A Comprehensive Review of Smart Grid Related Standards and Protocols

M. Kuzlu, *Senior Member, IEEE*, M. Pipattanasomporn, *Senior Member, IEEE*, and S. Rahman, *Fellow, IEEE*
Virginia Tech – Advanced Research Institute, Arlington, VA 22203
mkuzlu@vt.edu, mpipatta@vt.edu and srahman@vt.edu

***Abstract*-The emergence of the smart grid has led to the development of a diverse set of standards and protocols for achieving interoperability among smart devices. These smart grid related standards and protocols cover a wide variety of power system components and functionalities. In this paper, a comprehensive review of commonly used standards and protocols in the smart grid environment is provided, ranging from those related to the enterprise, control center and wide area monitoring, distributed generation, substation, demand response, metering, electric vehicles and cyber security.**

***Index Terms* - Smart grid standards and protocols, IEEE, *IEC and NIST*.**

I. Introduction

The smart grid is the next-generation electrical grid that makes use of advanced technologies to allow existing generation, transmission and distribution assets to operate more efficiently. It promises to increase the efficiency of today's electric power grids by around 9% by 2030 [1]. It also promises to deliver many positive impacts on the economy, the environment, energy security, and many aspects of everyday life [2]. With a growing number of smart devices and applications, standards and protocols have become a necessity for seamless integration of a number of devices and systems into the smart grid environment and enabling them to communicate and exchange information. Smart grid related standards and protocols have been developed by a number of Standards Development Organizations (SDOs), such as the Institute of Electrical and Electronic Engineers (IEEE), International Electrotechnical Commission (IEC) and National Institute of Standards and Technology (NIST). The U.S. Department of Energy (DOE) sponsored the launch of the Smart Grid Information Clearinghouse (SGIC) web portal [3] that provides information about smart grid projects worldwide, together with smart grid related standards and protocols and their brief descriptions.

A majority of previous publications focus on relevant standards in a specific domain. For example, with respect to the wide-area control and substations, authors in [4,5] review smart grid standards for Protection, Control, and Monitoring (PCM) applications, including substation protection and automation, wide area situation awareness, etc. Authors in [6] propose a framework for IEC 61968 messages and associated implementation profiles consisting of adaption for web services, business interfaces, asynchronous exchange pattern, plug & play and information flow control. Business challenges of IEC 61850 have been discussed in [7]. Authors in [8] discuss two most commonly used industrial automation standards, IEC 61850 and OPC Unified Architecture (OPC UA), to provide a service-oriented integration framework in the smart grid environment. With respected to distributed resources, authors in [9] provide a brief view of interconnection standards related to distributed resources. Authors in [10] review IEC and IEEE standards communication protocols for monitoring and control of distributed generators. In [11], authors discuss the IEEE 1547 series of standards and provide insight into systems integration and grid infrastructure. In [12] authors have developed a flexible information model, taking into considerations the common information model, for offshore smart grids based on the IEC 61400-25-2, IEC 61400-3 and IEC 61850-7 standards. In [13] authors propose a communication strategy for control of Distributed Energy Resources (DERs) based on selected communication standards, such as IEC 61850 and IEC 60870. Authors in [14] address challenges of deploying smarter grids, especially smart meter concerns. As cyber security is also a critical aspect in the smart grid environment, some studies also focus on cyber security standards. Authors in [15, 16] discuss security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the smart grid environment and analyze smart grid security standards.

In summary, as far as the literature search is concerned, a good number of existing work focuses on presenting smart grid related standards and protocols in a specific domain. There are yet a limited number of studies which provide comprehensive review of smart grid related standards encompassing all aspects of the smart grid, e.g., enterprise and control center, wide area monitoring, substations automation, distributed resources, demand response, metering, electric vehicles, and cyber security. Hence, it is the objective of this paper to review and discuss major standards, protocols, and challenges in these areas.

II. Standards and Protocols in the Smart Grid Environment

Fig. 1 summarizes commonly used smart grid related standards, categorized in the following areas: enterprise, control center and wide area monitoring; substation automation; distributed generation; demand response; metering; and electric vehicles. These standards are explained in more details below.

