel characteristics become vital. The testing results in [13] show that the main reason influencing the reliable communication of high-speed data on power line is the attenuation of the high-frequency signal, which exhibits more obviously in the branch of power line. It is almost impossible to use the frequency range from 10 to 20 MHz for the reliable communications from distribution transformer to end user, so it must be solved with the aid of means such as the repeater and the modulation schemes.

Beside the fact that feeder cables are not designed for data transmission, they are also prone to be interfered by the inverter's outcome. Therefore, PLC modems developed for domestic applications may not be suitable. Limitations and difficulties that obstruct transmission are revealed in [14]. Also, it underlines the possibility of communicating in such an environment and discusses the possible solutions such as the use of a pulsewidth modulation filter to overcome those limitations.

The majority of recent contributions have discussed PLC for high-data-rate applications like Internet access or multimedia communication serving a relatively small number of users. However, it lacks the consideration with PLC as an enabler for sensing, control, and automation in large systems comprising tens or even hundreds of components spread over relatively wide areas. In [15], the authors discussed communication network requirements common to such systems and presented transmission concepts for PLC to make use of the existing

power transmission and/or distribution infrastructure resources (i.e., power lines) to meet these requirements. In [16] the authors give an overview of DLC+VIT4IP (Distribution Line Carrier: Verification, Integration and Test of PLC Technologies and IP Communication for Utilities), a EU funded project under the 7th Framework Programme (FP7) that aims to extend the existing PLC technologies by developing efficient transport of IPv6 protocol, automatic measurement, configuration and management, and security. In addition, the project DLC+VIT4IP also exploits frequency ranges up to 500 kHz, to support systems serving larger smart grid applications.

B. Distributed Energy Resources

The legacy power generation and transmission concept is converting to a massively distributed energy generation landscape integrating an extensive number of variable and small renewable energy resources (DERs) such as wind [17]–[19], solar [20]–[22] installations with all their challenging effects on the smart grid.MetaPV [23] is a project demonstrated the provision of electrical benefits from photovoltaics (PV) on a large scale, showing the way toward cities powered by renewable energy sources. The project also demonstrates enhanced control capacities implemented into PV inverters, including active voltage control, low-voltage ride-through capability, autonomous grid operation, and interaction of distribution system control with PV systems. Smart control should enable an increase of the PV penetration in existing power grids and promote the use of more renewable energy sources in cities and industries at minimum additional investment costs. The MetaPV project is funded by the European Commission in the 7th Framework Programme, which consists of six partners from four EU countries.

New stakeholders (e.g. energy resource aggregators), more flexibility for the consumers (energy market place), and totally new concepts (loading of Electric Vehicles (EVs), usage of EVs as flexible power storage) have to be respected. Innovative monitoring and control concepts are required to operate these distributed energy resources in a reliable and safe way, so the communication technologies must support it. A key requirement for facilitating the distributed production of future grids is that communication and information are standardized to ensure interoperability. For example, the IEC 61850 standard, which was originally aimed at substation automation, has been expanded to cover the monitoring and control of DERs. By having a consistent and well-defined data model the standard enables a DER aggregator, such as a Virtual Power Plant (VPP), in communicating with a broad array of DERs. If the data model of IEC 61850 is combined with a set of contemporary web protocols, it can result in a major shift in how DERs can be accessed and coordinated. [24] describes how IEC 61850 can benefit from the REpresentational State Transfer (REST) service concept and how a server using these technologies can be used to interface with DERs as diverse as EVs and micro Combined Heat and Power (μCHP) units.

There are some works (e.g., [25]–[27]) in integrating DER generation into the traditional centralized carbon fuel based generation power grid. These energy sources include biomass etc. A key observation made in [25] is that existing power grids were designed in a one-direction radial mode without considering the communication with the emerging distributed renewable resource generation. In [26] it discussed the broader implications of the social acceptance of these new energy generation technologies, as they represent a significant departure from incumbent approach of traditional monolithic large scale energy generation. In addition, the implications of regulatory and economic factors also contribute to potential take-up and various deployment models to increase the adoption of these distributed renewable resource generators [27].

Every DER includes an Electronic Power Processor (EPP) to govern the power exchange with the smart grid and Switching Power Interface (SPI) to control the currents drawn from the smart grid. Such distributed EPPs and SPIs should perform cooperatively to take full advantage of smart grid potentiality (exploitation of renewable energy sources, power quality and transmission efficiency). To achieve this goal different approaches can be adopted, depending on the available communication capability. In [28] it discussed various control solutions applicable in absence of supervisory control, e.g., in residential micro-grids, where communication is possible between neighbor units only (surround control) or is not available at all (plug & play control). In micro-grids, where number and type of DERs and loads is unpredictable and may vary during time, cooperative operation can be achieved by simple cross-communication among neighbor EPPs, without centralized supervisor. In [29], it describes principles of cooperative operations with existing information and communication architectures, which allows exploitation of micro-grid capabilities without additional infrastructure investments.

C. Smart Metering

The Advanced Metering Infrastructure (AMI) is a key factor in the smart grid which is the architecture for automated, two-way communications between a smart utility meter and a utility company. A smart meter is an advanced meter which identifies power consumption in much more detail than a conventional meter and communicates the collected information back to the utility for load monitoring and billing purposes. Consumers can be informed of how much power they are using so that they could control their power consumption and the consequent carbon dioxide emission. By managing the peak load through consumer participation, the utility will likely provide electricity at lower and even rates for all.

AMI has already gained great attraction within the industry, with the advantages in accuracy and process improvement of on-line meter reading and control. In [30], additional benefits are suggested to be gained in managing power quality and asset management with AMI. This paper also discussed how reliability, operational efficiency, and customer satisfaction can be addressed with an AMI deployment. However, the benefits of AMI are countered by increasing cyber security issues [31]. The technologies require a communication infrastructure to provide interconnectivity. Hence, the vulnerabilities that expose other internetworking systems will ultimately lead to security threats to AMI systems.

D. Monitoring and Controlling

SCADA systems have been implemented to monitor and control electrical power grids for decades. The industrial experience shows that practical deployment of SCADA based systems may restrict it to the high voltage transmission networks only. In [32] the authors made the observation that existing monitoring and control systems are restricted to the (high-voltage) transmission network and not suitable for larger scale monitoring and control of the entire electrical grid. A distributed monitoring control system is proposed to manage the power grid. A grid computing solution is proposed to address these monitoring control needs and the results of the research for an off-line test environment is discussed. The key motivations also include the need to support sustainable and renewable energy source at the micro-generation level. As SCADA systems evolve, there is much interest in exploring the security vulnerabilities posed to these systems over communication network and/or internet technologies [33]–[35].

In [36], the solution applies existing Information and Communication Technology (ICT) systems in a hierarchical decomposition of the power grid into logical zones for monitoring and control. It outlines the impact to the control center responsible for management and control of the electrical network. It also proposes a framework for future control center in order to monitor and manage the smart grid. The EU FP6 project ADINE [37] is based on the Active Network Management (ANM) concept, where automation, ICT and power electronics are used to integrate more distributed generators by exploiting active resources instead of just reinforcing the network. The resources are mobilized through ancillary services or requirements. Five enabling solutions within ANM are pushed forward in the project: Protection relay and fault location applications, coordinated protection planning, voltage control with microturbine, centralized voltage control with SCADA/DMS.

The rest of this paper is organized as follows: the key motivations of smart grid communication infrastructures are discussed in section II. Several industrial trials are shown in section III. The detailed requirements are presented in section IV. The challenges are discussed in section V. Conclusions are drawn in section VI.

II. Motivations

In this section, we briefly highlight the key motivations of communication infrastructures in smart grid systems. As illustrated in Figure 2, the motivations are related to system, operation and environment aspects in emerging smart grid paradigm through communication infrastructures [38].

A. Enhanced Customer Experience

A key objective for communication infrastructures in smart grid systems is to improve service reliability and quality to customers which includes reduced outage times when a power system is interrupted, improved notification of electricity network problems and providing customers with proper options and tools to understand and optimize their energy usage to curtail the peak-hour usage to avoid power quality degradation or blackout [39].

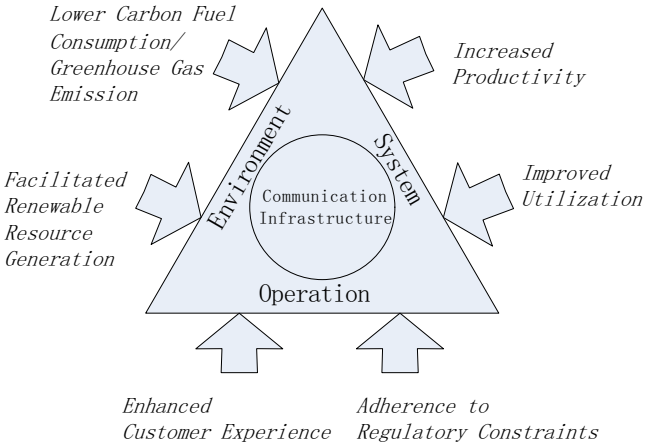


Fig. 2. Motivations of Smart Grid Communication Infrastructures [38]

B. Increased Productivity

Intelligent performance information and tools will allow utilities to undertake their current duties in a more efficient manner, with longer term benefits coming from automating the smart grid. These gains in productivity will help to reduce deployment costs and operational costs in managing the smart grid system [40].

C. Improved Utilization

The communication infrastructure in smart grid will provide detailed real-time data on distributed energy generation, electricity transmission, power consumption and market price. This information allows the utility operators to improve their decision making processes by identifying which components are likely to fail and the replacement strategy online [41].

