A Survey on Smart Grid Cyber-Physical System Testbeds

Mehmet Hazar Cintuglu, *Member, IEEE*, Osama A. Mohammed, *Fellow, IEEE*, Kemal Akkaya, *Senior Member, IEEE*, and A. Selcuk Uluagac, *Senior Member, IEEE*

***Abstract*—An increasing interest is emerging on the development of smart grid cyber-physical system testbeds. As new communication and information technologies emerge, innovative cyber-physical system testbeds need to leverage realistic and scalable platforms. Indeed, the interdisciplinary structure of the smart grid concept compels heterogeneous testbeds with different capabilities. There is a significant need to evaluate new concepts and vulnerabilities as opposed to counting on solely simulation studies especially using hardware-in-the-loop test platforms. In this paper, we present a comprehensive survey on cyber-physical smart grid testbeds aiming to provide a taxonomy and insightful guidelines for the development as well as to identify the key features and design decisions while developing future smart grid testbeds. First, this survey provides a four step taxonomy based on smart grid domains, research goals, test platforms, and communication infrastructure. Then, we introduce an overview with a detailed discussion and an evaluation on existing testbeds from the literature. Finally, we conclude this paper with a look on future trends and developments in cyber-physical smart grid testbed research.**

***Index Terms*—Cyber-physical systems, testbed, smart grid.**

I. Introduction

THE EXISTING power grid is expected to be restructured as a cyber-physical system including smart devices not only to carry power flow, but also to transmit data for advanced monitoring and control applications. Enhancement of the power grid using two-way flows of electricity and information is expected to form *smart grids* equipped with intelligent features such as self-healing, adaptive protection and control, customer involvement, and electric vehicles [1].

The smart grid concept embraces many research areas including sub-domains, such as bulk generation, non-bulk generation, transmission, distribution, customer, markets, operations, service providers and foundational support systems [2]–[4]. Optimization, automation and control of the smart grid is anticipated to be based on grid-integrated near real-time communications between advanced cyber-physical system sensors and devices. Advanced communication technologies are essential to save energy, reduce costs and increase the reliability of the grid [5]. However, cyber-physical infrastructure is the major driving force of the future smart grid vision as a foundational support system, meanwhile the key challenge for actual field deployment. Utilities and independent system operators seek proper ways to implement future smart grid concepts easily and securely for different application layers, such as metering, monitoring, operation, protection, automation and markets [6], [7].

The highly complex and interdisciplinary nature of the smart grid concept necessitates the implementation of testbeds with different capabilities for extensive experimental verifications. The smart grid research results so far have been mainly based on simulations [8]–[10]. However, real-world applications require prototype implementations on actual testbeds. Only in this way, a fast verification of concepts would spur research results that can be transferred to power system industry and broader public use. On the other hand, testbeds provide unique educational platforms for students as well as researchers for multi-user experimental facilities and proof of concept verifications for various smart grid domains.

Moreover, the advent of smart grid with extensive communication capabilities [11]–[14] yield new security vulnerabilities due to a high dependency on cyber information. The key challenge is to efficiently exploit communication and information technology infrastructure while ensuring the security by minimizing the susceptibility to cyber-attacks [15]–[18]. Aligned with the future smart grid visions, it is imperative to develop proper testbeds to test interoperability [19] and cyber security vulnerabilities [18]. Most testbeds are mainly built for particular project evaluation and verification purposes. Although few of the testbeds provide extensive capability to support all research areas, the majority do not provide a complete hardware/software test platform for all research area applications at the same time. Universities and research facilities usually consider specific requirements of the methods to be tested and develop the testbed platforms accordingly. However, the tightly coupled networked structure of the smart grid necessities a comprehensive testbed vision [20], [21] to be able to facilitate experiments simultaneously. All smart grid domains have to be evaluated individually, but at the same time need to be connected to achieve a global awareness of the ongoing research. Smart grid testbeds consist of hardware (physical) and software (cyber) components. Hardware structure includes generator stations, transmission lines and load models. On the

Manuscript received April 8, 2016; revised July 21, 2016 and September 15, 2016; accepted November 3, 2016. Date of publication November 10, 2016; date of current version February 22, 2017. This work was supported by the U.S. Department of Energy.

The authors are with the Energy Systems Research Laboratory, Cyber-Physical Systems Security Laboratory and Advanced Wireless and Security Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174 USA (e-mail: mohammed@fiu.edu).

Digital Object Identifier 10.1109/COMST.2016.2627399

TABLE I
LIST OF SMART GRID SURVEYS

Survey Area	Survey Content	Year of Publication	References
Physical Power Infrastructure	*Field demonstrations, Microgrids and Distributed energy resources*	2012 - 2014	[6]-[7]-[22]-[23]-[24]
Communication Networking	*Communication protocols, Quality of service (QoS), Time synchronization Communication routing protocols, Energy web, HANs, NANs, WANs*	2012 - 2013	[11]-[12]-[13]-[14]
Security and Privacy	*Cyber security, Data integrity, Privacy, Authentication, Encryption*	2012 - 2014	[15]-[16]-[17]-[18]
Smart Grid Protocols	*Information protocol standardization IEC 61850, IEC 61970/61968*	2010	[19]
Cloud Computing	*Cloud computing and communication for smart grid applications*	2013 - 2014	[20]-[21]

other hand, the cyber component consists of communication and information infrastructure. The implementation of testbeds is a challenging task due to hardware/software cost and highly qualified staff requirements.

The smart grid research, which requires electrical experimentations, such as protection and energy management, compels strict safety requirements for testbeds. Due to the high investment cost and safety concerns of hardware-based power system components, most of the testbeds adopt simulation or emulator platforms. In reality, very few of them are truly capable of facilitating experiments with actual generation units, transmission/distribution lines and load models. Although the number of existing testbeds are few, the relatively new research area attracts many institutions in smart grid field. In the near future, it is inevitable that many new testbeds will be introduced with various capabilities.

In this survey, we present a systematic study for smart grid cyber-physical testbeds with a focus on their domains, research goals, test platforms, and communication infrastructure. An extensive overview of existing testbeds is provided. Then, we evaluate the testbeds on research support capacity, communication capability, security and privacy awareness, protocol support and remote access capability. We believe that this survey will provide an extensive guideline for the new researchers who would like to explore this exciting research area. Furthermore, this paper can be used to determine the most convenient testbeds for the researchers to conduct their experiments.

The rest of the paper is structured as follows. Section II provides related work briefly and reemphasizes the main contributions of this paper. Section III introduces a background on smart grid application domains and priority research areas. Section IV analyzes the alternatives in developing smart grid cyber-physical testbeds and provides taxonomies in terms of the domain, research goal, implementation platform, and communication infrastructure. Section V provides an extensive overview of existing testbeds. Existing testbeds are evaluated by defined taxonomy perspectives in Section VI. Open research issues and desirable testbed features are discussed in Section VII. Section VIII concludes the paper.

II. RELATED WORK AND CONTRIBUTIONS

Although a number of survey papers already exist in literature on smart grid related concepts as shown in Table I, none of these previous surveys have focused on cyber-physical smart grid testbeds. This work is the first to discuss the requirements of testbed features in-depth, and how they meet expected solutions. List of design choices exploited by the existing testbeds for the institutions planning to build a new testbed were identified. A comprehensive taxonomy of the cyber-physical smart grid testbeds with respect to the application domain, research goals, and platform capabilities was presented. Provision of future works, experiments, capability extensions, and new trends that need to be added to testbeds were discussed. Our goal is to enlighten new testbed builders and to help standardize the cyber-physical testbed realization to facilitate real-world deployments with reduced cost and improved performance.

The main contributions of this paper are as follows: 1) we have provided a comprehensive background on smart grid cyber-physical systems concept and how testbeds are important to achieve actual implementation; 2) we have highlighted that all testbeds possess unique infrastructure and targets several research areas; 3) we have presented how existing testbeds conforms the smart grid domains and research areas defined by National Institute of Standards and Technology (NIST); 4) we have provided an evaluation of the existing testbeds by means of five defined features; 5) we have provided future trends and open research issues that needs to be taken into consideration while building new ones or rehabilitating the existing ones.

III. BACKGROUND ON SMART GRID

This section provides an overview of smart grid domains and research areas. The existing power grid was not designed in a flexible way to meet future demands including advanced metering, smart appliances, integration of renewable energy resources, and deregulated markets. The involvement of *smart* devices, communication, and management mechanisms are promising. However, the existing power grid may not be able to provide solutions to extensive demands with its current state. Therefore, to stimulate the smart grid realization,

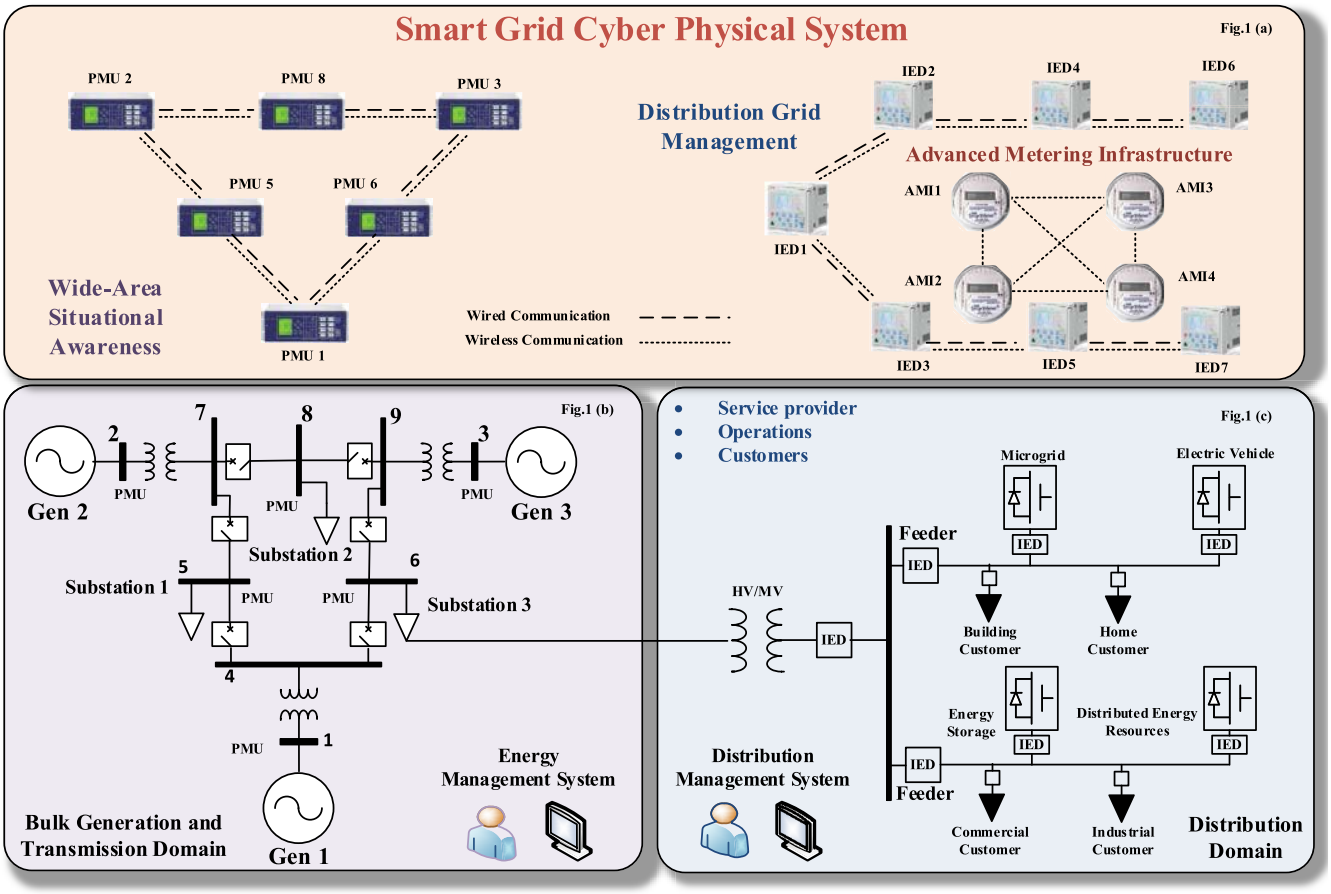

Fig. 1. An overview of Smart Grid Cyber-Physical infrastructure (a) Communication links of Phasor Measurement Units (PMU) in transmission energy management system, IEDs in distribution management system, and smart meters in advanced metering infrastructure. (b) Representation of bulk generation and transmission domains as standard IEEE 9 bus power system network. (c) Representation of distribution domain including service providers, operations and customers.