A. Enterprise, Control Center and Wide Area Monitoring

1) IEC 61970: IEC 61970 is known as Energy Management System Application Program Interface (EMS-API). It defines an information model with common objects in the area of electric transmission systems to provide a semantic model. IEC 61970 also provides an abstract API for data exchange independent of platform and technology. It can be used on different operating systems with different programming languages and different database systems.

978-1-5090-5938-6/17/$31.00 ©2017 IEEE

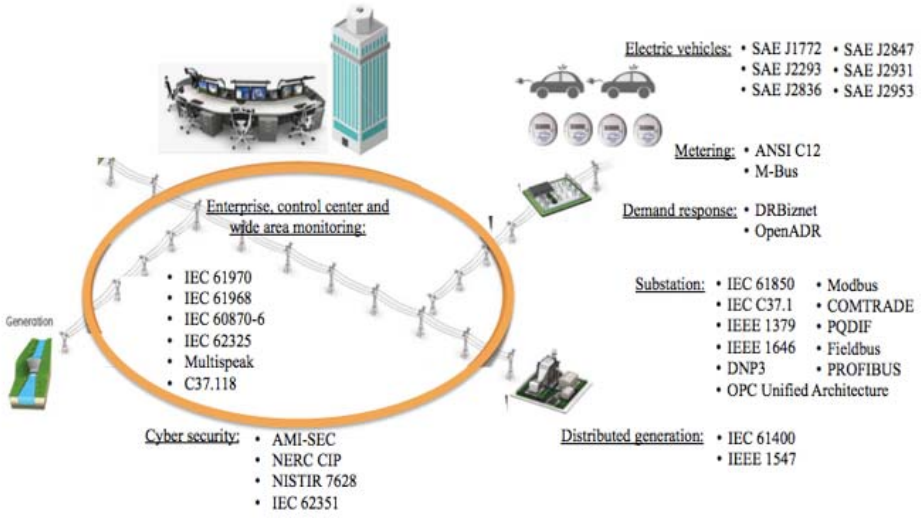

Figure 1. Commonly used smart grid standards and protocols

2) IEC 60870-6: IEC 60870-6 or Inter-Control Center Protocol (ICCP) defines systems used for tele-control, i.e., Supervisory Control and Data Acquisition (SCADA), in power system applications. A communication profile and standards for data transfer are defined in IEC 60870-6 to allow monitoring and control over wide area networks (WANs) among control centers. Based on client/server principles, ICCP provides a complete set of management tools and interfaces for SCADA, but does not include the discussion on authentication nor encryption [17].

3) IEC 62325: IEC 62325 is a series of standards that provide general guidelines regarding the use of ebXML (e-business eXtensible Markup Language) technology and architecture for communications in energy markets. The main objective of IEC 62325 is to facilitate the integration of independently developed market-based software applications by different vendors. IEC 62325 provides CIM-based message exchange semantics [18].

4) Multispeak: Multispeak, developed by the National Rural Electric Cooperative Association (NRECA), is an industry-wide standard that addresses the electric distribution domain with the focus on the U.S. market. It defines an information model documented in an Extensible Markup Language (XML) schema as well as a communication protocol based on web services and Simple Object Access Protocol (SOAP). It provides interoperability among different software applications used by electric utilities [19].

5) IEEE C37.118: IEEE C37.118 standards for Synchrophasors for Power Systems define requirements on a phasor measurement unit and relevant communication protocols for phasor data exchange. The protocol can be based on Ethernet, IP or fieldbuses. IEEE C37.118 is designed for reporting synchronized phasor measurement data. It specifies methods to quantify phasor measurements and test procedures to ensure that measurements follow the standard format [20].

B. *Substations Automation*

1) IEC 61850: IEC 61850 specifies communication networks and systems in substations with the objective to provide interoperability among intelligent electronic devices (IEDs), enabling them to perform protection, monitoring, control, and automation functions in substations. IEC 61850 provides the compatibility with CIM for monitoring, control and protection applications. To differentiate among different applications and prioritize traffic flows, IEC 61850 defines five types of communication services: Abstract Communication Service Interface (ACSI), Generic Object Oriented Substation Event (GOOSE), Generic Substation Status Event (GSSE), Sampled Measured Value multicast (SMV), and Time Synchronization (TS) [21].