D. Lower Carbon Fuel Consumption/Greenhouse Gas Emission

A smart grid has the potential to reduce electricity losses in the network and limit growth in demand, due to embedded monitoring of the high, medium and low voltage networks through communication infrastructures, therefore, lower carbon fuel consumption and greenhouse gas emission [42].

E. Facilitated Renewable Resource Generation

A smart grid will enable options for renewable generation and provide customers with the awareness and capabilities to reduce their energy consumption on carbon fuel based power [43].

F. Adherence to Regulatory Constraints

New regulatory demands include provisions for increased levels of asset data tracking (cost justification), and greater reliability targeting the implementation of communication infrastructure in smart grid [44].

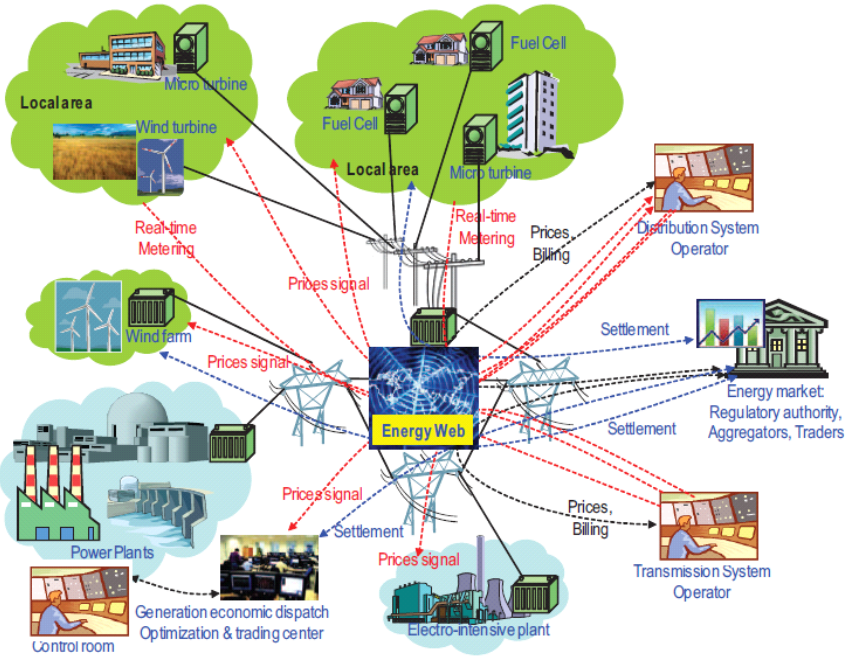


Fig. 3. Energy Web Infrastructure [45]

III. Case Studies

The industry has recently undergone a significant transformation of their ICT systems to support both current and future business models of smart grid operations. Moreover, the power industry is transforming from the traditional models of business to embrace a number of new and enhanced technologies that support future smart grid operations. This section summaries several smart grid industry projects which include energy web infrastructure for power generation and electricity market information exchange, smart metering infrastructure which support monitoring and retrieving both real-time and historical data, smart community for real-time power consumption monitoring and managing, ZigBee-based recording system with capability for consumers to view and manage their power consumption online, and future control center for power generation and distribution managing and deciding between utilities through public networks such as internet.

A. Energy Web

The increasing electricity demand and sustainable development of renewable energy resources offer opportunities for both utilities, brokers, customers to participate into the development of the emerging energy web. The basic idea of energy web is to use the Internet to gain bandwidth, reliability and interconnection for the smart grid. It realizes the on-demand and demand response in local area by establishing the balance of power generation and consumption.

In Figure 3, each power generator is interconnected with an adapted power supplier which has the proper capability of interpreting the real-time price signal received from the energy web infrastructure [45]. In order to match the consumption and generation, the participant strategy is adapted. In the power market model, each electricity user has option to become a power generator. The electricity price is generated real-time and sent to every participants by utility operators using the smart grid communication infrastructure from the electricity market. The electricity flows generated by the participants are monitored in real-time mode by utility operators who also operate the real-time metering infrastructures such as automatic meter reading (AMR) or AMI for establishing the energy demand and supply balance. While the historical records of both the power consumption and generation with their corresponding price are periodically sent to the related offices of the participants for financial settlement.

B. Smart Metering and Infrastructure

BC Hydro [46] is launching a smart metering and infrastructure (SMI) program. A multi-level common and integrated communication infrastructure to enable grid modernization is planned as illustrated in Figure 4. That means the communication infrastructure will not only support automated meter readings, customer home appliance connections, but also future distribution automation, substation automation and possibly mobile workforce management and other advanced applications which utilities could envision in the life span (20 years) of AMI infrastructure. This conforms to the industry vision of integrating communication and IT networks with the power delivery system, in order to provide system sensing and control capability [47].

This long term vision raises several key questions: How much data traffic will flow in the network and how much bandwidth should be planned for the communication network, especially for the wide area communication network? How much of the legacy communication network for system control purposes (e.g., SCADA system) can be leveraged to deliver a cost effective solution? These questions are addressed based

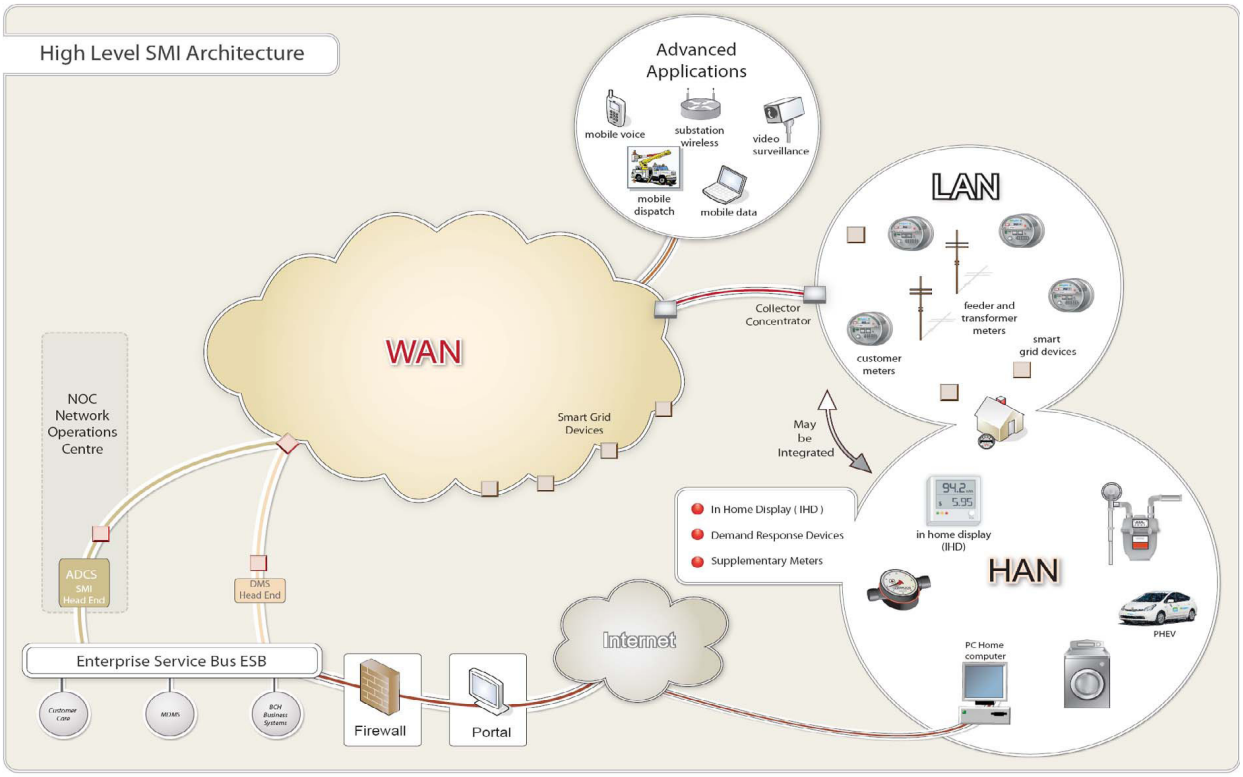


Fig. 4. High Level Common Communication Infrastructure Architecture [47]

on the expected new applications and with communication and control technology development and system life cycle cost minimization in mind.

C. Smart Community

A smart community trial deploys automated metering devices into customer's household. It may include gas, water and electricity automated metering. The smart community trial provides customers new tools to manage their energy consumption hence reduce the related carbon footprint.

Figure 5 provides an overview of the components. The trial involves the deployment to the scale of 1,000 houses that communicate using WiMax to several IT systems which manage the reading of water, gas, and electricity. Customers can access to an information portal via Home Area Networks (HAN). This may be accessed by an in-house display panel or the software based interfaces via the PDA, smart phone or home personal computer.

The home energy consumption is monitored by those appliances enabled with intelligent chips which may support the remote control of appliances operation from Internet. Support for electrical vehicles will also be provided for home. The data gathered from this trial can be made available further to the public, universities, and researchers for the energy efficiency and environmental protection.