NIST has defined interconnected domains and priority research areas [25], which are articulated below.

A. Smart Grid Domains

The smart grid is composed of 7 interconnected domains according to NIST [25]. Each domain and its sub-domains include corresponding devices, systems, or programs. The devices can be smart meters, distributed energy resources (DER), or intelligent electronic devices (IED). Various systems of these devices establish decision-making and information exchange between domains with intended applications. Individual domains have to be evaluated separately; however, there are common requirements, such as communication protocols, communication media, networking, and security. Fig. 1 illustrates an overview of smart grid cyber-physical system.

1) Customer Domain: Three types of end users exist: home, commercial/building, and industrial. With the emerging smart grid, end users are also in an ongoing change from consumers to producer-consumers (prosumers) by providing distributed energy generation, storage, and energy management [26], [27]. The main interaction of the prosumers and grid operators is realized through microgrid management. Microgrids are the small scale decentralized electricity networks featuring internal generation and distribution with individual priorities. Prosumers are expected to be equipped with a cyber-physical infrastructure and be aware of the consequences of their actions on the power grid.

2) Market Domain: Market management, retailing, aggregation, trading, market operations, and ancillary operations are the typical market domain applications [28]. Economical unit commitment, scheduling of DERs, and power sharing between multiple units in a microgrid are the major concerns. In open market conditions, utilities are no longer monopolized hence DER stakeholders are the private entities that can compete with regional utilities. The electricity trade can be handled locally in a region by several microgrid investors or cross-border trading by utility wholesale market and neighboring regional systems [29]. A vast number of DERs should be able to operate incorporating a large number of complicated operational functions. New generation grids require fast intelligent decision-making algorithms and advanced cyber-physical infrastructure since the power system operators will be inefficient in dealing with highly active and changing operations in the future grid.

3) Service Provider Domain: The dynamic market-driven ecosystem system is the major concern of the service providers, while ensuring a safe operation of the critical

power structure. Customer management, smart device installment, and smart building management which can respond to demand response signals and billing facilities are the typical applications in the service provider domain [30], [31].

4) Operation Domain: The operation domain is the entity responsible for safe and reliable operation of the power system. Energy management systems (EMS) handle the efficient operation of the transmission level operations, while distribution management systems (DMS) are utilized to handle distribution level. The applications of this domain includes extensive power system operations, such as monitoring, control, protection, and analysis.

5) Bulk Generation Domain: Traditional large scale generation units, such as nuclear, thermal, hydro plants, wind farms, and large scale solar generation are considered as bulk generation units. The generated power is delivered through transmission lines, thus the interaction with the transmission domain is the most critical interface for this domain.

6) Transmission Domain: Regional Transmission Operators or Independent System Operators (RTO/ISO) are the responsible entities for safe operation of the transmission domain. The generated power from bulk generation units is safely transferred to the distribution domain by the transmission domain with the help of generation (supply) and load (demand) balancing practices. Substations are the core components of the transmission domain where high voltage is reduced to distribution level across the electric supply chain.

7) Distribution Domain: The distribution domain serves the interconnection between transmission domains and the customer domain. Metering points, loads, DERs and microgrids are the components of the distribution domain.

B. Smart Grid Priority Research Areas

Smart grid research is prioritized on nine key functionalities: wide-area situational awareness, demand response and consumer energy efficiency, distributed energy resources, energy storage, electric transportation, advanced metering infrastructure, distribution grid management, cyber security and network communications [25]. A cyber-physical system, including cyber security and network communications is a common necessity for all key functionalities. We explain these seven key functionalities in detail below:

1) Wide-Area Situational Awareness: A major blackout, such as the one occurred August 14, 2003 in North American Eastern Interconnection, can result wide-scale power loss for millions of customers [32]. In order to avoid such devastating disasters, monitoring and display of the power system components is required across the interconnection over large geographic areas in near real-time. The aim of the situational awareness research is to diagnose, anticipate, and respond to prevent problems before disruptions arise. A safe, reliable, and economical electric power system requires advanced Wide-area monitoring, protection, and control (WAMPAC) capabilities and applications. Phasor measurement units (PMU) are the devices that provide time-synchronized coherent data from the entire network, which enables the complete system status to be observable and controllable in real-time [33]. Traditionally, most of the efforts have been shown for WAMPAC systems in transmission networks for various applications, including transient stability, modal estimation, and load shedding; and more recently, it has been realized that PMUs represent a useful contribution for the challenging operation of active distribution networks [34].

2) Demand Response and Consumer Energy Efficiency: Demand response (DR) in deregulated electricity markets provide a mechanism and incentives for utilities, business, industrial, and residential customers to lower energy use during times of peak demand or when the power reliability is at risk. Reliable operation of the electricity system necessitates a perfect balance between supply and demand in real-time [35], where DR is crucial for optimizing the balance of the power and supply through smart loads with an advanced communication infrastructure, such as a meshed network, cellular, cloud or Web-based energy information system [36].

3) Distributed Energy Resources (DER): This research area covers utility-independent generation units (non-bulk) and energy storage behind the prosumer energy meter. The generated power is mainly consumed on the prosumer premise as a negative load [37]. Although it is not favorable to distribution system operators (DSO), in some cases, reverse power might be drawn from the prosumer side. Advanced aggregated DERs would form independent grid architectures incorporating microgrids, which can be isolated from the grid in case of a utility outage to form a more resilient and sustainable system [38].

4) Energy Storage: The energy storage concept covers conversion of electrical energy from a power network into a form of energy which can be stored and converted back to electrical energy [39]. Electricity storage research includes many physical forms and is thus managed by various interdisciplinary engineering relationships such as pumped hydroelectric, compressed gas, flywheel (mechanic), battery, and super capacitor [40]. New storage capabilities – especially for distributed storage would benefit the entire grid, from generation to end use.

5) Electric Transportation: Economic and environmental incentives reshape the traditional transportation scheme by enabling large-scale integration of plug-in electric vehicles (PEV), which can significantly reduce dependence on oil and dramatically reduce the carbon footprint [41]. The research on electric transportation covers PEV battery banks, wired-wireless charging stations, and large-scale grid integration.

6) Advanced Metering Infrastructure (AMI): The research goal of AMI technology is an integration of technologies that provide an intelligent connection between consumers and system operators [42]. System operators implement a residential demand response and price signaling mechanism to serve according to dynamic pricing. It consists of communications between hardware and software with advanced local communication capabilities (e.g., Bluetooth, IrDA, and ZigBee protocols) and Internet communications (e.g., Wi-Fi, DSL, and UMTS) [43].

7) Distribution Grid Management: This research area focuses on active distribution operations including

Volt-Var optimization/control, conservation voltage reduction, power quality improvements, system reliability improvements, and outage management [44]. Advanced cyber-physical architectures on distribution grid management aims to maximize the performance of feeders, transformers, and other components of the networked distribution systems and to integrate with transmission systems and customer operations.

8) Cyber Security: The development of smart grid solutions are heavily dependent on power system communication and information infrastructures [45]. While total network and computer integration boost power system capability, vulnerabilities to cyber-attack threats drastically increases [46]. Existing cyber security solutions may not be favorable or efficient for smart grid cyber-physical system security concerns, but require domain specific approaches and solutions [47]. Hence, cyber security in smart grid considers specific communication protocols in various domains, such as the Distributed Network Protocol (DNP3.0), Modbus, IEEE Std. C37.118 and IEC 61850. Open research areas on cyber security for the smart grid includes confidentiality, integrity and availability, authentication, and vulnerability assessment [48], [49].

9) Network Communications: In smart grid operations, power utilities and costumers use a variety of public and private communication networks, both wired and wireless [50]. Utility network communication applications cover residential meters, transformer meters, feeder meters, and field distribution automation communication such as reclosers, switches, voltage regulators and capacitor banks [51]. Prosumer network communication facilitates mainly in Home Area Network (HAN) to intelligently manage devices. Wireless machine-to-machine (M2M) communication between smart meters eliminate human intervention necessity to operate the grid intelligently [52]. Wireless communication is one of the key aspects of realizing the smart grid visions using different technologies such as IEEE 802.11 based wireless LAN, IEEE 802.16 based WiMAX, 3G/4G cellular, LTE, ZigBee based on IEEE 802.15, and IEEE 802.20 based MobileFi [53], [54].

IV. Taxonomy of Existing Smart Grid Testbeds

In this section, we give an overview to the taxonomy: (1) The targeted research domain; (2) covered smart grid domains with respect to NIST definition; (3) type of test platform; (4) communication infrastructure.

Transforming the smart grid concepts in terms of cyber-physical systems into a more tangible perspective depends on the classification of the targeted research area, smart grid domains, and test platforms. Table II lists existing the cyber-physical smart grid testbeds considered in this survey. We added the year of publication to the reference list to be able to track the ideas and trends chronologically. However, it is important to note that the provided testbeds might be established and be in operating condition before the year of publication. Even though, we tried to include all the existing testbeds providing information via websites and publications, it might be practically impossible to cover all the projects.

A. Taxonomy Based on Research Area

A more realistic classification and accurate approach can be obtained with research goal base taxonomy. Some testbeds involve several research topics. Most of the topics naturally overlap. Fig. 2 shows the major research concentration of the surveyed testbeds. The demand response research area can be incorporated with electric vehicle research [64], home-area energy management [77], [82], energy efficiency [70] and microgrid management [80]. The main idea is to provide ancillary services to the utility with controllable load or generation resources based on dynamically varying price signals. An optimized mutual benefit can be obtained by the prosumer side to utilize cheaper energy or sell energy at good rates. On the other hand, utilities can exploit frequency and voltage support by advanced demand response management.

Wide-area situational awareness is the most critical and security-dependent research area. The failure of the system would cause nation scale blackouts. The complementary research areas are mainly cyber security [55], [69], [70], [78] and network communications [72], [96]. Distributed energy resources are the main components of the distribution network affiliated with the distribution grid management [57], [65] and energy storage research areas [68]. In fact, energy storage from the cyber-physical system perspective has never been studied in literature yet. Electric transportation and energy storage can be considered tightly coupled. The future nonfuel-based transportation systems is expected to be solely dependent on storage systems [64], [67]. V2G and G2V services are the most popular research topics in this area.

Advanced metering infrastructure refers to mainly smart meter research [99]. The research purpose is the system integration and to demonstrate the functionalities of smart meter networks (SMN) and M2M networks. Distribution grid management covers a wide area of applications. Multi-agent based management schemes are investigated in cyber-physical testbeds [65], [73], [74]. Extensive simulation platforms have been created [84]–[86]. Furthermore, real-world applications as a university campus [80] and an island [79] have been turned into open air testbed platforms.

From the cyber-physical system perspective, the most critical research was conducted on network communications and cyber security. The bi-directional communication requirement compels testbeds to enhance the communication backbone and security awareness. Network communication platforms have been implemented to investigate a wired and wireless communication backbone to safely enable data exchange between smart grid components using legacy protocols. Wireless testbed facilities [64], [97] offering TCP/IP, ATM, 802.11, GSM are rare; while most of the testbeds rely on a hardwired communication backbone. Various applications span different network topologies including home area network (HAN), neighborhood area networks (NAN), and wide area networks (WAN) [5]. Long Term Evolution (LTE) is a fourth generation (4G) cellular communication standard providing high-capacity, low-latency, secure, and reliable data-packet switching [112]. LTE is a promising choice for WAN communication technology including PMUs, IEDs and smart meters.

