Challenges and Opportunities for a Resilient and Safe Smart Grid

Sara Biyabani, Lou Gullo, and Sergio Panetta

Extreme weather, natural disasters and bad actors can all disrupt, damage, or destroy power systems infrastructure, and there is an immediate need for solutions that will mitigate multiple hazards. Fortunately, the characteristics of the Smart Grid that are distinct from the traditional power grid can also present opportunities for building a more reliable and resilient power generation and delivery system. Given the need for creating resilience in the Smart Grid as a whole system as well as its components, we invite participation of IEEE Members and others with interest or expertise in reliability to join the Smart Grid Program.

Some challenges that motivate the consideration of reliability within power systems today and in the immediate future are:

- the grid infrastructure is heterogenous in nature and aging at a fast pace, even though advanced digital control and automation are also being adopted at the same time.
- the intermittent renewable energy resources complicate the real-time delivery of power to the demand and, thus, raise concerns for secure and uninterruptible service.
- the liberalization of electricity markets has created expectations of sensible energy pricing and high quality of service, meaning that outages should be infrequent and any corrective measures immediate and efficient. extreme climate swings have introduced unprecedented concerns for service disruptions that may be catastrophically widespread.
- with rising tensions worldwide, another reliability aspect is that of modern and asymmetrical warfare, leading to cyber-physical security fears with attacks on system infrastructure and generating plants. ensuring the safety of consumers and operators is critical during both normal and abnormal operations.
- Lastly, on the technology-side, novel functionalities are allowed by advanced sensing, faster processing times and artificial intelligence, and they raise the bar for situational awareness and the expected response times to both disruptive and quality-of service phenomena. As a result, the need for reliability planning of the Smart Grid is an ongoing business and engineering effort driven by numerous factors, contradicting aims and an ever-evolving landscape of hardware, software, policies and decision making.

As a result, the need for reliability planning of the Smart Grid is an ongoing business and engineering effort driven by numerous factors, contradicting aims and an ever-evolving landscape of hardware, software, policies and decision making.

Smart Grid Characteristics and Opportunities for Enhanced Reliability and Resilience

The Smart Grid is defined as the integration of power, communications, and information technologies for an improved electric power infrastructure serving loads while providing for an ongoing evolution of end-use applications [1].

There are two major characteristics of the Smart Grid. One defining characteristic is distributed power generation by intermittent heterogenous sources. Distributed Energy Resources (DER) (i.e., wind, solar and storage) present more modular, scalable and flexible generation of energy. There is a need to create and enhance techniques to prevent faults that may lead to wildfires or other system disturbances; to integrate

renewable energy more seamlessly at the transmission and distribution levels; and to increase the integration of electrified vehicles, buildings, and other grid-edge devices.
Another characteristic of the Smart Grid that is distinct from the traditional power grid is that digital Communications systems and modern Information systems are as an integral part of the Smart Grid as the Power systems. Consequently, **Interoperability** between the three dimensions of the Smart Grid (Power, Communications and Information/Computer Systems) becomes critical for the operation, performance, and robustness of not only the Smart Grid components, but the Smart Grid as a whole. Consequently, Cybersecurity becomes as important as physical security of the Smart Grid infrastructure.

The IEEE Std 2030-2011 [1] defines the Smart Grid as a **System of Systems**. It provides a good way to conceptualize the Smart Grid as a whole and provides an engineering framework for how various components of the Smart Grid might interoperate with each other and could aid us in systematically examining how various Smart Grid components and subsystems could be made more reliable and resilient. (Detailed specific recommendations or standardizations concerning specific components or protocols are defined in other related standards under the IEEE Std 2030 umbrella, and not in the base standard.) It does not define the Smart Grid from the subjective perspective of any one Smart Grid component, such as the DER, Utility data server, or a Smart Building. The IEEE 2030 SGIRMTM, the Smart Grid Interoperability Reference Model, is based on systems engineering best practices and adopts the NIST seven functional "Domains": Generation, Transmission, Distribution, Customer, Markets, Control and Service Provider. We can think of the System of Systems that is the Smart Grid in terms of the three independent systems or dimensions or "Interoperability Architecture Perspectives, IAPs" defined by the IEEE 2030 SGIRMTM (where each perspective itself is made of the seven functional Domains listed above):

1. **Power Systems (PS):** Perspective comprises Power Generation, Transmission, Distribution and Customer Domains, together with Control and Service Provider and Markets. It is concerned with the production, consumption, transmission, and distribution of power.
2. **Communications Systems (CS):** Perspective comprises the communications networks and devices that connect various elements within a domain, and across domains, to each other. The common (public) Internet backbone infrastructure as well as dedicated or shared field area and other networks constitute this dimension and are concerned with the movement of physical data for communications (which is used by the following Information Technology Systems dimension for the purposes of command, control, monitoring, monetizing and alerting, etc.).
3. **Information Technology Systems (IT):** Perspective comprises the physical infrastructure of computer systems and networks, database and compute servers, edge devices and IoT (Internet of Things) that reside in various functional domains (such as Service Providers, Customers, Markets, etc.). This dimension is concerned with the abstract dataflows for specific applications such as Billing, Market Participation Activities and Bidding, Sensor Monitoring, analytics, and control and management of Distribution (DMS) and DER (DERMS).

In summary, the reliability and resilience of the Smart Grid then requires not only the Power Systems components of the Smart Grid to be reliable and resilient, but the Communication and the Information Systems' components and systems to also be reliable and resilient. A wealth of Reliability Best Practices [2] [3] for the design and operation of the building blocks of the Smart Grid already exists, but there are also new opportunities for engineering and deriving Best Practices specifically for the Smart Grid, especially in terms of the interactions between its diverse components and systems.