The detailed data on measurements, events, and faults can be viewed in an example in [48]. In order to retrieve the historical measurement data, the solution will be able to display the topology of network at selected historical time points. While the high voltage transmission network is usually

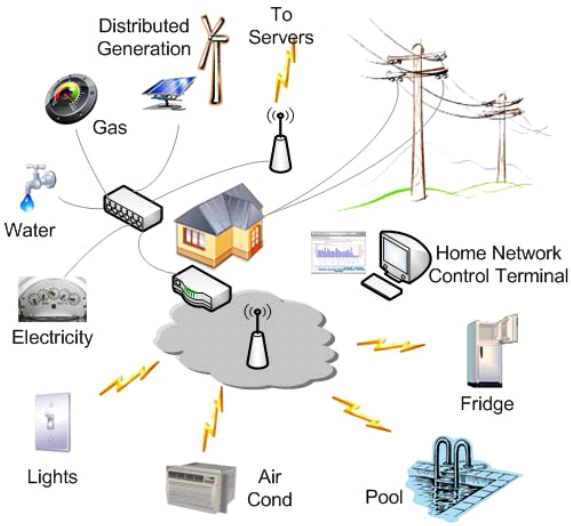


Fig. 5. Smart Community: Automated Metering Infrastructure [48]

static in terms of its network configuration, the medium and low voltage networks are considerably more volatile. Hence, such a historical network view will provide further input to the central control to assist in diagnosing network faults, and will also assist operators and engineers in the design of the smart grid communication infrastructure.

D. A ZigBee-Based Recording System

ZigBee has been designed as a low-cost and low-power-consumption wireless communication standard by ZigBee

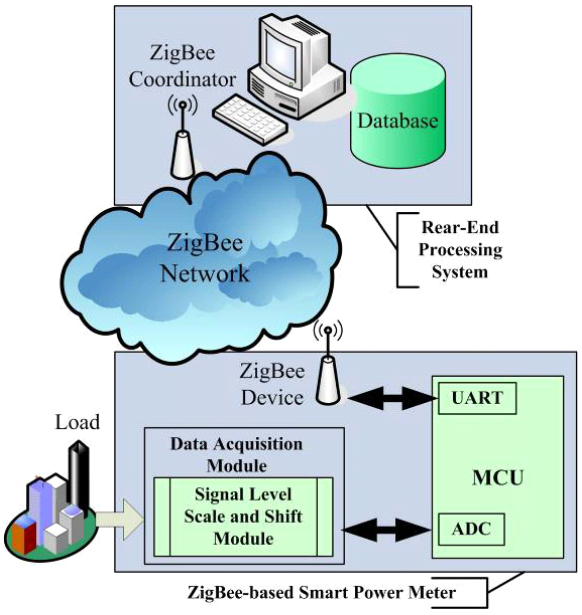


Fig. 6. System Architecture of a ZigBee-based Smart Meter Recording System [53]

Alliance [49]. The ZigBee application profile includes home automation, industrial plant monitoring, commercial building automation, automatic meter reading, telecom servicesecommerce, wireless sensor networks, personal and home area networks [50]–[52].

A smart power-meter and a back-end processing system are proposed in [53] to be equipped with ZigBee devices and ZigBee coordinators respectively. With the automatic networking characteristic of ZigBee, smart power meter serving as a node apparatus will communicate with the ZigBee coordinator of rear-end processing system and ZigBee network can then be constructed to accomplish the meter-reading function. After the ZigBee network was constructed, the rear-end processing system can send the request commands to the ZigBee coordinators and receive the power consumption data and outage event data from the power meters. Therefore, the automatic meter reading can be accomplished. The concept of the proposed outage recording system is illustrated in Figure 6 while an example of real-time data acquisition is shown in [53].

E. Future Control Center

In [54], the authors proposed a vision to design and develop the next-generation monitoring, analysis, and control technologies to move the industry towards a smarter transmission grid.

As shown in Figure 7, the vision for future control centers, also referred to as smart control centers, can be a critical part of the overall framework of the future smart grid. This vision has five key characteristics as discussed in the following.

1) Human-Centered Online Monitoring: Human-centered is the key characteristic of the next-generation monitoring functions in the future smart control centers. In this context, human-centered has two meanings: information-directed and customized. The next generation monitoring functions shall provide operators useful information rather than raw data. With more and more deployment of monitoring devices (e.g., equipment health sensors), it now has more data available to help system operators monitor the power system condition in real time. However, more data does not necessarily mean more information. We need to transform the huge volume of data into useful information. It is the operators responsibility to define what information is needed. Since the information is presented to system operators who are human beings, the monitoring functions shall employ advanced visualization techniques with the goal of helping each operator to digest information quickly.

2) Comprehensive Online Analysis: The next-generation online analysis functions shall help system operators determine comprehensive operating boundaries in real time. Comprehensive operating boundaries include both thermal limits and stability (voltage stability and transient stability) limits.

The next-generation online analysis functions shall apply a comprehensive approach to help system operators determine the operating boundaries. Comprehensive approach means combination of a simulation-based approach and a measurement-based approach.

3) From Reactive Analysis to Proactive Analysis: The present online analysis is based on the current operating condition. This does not consider future system conditions. In the future, online analysis shall take a proactive approach to perform look-ahead simulation on the future system conditions.

The integration of renewable energy sources will introduce more uncertainties into the power system. With the ability to foresee potential problems, the next-generation proactive online analysis will optimize resources (such as demand response and energy storage) in order to improve reliability and achieve economic operation.

By enabling sufficient foresight, the next-generation analysis functions allow system operators to take a proactive approach to develop optimal control strategies and mitigation plans.

4) From Isolated Protection and Control Strategy to Coordinated Protection and Control Strategy: Traditionally, each control scheme is designed to solve a particular problem. The parameters were developed based on offline simulations and largely remain fixed. There is a lack of coordination among protection and control systems. As modern power systems have become more interconnected with increasing stress levels, each disturbance may cause multiple protection and control schemes to respond. There may exist negative interactions that can worsen system conditions, which present challenges and risks in system operations.

When a power system experiences a disturbance, the next generation coordinated protection and control systems will perform according to the optimal control strategies developed by online security assessment and shall quickly bring the system to a stable operating condition with minimum control efforts.

5) Self-Healing System Control: The current restoration plans are developed through offline studies based on assumptions regarding likely scenarios. However, the restoration strategy developed from such studies may not work well

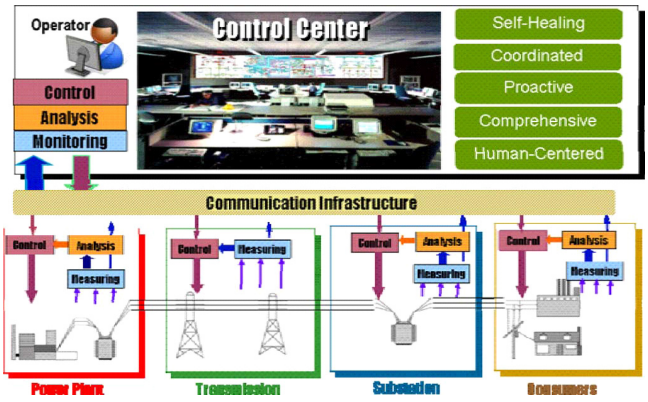


Fig. 7. Scopes of Future Control Center [54]

following a blackout because the real operational situation may vary from the assumed scenarios.

When part or all of the power system is blacked out, the next generation self-healing control scheme shall effectively restore the system and bring it back to a normal operating condition.

IV. Requirements

Monitoring/sensing, communication and control are the three fundamental building blocks that will convert a power distribution system into a smart grid. Monitoring/sensing will have the ability to detect malfunctions or deviations from normal operational ranges that would warrant actions. Further, since in a smart grid, a point of electricity consumption can also become a point of generation, the sensing process will be closely linked with the metering process. Communications will allow inputs from sensors to be conveyed to the control elements in the smart grid which will generate control messages for transmission to various points in the smart grid resulting in appropriate actions. The communication infrastructure has to be robust enough to accept inputs from a user and make it an integral part of the process. By the same token, the user must be capable of getting the appropriate level of information from the smart grid. The major requirements for smart grid communication infrastructures are discussed in the rest of this section.

A. QoS

In order to realize a practical smart grid communication infrastructure, it is necessary to have guaranteed Quality of Service (QoS) for the communication and networking technology used in the smart grid, ranging from power generation, transmission, distribution, to the customer applications.

1) Latency: The real-time operational data communications in smart grid include online sensor/meter reading and power system control signals. The communication is characterized by the fact that most of interactions must take place in real time, with hard time bound. The communication requirements define the design of the technical solutions. For real-time sensing/metering purposes, reading messages should be transmitted within a very short time frame. For instance, the maximum allowed time is in the range of 12-20 ms, depending on the type of protection scheme which origins from the fact that the disconnection of fault current should within approximately 100 ms. Power System Control signals mainly include supervisory control of the power process on secondary or higher levels. These systems are of the kind SCADA/EMS. Measured values must not be older than 15 seconds, when arriving at the control center. Breaking information shall arrive no later than 2 seconds after the emergency event has occurred [55].

2) Bandwidth: As more and more interconnected intelligent elements are added to the electricity network with the evolution of the smart grid, the communication infrastructure should be able to transport more and more messages simultaneously without severe effect on latency. The network bandwidth must increase faster than the demand of these interconnected intelligent elements in the network.