TABLE II
TAXONOMY OF EXISTING CYBER-PHYSICAL SMART GRID TESTBEDS

Testbed Name	Year of Publication	Targeted Research Area	Covered Smart Grid Domains	Test Platform Type	Reference
Sandia Lab (VCSE)	2008	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Simulator	[55]
Virtual Power System Testbed	2009	Cyber Security	Transmission, Operations	Simulator	[56]
CERTS	2009	Distributed Energy Resources	Operations	Hardware	[57]
Florida International University Smart Grid Testbed	2011	Wide Area Situational Awareness Distribution Grid Management Network Communications Cyber Security	Transmission, Operations, Customer	Hardware	[58]-[59]
TASSCS	2011	Cyber Security	Transmission, Operations	Simulator	[60]
University College Dublin	2011	Cyber Security	Transmission, Operations	Hybrid	[61]
SCADASim	2011	Cyber Security	Operations, Service provider	Simulator	[62]
SCADA Security Lab	2011	Cyber Security Network Communications	Transmission, Operations	Real-Time Simulator	[63]
PEV Parking Lot Testbed	2011	Electric Transportation Demand Response	Customer, Service provider	Simulator	[64]
WVSC Super Circuit	2011	Distribution Grid Management	Operations	Hardware	[65]
Queensland University	2011	Network Communications	Transmission, Operations	Real-Time Simulator	[66]
Electric Vehicle Test Bed	2012	Electric Transportation Energy Storage	Customer, Service provider	Hardware	[67]
Zhejiang University	2012	Distributed Energy Resources Energy Storage	Operations	Hardware	[68]
WAMS RTDS	2012	Wide Area Situational Awareness Network Communications	Transmission, Operations	Real-Time Simulator	[69]-[70]
NC at Charlotte	2012	Wide Area Situational Awareness	Bulk generation, Transmission	Real-Time Simulator	[71]
Kansas State University	2012	Wide Area Situational Awareness Network Communications	Transmission, Operations	Real-Time Simulator	[72]
Mosaik	2012	Distribution Grid Management	Operations	Simulator	[73]-[74]
DeterLab	2012	Cyber Security	-	Hardware	[75]
Oak Ridge ORNL DECC	2013	Distribution Grid Management	Operations	Hardware	[76]
VOLTTRON PNNL	2013	Demand Response Consumer Energy Efficiency Electric Transportation	Market, Service provider	Simulator	[77]
PowerCyber Testbed	2013	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Real-Time Simulator	[78]
Jeju Island, Korea	2013	Distribution Grid Management Demand Response Consumer Energy Efficiency	Customer, Service provider	Hardware	[79]
IIT Galvin Center	2013	Distribution Grid Management Demand Response Consumer Energy Efficiency	Operations, Service provider	Hardware	[80]
Florida State University	2013	Distribution Grid Management Demand Response	Operations, Service provider	Real-Time Simulator	[81]
Multiphysics Testbed	2013	Demand Response Consumer Energy Efficiency	Customer, Service provider	Hybrid	[82]
SEIL	2014	Distributed Energy Resources	Operations	Hardware	[83]
GridLAB-D PNNL	2014	Distribution Grid Management	Operations, Customer, Service provider	Simulator	[84]-[86]
Texas A&M	2014	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Real-Time Simulator	[87]-[88]
Cyber-Physical Testbed	2015	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Real-Time Simulator	[89]-[90]
VSCADA	2015	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Simulator	[91]
Network Intrusion Detection System (NIDS)	2015	Cyber Security Network Communications	Operations	Hybrid	[92]
CPSG	2015	Distribution Grid Management	Operations	Hardware	[93]
SGPS USF	2015	Wide Area Situational Awareness	Transmission, Operations	Real-Time Simulator	[94]
State University of New York	2015	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Hybrid	[95]
Cybersecurity Testbed for IEC61850	2015	Cyber Security Network Communications	Operations	Real-Time Simulator	[96]
INEL	2015	Wide Area Situational Awareness Cyber Security	Transmission, Operations	Hardware	[97]
NREL	2015	Distributed Energy Resources	Operations	Hardware	[98]

The standard smart grid communication protocols include MODBUS [113], DNP3 [114], IEC61850 [102] and IEEE Std. C37.118 [100] synchrophasor protocol. The standard IEEE Std. C37.118 involves synchrophasor measurements from power systems and the data information model [101]. IEC 61850 is the new international standard of communications,

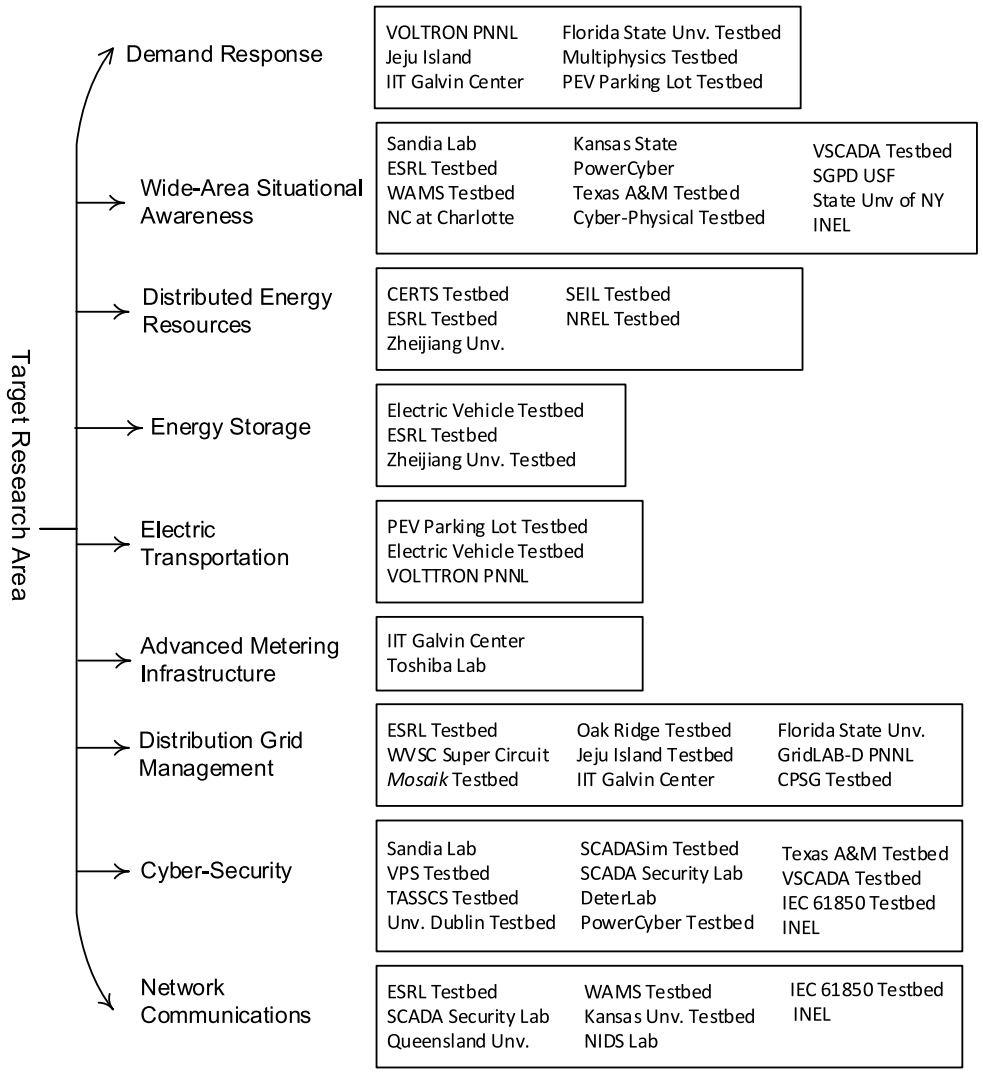

Fig. 2. Taxonomy based on targeted research area.

which enables integration of all substation functions such as protection, control, measurement and monitoring [102], [103].

Many testbeds implemented middleware solutions to create an interface between different power system protocols for real-time data exchange such as the open unified connectivity unified architecture (OPC UA) and data distribution service (DDS). In local substation protection schemes, the simple network time protocol (SNTP) is used to synchronize time in the network of IEDs, where the timing requirements for accuracy and reliability are not as demanding as for synchrophasor applications.

The time synchronization is generally established using IRIG-B code by a satellite clock to have a proper time reference value from a GPS clock to accomplish reliable synchronized measurements from the entire network.

Cyber security testbed platforms have been mainly implemented to investigate vulnerability of the power critical infrastructure along with wide-area situational awareness research. Security issues are investigated for smart grid data acquisition and control components such as remote terminal units (RTU), IEDs, smart meters, PMUs, and programmable logic controllers (PLC). Network device security challenges are also addressed including routers, firewalls, encryption, attack scenarios, intrusion analysis, countermeasures, and forensic analysis.

Various network attack scenarios were presented for smart grid applications. One of the most popular attack scenarios is the man-in-the-middle attack (MITM) aiming to intercept messages between the control center and field devices to accomplish falsified messages over the network. Denial of service (DoS) attacks intend to overload and flood the networks; thus, the operator cannot function properly. Another interesting attack has been introduced, as reply attack, which intends to modify the captured data to replicate activity.

The previously recorded data is reflected as normal operations in the control center and played back to the operator. In this way, the operator cannot observe and recognize the intrusion, while the adversary continues to send falsified commands to the field devices by replying the modified commands. Table III provides a list of cyber-attack testing capabilities of the testbeds.

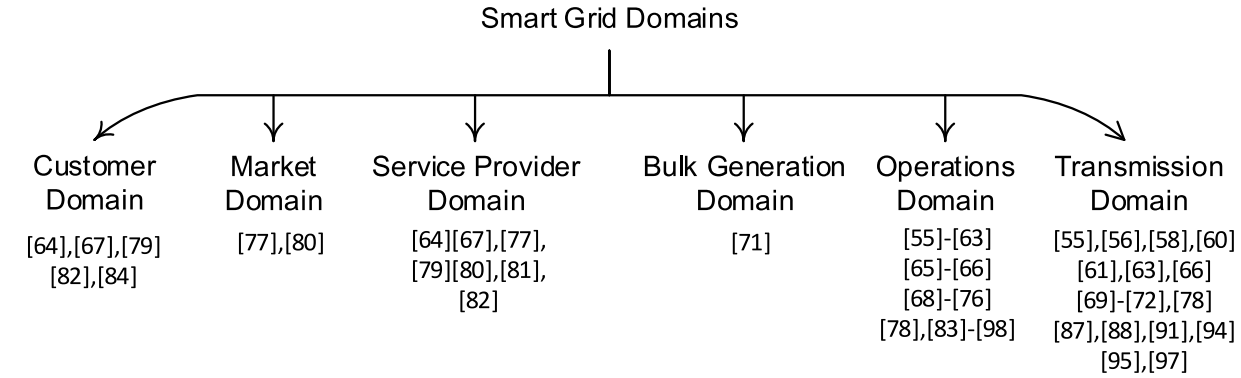

Fig. 3. Taxonomy based on NIST smart grid domains.

TABLE III
LIST OF CYBER-ATTACK SCENARIOS TESTING CAPABILITIES

Attack Type	Reference	Attack Type	Reference
Man-in-the-Middle	[55],[62], [75],[96]	*ARP Spoofing*	[60],[62] [75],[96]
Precision Insider	[55]	*Eavesdropping*	[62]
Rogue Software	[55]	*Malformed Packet*	[96],[75]
Denial of Service	[60], [61]	*Database attack*	[96],[75]

B. Taxonomy Based on NIST Grid Domain

While some of the testbeds focus only one specific domain, most of the testbeds aim to cover several application domains simultaneously. As shown in Fig. 3, a considerable amount of the research involved the customer, service provider, operations and transmission domains. Only a few testbeds focus on the market domain, however the bulk generation domain is not a major interest for smart grid testbeds. This is mostly related to the high cost to be invested for a bulk generation testbed.

