Framework 3.0: A Beginner's Guide

The goal of the smart grid—an emerging nationwide network that modernizes the electric power grid so that it incorporates information technology— is to deliver electricity reliably, efficiently, sustainably, and securely, while also supporting many new services and applications. With initial deployments, consumers are beginning to see benefits, based on the ability of a modernized national electrical grid to:

- Provide consumers with actionable and timely information about their energy usage
- Facilitate expanded use of renewable energy sources
- Improve resilience to disruption by natural disasters and attacks
- Reduce greenhouse gas emissions by enabling electric vehicles and new power sources
- Improve power reliability and quality
- Increase consumer choice, and enable new products, services, and markets

Smart grid technologies enable the integration of renewable, but intermittent, energy sources into the power grid.

To realize these many benefits, the smart grid community is building a modernized grid that is actually a complex, inter-related "system of systems." Unlike the grid of the past century, which primarily delivers electricity in a one-way flow from generator to outlet, the emerging smart grid will enable two-way flows of both electricity and information. As the grid is modernized, there will be many interconnected parts and processes, built and created by many different manufacturers, and used by a diverse array of stakeholders. "Interoperability," which is the ability of diverse systems and their components to work together, will be vitally important to the performance of the smart grid at every level.

"Interoperability" allows systems and their components to work together in a "plug-and-play" approach.

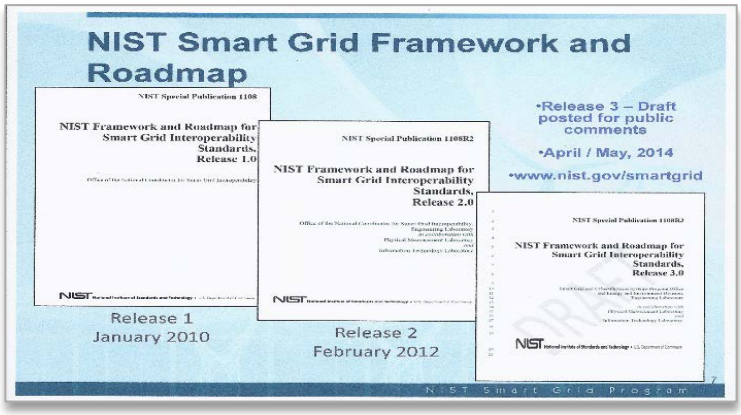
Just as the construction of a fully functioning modern home requires a detailed blueprint and a carefully coordinated construction plan, the development of the smart grid requires a framework and a roadmap for interoperability. A framework provides a common vision and vocabulary, a set of shared principles and practices, and a collective agreement on standards and protocols. A roadmap lays out the process—including steps, timetable, participants, priorities, intermediate goals, and more—required to make that vision a reality.

Framework 3.0 provides a blueprint for smart grid interoperability.

The task of developing such a framework and roadmap falls squarely within the mission of the National Institute of Standards and Technology (NIST). NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST has earned a reputation as an "honest broker" that works collaboratively with industry and other government agencies.

The electrical industry, in particular, has always had a strong partnership with NIST. Therefore, when the federal government charted the next steps for our country's energy future—as outlined in the "Energy Independence and Security Act of 2007 (EISA)"—NIST was given a key role. NIST was assigned "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems…" [EISA Section 1305]. The legislation also directed that the framework be "flexible, uniform, and technology neutral."

NIST began working on this assignment in 2008, and Release 1.0 of the Framework and Roadmap was published in January 2010. Release 2.0 was published in February 2012. The current document, Release 3.0, was published in September 2014, and its contents reflect the many advancements related to smart grid interoperability that we have witnessed since 2008.



Frameworks must evolve as technology advances.

The following paragraphs describe the contents of Framework 3.0. The **sentences in bold** highlight some of the important changes from previous versions of the framework.

Chapter 1, "Purpose and Scope," provides useful background information, such as reviewing how the federal government—and NIST, in particular—has been involved in the development of the smart grid. This chapter also defines key concepts and identifies the priority areas and functionalities on which NIST is focusing its smart grid program.