C. H. Hauser et al. concluded in [56] that a 10 millisecond average latency for a 400 bit message using a T1 line will result in a utilization of only 6% of the T1 bandwidth. In [55] the authors modeled the communication bandwidth requirements for a moderate size electricity distribution system. In this model, a distribution substation is connected to 10,000 feeders and each feeder connects to 10 customers. Assuming that every electric meter generates a message every second to the distribution substation, the total is 100,000 messages per second. The feeders themselves will generate messages to each other and to the distribution substation. The authors in [55] modeled the messages in the smart grid arriving at servers located at the control center as M/M/1 traffic. Then, the transmission line bandwidth is evaluated over 100 Mbps through the M/M/1 queuing model. It can be observed that this situation results in a very poor bandwidth utilization of the transmission facilities as well. Unfortunately, a higher level of utilization will not permit meeting the assumed latency constraint.

B. Interoperability

Interoperability of a smart grid is the ability of diverse systems to work together, use the compatible parts, exchange information or equipment from each other, and work cooperatively to perform tasks. It enables integration, effective cooperation, and two-way communications among the many interconnected elements of the smart grid. The National Institute for Standards and Technology (NIST) works as the first International Coordinator for smart grid interoperability [57].

NIST developed a framework that includes protocols and standards for information management to achieve interoperability of smart grid devices and systems [58]. NIST has developed a three phase approach to identify smart grid standards. Phase 1 addresses the engagement of stakeholders in a participatory public process to identify applicable standards and gaps in currently available standards and priorities for new standardization activities, ending with the final publication of the framework report after public comments have been incorporated. Phase 2 will establish a private-public partnership and form a smart grid interoperability panel to drive longer-term progress. Phase 3 will develop and implement a framework for testing and certification of how standards are implemented in smart grid devices, systems, and processes.

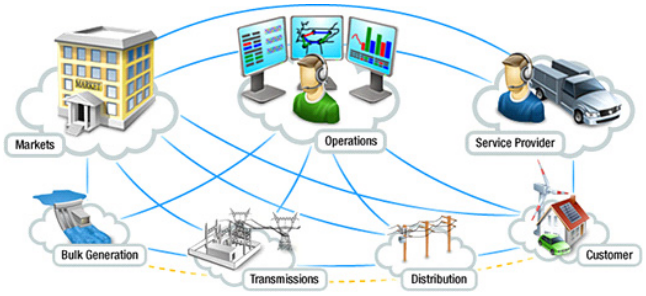


Fig. 8. NIST Conceptual Model [59]

As illustrated in Figure 8, the NIST conceptual reference model identifies seven domains as bulk generation, transmission, distribution, markets, operations, service providers, and customers and major actors and applications within each. The reference model also identifies interfaces among domains and actors and applications over which information must be exchanged and for which interoperability standards are needed.

For years, the utility industry has been using optical port communications, defined by ANSI C12.18, and telephone modem communications, defined by ANSI C12.21, to get metering data, defined by ANSI C12.19, from the field to the back office. While the two communication standards have been employed to great success, the missing was a standard method for using true network communications for exchanging the data. Recent work has completed by ANSI C12.22, a standard for interfacing the data communication networks, as well as updating the optical port and modem communication standards. This set of standards offers the industry an open and comprehensive protocol suite to transport the newly revised data standard, ANSI C12.19 [60].

C. Scalability

A smart grid communication infrastructure needs the scalability of accommodating more and more devices and services into it and more end-user interaction real-time monitoring of energy meters. As discussed by Lobo et al. [61], an IP-based network will provide an effective solution for the communication needs of the smart grid. An IP-based network as the backbone makes use of new technologies independent of the service implemented by the distributed network operator. The cost of deployment and maintenance can be reduced significantly using IP-based technologies.

D. Security

According to the Electric Power Research Institute (EPRI), one of the emergent requirements facing the smart grid development is related to cyber security of systems. As indicated in the EPRI report [62], cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.

There are many organizations working on the development of smart grid security requirements including North American Electrical Reliability Corporation-Critical Infrastructure Protection (NERC-CIP), ISA, IEEE (1402), the National Infrastructure Protection Plan (NIPP), and NIST [63].

One prominent source of requirements is the Smart Grid Interoperability Panel (SGiP) Cyber Security Working Group, previously NIST Cyber Security Coordination Task Group (CSCTG). NIST CSCTG was established to ensure the consistency in the cyber security requirements across all the smart grid domains and components. The draft document from the CSWG, NIST interagency Report (NIST IR) 7628 [64], continues to evolve. NIST and DoE Gridwise Architecture Council (GWAC) [65] has established Domain Expert Working Groups (DEWGs) [66]: Home-to-Grid (H2G), Building-to-Grid (B2G), Industrial-to-Grid (I2G), Transmission and Distribution (T&D) and Business and Policy (B&P). Furthermore, many other standards may apply, including ISO 17799 [67], FIPS 201 [68], other NIST SPs, and DISA Security Technical Implementation Guides (STIGs) [69]. Working with standards bodies, such as NIST and others, will be extremely important to ensure a highly secure, scalable, consistently deployed smart grid communication system, as these standards bodies will drive the security requirements of the smart grid communication systems [70].

One thing is consistent among the various standards bodies: the security of the smart grid communications will strongly depend on authentication, authorization, and privacy technologies. Privacy technologies are well matured. Federal Information Processing Standard (FIPS) has approved Advanced Encryption Standard (AES) and Triple Data Encryption Algorithm (3DES) solutions, offering strong security and high performance, are readily available. The specific privacy solutions required will depend on the type of communication resource being protected. As a specific example, NIST has determined that 3DES solution will likely become insecure by the year 2030. Considering that utility components are expected to have long lifetimes, AES would be the preferred solution for new components. However, it is expected the legacy functionality such as 3DES must be supported for system compatibility, therefore there is a risk of compromising the system [71].

Wireless links will be secured with technologies from well known standards such as 802.11i [72] and 802.16e [73]. Different wireless protocols have varying degrees of security mechanisms. Wired links will be secured with the technologies such as firewalls, virtual private networks (VPN) and IPSec. Higher layer security mechanism such as Secure Shell (SSH) and Security Socket Layer (SSL)/Transport Layer Security (TLS) should also be used. System architects and designers often identify the need for and specify the use of secure protocols, such as SSH and IPSec, but then skip the details associated with establishing security associations between end points of communications. Such an approach is likely to result in a system where the necessary procedures for secure key management can quickly become an operational nightmare. It

is due to the fact that, when system architects do not develop an integrated and comprehensive key management scheme, customers may be provided with few key management options, and often resort to manually pre-configuring symmetric keys. This approach is simple for the system designers, but it can be very expensive for the system owner/operator.

What has been learned from years of deploying and operating large secure network communication systems is that the efforts required to provision symmetric keys into thousands of devices can be too expensive or insecure. The development of key and trust management schemes for large network deployments is required; these systems can be leveraged from other industries, such as mobile radio systems and Association of Public-Safety Communications Officials (APCO) radio systems. Several APCO-deployed systems provide statewide wireless coverage, with tens of thousands of secure devices [74]. Trust management systems, based on public-key infrastructure (PKI) technology, could be customized specifically for smart grid operators, easing the burden of providing security which adheres to the standards and guidelines that are known to be secure.

All of the above technologies rely on some sort of key management. Considering that the smart grid will contain millions of devices, spread across hundreds of organizations, the key management systems used must be scalable to extraordinary levels. Further, key management must offer strong security (authentication and authorization), inter-organization interoperability, and the highest possible levels of efficiency to ensure that unnecessary cost due to overhead, provisioning, and maintenance are minimized. It is likely that new key management systems (specialized to meet the requirements of smart grid) will be needed.

E. Standardization

The smart grid involves various standards in many fields such as power generation, delivery and control besides communications. IEEE has recently taken the initiative to define these standards and write guidelines on how the smart grid should operate using the latest technology in power engineering, control, communications, and information technology. The standards group that was created is known as the IEEE P2030 group [75]. Three task forces were formed to tackle distribution systems including the integration of different energy sources, transmission substations, load side requirements, and cyber security. These task forces will focus on power engineering technology, information technology, and communication technology. The power engineering technology group will work on the functional requirements of interoperability, drawing on various existing and ongoing efforts by groups such as International Society of Automation (ISA) and International Electrotechnical Commission (IEC). IEC TC57 WG13 [76] is currently drafting the new international standards for use in improving overall transmission grid reliability and security. This work directly supports the NIST smart grid interoperability.

The information technology group will look at the issues of privacy, security, data integrity, interfaces, and interoperability. The communication technology group will define the communication requirements between devices in the smart grid and establish boundaries for generation, transmission, and distribution in conjunction with the customers [77].

Implementing standards is a major issue in transitioning towards advanced sensing/automation, and also is a crucial step in creating smart grid communication infrastructure. As communication systems in smart grid are usually from different vendors with their own legacies, which are proprietary and have no dual interoperability. The identified standards which govern the necessary integration of different functions are specified by IEC.

V. Challenges

The proliferation of wireless/wired sensors and communication devices and the emergence of embedded computing represents an opportunity to develop applications for connected environments in general, and especially management systems that address urgent challenges facing the smart grid communication infrastructure. The challenges include the deployment of large-scale embedded computing, legacy power grids, intelligent appliances, and next-generation communications and collaborations that will provide the foundation for a post-carbon society. In this section, we discuss the context that gives these challenges urgency as well as the technical challenges that need to be addressed by smart grid communication infrastructures.

A. Complexity

A smart grid communication infrastructure is a system of systems and it is extremely complex. As a consequence, modeling, analysis and design a suitable communication infrastructure meet many new challenges. The models to be used must be capable of accounting for uncertainty as a way to simulate emerging behavior. The numerical tools to perform the analysis must be capable of solving very large scale problems. In fact, the power system is tightly coupled and non-linear [78] and does not benefit from the sparsity that typically characterized this problem. The control system and particularly communication infrastructure must be designed to manage uncertainty and inconsistencies to be resilient or gracefully degrade when necessary. Finally the performance metric must be adjusted to the new nature of the power system. The challenges in modeling the complexity of a smart grid communication infrastructure are summarized in the following.