The customer domain primarily considers large penetration of plug-in hybrid electric vehicle (PHEV) [64], [67] and demand side management [79], [82], [84] allowing customer participation with the smart grid concept. The comprehensive cyber-physical system is required to enable vehicle-to-grid and grid-to-vehicle services with a communication interface.

Real-time management is the main challenge of consumer participated networks. Wireless communication infrastructure plays a vital role for realization. Demand side management requires wide spread smart meter deployment to be able to acquire the generated data and if allowed, send feedback to customer actuators such as load curtailment. The market domain includes intelligent agent involvement for marketing negotiations where human intervention is not possible. Agents can include a historic interface, weather forecast and auction scheme negotiations [77]. Very few cyber-physical testbeds have focused on real-time market domain applications. Smart building, smart meter and billings are the main concerns of the service provider domain. Microgrids are deployed to cut down electricity bills in university campuses using renewable energy resources [80] and buildings are becoming intelligently controlled to save energy [81].

Although the smart grid concept aims to take bulk generation's place with DERs, due to the complicated operation of vast number of units, bulk generation is still the primary supply of the existing power grid. Voltage and frequency stability, problems are studied in PMU owned testbeds. Real-time modeling and validation of bulk generation parameters are primary research topics [71]. A service provider and operation domains cover both distribution and transmission operations, thus, inherently most of the testbeds are in these domain areas.

C. Taxonomy Based on Platform Type

We classify the testbed platforms into four categories: 1) Simulator types, which only implements power system and network communication simulators; 2) Hybrid types including hardware-in-the-loop (HIL) devices (PLC, PMU, IED, etc.) along with the simulation interface; 3) Real-time digital simulator (RTDS)-based testbeds; 4) Hardware-based platforms including actual or emulated power system and communication components.

The easiest way to create a virtual smart grid testbed is to integrate power system and network communication simulators. A variety of power system simulation software is available in market (PowerFactory DigSilent [78], Matlab/Simulink [64], etc.). Most of them allow an Application Program Interface (API) to be integrated. A network simulator (OPNET [55], [87], OMNET++ [62], NS2 [91], NS3 [89], etc.) can be integrated to achieve a co-simulation environment. In some of the testbeds, actual data acquisition and actuator components (RTU, PLC, PMU, and IED) are integrated with power system simulators using middleware to enable HIL simulations. OPC UA [91] and OSISoft [63] middleware platforms are heavily used for real-time data integration.

RTDS with a focus on electromagnetic transients (EMT) has recently gained popularity due to its convenience. Simulations are carried out with discrete-time and constant step durations. They offer discrete-time step solvers that each variable of system state is solved successively as a function of variables and states [104]. Most of the smart grid testbeds implement RTDS [61], [78], [81], [96] or OPAL-RT [94] platforms

TABLE IV
TAXONOMY OF SMART GRID CYBER-PHYSICAL TESTBED COMMUNICATION INFRASTRUCTURE

Testbed Name	Communication Protocols	Technology	Network Type	Wireless/Wired
Sandia Lab (VCSE)	DNP3.0, Modbus	Ethernet, RS232	WAN, LAN	-
Virtual Power System Testbed	DNP3.0	Ethernet	WAN,LAN	-
FIU Testbed	IEC 61850, C37.118, Modbus, DNP3.0, OPC UA	Ethernet, RS232, Cloud	WAN,LAN	Wired, Wireless
TASSCS	DNP3.0, Modbus	Ethernet	WAN,LAN	Wired
SCADASim	DNP3.0, Modbus	Ethernet	WAN,LAN	-
SCADA Security Lab	DNP3.0, Modbus, IEC 61850, C37.118	Ethernet, RS232, Cloud	WAN,LAN	Wired, Wireless
DeterLab	N/A	Ethernet	WAN, LAN	Wired
PowerCyber Testbed	IEC 61850, C37.118, Modbus, DNP3.0, OPC UA	Ethernet	WAN,LAN	Wired
Network Intrusion Detection System (NIDS)	Modbus	Ethernet	WAN,LAN	Wired
Jeju Island, Korea	N/A	Ethernet, Wi-Fi	WAN, LAN, HAN	Wired, Wireless
Florida State University	N/A	Ethernet	WAN	Wired
WAMS RTDS	C37.118	Ethernet	WAN	Wired
NC at Charlotte	IEC 61850, C37.118, Modbus, DNP3.0	Ethernet	WAN	Wired
Kansas State University	C37.118	Ethernet	WAN	Wired
Cyber-Physical Testbed	IEC 61850, C37.118, DNP3.0	Ethernet	WAN	Wired
VSCADA	OPC DA	Ethernet	WAN	-
(CPSG)	C37.118	Ethernet	WAN	Wired
Smart Grid Power System	C37.118, IEC 61850, DNP3.0	Ethernet RS232	WAN	Wired
State University of New York	C37.118, OPC DA	Ethernet, Wi-Fi, Cloud	WAN	Wired, Wireless
Cybersecurity Testbed for IEC61850	IEC 61850, C37.118	Ethernet	LAN	Wired
Queensland University	IEC61850	Ethernet	LAN	Wired
University College Dublin	IEC 61850, DNP3.0, OPC UA	Ethernet	LAN	Wired
WVSC Super Circuit	FIPA	Wi-Fi	FAN	Wireless
Mosaik	FIPA	Ethernet	FAN	-
IIT Galvin Center	IEC 61850, C37.118, Modbus, DNP3.0	Ethernet, Wi-Fi	FAN	Wired, Wireless
PEV Parking Lot Testbed	ZigBee, Bluetooth, Home plug	Wi-Fi	FAN,HAN	Wireless
Multiphysics Testbed	N/A	Ethernet	HAN	Wired
VOLTTRON PNNL	Modbus	Ethernet	HAN	Wired
Electric Vehicle Test Bed	IEC61850	Ethernet	HAN	Wired

to model power grid. RTDS is easier to deploy and more favorable than actual power system hardware due to safety reasons. Actual data acquisition and actuator components can be integrated as well with the provided APIs. Hardware-based platforms include both an actual or emulator based power system and actual data acquisition and actuator components. The number of hardware-based platforms are small due to the high investment cost, skilled staff requirements, and safety risks. Most of the national laboratories are hardware based testbeds [57], [79], [97], [98], and a small number of leading research universities [58], [59], [68], [80] include hardware-based testbeds.

D. Taxonomy Based on Communication Infrastructure

In this section, we highlight the taxonomy of smart grid cyber-physical system testbed communication infrastructure as given in Table IV. Smart grid requires various sensors and actuators to communicate with one another over wired transmission lines or wirelessly. In a standard definition, 3 basic types of communication networks are defined: (i) local area networks; (ii) wide area networks; and (iii) Internets. However, home area network and field area network can be considered as LAN type. HANs are used for interaction of intelligent devices within a home network. FAN is an architecture for distribution automation, protection and control purposed. Furthermore, substation systems fall into LAN network type. WAN are used to collect data over bulk generation and transmission domain mainly using PMU data. On the other hand, the requirement of network type, communication protocol and communication media differs significantly according to smart grid domain and research area. While C37.118 synchrophasor protocol mainly implemented on

WAN, IEC61850 is the best choice for substation automation. As can be deduced from the Table IV, wireless communication is implemented mainly in HANs.

V. Overview of Existing Testbeds

In this section, we explain the features of the testbeds in detail as classified in the previous section. Each testbed stands on unique features, thus it is crucial to evaluate each individually. Although each testbed can deal with several research aspects at the same time, we allocated them according to most significant features.

A. Hardware-Based Large Scale Testbeds

The number of existing hardware-based large scale testbeds is few due to implementation complexity and higher costs.

Idaho National Laboratory (INL) offers the most comprehensive smart grid cyber-physical platform allowing the highest number of the multiple research areas. The open-air testbed operates a 61 mile, 138kV dual-fed power loop with seven substations, in which some sections can be isolated independently for real-time testing. The cyber security part of the testbed offers supervisory control and data acquisition (SCADA), a power grid, a mock chemical mixing facility, wireless and physical security testbeds. The telecommunication testbed includes large scale end-to-end testing of 3G/4G cellular, land mobile radios, wireless local area network, and backhaul (microwave, FSO, satellite) systems. INL possesses capabilities and expertise in a number of control system applications. Also, INL maintains multiple layers of firewalls, intrusion detection systems, hybrid systems, and encryption links for unclassified network operating centers, classified, and geographically distributed high-speed networks [97].

National Renewable Energy Laboratory (NREL) is another national lab [98] which mainly focuses on characterizing the performance and reliability of DER systems, supporting standards development, and investigate emerging, complex system integration challenges. NREL researchers are working to develop and validate procedures for the IEEE 1547 standard for DER interconnected with electric power systems and IEEE P1547.1 standard conformance test procedures for equipment interconnecting DERs with electric power systems.

The Jeju Island presents a real-world smart grid testbed platform in corporation of (KEPCO) South Korea Electronic Power, as one of the earliest hardware platform examples and is expected to become the world's largest smart grid community that allows testing of the most advanced technologies, R&D results, and business models [79].

Illinois Institute of Technology (IIT) microgrid was built to empower university campus consumers to provide economically viable, green technology, resilience, and self-healing capabilities in case of an outage [80]. The microgrid features two 4-MW gas turbines as conventional resources, 140 kW solar PV cells, an 8 kW wind turbine incorporating EV charging stations, and a 500-kWh storage system. This cyber physical structure is mainly the implementation of advanced metering infrastructure and equipped with 12 PMUs including middleware both wired and wireless communication capabilities.

Energy Systems Research Laboratory (ESRL) at Florida International University is one of the most comprehensive testbeds featuring hardware and a complete cyber-physical infrastructure simultaneously [58], [59]. Multiple research area studies are facilitated in this hardware-based testbed setup including a total power capability of up to 136-kW with conventional generation, renewable units, and storage capabilities. PMUs, IEDs, and PLCs are integrated with actual generation stations that form a complete platform for a variety of smart grid domains.

B. Security Oriented Testbeds

Most of the testbeds consider security and privacy research as a priority. ***The Virtual Control System Environment (VCSE)*** technology developed at Sandia National Laboratories is aimed to investigate SCADA vulnerabilities of energy systems [55]. Wide area situational awareness and cyber security research areas were aimed by analyzing and developing possible cyber-attacks. Specifically in this testbed, the encryption and secured data communication channels on Internet protocol (IP)-routed computer networks are investigated. The power system simulator is integrated with simulated RTUs and human machine interfaces (HMI) to experiment cyber-attack scenarios. Various attack cases, such as MITM, precision insider, and rogue software attacks are realized in dynamic power simulator experiments using DNP3 and Modbus protocols. An OPNET network communication module is used to create the network topology. The network traffic is monitored using either Wireshark [115] or Automatic Control System (ACS) Monitoring and Analyses System (AMAS).

Testbed for Analyzing Security of SCADA Control System (TASSCS) focuses on securing and protecting SCADA systems against a wide range of cyber-attacks using evaluations such as detection rate, false alerts, and effectiveness of the protection techniques [60]. The setup consists of simulated RTUs and PLCs using Modbus and DNP3 protocols incorporated with a power system simulator and OPNET network simulator program. The attack scenarios studied include: 1) unauthorized access to a PLC device; 2) blocking field sensors from reporting false data or events; 3) spoofing a master control or HMI station; 4) device scanning and function scanning; 5) MITM (message relay); 6) request tampering (modification of frames); 7) malicious function injection; and 8) denial of service (DoS) attack.

The intrusion and defense testbed in University College Dublin features a cyber power system consisting of a power system simulator and substation automation platform [61]. Cyber security intrusion and anomaly detection concepts can be tested in this setup. The testbed consists of two control centers, two substations and remote access to Iowa State University testbed. The inter-control center communications protocol (ICCP) and DNP 3.0 protocols are utilized between substation devices and control centers. IEC 61850 based IEDs are communicated with the power system simulator

through OPC (Object Linking and Embedding for Process Control). User interfaces of IEDs are established via MMS (Manufacturing Message Specification) protocol and circuit breaker control is established using Generic Object Oriented Substation Event (GOOSE) messages. Remote access is realized by Virtual Private Network (VPN) protocols to connect to Iowa State University.