Reliability within Smart Grid systems can be planned and implemented along the lines of the following activities (not an exhaustive list):

A. Identify **reliable components** and parts that implement the Smart Grid.

B. Conceptualize and design **Engineered Resilient Systems**, ERS, that implement specific functionality of the Smart Grid, and
C. Determine **novel reliability processes** to implement and operate all things Smart Grid.
D. Contribute to **standards** that integrate best practices and metrics from Reliability with Smart Grid-related Standards.

Smart Grid as an Industrial Application

Components of the Smart Grid can be viewed as industrial applications. For example, Microgrids are industrial applications that benefit from the best practices developed by the IEEE Industry Applications Society.

The Industry Applications Society is involved in:

- the advancement of the theory and practice of electrical and electronic engineering in the development, design, manufacture and application of electrical systems, apparatus, devices, and controls to the processes and equipment of industry and commerce.
- promotion of safe, reliable and economic installations.
- industry leadership in energy conservation and environmental, health, and safety issues.
- creation of voluntary engineering standards and recommended practices.

Call to Action

Given the need for creating resilience and safety in the Smart Grid as a whole system as well as its components, we invite participation of IEEE Members and others with interest or expertise in Reliability and in Industry Applications to join the Smart Grid Program. Please join Smart Grid for free (/join) (if you haven't already) and indicate your area/s of interest at https://bit.ly/IEEEReliableSmartGrid.

To that end, the IEEE Smart Grid Program, IEEE Reliability Society, and IEEE Industry Applications Society will collaborate on the development and enhancement of a safe, reliable and resilient Smart Grid.

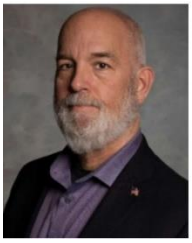
References

[1] IEEE Std 2030-2011. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.
[2] IEEE Std 1332-2012, IEEE Standard Reliability Program for the Development and Production of Electronic Products.
[3] IEEE Std 1624-2008, IEEE Standard for Organizational Reliability Capability

Biography

Sara Biyabani is the Vice Chair of IEEE Smart Grid Program. She is a computer architect who has delivered industry-leading products ranging from CPUs, ASICs, handhelds, embedded and graphics

systems to datacenter servers and supercomputer interconnects. She is the Founder and CTO of an emerging technologies startup. She works on distributed computing and analytics for intelligently integrating distributed energy resources into the power grid, IoT and communications for SmartGrid and EV-charging, and on standardization efforts in interdisciplinary areas covering the SmartGrid and energy efficiency and power proportionality in digital systems and analog radio-transmitter technologies. Sara is an IEEE Senior Member and active in IEEE PES, Communications & Computer Societies and IEEE-SA, serving on RevCom. She is the Chair of IEEE Energy Efficient Comm Hardware Standards IEEE 1924.1-2022 & 1923.1-2021, and has contributed to the development of several SmartGrid standards including 2030-2011, 1547 & 2030.2 and currently leads IEEE 2030 SGIRM Revision. Sara has a Masters degree in Electrical & Computer Engineering and a Bachelors degree in Physics & Computer Science. She holds a patent in unified memory architecture design and has numerous publications. She is the recipient of the 2022 IEEE-SA Medallion Award.



Louis J Gullo is the VP of the IEEE Reliability Society (RS) Technical Activities (TA). He is a member of the IEEE RS Administrative Committee (AdCom) and Executive Committee (ExCom). He has been the Chair of the IEEE RS Standards Committee since 2006. He is a member of the ExCom for the IEEE Computer Society (CS) Systems Software Engineering Standards Committee (S2ESC). He received the IEEE Reliability Engineer of the Year award in 2016. He is the founder and past chair of the IEEE RS Arizona (AZ) Chapter. He is an IEEE Senior Member.

Lou is a Staff Systems Engineer at Northrop Grumman Corporation. He leads the Condition-Based Maintenance Plus (CBM+) Prognostics and Health Management (PHM) team on the Sentinel Program at Northrop Grumman. He is the Subject Matter Expert (SME) for Design for Testability (DfT), Logistics Data System (LDS) Interfaces, and Software Reliability.

He has over 35 years of experience in system engineering, hardware, and software reliability, maintainability, testability, prognostics, safety, security, and fault management for the military, space, telecommunications, and commercial electronics industries. He was awarded a US Patent in January 2004 for Reliability Assessment Program (RAP) and has two patents pending. He is the editor and author of 3 books, titled: “Design for Reliability”, “Design for Safety”, and “Design for Maintainability”, published by John Wiley and Sons, Inc..

Sergio Panetta is the VP of Engineering at I-Gard Corporation. A graduate of McMaster University (BEng ’83, MEng ’97) with almost 4 decades of electrical engineering experience in switchgear design, commissioning and troubleshooting, and power system protection and Power system grounding. Sergio continues to actively increase awareness on Electrical Safety on a global front. A Senior Member of the IEEE, member of the IET, and has been awarded Consulting Engineering status with the PEO professional body. Sergio is a member of several industry working groups such as the working group chair of 3003 (Grounding and Bonding which addresses standards like, 3003.1, 3003.2 and Green Book) Chair of C57.32a, Representing Canada for TC14, and, TC 64 for IEC Committees. Vice Chair of Industrial and Commercial

Power Systems. Sergio is actively dealing with electrical safety and best practices including CSA, IEEE, IEC, and UL, he is the author and owner of several US Patents related to electrical safety.