1) Need to support multi-physics approach: Systems are so tightly interconnected that is not possible to simply simulate the electrical subsystem [79]

2) Need to support multidisciplinary approach: Different users will have to work at the same scenario, each of them focusing on different aspects (control, power flow, communications) [80], [81].

3) Need to support dynamic and reconfigurable model level definition: This is probably the most challenging element. While different users interact with the simulation schematic they need to focus on different details of the system. The next generation simulation system should support this process automatically [82], [83].

4) Need to provide high-level graphic visualization to support system: While engineers may want to focus on the details of graphs, system analysis requires different types of visualization able to synthesize a "system-picture" [84].

5) Need to provide support for uncertainty propagation: Uncertainty is presented in the power system for different reasons and from various sources. And therefore it is to be accounted for in the design and in the operation, as it will be dependent on static and dynamic state estimation [85].

B. Efficiency

Realization of the future smart grid requires meeting the ever increasing efficiency challenges by harnessing modern communication and information technologies to enable a communication infrastructure that provides grid-wide coordinated monitoring and control capabilities. Such communication infrastructure should be capable of providing fail proof and nearly instantaneous bidirectional communications among all devices ranging from individual loads to the grid-wide control centers including all important equipment at the electricity distribution and transmission system. This involves processing vast number of data transactions for analysis and automation. It requires a high performance communication infrastructure capable of providing fast intelligent local sub-second responses coordinated with a higher level global analysis in order to prevent or contain rapidly evolving adverse events [86]. It needs to meet the challenges in the following.

1) Better Telemetry: Phasor Measurement Unit (PMU) technology [87] can offer faster, time-stamped, higher accuracy and sub-second scanning to enable timely grid-wide situational awareness [87].

2) Faster Controls: Based on power electronics, smart grid communication infrastructure enables fast automated control actions, for voltage and power flow management at electricity generation, transmission and distribution systems.

3) More Robust Controls: Proactive and adaptive adjustment of protection and communication settings for wide area monitoring and controls support intentional islanding, which is beyond currently employed ad-hoc schemes in system protection.

4) Embedded Intelligent Device Communications: To enable adaptive and intelligent communications for device level fault diagnosis and bad data identification, operations and the constraints should be prescribed by system operators or control centers, intelligent remedial action scheme (RAS)/system protection schemes (SPS), autonomous restoration of equipment and autonomous local control actions [88].

5) Integrated and Secure Communications: Highly distributed and pervasive communications based on open standards allow flexible network configurability to assure fail-proof monitoring and automation for bidirectional communications between all operators and customers.

6) Enhanced Computing Capabilities: Fail-proof and secure communication systems for reliable analysis support operator decisions and autonomous intelligent agents a geographically and temporally coordinated hierarchy through the grid-wide communication infrastructure [89].

7) Internet Technology: Internet protocols to facilitate data exchange, process control and cyber security implement a distributed architecture with open interfaces. Plug-and-play hardware and software components in a service oriented architecture is based on communication standards and technologies such as message oriented middleware and web services to enable seamless integration of the IT infrastructure ranging from lowest equipment level Intelligent Electronic Devices (IEDs) to all higher application levels [90].

C. Reliability

A framework for cohesive integration of reliability technologies facilitate convergence of the needed standards and protocols, and implementation of necessary analytical capabilities. This subsection reviews the impact of a communication infrastructure to the reliability of a smart grid. An ideal mix of the current communication and control techniques are expected to lead a flatter net demand that eventually accentuates many reliability issues further. A grid-wide communication architectural framework to meet these reliability challenges are discussed in the following [91].

1) Renewable Resources: Renewable resources generally have adverse challenges on smart grid reliability due to the following factors: variability and low capacity, factors making the net demand profile steeper, low correlation with the load profile especially in the case of wind resource, relatively high forecast errors especially for longer horizons, congestion issues at transmission level due to large installations and at distribution level due to dispersed resources. Operational performance issues such as voltage and regulation.

To address the variability of the net demand, as renewable resources growing over the long run, efficient communication infrastructure for information exchange among demand response, storage devices and utilization of plug-in electric vehicles (PEVs)/plug-in hybrid electric vehicles (PHEV) will complement the remedies [92].

2) Demand Response: Demand response allows consumer load reduction in response to emergency and high price conditions on the smart grid. Such conditions are more prevalent during peak load or congested operation as illustrated in Figure 9 [93]. Non-emergency demand response in the range of 5% to 15% of system peak load can provide substantial benefits in reducing the need for additional resources and lowering real-time electricity prices [2]. Demand response does not substantially change the total energy consumption since a large fraction of the energy saved during the load curtailment period is consumed at a more opportune time - thus a flatter load.

3) Load Management: Load rejection as an emergency resource to protect the smart grid from disruption is well understood and is implemented to operate either by system operator command or through under-frequency and/or under-voltage relays. In a smart grid, the load rejection schemes can be enhanced to act more intelligently and based on customer participation.

Price based demand response/load management as a system resource to balance demand and supply has not been widely adopted yet. Contract based participation has been typically

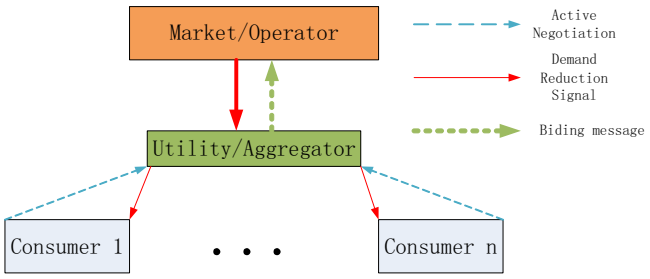


Fig. 9. Communications for Demand Response [93]

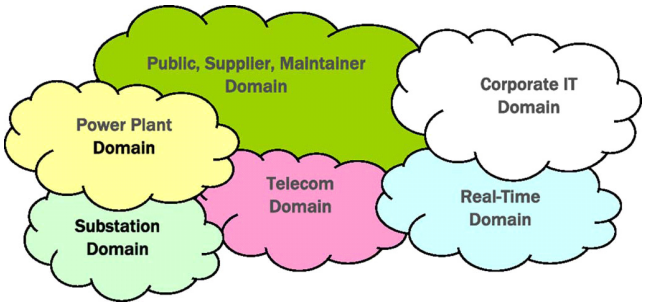


Fig. 10. Information Security Domains [99]

below 5% of peak load [94]. In a smart grid, real-time price information enables wider voluntary participation by consumers. Demand response can be implemented through either automatic or manual response to price signals, or through a bidding process based on direct communications between the consumers and the market/system operators or through intermediaries such as aggregators or local utilities.

4) Storage Devices: Most of the existing storage resources are hydro and pumped storage. However, growth potential for these resources is much smaller than the need for storage necessary to counter growing net demand variability presented by new wind and solar resources. Various storage technologies are emerging to fill the gap. Battery storage appears to be most promising due to improvements in technology as well as economies of scale.

Storage resources tend to make the net demand profile flatter and, as such, are expected to improve reliability. In addition, most battery storage devices can respond in time scales of seconds. Hence they can become valuable enablers of fast controls in a smart grid. Storage resources of various sizes can be distributed throughout the grid ranging from end user loads to major substations and central power stations. This feature can help to alleviate congestion at both transmission and distribution levels [95].

5) Electric Transportation: Plug-in electric vehicles (PEV, PHEV, etc.) continue to become more popular as environmental concerns increase. They are a significant means to reduce green house gases and reliance on fossil fuels. They will be a significant factor in load growth with a potential to eventually consume 600 TWh/year assuming 30 kwh for a 100-mile trip [96], and 10,000 miles per year for 200 million vehicles in the U.S. For greater adoption of all-electric vehicles, the issue of recharge time has to be resolved. Long recharge times lead to generally unacceptable level of vehicle unavailability and short recharge times have potential to increase congestion, especially at the distribution levels [97].

From reliability viewpoint, electric transportation has features similar to both demand response resources and storage resources. As PHEVs present a significant factor of load growth, this can also aggravate the demand variability and associated reliability problems depending on the charging schemes and consumer behavioral patterns.

D. Security

Based on the evolution of power system communication infrastructures and the concern of cyber security, many new issues have arisen in the context of smart grid.

1) Information Security Domains: Since the SCADA/EMS systems have become increasingly integrated, it becomes more difficult to treat the system structure in terms of parts or subsystems. The physical realization of various functions is less evident from a user perspective. Instead, it becomes more natural to study a SCADA/EMS system in terms of domains. This concept in application to power systems was introduced in [98].

A domain is a specific area, wherein specific activities/business operations are going on and they can be grouped together. The security domains are introduced in Figure 10 [99].

When communicating across power utilities, different organizations and companies, using communication networks, the security domains should be recognized. For example, a power utility company could define a security domain and related policies and procedures for its telecontrol activity to assure compliance with legislative or regulatory requirements. If similar definitions, procedures, policies, etc. were developed by other power utility companies, it would be easier to discuss and define common rules for the information exchange or the usage of common resources in a communication infrastructure. However today, there are no common definitions including the term security. Also, there are no common control system security policies or procedures, although groups such as IEC [100], ISA [101], and NIST [102], [103], are working on generic policies and procedures.