SCADASim is designed to simulate industrial and critical infrastructure functions such as electricity, gas, water, waster, railway, and traffic [62]. Four main types of attacks are studied: DoS, MITM, eavesdropping, and spoofing. SCADASim is built on top of OMNET++ discrete event simulation engine and consists of modules that communicate with each other through message passing. OMNET++ can be integrated with external applications such as source code, shared libraries, and sockets. Source code needs to be compiled together with the simulation for a final simulation binary generation. A shared library can be linked to a previously compiled dynamic or static binary library to be linked to the simulation code. Using sockets, OMNET++ can create objects that act as a server proxy to the external world. SCADASim provides three gate implementations: Modbus Gate, DNP3Gate, and HTTP Gate. These gate implementations are useful for remote access. However, other protocols can be implemented as extensions. SCADASim provides built-in modules such as RTU, PLC and modules that represent types of attacks. (e.g., a DoS module.)

Mississippi State University's SCADA Security Laboratory and Power and Energy Research Laboratory features a cyber-physical testbed for multiple critical infrastructures by commercial hardware and software over common industrial control system routable and non-routable networks [63]. Cyber-security vulnerabilities and forensic studies are performed using Modbus and DNP3 protocol supported devices. This comprehensive laboratory features RTDS, OSISoft PI Historian middleware, and a substation GPS clock for time synchronization. Multiple protocols are supported including Modbus, DNP3, GOOSE and IEEE Std. C37.118. The wireless communication setup features a SCADA interface for a water storage tank, a raised water tower, a factory conveyor, gas pipeline and industrial blower control. Another setup is an electric substation control system consisting of RTDS, PMUs, PLCs and NI PXI and Data Acquisition Devices.

DeterLab is another security research and educational platform situated in University of Southern California, focusing on a free-for-use experimental facility [75]. The platform consists of more than 400 general-purpose computing nodes, hardware devices, and a set of tools for cyber security experimentation using a Web-based interface. 2600 research and education users utilize the testbed worldwide. An educational platform is reserved by submitting a short online form for each work, experiment and project assignment. The testbed supports several exercises including buffer overflows, pathname attacks, SQL injections, OS hardening, computer forensics, network intrusion detection, address resolution protocol (ARP) spoofing, MITM, TCP SYN flooding, and worm modeling.

Virtual Power System Testbed (VPST) at University of Illinois at Urbana-Champaign provides a facility to integrate other testbeds across the country to analyze the nature of cyber-attacks on a large scale power grid and to ensure the system reliability nationwide [56]. This testbed is one of the few examples that provide a remote connection access opportunity. The project anticipates leveraging the cyber-attack capability of DETER [75] while integrating the real world power equipment of INL [97].

The principal motive of this lab is to assimilate itself with different test beds nationwide in order to inspect the reliability and security of system equipment and SCADA protocols. Strategies can be analyzed against a multitude of network conditions including loss of networks, congested networks, and insecure environments. Some related network communication statistics such as bandwidth usage, latency, dropped packets, success ratio for communications, and overhear incurred can be studied. Inter-testbed connection requirements include secure connectivity, performance, resource allocation, reproducibility and fidelity.

Network Intrusion Detection Systems (NIDS) implements a HIL and cyber-in-the-loop Matlab/Simulink environment using Modbus protocol [92]. Simulation of a PLC is enabled using libmodbus open source C code. A set of intrusion detection rules was implemented to check abnormality or attack conditions relying on a packet sequence and the time gap between cycles of packets.

IEC 61850 Cybersecurity Testbed at Queen's University Belfast, U.K. focuses on IEC 61850 vulnerabilities [96]. A fuzz testing platform was implemented including a RTDS and actual IEDs and merging units (MU). The implemented fuzzer sends virtually unlimited test cases using invalid or falsely manipulated data within the framework defined by a given protocol specification. Using effective test cases as input information enables security vulnerabilities to be found in the application, which were not anticipated by the protocol designers or software developers. The platform considers the IEC 61850 framework in detail, including MMS, Sampled Value (SV), GOOSE, IEEE 1588 Precision Time Protocol (PTP), and Simple Network Time Protocol (SNTP) protocols. A variety of cyber-attacks have been performed including reconnaissance, malformed packet, DoS, ARP, MITM, configuration tampering, and database attacks.

Queensland University in Australia owns a digital test platform for the automation of substations operating at high voltage levels of 110 kV and above [66]. The testbed features SV, GOOSE, MMS, PTPv2 supported IEDs and a RTDS. IEEE Std. 1588-2008 Precision Time Protocol version 2 (PTPv2) for precision timing [105]. IEC 61850-9-2 details high speed sampled values (SV) over an Ethernet network. IEC 61850-8-1 defines how transduced analogue values and digital statuses can be transmitted over an Ethernet network using GOOSE and MMS.

C. Wide-Area Control Oriented Testbeds

Testbed at University of North Carolina at Charlotte mainly focuses on bulk generation and transmission system parameter identification [71]. The testbed consists of a RTDS, PMUs and IEDs, and is capable of various communication protocols including IEC 61850, DNP3 and IEEE

Standard C37.118. A hardware based synchronous generator is implemented for parameter identification and the rest of the power system was modeled in RTDS. The IEEE Std. C37.118 involves synchrophasor measurements from power systems and the data information model [100], [101]. Synchrophasor applications explicitly deal with the system disturbances of dynamic operation of complicated systems. High sampled data acquisition can reach up to 60 messages per second. The synchrophasor measurements are evaluated according to total vector error (TVE) expression where the theoretical values of a sinusoid signal vary from the values obtained from a PMU. A phasor data concentrator (PDC) can be considered as a station in a communication network, where PMUs populate time-aligned measurements. The deployed PMUs in the system send acquired data with time-stamp information to a PDC. The collected data from a number of PMUs are sorted and correlated according to the time-stamp value. This enables comparable real-time monitoring of the system with high precision sampling. The collected data is also stored in a large database system for accurate post mortem applications such as fault event monitoring, loss-of-mains, and blackout analysis. Synchrophasor measurements provide the time reference for critical applications, such as fault event analysis and protection using highly reliable satellite clocks. Inaccurate time-stamps can cause misdiagnosing of the network and degrade controllability of the distribution network. The Inter-Range Instrumentation Group (IRIG-B) time code is widely accepted for time distribution in substations.

A wide area situational awareness and network communication testbed at Kansas State University includes RTDS and actual PMUs [72]. Software defined networks (SDN, OpenFlow) in particular for communication and cyber physical systems was implemented in network simulation/emulation platforms using Mininet to model and test the communication network applications for smart grid cyber physical systems. SDN is a new approach towards managing and controlling communication networks. It was developed for experimenting with new algorithms and protocols on public communication networks. The future benefits of SDN for the smart grid is still an open research area [106].

The PowerCyber testbed at Iowa State University is one of the most comprehensive smart grid testbeds supporting information and communication technology (ICT) and security [78]. The testbed implements RTDS and Internet-Scale Event and Attack Generation Environment (ISEAGE) WAN emulation. The research mainly focuses on voltage and rotor angle stability. RTDS and the DigSilent Power system simulator are implemented for power system modeling, where IEDs and PLCs are integrated as hardware components. Power Factory Digsilent is integrated with OPC protocol communication. OPC was originally utilized to abstract various PLC protocols into an interoperable interface for a secure and reliable data exchange [107]. The advent of smart grid interoperability efforts led to the development of OPC UA, which keeps all the functionality of the original OPC Data Access (DA), but switches from Microsoft-COM/DCOM technology to state-of-the-art Web services technology. OPC UA is not directly compatible with the classic OPC, since they use different technology. OPC UA uses a framework based on client and server architecture, in which the server provides real-time data to clients. Moreover, it can be implemented with Java or .Net platforms eliminating the need to use Microsoft Windows-based platforms. The OPC UA modeling is based on nodes and references between the nodes. A node can have different sets of attributes connected through references.

Cyber-Physical System Testbed at Texas A&M University implements RTDS, LabVIEW PXI modules and an OPNET platform [87], [88]. The OPNET modeler can simulate a complicated networking environment that supports various industrial protocols and technologies. It enables researchers to evaluate the performance of a network that is comprised of virtual network and physical networking devices in real-time. The key features of OPNET are the modeling and simulation cycle, hierarchical modeling, detailed library modeling and automatic simulation generation [108]. There are various network simulator options that can be implemented in this cyber-physical testbed such as NS-2, NS-3 and Mininet.

One of the most comprehensive cyber-physical system testbeds in ***Washington State University*** implements RTDS and, a network simulator (NS-3) incorporating actual RTUs, PMUs and PDC [89], [90]. A virtual IEEE 14 bus system was implemented to investigate wide area situational awareness, cyber security and network communications research areas. NS-3 is an open-source network simulator software that various power system communication protocols can be implemented [109]. NS-3 runs on a dedicated server to emulate the communication network in real-time.

Wide Area Measurement System (WAMS) testbed at North Carolina State University is one of the first testbeds proposing remote access and a network of associated cloud testbeds [69], [70]. The testbed mainly focuses on wide area situational awareness and network communications. The facility is being extended for a multi-port, multi-user, and multi-vendor network of PMUs spread across three university campuses: NC State, Duke University, and University of North Carolina Chapel Hill. The test platform is based on RTDS, actual PMUs, and IEDs. A PDC is also implemented involving the IEEE 9 bus and IEEE 39-bus New England System. This testbed allows users to create custom topologies using resources from multiple federated providers using Open Resource Control Architecture (ORCA) to orchestrate the networked cloud resource provisioning

Virtual SCADA (VSCADA) power system utility security framework was implemented at Virginia Tech. [91]. Various power system simulation platforms including PSSE, PSLF, and MatPower are integrated with NS2/OPNET network communication simulators. OPC UA middleware integrates the simulation platforms using Python scripting language for process database and HMI applications.

University of South Florida (USF) Smart Grid Power System Lab (SPS) features a testbed including communication and control architectures using an OPAL-RT real-time simulator [94]. PMUs are synchronized with a GPS clock reference signal. Labview and National Instruments Data Acquisition Devices (DaQ) are used for actual voltage generation. Various communication protocols have been

leveraged such as SEL, Modbus, DNP3 C37.118 and IEC 61850. OSIsoft is implemented as a middleware for real-time infrastructure solution.

D. Wireless Communication Oriented Testbeds

Very few testbeds have implemented a wireless communication setup. ***The digital testbed for Plug-in electric vehicles (PEV) at North Carolina State University*** investigates wide range of charging and control scenarios [64]. The communication technologies related to PEV are explored. The setup consists of a hardware robot PEV and Matlab/Simulink-based virtual simulation-based customers and charging stations. The ZigBee communication protocol based on IEEE 802.15.4 mesh network are implemented. ***Cyber-Physical System (CPS) in The State University of New York*** implemented a testbed based on utilization of the eXtensible Messaging and Presence Protocol (XMPP) allowing multiple users, devices, and applications to share critical information by implementing Transport Layer Security (TLS) to encrypt the data links [95]. A simple one machine and a load model is integrated with PMUs and a cloud server.

E. Interoperability and Agent-Based Control Testbeds

The future smart grids require fast and intelligent decision making algorithms with an efficient communication infrastructure since power system operators are ineffective to deal with highly active and constantly varying operations. Multi-agent based decision making algorithms incorporating real-time communicative devices offer a reliable solution for decision making without human intervention. Agent systems have applications in a variety of research domains in smart grids. ***West Virginia Super Circuit (WVSC)*** Smart Grid Demonstration project implemented a hardware-based multi-agent systems for distribution automation and control [65]. The facility can demonstrate various distributed network applications such as energy storage, DER penetration and dynamic feeder reconfiguration. Agent Communication Language (ACL) by Foundation for Intelligent Physical Agents (FIPA) is adopted for interoperability as a universal communication protocol [110]. The standardization of agent-based technologies is an ongoing research that few standards have yet to realize to its fullest potential. FIPA specifications help to allow an easy interoperability between agent systems with agent communication language and transport level protocols. ACL represents a communicative act intended to perform actions with precisely defined syntax and semantics [111].