2) IEEE C37.1: IEEE C37.1 – IEEE Standard for SCADA and Automation Systems – specifies the definition, specification, and application for supervisory control and automation systems for substations. IEEE C37.1 defines system architectures and functions in a substation including protocol selections, human machine interfaces and implementation issues. It also covers network performance requirements related to reliability, maintainability, availability, security, expandability and changeability [22].

3) IEEE 1379: IEEE 1379 provides implementation guidelines and practices for communications and interoperation of IEDs and remote terminal units (RTUs) in an electric substation. It covers a recommended practice for adding data elements and message structures. This standard helps eliminate the need for time consuming and costly efforts to interface equipment to other equipment in a substation [23].

4) IEEE 1646: IEEE 1646 defines communication delivery times for information exchanged among equipment internal and external to substation protection, control, and data acquisition systems. It defines communication delays as the time spent in the network between applications running at two end systems, including both processing and transmission delays [24].

5) DNP3: DNP stands for Distributed Network Protocol. As an open communication protocol, DNP3 is generally used in SCADA systems to specify communication protocols among different components, i.e., a SCADA master station, RTUs

and IEDs. DNP3 is generally used in substations for equipment monitoring and control. The new version of the DNP3 standard (IEEE Std 1815-2012) provides more security features, including the discussion of public key infrastructure and remote key exchanges [25].

6) Modbus: Modbus is an open serial communications protocol which is often used in various applications, such as industrial/building automation, energy management, substation automation, etc. Modbus is used to connect a SCADA master station with RTUs. Modbus defines a messaging structure based on master-slave/client-server communications. It supports serial (two transmission modes: ASCII and RTU), as well as Ethernet (TCP/IP) protocols [26].

7) OPC Unified Architecture: OPC, Object Linking and Embedding (OLE) for Process Control, is a set of standard OLE/COM (component object model) interface protocols that provides interoperability among automation and control applications, field systems and devices, and enterprise applications in the process control industry. The OPC Unified Architecture (OPC UA) is developed by the OPC Foundation and standardized as IEC 62541. OPC UA defines the communication infrastructure and information model. It offers mapping to HTTP/SOAP based web services [27].

*8) IEEE C37.111: C*OMTRADE (Common format for Transient Data Exchange for power systems) is a file format, which is used to store electrical parameters (e.g., current, voltage, power, frequency, etc.) recorded by IEDs during a power systems disturbance event. COMTRADE files obtained from different substations can be used to investigate power disturbance events to understand causes and possible mitigation strategies for future events. The COMTRADE file format has been standardized as C37.111 [28].

9) IEEE 1159.3: PQDIF, known as IEEE Std. 1159.3, is a binary file format suitable for exchanging power quality related measurement and simulation data (e.g., voltage, current and power measurements). It was initiated by IEEE and EPRI to standardize data formats from a variety of simulations, measurements and analysis tools for power quality engineers from many vendors. PQDIF is similar to COMTRADE in structure, but is used primarily to convey power quality data instead of transient disturbance data [29].

10) IEC 61158 (Fieldbus): Fieldbus or IEC 61158 is an industrial computer network protocol used for real-time distributed control. Fieldbus is used at the bottom of the control chain that links PLCs to field components, for example, sensors, actuators and electric motors. Fieldbus supports different network structures, e.g., daisy-chain, star, ring [30].

11) PROFIBUS: PROFIBUS (Process Field Bus) is a communication protocol for field bus communication, which is mainly used in the automation technology. There are two types of PROFIBUS in use today: PROFIBUS DP and PROFIBUS PA, where DP is Decentralized Peripherals; and PA is Process Automation. The former is used to operate sensors and actuators via a centralized controller. The latter is used to monitor measuring equipment via a process control system [31].

C. Distributed Resources and Demand Response

1) IEC 61400: IEC 61400 provides information exchange standards and design requirements for monitoring and control of wind power plants. IEC61400 addresses interoperability issue in communication systems. IEC 61400 allows information exchange between a control center and wind power plants independent of wind turbine manufacturers. It also specifies a set of design requirements to ensure robustness in wind turbine designs. These include design requirements for small wind turbines, offshore wind turbines, wind turbine gearboxes, acoustic noise measurement techniques, wind turbine power performance testing, measurement and assessment of power quality characteristics of grid connected wind turbines, rotor blades testing and lightning protection [32].

2) IEEE 1547: IEEE 1547 specifies standards for interconnecting distributed resources with electric power systems. It addresses the physical and electrical interconnection and interoperability of distributed energy resources with electric power systems by providing requirements for performance, operation, testing and safety. It also addresses information modeling, use case approaches, and an information exchange template [33].

3) DRBiznet: DRBizNet (Demand Response Business Network) is a highly flexible, reliable and scalable platform to support DR applications. DRBizNet has a service-oriented architecture and provides a standardized web services interface. It enables market operators and utilities to efficiently, reliably and securely manage DR processes. It defines and manages custom DR programs for any market. It enables automatic notifications to customers, aggregators, and distribution/grid operators and triggers any type of intelligent load control devices [34].

4) OpenADR: Open Automated Demand Response (OpenADR) is a communication protocol providing a standardized information model in the area of demand response. The protocol relies on web services, Web Service Definition Language (WSDL), SOAP, and XML. It was developed to provide a common information exchange between utilities or independent system operators and electricity customers. OpenADR also specifies information that can be exchanged during DR and DER events, for example, event name, event identification, event status, operating mode, reliability and emergency signals, renewable generation status and electricity price signals [35].

D. Metering

1) ANSI C12: ANSI C12 is mostly used in North American market. ANSI C12 suite (e.g., ANSI C12.18, 12.19, 12.20, 12.21, 12.22) defines protocol for metering applications. It specifies requirements and guidance on protocol specification for optical ports, end device data tables, electric meter accuracy classes, protocol specification for telephone modem communications and interfacing to data communication networks.

2) M-Bus: M-Bus or EN 13757-4 is also known as Meter-Bus. It is widely used for remote utility meter readings, such as electricity and gas. M-Bus is designed for low-cost, battery-powered devices. M-Bus can also be used for building energy management applications, such as alarm systems, heating/cooling/ lighting control [36].

E. Electric Vehicles (EV)

Electric Vehicle standards are established by the Society of Automotive Engineers (SAE), which a global engineering society in automotive, aerospace, and related commercial-vehicle industries [37].

1) SAE J1772: Electric Vehicle and Plug in Hybrid Electric Vehicle (PHEV) Conductive Charge Coupler -- discusses general requirements (physical, electrical, functional and performance) to facilitate conductive charging of EV/PHEV in North America. It specifies charging methods and connector requirements for Level 1, level 2 and DC chargers.

2) SAE J2293: SAE J2293-Energy Transfer System for Electric Vehicles- provides requirements for EV and the off-board electric vehicle supply equipment (EVSE). It covers functional requirements and system architectures, as well as communication requirements and network architectures for transferring electrical energy to an EV from an electric utility in North America.

3) SAE J2836: SAE J2836 specifies use cases for communications between plug-in electric vehicles (PEV) and the electric power grid, between PEV and off-board DC chargers and between customers and PEV, as well as use cases for diagnostic communication and wireless charging communication. Additionally, it also defines use cases for PEV communicating as distributed energy sources.

4) SAE J2847: SAE J2847 specifies requirements and specifications for communications for PEV using Smart Energy Profiles (SEP) 2.0, between PEV and off-board DC charger, for PEV as a distributed energy sources, between PEV and their customers, and between wireless charged vehicles and wireless EV chargers. Additionally, it also establishes communication requirements for diagnostics between PEV and EVSE.

5) SAE J2931: SAE J2931 covers communications for PEV, including inband signaling communication, PLC communication, broadband PLC communication between PEV and the EVSE. This set of standards also establishes the requirements for digital communication between PEV/EVSE and the utility or service provider, Energy Services Interface (ESI), Advanced Metering Infrastructure (AMI) and Home Area Network (HAN). It also establishes the security requirements for such communications.

6) SAE J2953: SAE J2953 addresses the interoperability issue of PEV and EVSE. It establishes requirements and specifications by which a specific PEV and EVSE pair can be considered interoperable. In addition, it also establishes test procedures to ensure the interoperability of PEV and EVSE from different vendors. SAE J2953 has three levels of interoperability testing: Tier 1 - mechanical interoperability, charge functionality, safety feature functionality; Tier 2 - indefinite grid events, dynamic grid events; and Tier 3 - ampacity control, scheduled charge, staggered scheduled charge, and charge interrupt/resume.

F. Cyber Security

There are a number of standards that are applicable to information security in the smart grid environment. There are also a number of cyber security use cases. This section only discusses major ones. The list of other cyber security related standards can be obtained from UCA International Users Group (UCAIug) [38].

1) AMI System Security Requirements (AMI-SEC): AMI-SEC is developed by the AMI-SEC Task Force [39] to provide a set of security requirements for AMI, which benefits the utility industry and vendors. These security requirements aim for use during the procurement process of AMI and smart meters. The scope of AMI-SEC covers components of the entire AMI system, ranging from AMI communications network device, AMI forecasting system, AMI head end, AMI meter, AMI meter management system to home area network interface of the smart meter. It also includes recommended controls of system and communication protection, such as cryptographic key establishment and management, transmission of security parameters, denial-of-service protection, public key infrastructure certificates and many more.

2) NERC CIP: The North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC CIP) plan is a set of requirements to secure assets required for operating bulk electric power systems in North America. NERC CIP covers a wide range of topics [40], such as personnel & training in cyber security, critical cyber asset identification, security management controls, electronic security perimeter(s), incident reporting and response planning, information protection, recovery plans for critical cyber assets, as well as physical security.

3) NISTIR 7628: NISTIR 7628 is the guidelines for smart grid cyber security, which has three volumes: Vol. 1 – smart grid cyber security strategy, architecture, and high-level requirements; Vol. 2 – privacy and the smart grid; and Vol. 3 – supportive analyses and references. These documents were originally issued on August 2010 as a companion document to the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108). NISTIR 7628 Revision 1 (3 volumes) [41] was issued in September 2014. NISTIR 7628 presents a comprehensive framework that can help guide the development of effective cyber security strategies. It provides guidance to assess cyber security risks and help identify appropriate cyber security requirements.

4) IEC 62351: The scope of the IEC 62351 is to define cyber security requirements for power systems management and associated information exchange. IEC 62351-1 introduces the reader to various aspects of communication network and system security associated with power system operations. IEC 62351-2 defines terms and acronyms used in IEC 62351 standards. IEC 62351-3 to IEC 62351-6 specifies messages, procedures and algorithms for securing Manufacturing Message Specification (MMS) based applications. IEC 62351-7 to IEC 62351-11 address end-to-end information security, including security policies, access control, key management, and others [42].

III. CHALLENGES

A number of smart technologies have been deployed to enable two-way communications with the aim to make the electricity grid smarter. One fundamental attribute that is vital for the integration of a number of smart devices to enable smart grid applications is interoperability among various devices and platforms. While much progress has been made for smart grid deployment and implementation, many challenges in the area of smart grid related standards and protocols still need to be addressed [43]. ***The major challenge is device and platform interoperability:*** Interoperability is the ability of different devices and platforms to

exchange information and work cooperatively to accomplish smart applications. ***The second is the lack of awareness:*** Even though many smart grid related standards exist, there is the lack of awareness of available smart grid standards and protocols, as well as the lack of guidelines for applying them in smart grid deployment. ***The third is technical challenges:*** The electric power grid comprises a large number of electrical components that are tightly coupled together and operating dependently. ***The forth is the complexity:*** The smart grid is an extremely complex system, including many subsystems. In many smart grid projects, smart grid standards developed by different SDOs are used together.

IV. Conclusion

A number of organizations and user groups are working on smart grid standards and protocols to guide the successful deployment of and customer engagement with the smart grid. This paper reviews commonly used smart grid standards and protocols for smart grid applications, ranging from enterprise and control center, wide area monitoring, substations automation, distributed resources, demand response, metering, electric vehicles to cyber security. Most commonly used standards/protocols under discussion are enterprise, control center and wide area monitoring (IEC 61970, IEC 61968, IEC 60870-6, IEC 62325, Multispeak, OPC UA, C37.118), substations automation (IEC 61850, IEEE C37.1, IEEE 1379, IEEE 1646, DNP3, Modbus, COMTRADE, PQDIF, Fieldbus, PROFIBUS), distributed resources and demand response (IEC 61400, DRBiznet, OpenADR, IEEE 1547), metering (ANSI C12, M-Bus), electric vehicles (SAE J1772, SAE J 2293, SAE J2836, SAE J2847, SAE J2931, SAE J2953), cyber security (AMI-SEC, NERC CIP, 3, NISTIR 7628, IEC 62351). The paper also discusses challenges in smart grid standards. It is expected that this paper can provide an insight into smart grid standards that support a variety of smart grid applications.

References

[1] "What is smart grid?" [Online]. Available: http://www.whatissmartgrid.org/

[2]"Strategic R&D Opportunities for the Smart Grid", http://www.nist.gov/smartgrid/upload/Final-Version-22-Mar-2013-Strategic-R-D-Opportunities-for-the-Smart-Grid.pdf.

[3]Smart Grid Related Standards, [Online]. Available https://www.sgiclearinghouse.org/Standards

[4] Kanabar, M.G.; Voloh, I.; McGinn, D., "A review of smart grid standards for protection, control, and monitoring applications," Protective Relay Engineers, 2012 65th Annual Conference for, vol., no., pp.281-289, 2-5 April 2012.

[5] Kanabar, M.G.; Voloh, I.; McGinn, D., "Reviewing smart grid standards for protection, control, and monitoring applications," IEEE Innovative Smart Grid Technologies (ISGT), pp.1-8, 16-20 Jan. 2012.

[6] Guangxian Lv; Jianghe Zhao; Jian Su; Disi Zhang, "Research on IEC 61968 Standard Oriented Function Framework of Adapter in Smart Distribution Grid," Digital Manufacturing and Automation (ICDMA), 2013 Fourth International Conference, pp.1061-1065, 29-30 June 2013.

[7] Ayers, L.M., "Implementing Smart Grid standards: A letter from the trenches," IEEE Innovative Smart Grid Technologies Asia (ISGT), pp.1-5, 13-16 Nov. 2011.

[8] Sucic, S.; Rohjans, S.; Mahnke, W., "Semantic smart grid services: Enabling a standards-compliant Internet of energy platform with IEC 61850 and OPC UA," IEEE EUROCON, pp.1375-1382, 1-4 July 2013.

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

[10] Jaloudi, S.; Ortjohann, E.; Schmelter, A.; Wirasanti, P.; Morton, D., "Communication strategy for grid control and monitoring of distributed generators in Smart Grids using IEC and IEEE standards," IEEE Innovative Smart Grid Technologies (ISGT Europe), pp.1,6, 5-7 Dec. 2011.

[11] Basso, T.; Hambrick, J.; DeBlasio, D., "Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards," IEEE Innovative Smart Grid Technologies (ISGT), pp.1-7, 16-20 Jan. 2012.

[12] Trinh Hoang Nguyen; Prinz, A.; Friiso, T.; Nossum, R., "Smart grid for offshore wind farms: Towards an information model based on the IEC 61400-25 standard," IEEE Innovative Smart Grid Technologies (ISGT), pp.1-6, Jan. 2012.

[13] Jaloudi, S.; Ortjohann, E.; Schmelter, A.; Wirasanti, P.; Morton, D., "General communication strategy for control of distributed energy resources in smart grids via international standards," Intelligent System Application to Power Systems (ISAP) Conference, pp.1-6, 25-28 Sept. 2011.

[14] Schneiderman, R., "Smart Grid Takes on Critical Standards Challenges," in Modern Standardization: Case Studies at the Crossroads of Technology, Economics, and Politics, 1, Wiley-IEEE Standards Association, 2015, pp.288.

[15] Wenye Wang, Zhuo Lu, Cyber security in the Smart Grid: Survey and challenges, Computer Networks, vol. 57, no.5, pp. 1344–1371, 7 April 2013.

[16] Yong Wang; Da Ruan; Dawu Gu; Gao, J.; Daming Liu; Jianping Xu; Fang Chen; Fei Dai; Jinshi Yang, "Analysis of Smart Grid security standards," IEEE Computer Science and Automation Engineering (CSAE) Conference, vol.4, pp.697-701, 10-12 June 2011.

[17]IEC 60870-6 (ICCP), [Online]. Available: http://xanthus-consulting.com/IntelliGrid_Architecture/New_Technologies/Tech_IEC_60870-6_(ICCP).htm,

[18] Sabari Chandramohan, L.; Ravikumar, G.; Doolla, S.; Khaparde, S.A., "Business Process Model for Deriving CIM Profile: A Case Study for Indian Utility," IEEE Transactions on Power Systems, vol.30,no.1, pp.132-141, Jan. 2015.

[19] MultiSpeak [Online]. Available: http://www.multispeak.org/Pages/default.aspx.

[20] C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems, [Online]. Available: https://standards.ieee.org/findstds/standard/C37.118.1-2011.html

[21] Mackiewicz, R.E., "Overview of IEC 61850 and benefits," IEEE Power Engineering Society General Meeting, pp.8, 2006.

[22] IEEE Standard for SCADA and Automation Systems - Redline," IEEE Std C37.1-2007 (Revision of IEEE Std C37.1-1994), May 2008.

[23] 1379-2000 - IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation, [Online]. Available: https://standards.ieee.org/findstds/standard/1379-2000.html

[24] 1646-2004 - IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation, [Online]. Available: http://standards.ieee.org/findstds/standard/1646-2004.html

[25] The Distributed Network Protocol, [Online]. Available: https://www.dnp.org/default.aspx.

[26] Modbus, [Online]. Available: http://www.modbus.org/.

[27] OPC Unified Architecture Specification, [Online]. Available: https://scadahacker.com

[28] COMTRADE IEEE Std C37.111-1991, pp.1, 1991.

[29] IEEE 1159-3 PQDIF, [Online]. Available: http://www.pqview.net/pqdif.asp

[30] Fieldbus Foundation, [Online]. Available: http://www.fieldbus.org/

[31] PROFIBUS - PROFINET, [Online]. Available: http://www.profibus.com/

[32] EIC61400-1[Online]. Available: http://homes.civil.aau.dk/rrp/BM/BM8/r.pdf

[33] IEEE 1547 Series of Interconnection Standards, [Online]. Available: http://grouper.ieee.org/groups/scc21/1547_series/1547_series_index.html

[34] Designing a Demand Response Business Network for California, [Online]. Available: http://eetd.lbl.gov/news/events/2005/03/08/designing-a-demand-response-business-network-for-california

[35] The OpenADR Alliance, [Online]. Available: http://www.openadr.org/

[36] The M-Bus: An Overview, [Online]. Available: http://www.m-bus.com/

[37] SAE Standards, [Online]. Available: http://standards.sae.org/

[38] List of Cybersecurity for Smart Grid Standards and Guidelines, [Online]. Available: http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf

[39]AMI-SEC Task Force Overview, [Online]. Available: http://osgug.ucaiug.org/utilisec/amisec/default.aspx

[40] CIP Standards [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[41] Guidelines for Smart Grid Cybersecurity [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[42] IEC 62351 Security Standards for the Power System Information Infrastructure, [Online]. Available: http://iectc57.ucaiug.org

[43] Schneiderman, R., Smart Grid Takes on Critical Standards Challenges, Wiley-IEEE Standards Association, 2015.