2) Government Coordination on SCADA Security: A government coordination action between different authorities and agencies were started in [104], focusing on SCADA security. The action is based on the participation of the power utilities, water companies, and railway systems, which have SCADA systems as the critical part of operations. Also, the security policies are represented. Here, the expertise is gathered and experiences are shared, including both domestic and international knowledge; everything with the purpose of securing the SCADA systems being part of the critical information infrastructures. As a natural step, the SCADA Security Guideline has been developed in [105]. Also, technical guidelines and administrative recommendations are developed which are available for free downloading, that support the securing actions of the SCADA systems in the different areas of operations: power, water, and transportation.

3) De-Coupling Between Operational SCADA/EMS and Admin IT: When the existing SCADA/EMS systems are being

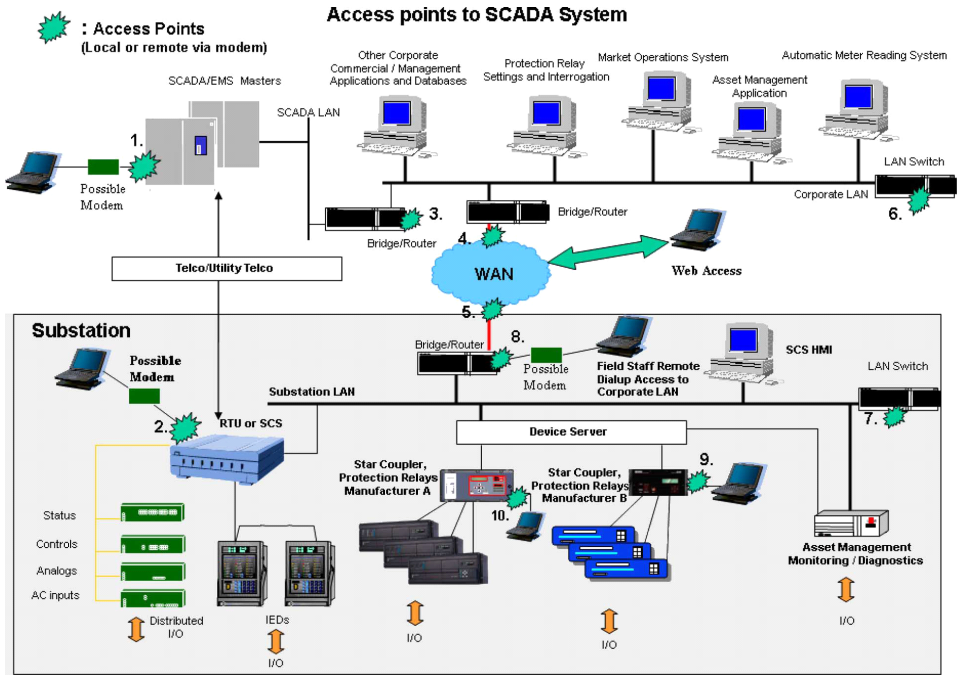


Fig. 11. Vulnerable Access Points to SCADA System [99]

refurbished or replaced, the information and IT security issues must be taken into account. If a SCADA/EMS system is to be refurbished, the operational SCADA/EMS system part must be shielded from the administrative part, such that the operational part is protected from digital threats that are possible over the Internet connection. If a SCADA/EMS system is to be replaced, it is then a good occasion to reconsider an overall system structure, and then incorporate IT security on all SCADA/EMS levels. A way towards this more secure state is to, if possible, de-couple the operational SCADA/EMS system and the administrative IT system. Also, an alternative may be to secure the firewall configuration in between operational and administrative parts.

4) Threats: The fact that SCADA/EMS systems are now being interconnected and integrated with external systems creates new possibilities and threats in cyber security. Some of these new issues have been emphasized in [98] and [106]. The various interconnections of a substation were investigated in [107], as shown in Figure 11. All the numbered access points (1-10) elucidates the possible points where to the substation can be accessed. This number creates an operational environment that implies possible digital entrances and hence digital vulnerabilities at the same time.

5) Vulnerability: As presented in [108], using a wireless sensor network (WSN) in AMI in a smart grid is so vulnerable to be attacked by an intelligent adversary even with an ordinary microwave stove. Brodsky et al. [109] documented a denial-of-service attack on IEEE 802.15.4 wireless sensor networks used within the smart grid. The equipment needed for such an attack is inexpensive (about $70).

6) Privacy: The privacy of terminal customers and smart metering networks is important to the eventual acceptance by the public. Research in this area is going on and smart meter users will need to be reassured that their data is secure. In [110] the authors describe a method for securely anonymizing frequent (e.g., every few minutes) electrical metering data sent by a smart meter. Although such frequent metering data may be required by a utility or electrical energy distribution network for operational reasons, this data may not necessarily need to be attributable to a specific smart meter or consumer. However, it needs to be securely attributable to a specific location (e.g. a group of houses or apartments) within the smart grid.

VI. Conclusion

In this paper, we presented the background and motivation for smart grid communication infrastructures. We showed that a smart grid built on the technologies of sensing, communications, and control technologies offer a very promising future for utilities and users. We reviewed several industrial trials and summarized the basic requirements of communication infrastructures in smart grid paradigm. Efficiency, reliability and security of interconnected devices and systems are critical to enabling smart grid communication infrastructures. Interoperability must be achieved while avoiding being isolated into noncompetitive technical solutions and the need for wholesale replace of existing power communication systems. Alignment behind technical standards must be balanced with creating an environment that encourages innovation so that the overall communication infrastructure may continue to evolve. Based on the above survey, we can focus on those challenges to smart grid communication infrastructures in both system design and operations to make it more efficient and secure.

References

[1] U.S. Department of Energy, [online] Available: www.oe.energy.gov.

[2] F. Rahimi and A. Ipakchi, "Demand Response as a Market Resource Under the Smart Grid Paradigm," IEEE Trans. Smart Grid, vol.1, no.1, pp.82-88, June 2010.

[3] U.S. Department of Energy, National Energy Technology Laboratory, "A vision for the modern Grid," March 2007.

[4] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," IEEE Network, vol.25, no.5, pp.6-14, September-October 2011.

[5] S. Massoud Amin and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," IEEE Power and Energy Mag., vol. 3, pp. 34-41, 2005.

[6] A. Vaccaro and D. Villacci, "Performance analysis of low earth orbit satellites for power system communication," Electric Power Systems Research, vol. 73, pp. 287-294, 2005.

[7] IEC-TC 57, "Communication networks and systems in substations- Part 1: Introduction and overview," IEC Standard IEC/TR 61850-1, Edition 1.0, 2003.

[8] J. G. Cupp and M. E. Beehler, "Implementing Smart Grid Communications" TECHBriefs 2008 No. 4, pp. 5-8.

[9] A. Ghassemi, S. Bavarian, and L. Lampe, "Cognitive Radio for Smart Grid Communications," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 297-302, 2010.

[10] K. Jeonggil, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, and P. Levis, "Connecting low-power and lossy networks to the internet," IEEE Commun. Mag., vol. 49, pp. 96-101, 2011.

[11] V. Madani, A. Vaccaro, D. Villacci and R. L. King, "Satellite Based Communication Network for Large Scale Power System," 2007 iREP Symposium - Bulk Power System Dynamics and Control - VII, Revitalizing Operational Reliability, August 19-24, 2007, Charleston, SC, USA.

[12] D. Dzung, I. Berganza, and A. Sendin, "Evolution of powerline communications for smart distribution: From ripple control to OFDM," in 2011 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2011), pp. 474-478.

[13] M. Y. Zhai, "Transmission Characteristics of Low-Voltage Distribution Networks in China Under the Smart Grids Environment," IEEE Trans. Power Del., vol. 26, pp. 173-180, 2011.

[14] N. Ginot, M. A. Mannah, C. Batard, and M. Machmoum, "Application of Power Line Communication for Data Transmission Over PWM Network," IEEE Trans. Smart Grid, vol. 1, pp. 178-185, 2010.

[15] G. Bumiller, L. Lampe, and H. Hrasnica, "Power line communication networks for large-scale control and automation systems," IEEE Commun. Mag., vol. 48, pp. 106-113, 2010.

[16] A. Haidine, B. Adebisi, A. Treytl, H. Pille, B. Honary, and A. Portnoy, "High-speed narrowband PLC in Smart Grid landscape - State-of-the-art," in IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2011), pp. 468-473, 2011.

[17] U.S. Department of Energy, Energy Efficiency and Renewable Energy, "Annual Report on US Wind Power Installation, Cost and Performance Trends: 2007," May 2008.

[18] I. Marti, "Evaluation of Advanced Wind Power Forecasting Models," European Wind Energy Conference, Athens, Feb 27- Mar 2, 2006.

[19] The New York State Energy Research and Development Authority, "The Effects of Integrating Wind Power on Transmission System Planning, Reliability and Operations, Report on Phase 2: System Performance Evaluation," Albany, NY, March 4, 2005.

[20] "Waiting for the sunrise (solar energy forecast) (Science and Technology)," The Economist , May 19, 1990.

[21] U.S. DoE Solar Energy Technologies Program, "Solar Energy Industry Forecast: Perspectives on U.S. Solar Market Trajectory", May 30, 2008.

[22] National Renewable Energy Laboratory, "Executive Summary: Assessment of Parabolic Trough and Power Tower Solar Technology Cost and Performance Forecasts," October 2003.

[23] T. Van Loon, T. Vu Van, A. Woyte, F. Truyens, B. Bletterie, J. Reekers, B. Blazic, and R. Engelen, "Increasing photovoltaics grid penetration in urban areas through active distribution systems: First large scale demonstration," in Third International Conference on Infrastructure Systems and Services: Next Generation Infrastructure Systems for Eco-Cities (INFRA 2010), pp. 1-4, 2010.

[24] A. B. Pedersen, E. B. Hauksson, P. B. Andersen, B. Poulsen, C. Træholt, and D. Gantenbein, "Facilitating a Generic Communication Interface to Distributed Energy Resources: Mapping IEC 61850 to RESTful Services," First IEEE International Conference onSmart Grid Communications (SmartGridComm 2010), pp. 61-66, 2010.

[25] D. Infield and F. Li, "Integrating micro-generation into distribution systems: a review of recent research," in Proc. IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, July 2008.

[26] R. Sauter and J. Watson, "Strategies for the deployment of micro-generation: Implications for social acceptance", Elsevier, Energy Policy, Vol. 35, Iss.5, pp.2770-2779, May 2007.

[27] J. Watson, R. Sauter, B. Bahaj, P. James, L. Myers and R. Wing, "Domestic micro-generation: Economic, regulatory and policy issues for the UK," Energy Policy, Vol. 36, Iss. 8, Pages 3095-3106, August 2008.

[28] P. Tenti, A. Costabeber, and P. Mattavelli, "Improving power quality and distribution efficiency in micro-grids by cooperative control of Switching Power Interfaces," International Power Electronics Conference (IPEC 2010), pp. 472-479, 2010.

[29] A. Costabeber, P. Tenti, and P. Mattavelli, "Surround control of distributed energy resources in micro-grids," IEEE International Conference on Sustainable Energy Technologies (ICSET 2010), pp. 1-6, 2010.

[30] D. Backer, "Power Quality and Asset Management The Other Two-Thirds of AMI Value," IEEE Rural Electric Power Conference, pp. 6-8, May 2007.

[31] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrastructure (AMI)," Proceedings of IEEE Power and Energy Society General Meeting Conversion and Delivery of Electrical Energy in the 21st Century, July 2008.

[32] G. A. Taylor, M. R. Irving, P. R. Hobson, C. Huang, P. Kyberd, and R. J. Taylor, "Distributed monitoring and control of future power systems via grid computing," IEEE Power Engineering Society General Meeting, 2006.

[33] E. Chikuni, M. Dondo, "Investigating the security of electrical power systems SCADA," IEEE AFRICON 2007, pp.1-7, Sep 2007.

[34] C. Ten, C. Liu, and M. Govindarasu, "Cyber-vulnerability of power grid monitoring and control systems," In Proceedings of the 4th Annual Workshop on Cyber Security and information intelligence Research (CSIIRW '08), Oak Ridge, Tennessee, May 12 - 14, 2008.

[35] J. D. Fernandez and A. E. Fernandez, "SCADA systems: vulnerabilities and remediation," Journal of Computing Sciences in Colleges archive,Vol. 20, Iss. 4, pp.160-168, April, 2005.

[36] Y. Serizawa, et al., "Present and future ICT infrastructures for a smarter grid in Japan," in Innovative Smart Grid Technologies (ISGT2010), pp. 1-5, 2010 .

[37] O. Samuelsson, S. Repo, R. Jessler, J. Aho, M. Karenlampi, and A. Malmquist, "Active distribution network - Demonstration project ADINE," in IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe 2010), pp. 1-8, 2010.

[38] F. Rahimi and A. Ipakchi, "Overview of Demand Response under the Smart Grid and Market paradigms," in Innovative Smart Grid Technologies (ISGT 2010), pp. 1-7, 2010.

[39] R. Davies, "Hydro one's smart meter initiative paves way for defining the smart grid of the future," in Power & Energy Society General Meeting, 2009. (PES '09),pp. 1-2, 2009.

[40] E. Santacana, et al., "Getting Smart," Power and Energy Magazine, IEEE, vol. 8, pp. 41-48, 2010

[41] D. Sun, "The Utilization and Development Strategies of Smart Grid and New Energy," in Proceedings of Asia-Pacific Power and Energy Engineering Conference (APPEEC 2010), pp. 1-4, 2010.

[42] C. Jaeseok, J. Park, M. Shahidehpour and R. Billinton, "Assessment of CO2 reduction by renewable energy generators," in Innovative Smart Grid Technologies (ISGT), pp.1-5, 2010.

[43] F. A. Rahimi, "Challenges and opportunities associated with high penetration of distributed and renewable energy resources," in Innovative Smart Grid Technologies (ISGT), 2010, 2010, pp. 1-1.

[44] G. Lorenz, "Regulatory framework to incentivise Smart Grids deployment - EURELECTRIC views," The 20th International Conference and Exhibition on Electricity Distribution - Part 2, 2009. (CIRED 2009), pp. 1-26, 2009.

[45] D. Tuan, "The Energy Web: Concept and challenges to overcome to make large scale renewable and distributed energy resources a true reality," in 7th IEEE International Conference on Industrial Informatics, pp.384-389, 2009.

[46] http://www.bchydro.com/planning_regulatory/projects/smart_metering_infrastructure_program.html.

[47] W. Luan, D. Sharp, S. Lancashire, "Smart grid communication network capacity planning for power utilities," 2010 IEEE PES Transmission and Distribution Conference and Exposition, pp.1-4, 19-22 April 2010.

[48] A. Clark, C. J. Pavlovski, and J. Fry, "Transformation of energy systems: The control room of the future," in Proceedings of IEEE Electrical Power & Energy Conference (EPEC), 2009, pp. 1-6.

[49] ZigBee Specification, ZigBee Alliance, ZigBee Document 053474r17, January 2008.

[50] M. Fang, J. Wan, X. Xu, and G. Wu, "System for Temperature Monitor in Substation with ZigBee Connectivity," IEEE International Conference on Communication Technology, pp. 25-28, Nov. 2008.

[51] B. Chen, M. Wu; S. Yao, B. Ni, "ZigBee Technology and its Application on Wireless Meter-reading System," IEEE International Conference on Industrial Informatics, Aug. 2006, pp. 1257 - 1260.

[52] S. W. Luan, J. H. Teng, S. Y. Chan, L. C. Hwang, "Development of a Smart Power Meter for AMI Based on ZigBee Communication," IEEE 8th International Conference on Power Electronics and Driver Systems, Taiwan, Paper No. 284, 2009.

[53] S. W. Luan; J. H. Teng, S. Y. Chan, L. C. Hwang, "Development of an automatic reliability calculation system for advanced metering infrastructure," 8th IEEE International Conference on Industrial Informatics (INDIN 2010), pp.342-347, 13-16 July 2010.

[54] P. Zhang, F. Li, N. Bhatt, "Next-Generation Monitoring, Analysis, and Control for the Future Smart Control Center," IEEE Trans. Smart Grid, vol.1, no.2, pp.186-192, Sept. 2010.

[55] A. Aggarwal, S. Kunta, P. K. Verma, "A proposed communications infrastructure for the smart grid," in Innovative Smart Grid Technologies (ISGT), 2010, pp. 1-5.

[56] C. H. Hauser, D. E. Bakken, I. Dionysiou, K. H. Gjermundrod, V. S. Irava, J. Helkey, A. Bose, "Security, trust, and QoS in Next generation control and communication for large power systems," Int. J. Critical Infrastructures, Vol. 4, 2008.

[57] Smart Grids Interoperability Standards Project, [online] Available http://www.nist.gov/smartgrid/.

[58] NIST framework and Roadmamp for Smart Grid interoperability standards release 1.0.

[59] IEEE Smart Grid, [online] Available http://smartgrid.ieee.org/nist-smartgrid-framework.

[60] A. F. Snyder and M. T. G. Stuber, "The ANSI C12 protocol suite - updated and now with network capabilities," in Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources (PSC 2007), pp. 117-122, 2007.

[61] F. Lobo, A. Cabello, A. Lopez, D. Mora, and R. Mora, "Distribution Network as communication system," in SmartGrids for Distribution, 2008. IET-CIRED. CIRED Seminar, 2008, pp. 1-4.

[62] Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, Jun. 17, 2009.

[63] S. Hurd, R. Smith, G. Leischner, "Tutorial: Security in Electric Utility Control Systems," 61st Annual Conference for Protective Relay Engineers, pp.304-309, 1-3 April 2008.

[64] Draft Smart Grid Cyber Security Strategy and Requirements, NIST IR 7628, Sep. 2009.

[65] GridWise Architecture Council Interoperability Framework, http://www.gridwiseac.org/pdfs/interopframework_v1_1.pdf.

[66] R. DeBlasio, C. Tom, "Standards for the Smart Grid," IEEE Energy 2030 Conference, pp.1-7, 17-18 Nov. 2008.

[67] M. Masera, A. Stefanini and G. Dondossola, "The Security of Information and Communication Systems and the E+I Paradigm," in Critical Infrastructures at Risk. vol. 9, A. V. Gheorghe, M. Masera, M. Weijnen and D. Vires, Eds., Springer Netherlands, 2006, pp. 85-116.

[68] B. Stephens, "System-Wide Information Management (SWIM) Demonstration Security Architecture," IEEE/AIAA 25th Digital Avionics Systems Conference, pp.1-12, 15-19 Oct. 2006.

[69] P. Lund; "The Danish Cell Project - Part 1: Background and General Approach," IEEE Power Engineering Society General Meeting, pp.1-6, 24-28 June 2007.

[70] IEEE Std 1547.3, "IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected With Electric Power Systems," vol., no., pp.1-158, 2007.

[71] G. Deconinck, "Metering, Intelligent Enough for Smart Grids?," in Securing Electricity Supply in the Cyber Age. vol. 15, Z. Lukszo, et al., Eds., Springer Netherlands, 2010, pp. 143-157.

[72] IEEE Std 802.11i, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," pp. 1-175, 2004.

[73] IEEE Std 802.16e, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," pp. 1-822, 2006.

[74] U.S. Department of Energy, "Wireless Procurement Language in Support of Advanced Metering Infrastructure Security", 2009.

[75] IEEE P2030, Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads. July 2009.

[76] D. Becker, T. L. Saxton, and M. Goodrich, "CIM standard for dynamic model exchange," in IEEE Power and Energy Society General Meeting, pp. 1-3, 2010.

[77] IEEE Unifies Power, Communications, and IT with launch of Smart Grid Interoperability Standards Project P2030. IEEE Standards Association P2030, June, 2009.

[78] S. L. Woodruff, "Complexity in power systems and consequences for real-time computing", IEEE PES Power Systems Conference and Exposition, 10-13 Oct. 2004.

[79] R. Dougal, T. Lovett, A. Monti and E. Santi, "A Multilanguage Environment For Interactive Simulation And Development Of Controls For Power Electronics," IEEE PESC01.

[80] R. Dougal, A. Monti and F. Ponci, "The Incremental Design Process for Power Electronic Building Blocks," invited paper for IEEE PES Annual Meeting 2006.

[81] R. Dougal and A. Monti, "The Virtual Test Bed as a tool for rapid system engineering," IEEE Systems Conference, April 2007.

[82] L. Cristaldi, A. Ferrero, M. Lazzaroni, A. Monti and F. Ponci, "Multiresolution Modeling: an Experimental Validation," IEEE-IMCT02, Ankorage (USA), 21-23 May 2002.

[83] F. Ponci, A. Monti and E. Santi, "Discrete-Time Multi- Resolution Modeling of Switching Power Converters Using Wavelets," SIMULATION, Transactions of the Society for Modeling and Simulation International, February 2009, vol. 85, no. 2, pages 69-88.

[84] A. Monti and R. Dougal, "The Virtual Test Bed Concept For Virtual Prototyping Of Complex Systems," in Proc. AED, 2004.

[85] R. Rios-Zalapa, X. Wang, J. Wan, K. Cheung, "Robust dispatch to manage uncertainty in real time electricity markets," Innovative Smart Grid Technologies (ISGT), pp.1-5, 19-21 Jan. 2010.

[86] R. Krebs, B. M. Buchholz, Z. A. Styczynski, K. Rudion, C. Heyde, Y. Sassnick, "Vision 2020 ł Security of the network operation today and in the future. German experiences," IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp.1-6, 20-24 July 2008.

[87] M. Amin, "Energy Infrastructure Defense Systems," Proc. IEEE , vol.93, no.5, pp.861-875, May 2005.

[88] J. Wen, P. Arons, W.-H. E. Liu, "The role of Remedial Action Schemes in renewable generation integrations," Innovative Smart Grid Technologies (ISGT), pp.1-6, 19-21 Jan. 2010.

[89] M. McGranaghan, D. Von Dollen, P. Myrda, E. Gunther, "Utility experience with developing a smart grid roadmap," IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, pp.1-5, 20-24 July 2008.

[90] M. Kezunovic, F. Xu, B. Cuka, P. Myrda, "Intelligent processing of IED data for protection engineers in the Smart Grid," MELECON 2010 - 2010 15th IEEE Mediterranean Electrotechnical Conference, pp.437-442, 26-28 April 2010.

[91] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid," IEEE Trans. Smart Grid, vol. 1, pp. 57-64, 2010.

[92] K. Mets, T. Verschueren, W. Haerick, C. Develder, F. De Turck, "Optimizing smart energy control strategies for plug-in hybrid electric vehicle charging," IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps), pp.293-299, 19-23 April 2010.

[93] K. Moslehi and R. Kumar, "Smart Grid - a reliability perspective," in Innovative Smart Grid Technologies (ISGT 2010), pp. 1-8, 2010.

[94] Markets Committee of the ISO/RTO Council, "Harnessing the Power of Demand - How ISOs and RTOs Are Integrating Demand Response into Wholesale Electricity Markets," October 16, 2007.

[95] R. N. Anderson, "The Distributed Storage-Generation Smart Electric Grid of the Future", white paper, Columbia University.

[96] R. Gawel, "Tesla's Tests Confirm Roadster's 245-Mile Range," Electronic Design, November 5, 2007.

[97] S. Acha, T. C. Green, N. Shah, "Effects of optimised plug-in hybrid vehicle charging strategies on electric distribution network losses," IEEE PES Transmission and Distribution Conference and Exposition, pp.1-6, 19-22 April 2010.

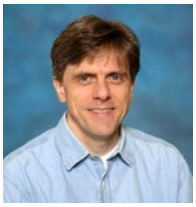
[98] G. Ericsson, O. Torkilseng, G. Dondossola, T. Jansen, J. Smith, D. Holstein, A. Vidrascu, and J.Weiss, "Security for Information Systems and Intranets in Electric Power Systems," Tech Brochure (TB) 317 CIGR, 2007.

[99] G. Ericsson, "Cyber Security and Power System Communication–Essential Parts of a Smart Grid Infrastructure," IEEE Trans. Power Delivery, vol.25, no.3, pp.1501-1507, July 2010.
[100] IEC, Power System Control & Associated Communications-Data & communication Security 62351 part 1-8, TS.
[101] ISA 99 [Online]. Available: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=682
[102] NIST, Computer Security Division, Computer Security Resource Centre. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html.
[103] NIST ICS Security Project [Online].Available: http://csrc.nist.gov/seccert/ics/index.html.
[104] Swedish Civil Contingencies Agency, "SCADA Security Coordination".
[105] Swedish Civil Contingencies Agency,"Guide to Increased Security in Process Control Systems for Critical Societal Functions".
[106] G. Ericsson, O. Torkilseng, G. Dondossola, L. Pitre-Cambacds, S. Duckworth, A. Bartels, M. Tritschler, T. Kropp, J.Weiss, and R. Pellizzonni, "Treatment of Information Security for Electric Power Utilities (EPUs)," Technical Brochure (TB), CIGRE, to appear 2010.
[107] P. Roche; "Cyber security considerations in power system operations," CIGRE Electra No. 218, February 2005.
[108] T. Goodspeed, D. R. Highfill and B.A. Singletary, "Low-level Design Vulnerabilities in Wireless Control Systems Hardware," Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp.3-1-3-26, January 21- 22, 2009.
[109] J. Brodsy and A. McConnell, "Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks," Proceedings of the SCADA Security Scientific Symposium 2009 (S4), pp. 2-1-2 -11, January 21-22, 2009.
[110] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010), pp. 238-243, 2010.

Ye Yan is a Ph.D. student in the Department of Computer and Electronics Engineering (CEEN), University of Nebraska-Lincoln (UNL). His current research articles on wireless network, network security, and smart grid communication has been published in IEEE and other international journals and conferences. He has been serving as TPC members on several IEEE conferences and reviewers for many international journals and conferences. He is a student member of IEEE.

Yi Qian is an Assistant Professor in the Department of Computer and Electronics Engineering, University of Nebraska-Lincoln (UNL). His research interests include information assurance and network security, network design, network modeling, simulation and performance analysis for next generation wireless networks, wireless ad-hoc and sensor networks, vehicular networks, broadband satellite networks, optical networks, high-speed networks and the Internet. Prior to joining UNL, he worked in the telecommunications industry, academia, and the U.S. government. Some of his previous professional positions include serving as a senior member of scientific staff and a technical advisor at Nortel Networks, a senior systems engineer and a technical advisor at several start-up companies, an Assistant Professor at University of Puerto Rico at Mayaguez, and a senior researcher at National Institute of Standards and Technology. He has a successful track record to lead research teams and to publish research results in leading scientific journals and conferences. Several of his recent journal articles on wireless network design and wireless network security are among the most accessed papers in the IEEE Digital Library. Dr. Yi Qian is a member of ACM and a senior member of IEEE. He is currently serving as the Vice Chair for Conferences - Communications and Information Security Technical Committee (CISTC) for IEEE Communications Society. He is also serving as the IEEE Communications Society CISTC Representative to the Ad Hoc Committee on Smart-Grid Communications.

Hamid Sharif is the Charles J. Vranek Professor of the College of Engineering at the University of Nebraska-Lincoln. He is also the Director of the Advanced Telecommunications Engineering Laboratory (TEL) at University of Nebraska. Professor Sharif has published a large number of research articles in international journals and conferences and has been the recipient of a number of best paper awards. Dr. Sharif has been serving on many IEEE and other international journal editorial boards and currently is the co-editor-in-chief for the Wiley Journal of Security and Communication Networks. He has contributed to the IEEE in many roles including the elected Chair of the Nebraska Section, elected Chair of the Nebraska Computer Chapter, elected Chair of the Nebraska Communications Chapter, and the Chapter Coordinator for the IEEE Region 4 in US.



David Tipper is an Associate Professor and Director of the Graduate Telecommunications and Networking Program at the University of Pittsburgh. He is a graduate of the University of Arizona (Ph.D. EE, M.S.S.I.E.) and Virginia Tech (B.S.E.E.). His current research focuses on network design, energy efficiency, information assurance techniques, time varying network performance analysis and control.