Mosaik [73] is a smart grid simulation API for a semantic based standard for interchanging simulations. Agent based simulation is interchanged in simulation platforms [74]. Various agent-based simulations are investigated to create the dynamic behavior of complex systems such as smart grid.

VOLTTRON intelligent agent platform was developed at the Pacific Northwest National Laboratory (PNNL) as an open source project mainly focusing on coordination of PEV charging with home energy utilization [77]. Important implementation services such as resource discovery, secure agent mobility, and interacting with smart and legacy devices are deployed. VOLTTRON provides platform services resource management, authentication, authorization, cryptographic agent code verification, and directory services.

VI. Evaluation of Cyber-Physical Testbeds

One of the major motivations of this study is to specifically define a set of desired features for cyber-physical smart grid testbeds to use as a metric so as to be able to compare the existing testbeds. Considering the needs of the researchers and the nature of experiments on the smart grid, we consider the following features as desirable: 1) Multiple research area support: The capability of a testbed to perform in more than one target research areas. Testbeds should support testing of interdependency of multiple research areas; 2) Heterogeneous communication backbone: This is the underlying communication network among the components. The testbeds should support both wireless and legacy protocols; 3) Security & privacy awareness: This refers to implemented encryption and public keys for communication protocols; 4) Multiple communication protocol support: A testbed should implement specific smart grid communication protocols utilized in smart meters, IEDs and PMUs; and 5) Remote connection access; A testbed should offer a remote access utilizing an Internet connection for third party users. Table V provides a comprehensive evaluation overview of the surveyed testbeds.

Testbeds can be built to support multiple research areas at the same time. In fact, most of the research areas require interdependent infrastructure. Communication backbone is the most critical infrastructure of future smart grids, hence a comprehensive solution can be obtained by heterogeneous communication capability including both wired and wireless infrastructure. Testbeds are expected to be equipped with heterogeneous communication backbone capability.

Security and privacy is another major concern considering the abundant communication requirement of cyber-physical testbeds. Testbeds are also expected to address security and privacy of the data information or equipped with a satisfactory awareness. The smart grid concept also covers an extensive control, automation and protection applications such that a single standard may not meet all the required forms of monitoring and information exchange demands. Application specific legacy communication protocols should be adopted in cyber-physical testbeds while ensuring real-time data exchange and interoperability concerns.

Testbed networks along large geographic distances would allow students and researchers to conveniently perform remote smart grid experiments. As a new generation of networked applications emerge, a diverse solution for large deployments of smart devices becomes possible. Testbeds are mainly built for a particular project evaluation and verification purposes, but they do not provide a complete hardware/software test platform for comprehensive applications such as renewable integration and cyber-security at the same time. With the advent of integrated remote access testbeds, extensive experimental platforms can be developed. Collaboration of the testbeds which are built for various smart grid test platforms

TABLE V
EVALUATION OF SMART GRID CYBER-PHYSICAL TESTBEDS

Testbed Name	Multiple Research Area Support	Heterogeneous Communication	Security & Privacy Awareness	Multiple Protocol Support	Remote Connection Access
Sandia Lab (VCSE)	✓	×	✓	✓	×
Virtual Power System Testbed	✓	×	✓	✓	✓
CERTS	✓	×	×	×	×
FIU Testbed	✓	✓	✓	✓	✓
TASSCS	✓	×	✓	✓	×
University College Dublin	✓	×	✓	✓	✓
SCADASim	✓	×	✓	✓	×
SCADA Security Lab	✓	✓	✓	✓	×
PEV Parking Lot Testbed	✓	✓	×	×	×
WVSC Super Circuit	✓	✓	×	×	×
Queensland University	✓	×	×	✓	×
Electric Vehicle Test Bed	✓	×	×	✓	×
Zhejiang University	✓	×	×	×	×
WAMS RTDS	✓	×	×	✓	✓
NC at Charlotte	✓	×	×	✓	×
Kansas State University	✓	×	×	✓	×
Mosaik	✓	×	×	×	×
DeterLab	✓	×	✓	×	✓
Oak Ridge ORNL DECC	✓	×	×	×	×
VOLTTRON PNNL	✓	×	×	×	×
PowerCyber Testbed	✓	×	✓	✓	×
Jeju Island, Korea	✓	✓	×	✓	✓
IIT Galvin Center	✓	✓	×	✓	×
Florida State University	✓	×	×	×	×
Multiphysics Testbed	✓	×	×	×	×
Smart Energy Integration Lab	✓	×	×	×	×
GridLAB-D	✓	×	×	×	×
Texas A&M	✓	×	✓	✓	×
Cyber-Physical Testbed	✓	×	✓	✓	×
VSCADA	✓	×	✓	✓	×
Network Intrusion Detection System (NIDS)	✓	×	✓	✓	×
(CPSG)	✓	×	×	✓	×
Smart Grid Power System	✓	×	×	✓	×
State University of New York	✓	×	✓	✓	✓
Cybersecurity Testbed for IEC61850	✓	×	✓	✓	×
INL	✓	✓	✓	✓	×
NREL	✓	×	×	×	×
SUMMARY TOTAL	***37***	*7*	***16***	***24***	*7*

can serve a special role in bringing together diverse experimental opportunities. Remote connection access is one of the critical requirements of the cyber-physical smart grid testbeds.

VII. TRENDS AND OPEN RESEARCH ISSUES

In this section, we first highlight the trends on smart grid cyber-physical testbeds. Then, we provide a discussion about

the open research areas. Comparing the earlier and the current research works, we identified the following trends:

Communication-dependent power grid: Modern sensor networks stimulate the flexibility and application range for wide area implementation of smart grids. To conduct wireless communication experiments comparable to a real world environment, there is a significant need for wireless communication testbeds specifically for smart grids. This backbone would allow more dynamical topology changes and field deployments. Testbeds should initiate outdoor deployments as well as laboratory scale indoor applications.

Wired communication technologies for distributed control applications such as market negotiations, power sharing, aggregation, and protection may not be adequate. Therefore, the smart grid requires an extensive wireless communication research effort including new protocols and enhancing the existing ones.

Security & privacy awareness: Any research domain in smart grids should be accompanied with a cyber-physical interface. Along with the targeted research area, related security concepts are inherently involved while building a testbed. Any testbed without specific security and privacy consideration can be assumed as an evolving work. Thus far, many security studies focused on intrusion detection and attack demonstrations. However, to achieve the future goals and provide a robust mechanism, further countermeasure techniques and algorithms should be developed and verified in cyber-physical smart grid testbeds. Online and offline forensic analysis research should be encouraged. Encryption and certificate methods need to be studied.

Software Defined Networks: The recently emerged software defined networking (SDN) paradigm can perfectly address resilient and secure data collection challenges by splitting controls of networks and data flow operations. The major goal of SDN is to interact with the switches, and thus create an open networking architecture for everyone. In this way, one can get a global view of the entire network and make global changes without having to access to each device's unique hardware. Therefore, various large-scale network architectures can be deployed and maintained with ease while still featuring resiliency and robustness. The data communication of smart grid necessitates upgrading the existing infrastructure with various components. SDN-enabled devices would offer a resilient communication infrastructure in all smart grid domains.

Data Interoperability: Interoperability is the ability of two or more devices to exchange information and work together in a system. This is achieved using published objects and data definitions, standard commands and protocols. The smart grid interoperability requirements are clear. All stakeholders need to use commonly agreed upon compatible data exchange formats for fully integrated framework. The power system framework must work together not just across the technical domains of the smart grid but across stakeholder communities in enterprises not part of the existing utility industry. The future challenges include expanding existing protocols and providing ongoing definition of information models and information exchange requirements.

Distributed control: Centralized control methods of operation require a high performance central processing unit and are more susceptible to single point failures, where managing the vast amount of data generated from the extensive deployment of smart devices becomes infeasible. In contrast to centralized control, the emerging smart grid concept is in a trend to adopt distributed methods as a result of the highly dynamic behavior of the power grid. Distributed control approaches intend to provide autonomy for different control layers by enabling an event-driven peer-to-peer communication structure, where central control schemes mainly rely on master-slave interactions. In power system applications, the implementation of distributed control is established using multi-agent frameworks, which are composed of interacting multiple intelligent agents to achieve a global or a local objective function. Testbeds implementing real-time multi-agent based control schemes need to be increased.

Interconnection of testbeds: Most institutions may not afford to construct multiple research area testbeds with various hardware and software environment conditions to carry out experimental research. There is a trend to form testbed federations to merge testbeds with different capabilities. Establishing interconnected testbeds is not a simple task. It also necessities university or institution-wide management and approval. Furthermore, power system applications are considered as high safety risk experiments. However, the interconnection of individual testbeds can be realized in several forms such as using virtual private networks (VPN) and cloud based communication via Internet. Realization of a combination of virtual components is a non-trivial challenge and should be supported with a common API for all participants. Interoperability and standard communication protocols can be a problem solver in such circumstances.

VIII. Conclusion

In this survey, we presented an overview of smart gird cyber-physical testbeds. We discussed the underlying research effort and design considerations involved in developing these testbeds. We provided a four step taxonomy considering smart grid domains, research areas, application platforms and communication infrastructure. Then, we presented existing testbeds and evaluated them for their various criteria. Open research issues were identified for the vision of actual smart grid realization. Although numerous smart grid cyber-physical testbed studies were conducted, the majority of the performance evaluation are simulation based. The inherent complexities of the smart grid make it very difficult to model all details in simulation platforms. The analysis and discussions in this paper can provide useful insight for researchers to assist them in constructing their own smart grid testbeds that can provide the most benefit to its designers and users.

To conclude, the lessons learned from this survey of the state-of-the-art cyber-physical smart grid testbeds are:

- *Communication infrastructure* is essential for smart grid visions. Most of the testbeds focus on the communication oriented smart grid research in terms of data communication, communication protocols, privacy and

security of the enhanced communication infrastructure. Smart grid realization is emerging in all domains including home devices, distribution field devices, substation devices and wide-area control devices. The network type is different in each domain, as well as implemented communication protocols. Future testbed builders should take communication protocols and network types for domain specific applications. Furthermore, the trend shows the emergent requirement of wireless communication, wireless communication testbeds are not abundant as wired communication system. Wireless communication is an acceptable solution for HANs, however still not reliable for most of the FAN and WAN critical power system applications.

- *The accurate selection of targeted research area* determines the success of the testbeds. It may not be possible that a single testbed allows experiments for all smart grid concepts. Furthermore, initial investment and operational costs would increase without wise preliminary decision. It is recommended that research groups should concentrate on their specific area of interest and do the investment according to their specific needs.
- *Test platform selection* is a tradeoff between more realistic results can be obtained from hardware-based platforms and extensive scalability feature of the simulation platforms. Since hardware-in-the-loop experiments are carried out with few number of generation units, transmission lines and load model, the simulation platforms would provide solutions for further computational complexity. Operational and investment is very costly in hardware-based testbeds by means of energy efficiency since the platforms involves generator, load and distribution/transmission models as well as enhanced sensors and actuators. Therefore, mostly governmental supported testbeds enjoy the opportunity to work on hardware-based testbeds. However, universities may leap at an opportunity to build tailor-made small scale testbeds with relatively lower cost taking the advantage of research students. These testbeds will most probably be operating in low power and voltage ratings instead of being commercially purchased high voltage and big power generation plants.
- Even though the distributed energy resource research is the center of attention now, the outdated bulk generation power domain research should not be totally abandoned. The smart grid realization solely depending on intermittent generation profiles may not be possible without a robust bulk generation infrastructure.
- The grid is envisioned to undergo dramatic changes by incorporating a large number of sensors and actuators. To be able to operate this large-scale complex system the research trend of *decentralized and distributed control* replaces central control and optimization methods. Distributed control techniques require peer-to-peer communication capability of the smart grid devices. The communication infrastructure of the testbeds should be ready to address this emerging need.
- *Interconnection of the testbeds* would provide excellent opportunity to combine testbeds with different capabilities. This will provide an opportunity to reduce the investment and operational costs of the testbeds, while encouraging the cooperation among various researchers among the smart grid field. Therefore, testbeds should be designed to provide a remote interface for interconnection.

