Analyzing Cyber Requirements for the Smart Grid Applications

Anurag K. Srivastava(✉)

The School of Electrical Engineering and Computer Science, Washington State University,
Pullman, WA 99163, USA
asrivast@eecs.wsu.edu

Abstract. With the development of the smart grid technology, networking technology (NT) plays a significant role in the smart grid. NT enables to realize the smart grid vision mainly focused on (a) wide area monitoring and control for transmission system (b) distribution automation for low voltage distribution system and (c) smart metering for prosumer's participation. Synchrophasor technology enables better situational awareness and decision support and smart meters deployment for end-users constitutes major investment as part of the smart grid development for power distribution system. The two-way communications between 'power utility' and 'smart meters installed near end-user customers' assisted by meter data management systems helps to potentially realize numerous applications for enhanced reliability and efficiency of active distribution system. NT also brings cyber vulnerabilities and it is important to analyze the impact of possible cyber-attacks on the power grid. In this invited talk, networking and data delivery requirements will be discussed for wide area monitoring and smart metering applications as well as a real-time, cyber-physical co-simulation testbed to do cyber-physical analysis.

Keywords: Smart grid · Wide area monitoring and control · Distribution automation · Smart metering · Networking technologies

1 Cyber Requirements for Wide Area Monitoring and Control

The availability of synchronized measurements has made the development of data-driven power system applications possible to enhance the reliability of the power grid [1]. The PMUs provide synchronized time stamped measurements several times a second to enable monitoring of dynamic system response, which was not possible using legacy system, having refresh rate of 4 s [2, 3]. Most of the synchrophasor applications can be classified in several categories following different criteria. Based on the level of adoption by different power system utilities, applications can be classified as (a) existing industry applications and (b) evolving applications. Applications can also be classified based on time criticality, (a) real time online applications and (b) offline applications. Some of the examples of real time applications will be oscillation monitoring, voltage stability monitoring and angle/frequency monitoring, which are already implemented in control centers while examples of offline applications are engineering analysis and includes model validation and post-mortem analysis [2–4]. The data rate and latency

E.T. Lau et al. (Eds.): SmartGIFT 2017, LNICST 203, pp. 151–154, 2017.
DOI: 10.1007/978-3-319-61813-5_15

required by some applications may be higher than other applications and will require different kind of NT as shown in Table 1.

Table 1. Data and latency requirements for synchrophasors applications

Class	Basic description	Sampling/date rate	Required latency
A	Feedback control	Fast	Fast
B	Open loop control	Medium	Medium
C	Visualization	Medium	Medium
D	Event analysis	Fast	Slow
E	Research/ experimental	N/A	N/A

2 Cyber Requirements for Smart Metering Applications

Cyber requirements for smart meter applications are shown in Table 2.

Table 2. Data and communication requirement for smart meter applications

Application	Quantity	Rate	Data destination	Real time requirements	Criticality	Frequency
Outage detection	High	Few minutes	DMS	Minutes	Low	Frequent
Distribution state estimation	High	Seconds/ minutes	DMS	Second to minutes	Medium to high	Frequent
Billing information	Medium to low	Several days/ month	Billing center/ enterprise	Hours	Very low	Time to time
Voltage control	High to medium	Seconds	Feeder device/ substation/ operating center	Seconds	High	Very frequent
Demand response	High	Seconds	At load/ substation/DMS	Seconds to minutes	High	Frequent
Power quality monitoring	Low to medium	Seconds	Feeder device/ substation/ operating center	Second	Very high	Time to time
Tamper Detection	Medium to low	Days	Billing center	Hours	Very low	Time to time
Load forecasting	Very high	Minutes	Operating center	Hours	Very low	Frequent
Load modeling	High	Minutes	Substation/ operating center	Minutes	Low	Frequent

Requirements are shown in terms of data quantity, rate, data destination, real time requirements, criticality and frequency as shown in Table 2. Applications including outage detection, distribution state estimation, billing information, voltage control, demand response, power quality monitoring, tamper detection, load forecasting, load modeling have been discussed in Table 2. Most of these applications assume tight integration of smart meter data and SCADA data [5]. Communication technologies to meet the requirements include WiFi, Zigbee and several other technologies [6] as highlighted in Table 3.

Table 3. Communication technology for smart meter applications

Comm. Tech.	Application domain	Coverage range	Data rate	Benefits	Limitations
PLC	HAN, NAN, WAN	1–3 km	2–3 Mbps	No extra cabling fee, high security	High noise, low scalability
WiFi	HAN, WAN	100 m, 1 km	Up to 54 Mbps	Free license, mature development	Low security, low scalability
ZigBee	HAN	<50 m	250 kbps	Low cost, easy implementati on	Low security, short range, low data rate
Cellular Network (3G, LTE)	HAN, NAN, WAN	1–10 km	Up to 70 Mbps	Mature development, long range	Low security, low costly spectrum fees, low scalability

Acknowledgments. Author would like to thank his colleagues for number of brainstorming sessions related to cyber infrastructure for the smart grid specially Dr. Hauser, Dr. Bakken, Dr. Hahn and Dr. Liu at Washington State University and Prof. Roy at University of Washington.

References

1. Tushar, Banerjee, P., Srivastava, A.K.: Synchrophasor applications for load estimation and stability analysis. In: IET Power and Energy Series, Synchronized Phasor Measurements for Smart Grids (2017)
2. Liu, R., Goodfellow, R., Srivastava, A.K.: A testbed for closed loop cyber-physical-social system simulation and security analysis. In: Cyber-Physical-Social Systems and Constructs in Electric Power Engineering. IET (2016)
3. Liu, R., Vellaithurai, C., Biswas, S., Gamage, T., Srivastava, A.: Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Trans. Smart Grid **6**(5), 2444–2453 (2015)
4. Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., Adhikari, U.: Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans. Smart Grid **4**(1), 235–244 (2013)

5. Venkataramanan, V., Srivastava, A., Hahn, A.: Real-time co-simulation testbed for microgrid cyber-physical analysis. In: Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), CPSWeek, Vienna, April 2016
6. Venkataramanan, V., Zhou, Y., Srivastava, A.: Analyzing impact of communication network topologies on reconfiguration of networked microgrids. In: North American Power Symposium, Denver, September 2016