Chapter 2, "Smart Grid Visions," provides a high-level description of the envisioned smart grid, including benefits, costs, and international aspects. This chapter describes how and why standards and interoperability are so important for the smart grid.

Chapter 3, "Smart Grid Interoperability Panel," describes how NIST has convened and engaged the many diverse stakeholders from across the broad smart grid community—with the goal of coordinating and accelerating the development of standards and protocols that will ensure smart grid interoperability. The Smart Grid Interoperability Panel (SGIP) is the organization that NIST established in November 2009 for this purpose. **In 2013, the SGIP transitioned its functions from a government-funded public-private partnership to an industry-led, non-profit organization, Smart Grid Interoperability Panel 2.0, Inc. NIST maintains a prominent leadership role in the activities of the SGIP, and provides some funding through a cooperative agreement program.** The history, objectives, structure, and outputs of the SGIP organization are outlined in this chapter (and in Appendix D: SGIP Committees, Domain Expert Working Groups (DEWGs), and Priority Action Plans (PAPs)).

2009 – 2012 **2013 - ongoing**

The SGIP provides a good example of industry and government working together.

Chapter 4, "Standards Identified for Implementation," is a very useful chapter for many readers, especially non-experts, because it provides specific information about the standards and protocols that NIST has identified as supporting interoperability of the smart grid. These are the building blocks for interoperability. NIST uses listed guiding principles and criteria, described in this chapter, in the standard review and identification process. The 74 standards thus identified (**including 7 standards not included in earlier releases of the framework**) are listed in Table 4-1. This detailed 67-page table groups the standards and protocols into four sections: Standards and Specifications; Cross-cutting Standards; Requirements and Guidelines; and Cybersecurity. For each standard, the table includes:

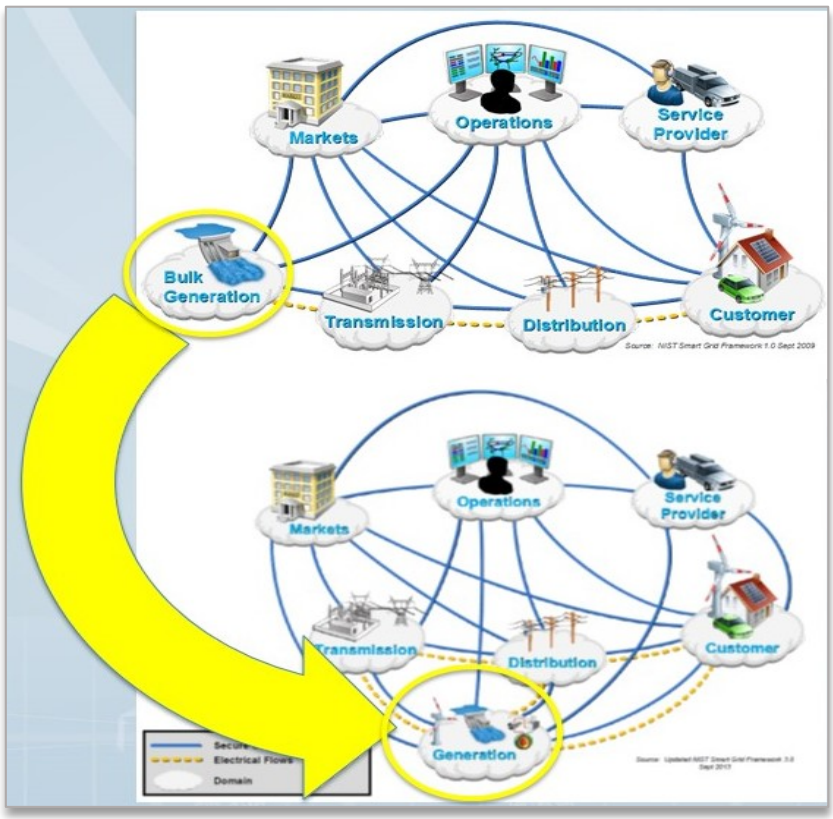
- The name and/or number for the standard
- A link to the website of the relevant standards-setting organization
- The application for which the standard is used
- Comments that briefly describe the purpose and function of the standard
- **The relevant smart grid architectural domains**
- The cybersecurity review of the standard, from the SGIP's Smart Grid Cybersecurity Committee
- Information on whether the standard is included in the SGIP's Catalog of Standards **(and, if so, a link to additional detailed background information available through the SGIP Catalog of Standards' search page)**

This chapter also discusses the process for identifying future smart grid standards. In all, hundreds of standards will likely be required to build a safe and secure smart grid that is interoperable, end to end. Therefore, the list of identified standards will continue to grow as the smart grid is developed, new needs and priorities are identified, and new technologies emerge.

NIST has identified several standards important for interoperability of electric vehicle charging.

Chapter 5, "Architectural Framework," describes how the various "building-block" standards fit into the overall structure of the smart grid. Because the smart grid is an evolving networked system of systems, this high-level architectural model encourages a common perspective of the smart grid; identifies key interactions and interfaces; and provides guidance for standards-setting organizations (SSOs) developing more detailed views of smart grid architecture. Architectural goals for the smart grid are outlined in this chapter, and include such characteristics as capability to support a broad range of technology options, flexibility, upgradeability, security, and interoperability. The earlier versions of the smart grid framework document depicted and defined a conceptual model with seven domains. In Framework 3.0's Chapter 5 and Appendices B and C, extensive work has been done to refine and extend that model, in the following ways:

- **Modifying the conceptual domain model to reflect the growing importance of distributed generation by renaming and moving the "bulk generation" domain into a "generation" domain with interactions with multiple domains (see diagram below)**
- **Aligning and harmonizing the architecture with similar work being done by the European community's Smart Grid Coordination Group (SG-CG)**
- **Describing a new "Smart Grid Architecture Model" (SGAM) that uses the concepts of abstraction layers and stakeholder viewpoints in an enterprise-wide service-oriented approach**
- **Identifying future work needed to define a semantic framework**



The conceptual domain model used in Framework 1.0 and 2.0 (top) was modified in Framework 3.0 (bottom).

Chapter 6, "Cybersecurity Strategy," addresses a subject that has received very significant attention in recent months from the smart grid community, federal government, and general public. The goal of this chapter is to assist the stakeholder community better secure their smart grid systems. NIST has been heavily involved through both its leadership role with the SGIP's Smart Grid Cybersecurity Committee (SGCC) and its collaborative interactions with other government agencies and industry working groups. **This chapter reviews a number of new and revised publications that will be useful to cybersecurity experts, as well as non-experts, in the smart grid community.** The publications include the following:

- Publications from the SGCC and its six technical subgroups
    - NIST Interagency Report (NISTIR) 7628, Revision 1, "Guidelines for Smart Grid Cybersecurity" (This comprehensive three-volume report was originally published in August 2010. **Revision 1 was published in September 2014.**)
    - Companion documents to NISTIR 7628 that are written for implementers: "Guide for Assessing the High-Level Security Requirements in NISTIR 7628" and "NISTIR 7628 User's Guide"
    - Soon-to-be-published white papers: "Cybersecurity Defense in Depth and Breadth," "Risk Management Process Case Study," and "Cloud Computing in the Smart Grid,"
- Publications from the U.S. Department of Energy (DOE)
    - Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
    - DOE Electricity Subsector Cybersecurity Risk Management Process
- **"The Framework for Improving Critical Infrastructure Cybersecurity"**
- **The result of a year-long collaboration between industry, government, and academia, NIST led the development of this framework and accompanying roadmap in response to Executive Order 13636: Improving Critical Infrastructure Cybersecurity.**
- NISTIR 7823, Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework.

Cybersecurity becomes very important as information technology is incorporated with the legacy power grid.

Chapter 7, "Smart Grid Testing and Certification Framework," addresses the important practical reality that, while standards are the foundation for interoperability, testing is required to ensure true interoperability. Interoperability testing programs provide the verification that the standards have been implemented appropriately and consistently. Testing and certification is taking on increased urgency as industry reaches consensus on the underlying standards for the smart grid (discussed in Chapter 4). Although many standards have now been identified, there remains a large gap in the availability of test programs corresponding to these standards. **In Release 3.0 of the Framework, the discussion of testing and certification has been significantly expanded to respond to this need. The centerpiece of the new material is Version 2 of the "Interoperability Process Reference Manual (IPRM)," published in 2012 by the SGIP's Smart Grid Testing and Certification Committee (SGTCC).** The IPRM provides recommendations and best practices, and it will be useful as a guide for readers who are setting up new test programs or improving existing test programs. Version 2 has an operational focus, whereas Version 1 had an informational focus. Chapter 7 also discusses how NIST and the SGIP have expanded their engagement with existing and potential interoperability testing and certification authorities (ITCAs), labs, certifiers, and accreditors. **To date, seven ITCAs have announced plans to implement the IPRM recommendations within their programs (NEMA, UCAIug 61850, UCAIug Green Button, OpenADR, MultiSpeak, SEP2 Consortia, and USnap Alliance).**

The "Green Button" standard provides a secure way to get your energy usage information electronically.

Chapter 8, "Cross-Cutting and Future Issues," contains a high-level overview of three areas of interest to the smart grid community:

- "Electromagnetic compatibility (EMC)" refers to the ability of devices to function properly in a given environment without causing or suffering from electromagnetic interference. The smart grid's sophisticated electronic sensing, control, and communications systems are being exposed to an ever-increasing number of possible electromagnetic disturbances and interference, both man-made and natural. **This chapter discusses the December 2012 SGIP white paper, "Electromagnetic Compatibility and Smart Grid Interoperability Issues," which presents a compilation of important smart grid EMC issues, identified gaps in standards, and recommendations for specifying appropriate EMC tests and standards for smart grid devices.**

- Issues of implementability, safety, reliability, and resilience are becoming increasingly important for utilities, regulators, and consumers. Smart grid technologies, such as microgrids, offer the promise of solutions to these challenges. To address some of these issues, **the SGIP created the Implementation Methods Committee (IMC) and established Priority Action Plan (PAP) 24: "Microgrid Operational Interfaces." The NIST smart grid laboratory programs include a focus on advanced technologies and interoperability for microgrid scenarios**.
- Although the focus of this Framework document is on standards and protocols to ensure interoperability, it is important to note that standards and protocols are not enough. There is also a clear need for R&D—to take advantage of new data, innovations, technologies, and functionalities. To help identify the major technical and societal issues impeding advanced development of the smart grid, and to determine a set of recommended actions to address these issues, **the NIST Smart Grid and Cyber-Physical Systems Program Office, in collaboration with the Renewable and Sustainable Energy Institute (RASEI), hosted an invitational workshop in August 2012. The primary output of the workshop was a high-level document, "Strategic R&D Opportunities for the Smart Grid," published in March 2013.**

This final chapter also outlines the key role that NIST will play in the future of the smart grid. A key objective of NIST's effort is to create a self-sustaining, ongoing standards process that supports continuous innovation as grid modernization continues in the decades to come. NIST and the SGIP will continue to work with standards-setting organizations and other stakeholders to fill the gaps and improve the standards that form the foundation of the smart grid. New cybersecurity guidelines will address emerging new threats. NIST will continue to explore partnership opportunities with the private sector for the creation of testing and certification programs consistent with the SGIP testing and certification framework. NIST will continue to ensure coordination with related international smart grid standards efforts, maintaining U.S. leadership going forward. NIST will support the needs of federal, state, and local regulators in standardization matters in the regulatory arena. In addition to its leadership role in the SGIP, NIST is increasing its measurement research program in areas related to smart grid interoperability. To this end, NIST is developing an integrated smart grid testbed facility for full measurement, characterization, and validation of smart grid technology and interoperability standards, with a particular emphasis on smart microgrids.