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[2] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[3] *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), End-Use Applications, and Loads*, IEEE Standard 2030-2011, pp. 1–126, Sep. 10, 2011.

[4] F. Leccese, "An overview on IEEE Std 2030," in *Proc. 11th Int. Conf. Proc. Environ. Elect. Eng. (EEEIC)*, Venice, Italy, 2012, pp. 340–345.

[5] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Comput. Netw.*, vol. 56, no. 11, pp. 2742–2771, 2012.

[6] L. Hernandez *et al.*, "A survey on electric power demand forecasting: Future trends in smart grids, microgrids and smart buildings," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1460–1495, 3rd Quart., 2014.

[7] I. Colak, E. Kabalci, G. Fulli, and S. Lazarou, "A survey on the contributions of power electronics to smart grid systems," *Renew. Sustain. Energy Rev.*, vol. 47, pp. 562–579, Jul. 2015.

[8] W. Li, M. Ferdowsi, M. Stevic, A. Monti, and F. Ponci, "Co-simulation for smart grid communications," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2374–2384, Nov. 2014.

[9] A. M. Kosek, O. Lünsdorf, S. Scherfke, O. Gehrke, and S. Rohjans, "Evaluation of smart grid control strategies in co-simulation—Integration of IPSYS and mosaik," in *Proc. Power Syst. Comput. Conf. (PSCC)*, Wrocław, Poland, Aug. 2014, pp. 1–7.

[10] C.-H. Yang, G. Zhabelova, C.-W. Yang, and V. Vyatkin, "Cosimulation environment for event-driven distributed controls of smart grid," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1423–1435, Aug. 2013.

[11] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, 2011.

[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, 1st Quart., 2013.

[13] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[14] Z. Fan *et al.*, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, 1st Quart., 2013.

[15] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[16] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[17] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, 2013.

[18] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 1954.

[19] S. Rohjans *et al.*, "Survey of smart grid standardization studies and recommendations," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 2010, pp. 583–588.

[20] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[21] B. Genge, A. Beres, and P. Haller, "A survey on cloud-based software platforms to implement secure smart grids," in *Proc. 49th Int. Univ. Power Eng. Conf. (UPEC)*, Cluj-Napoca, Romania, 2014, pp. 1–6.

[22] E. Hossain, E. Kabalci, R. Bayindir, and R. Perez, "Microgrid testbeds around the world: State of art," *Energy Convers. Manag.*, vol. 86, pp. 132–153, Oct. 2014.

[23] M. H. Cintuglu, H. Martin, and O. A. Mohammed, "Real-time implementation of multiagent-based game theory reverse auction model for microgrid market operation," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 1064–1072, Mar. 2015.

[24] T. Ma, M. H. Cintuglu, and O. A. Mohammed, "Control of hybrid AC/DC microgrid involving storage, renewable energy and pulsed loads," *Proc. IEEE Ind. Appl. Soc. Annu. Meeting,*, Addison, TX, USA, 2015, pp. 1–8.

[25] G. Locke and P. D. Gallagher, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2010.

[26] S. Grijalva and M. U. Tariq, "Prosumer-based smart grid architecture enables a flat, sustainable electricity industry," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Anaheim, CA, USA, 2011, pp. 1–6.

[27] S. Grijalva, M. Costley, and N. Ainsworth, "Prosumer-based control architecture for the future electricity grid," in *Proc. IEEE Int. Conf. Control Appl. (CCA)*, Denver, CO, USA, 2011, pp. 43–48.

[28] D. Ilic, P. G. Da Silva, S. Karnouskos, and M. Griesemer, "An energy market for trading electricity in smart grid neighbourhoods," in *Proc. 6th IEEE Int. Conf. Digit. Ecosyst. Technol. (DEST)*, Campione d'Italia, Italy, 2012, pp. 1–6.

[29] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power Energy Mag.*, vol. 3, no. 5, pp. 34–41, Sep./Oct. 2005.

[30] 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, Jun. 2010.

[31] F. Rahimi and A. Ipakchi, "Overview of demand response under the smart grid and market paradigms," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Gaithersburg, MD, USA, 2010, pp. 1–7.

[32] G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[33] A. Mazloomzadeh, M. H. Cintuglu, and O. A. Mohammed, "Development and evaluation of a laboratory based phasor measurement devices," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2015, pp. 1–5.

[34] M. H. Cintuglu, A. T. Elsayed, and O. A. Mohammed, "Microgrid automation assisted by synchrophasors," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2015, pp. 1–5.

[35] M. H. Albadi and E. F. El-Saadany, "A summary of demand response in electricity markets," *Elect. Power Syst. Res.*, vol. 78, no. 11, pp. 1989–1996, Nov. 2008.

[36] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Trans. Ind. Informat.*, vol. 7, no. 3, pp. 381–388, Aug. 2011.

[37] H. Vogt, H. Weiss, P. Spiess, and A. P. Karduck, "Market-based prosumer participation in the smart grid," in *Proc. 4th IEEE Int. Conf. Digit. Ecosyst. Technol. (DEST)*, Dubai, UAE, Apr. 2010, pp. 592–597.

[38] M. H. Cintuglu, T. A. Youssef, A. T. Elsayed, and O. A. Mohammed, "Frequency and voltage control of microgrids upon unintentional cascading islanding," in *Proc. SoutheastCon*, Fort Lauderdale, FL, USA, Apr. 2015, pp. 1–6.

[39] A. Mohd, E. Ortjohann, A. Schmelter, N. Hamsic, and D. Morton, "Challenges in integrating distributed energy storage systems into future smart grid," in *Proc. IEEE Int. Symp. Ind. Electron. (ISIE)*, Cambridge, U.K., Jun./Jul. 2008, pp. 1627–1632.

[40] B. P. Roberts and C. Sandberg, "The role of energy storage in development of smart grids," *Proc. IEEE*, vol. 99, no. 6, pp. 1139–1144, Jun. 2011.

[41] W. Su, H. Eichi, W. Zeng, and M.-Y. Chow, "A survey on the electrification of transportation in a smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 8, no. 1, pp. 1–10, Feb. 2012.

[42] J. C. Zhang and Z. Y. Chen, "The impact of AMI on the future power system," *Autom. Elect. Power Syst.*, vol. 34, no. 2, pp. 20–23, 2010.

[43] S. Karnouskos, O. Terzidis, and P. Karnouskos, "An advanced metering infrastructure for future energy networks," in *New Technologies, Mobility and Security*. Dordrecht, The Netherlands: Springer, Jan. 2007, pp. 597–606.

[44] R. Das *et al.*, "Distribution automation strategies: Evolution of technologies and the business case," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 2166–2175, Jul. 2015.

[45] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Draft Interagency Tech. Rep. NISTIR 7628, 2009.

[46] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[47] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[48] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proc. Power Energy Soc. Gen. Meeting*, Minneapolis, MN, USA, Jul. 2010, pp. 1–5.

[49] X. Li *et al.*, "Securing smart grid: Cyber attacks, countermeasures, and challenges," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, Aug. 2012.

[50] A. Zaballos, A. Vallejo, and J. M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 30–37, Sep./Oct. 2011.

[51] W. Luan, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in *Proc. IEEE PES Transm. Distrib. Conf. Expo.*, New Orleans, LA, USA, 2010, pp. 1–4.

[52] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[53] Z. M. Fadlullah, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[54] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *Proc. Power Energy Soc. Gen. Meeting*, Minneapolis, MN, USA, 2010, pp. 1–7.

[55] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy, "Cyber effects analysis using VCSE," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2008-5954, Sep. 2008.

[56] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, "The virtual power system testbed and inter-testbed integration," in *Proc. CSET*, Montreal, QC, Canada, 2009, p. 5.

[57] J. Eto *et al.*, "Overview of the CERTS microgrid laboratory test bed," in *Proc. CIGRE/IEEE PES Joint Symp. Integr. Wide Scale Renew. Resources Power Del. Syst.*, Calgary, AB, Canada, 2009, p. 1.

[58] V. Salehi, A. Mohamed, A. Mazloomzadeh, and O. A. Mohammed, "Laboratory-based smart power system, part I: Design and system development," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1394–1404, Sep. 2012.

[59] V. Salehi, A. Mohamed, A. Mazloomzadeh, and O. A. Mohammed, "Laboratory-based smart power system, part II: Control, monitoring, and protection," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1405–1417, Sep. 2012.

[60] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Anaheim, CA, USA, 2011, pp. 1–7.

[61] J. Hong *et al.*, "An intrusion and defense testbed in a cyber-power system environment," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, 2011, pp. 1–5.

[62] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim—A framework for building SCADA simulations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011.

[63] T. Morris *et al.*, "A control system testbed to validate critical infrastructure protection concepts," *Int. J. Crit. Infrastruct. Protect.*, vol. 4, no. 2, pp. 88–103, 2011.

[64] W. Su, W. Zeng, and M.-Y. Chow, "A digital testbed for a PHEV/PEV enabled parking lot in a smart grid environment," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Washington, DC, USA, 2012, pp. 1–7.

[65] R. Belkacemi, A. Feliachi, M. A. Choudhry, and J. E. Saymansky, "Multi-agent systems hardware development and deployment for smart grid control applications," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, 2011, pp. 1–8.

[66] D. M. E. Ingram, D. A. Campbell, P. Schaub, and G. Ledwich, "Test and evaluation system for multi-protocol sampled value protection schemes," in *Proc. IEEE Trondheim PowerTech*, Trondheim, Norway, 2011, pp. 1–7.

[67] F. Marra *et al.*, "Implementation of an electric vehicle test bed controlled by a virtual power plant for contributing to regulating power reserves," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, 2012, pp. 1–7.

[68] B. Zhao, X. Zhang, and J. Chen, "Integrated microgrid laboratory system," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 2175–2185, Nov. 2012.

[69] A. Chakrabortty and Y. Xin, "Hardware-in-the-loop simulations and verifications of smart power systems over an Exo-GENI testbed," in *Proc. 2nd GENI Res. Educ. Exper. Workshop (GREE)*, Salt Lake City, UT, USA, 2013, pp. 16–19.

[70] M. Weiss, A. Chakrabortty, and Y. Xin, "A multi-user network testbed for wide-area monitoring and control of power systems using distributed synchrophasors," in *Proc. 4th Int. Conf. Future Energy Syst.*, Berkeley, CA, USA, 2013, pp. 291–292.

[71] V. P. Tran, S. Kamalasadan, and J. Enslin, "Real-time modeling and model validation of synchronous generator using synchrophasor measurements," in *Proc. North Amer. Power Symp. (NAPS)*, Manhattan, KS, USA, 2013, pp. 1–5.

[72] *A Smart Laboratory*, Kansas State Univ., Manhattan, KS, USA, 2015. [Online]. Available: http://www.k-state.edu/perspectives/winter-2015/smartlab.html

[73] S. Schütte, S. Scherfke, and M. Sonnenschein, "Mosaik-smart grid simulation API," in *Proc. SMARTGREENS*, Porto, Portugal, 2012, pp. 14–24.

[74] S. Schütte, S. Scherfke, and M. Tröschel, "Mosaik: A framework for modular simulation of active components in smart grids," in *Proc. IEEE 1st Int. Workshop Smart Grid Model. Simulat. (SGMS)*, Brussels, Belgium, 2011, pp. 55–60.

[75] J. Mirkovic and T. Benzel, "Teaching cybersecurity with DeterLab," *IEEE Security Privacy*, vol. 10, no. 1, pp. 73–76, Jan./Feb. 2012.

[76] *Grid Security: Distributed Controls Test Bed Research Capabilities and Facilities at the Distributed Energy Control and Communication*. Accessed on Apr. 8, 2016. [Online]. Available: http://web.ornl.gov/sci/renewables/docs/factsheets/Security-DECC.pdf

[77] J. Haack *et al.*, "VOLTTRON^{TM}: An agent platform for integrating electric vehicles and smart grid," in *Proc. Int. Conf. Connected Veh. Expo (ICCVE)*, Las Vegas, NV, USA, 2013, pp. 81–86.

[78] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[79] *South Korea: Jeju Island Smart Grid Test-Bed Developing Next Generation Utility Networks*. Accessed on Apr. 8, 2016. [Online]. Available: http://www.gsma.com/connectedliving/wpcontent/uploads/2012/09/cl_jeju_09_121.pdf

[80] M. Shahidehpour and M. Khodayar, "Cutting campus energy costs with hierarchical control: The economical and reliable operation of a microgrid," *IEEE Electrific. Mag.*, vol. 1, no. 1, pp. 40–56, Sep. 2013.

[81] M. J. Stanovich *et al.*, "Development of a smart-grid cyber-physical systems testbed," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Washington, DC, USA, 2013, pp. 1–6.

[82] C. Molitor *et al.*, "Multiphysics test bed for renewable energy systems in smart homes," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1235–1248, Mar. 2013.

[83] F. Huerta, J. K. Gruber, M. Prodanovic, and P. Matatagui, "A power-HIL microgrid testbed: Smart energy integration lab (SEIL)," in *Proc. IEEE Energy Convers. Congr. Expo. (ECCE)*, Pittsburgh, PA, USA, 2014, pp. 3998–4003.

[84] *GridLAB-D^{TM} A Unique Tool to Design Smart Grid*. Accessed on Apr. 8, 2016. [Online]. Available: http://www.gridlabd.org/brochures/20121130_gridlabd_brochure.pdf

[85] K. P. Schneider, J. C. Fuller, and D. Chassin, "Evaluating conservation voltage reduction: An application of GridLAB-D: An open source software package," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, San Diego, CA, USA, 2011, pp. 1–6.

[86] D. P. Chassin, K. Schneider, and C. Gerkensmeyer, "GridLAB-D: An open-source power systems modeling and simulation environment," in *Proc. IEEE/PES Transm. Distrib. Conf. Expo.*, Chicago, IL, USA, 2008, pp. 1–5.

[87] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in *Proc. North Amer. Power Symp. (NAPS)*, Pullman, WA, USA, 2014, pp. 1–6.

[88] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. IEEE Int. Workshop Tech. Committee Commun. Qual. Rel. (CQR)*, Charleston, SC, USA, 2015, pp. 1–6.

[89] C. B. Vellaithurai, S. S. Biswas, and A. K. Srivastava, "Development and application of a real-time test bed for cyber-physical system," *IEEE Syst. J.*, vol. PP, no. 99, pp. 1–12.

[90] S. S. Biswas, F. Shariatzadeh, R. Beckstrom, and A. K. Srivastava, "Real time testing and validation of smart grid devices and algorithms," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PES)*, Vancouver, BC, Canada, 2013, pp. 1–5.

[91] A. Vaccaro, M. Popov, D. Villacci, and V. Terzija, "An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification," *Proc. IEEE*, vol. 99, no. 1, pp. 119–132, Jan. 2011.

[92] G. Koutsandria *et al.*, "A real-time testbed environment for cyber-physical security on the power grid," in *Proc. 1st ACM Workshop Cyber Phys. Syst. Security PrivaCy*, Denver, CO, USA, 2015, pp. 67–78.

[93] D. Hawbaker *et al.*, "Cyber physical smart grid," in *Proc. NCUR*, Cheney, WA, USA, 2015, pp. 100–106.

[94] H. G. Aghamolki, Z. Miao, and L. Fan, "A hardware-in-the-loop SCADA testbed," in *Proc. North Amer. Power Symp. (NAPS)*, Charlotte, NC, USA, 2015, pp. 1–6.

[95] *Test Bed for a Cyber-Physical System Based on Integration of Advanced Power Laboratory and eXtensible Messaging*. Accessed on Apr. 8, 2016. [Online]. Available: https://www.ece.cmu.edu/∼electriconf/posterpdf_2015/Matin_Meskin Poster.pdf

[96] Y. Yang *et al.*, "Cybersecurity test-bed for IEC 61850 based smart substations," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Denver, CO, USA, 2015, pp. 1–5.

[97] *INEL Test Range, Protecting Nation's Infrastructure*. Accessed on Apr. 8, 2016. [Online]. Available: http://www4vip.inl.gov/research/idaho-test-range/d/idaho-test-range.pdf

[98] *NREL Distributed Energy Resources Test Facility*, NREL, DER, Golden, CO, USA, 2015.

[99] *Toshiba's Smart Meter Network Testbed*. Accessed on Apr. 8, 2016. [Online]. Available: http://static1.1.sqspcdn.com/static/f/679473/25461572/1411396794260/Sep15_10_Thompson_DIWINE.pdf?token=%2F5OAy1Qr0iNVPzIKx6QPnjCN0i0%3D

[100] *Synchrophasor Measurements for Power Systems*, IEEE Standard C37.118.1, 2011.

[101] *Synchrophasor Data Transfer for Power Systems*, IEEE Standard C37.118.2, 2011.

[102] R. E. Mackiewicz, "'Overview of IEC 61850 and benefits," in *Proc. IEEE PES Power Syst. Conf. Expo. (PSCE)*, Atlanta, GA, USA, Oct./Nov. 2006, pp. 623–630.

[103] *Communication Networks and Systems in Substations—Part 7–2, Basic Communication Structure for Substation and Feeder Equipment-Abstract Communication Service Interface (ACSI)*, Int. Electrotech. Committee, Geneva, Switzerland, IEC 61850, 2003.

[104] R. Kuffel, J. Giesbrecht, T. Maguire, R. P. Wierckx, and P. McLaren, "RTDS-a fully digital power system simulator operating in real time," in *Proc. IEEE Commun. Power Comput. Conf. (WESCANEX)*, vol. 2. Winnipeg, MB, Canada, 1995, pp. 300–305.

[105] J. Eidson and K. Lee, "IEEE 1588 standard for a precision clock synchronization protocol for networked measurement and control systems," in *Proc. 2nd ISA/IEEE Sensors Ind. Conf.*, Houston, TX, USA, 2002, pp. 98–105.

[106] N. Dorsch, F. Kurtz, H. Georg, C. Hagerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Venice, Italy, Nov. 2014, pp. 422–427.

[107] W. Mahnke, S.-H. Leitner, and M. Damm, *OPC Unified Architecture*. Heidelberg, Germany: Springer, 2009.

[108] X. Chang, "Network simulations with OPNET," in *Proc. 31st Conf. Winter Simulat. Simulat. Bridge Future*, vol. 1. Phoenix, AZ, USA, Dec. 1999, pp. 307–314.

[109] T. R. Henderson, M. Lacage, and G. F. Riley, "Network simulations with the ns-3 simulator," in *Proc. SIGCOMM Demo.*, Seattle, WA, USA, 2008, p. 527.

[110] S. Li and M. M. Kokar, "Agent communication language," in *Flexible Adaptation in Cognitive Radios*. New York, NY, USA: Springer, 2013, pp. 37–44.

[111] F. Bellifemine, A. Poggi, and G. Rimassa, "Developing multi-agent systems with a FIPA-compliant agent framework," *Softw. Pract. Exp.*, vol. 31, no. 2, pp. 103–128, 2001.

[112] G. Karagiannis *et al.*, "Performance of LTE for smart grid communications," in *Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance*. Cham, Switzerland: Springer, 2014, pp. 225–239.
[113] *Modbus Organization*. (Apr. 2016). [Online]. Available: http://www.modbus.org
[114] *Distributed Network Protocol*. (Apr. 2016). [Online]. Available: http://www.dnp.org
[115] G. Combs. (2007). *Wireshark*. [Online]. Available: http://www.wireshark.org/lastmodified

Mehmet Hazar Cintuglu received the B.S. and M.S. degrees in electrical engineering from Gazi University, Ankara, Turkey, in 2008 and 2011, respectively. He is currently pursuing the Ph.D. degree with the Energy Systems Research Laboratory, Electrical and Computer Engineering Department, College of Engineering and Computing, Florida International University, Miami, FL, USA. From 2009 to 2011, he was a Power Systems Project Engineer with an electric utility company in Turkey. His current research interests include multiagent systems, distributed control, cyber physical systems for active distribution networks, and microgrids.

Osama A. Mohammed received the master's and doctoral degrees in electrical engineering from Virginia Tech in 1981 and 1983, respectively. He is a Professor of Electrical Engineering and the Director of the Energy Systems Research Laboratory, Florida International University, Miami, FL, USA. He has performed research on various topics in power and energy systems in addition to design optimization and physics passed modeling in electric drive systems and other low frequency environments. He is a world renowned leader in electrical energy systems. He has performed research in the area of electromagnetic signature, wideband gap devices and switching, and ship power systems modeling and analysis. He has current active research projects for several federal agencies dealing with power system analysis and operation, smart grid distributed control and interoperability, cyber physical systems, and co-design of cyber and physical components for future energy systems applications.

He has published over 450 articles in refereed journals and other IEEE refereed international conference records. He has also authored a book and several book chapters. He was a recipient of the prestigious IEEE Power and Energy Society Cyril Veinott Electromechanical Energy Conversion Award and the 2012 Outstanding Research Award from Florida International University. He is an elected fellow of the Applied Computational Electromagnetic Society.

Kemal Akkaya received the Ph.D. degree in computer science from the University of Maryland, Baltimore County in 2005. He is an Associate Professor with the Department of Electrical and Computer Engineering, Florida International University. He joined the Department of Computer Science, Southern Illinois University, as an Assistant Professor, where he was an Associate Professor from 2011 to 2014. He was also a Visiting Professor with George Washington University in 2013, where he leads the Advanced Wireless and Security Lab (ADWISE) with the ECE Department. He has published over 100 papers in peer-reviewed journal and conferences. His current research interests include security and privacy, energy aware routing, topology control, and quality of service issues in a variety of wireless networks such as sensor networks, multimedia sensor networks, smart-grid communication networks, and vehicular networks. He was a recipient of the Top Cited Article Award from Elsevier in 2010. He is the Area Editor of *Ad Hoc Networks* (Elsevier) and serves on the editorial board of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He has served as the Guest Editor for the *Journal of High Speed Networks*, *Computer Communications*, and *Ad Hoc Networks* and in the TPC of many leading wireless networking conferences including IEEE ICC, Globecom, LCN, and WCNC.

A. Selcuk Uluagac received the M.Sc. degree in electrical and computer engineering from Carnegie Mellon University in 2002, the M.Sc. degree in information security from the School of Computer Science, Georgia Institute of Technology (Georgia Tech), in 2009, and the Ph.D. degree with a concentration in information security and networking from the School of ECE, Georgia Tech, in 2010. He was a Senior Research Engineer with Symantec. He was a Senior Research Engineer with the School of Electrical and Computer Engineering (ECE), Georgia Tech. He is currently a member of the faculty with the Department of ECE, Florida International University. The focus of his research is on cyber security topics with an emphasis on its practical and applied aspects. He is interested in and currently working on problems pertinent to the security of Internet of Things and cyber-physical systems. He was a recipient of the Faculty Early Career Development (CAREER) Award from the U.S. National Science Foundation (NSF), in 2015 and the Outstanding ECE Graduate Teaching Assistant Award from the School of ECE, Georgia Tech, in 2007. He was selected to receive a fellowship from the U.S. Air Force Office of Sponsored Research's 2015 Summer Faculty Fellowship Program in 2015. He is also an active member of ACM and ASEE and a regular contributor to national panels and leading journals and conferences in the field. He is currently the Area Editor of the *Journal of Network and Computer Applications* (Elsevier) and serves on the Editorial Board of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS.