The Evolving Smart Grid: What's New in the NIST Framework and Roadmap

May 2, 2014

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Introduction

Chris Greer **chris.greer@nist.gov**

Director, Smart Grid and Cyber-Physical Systems Program Office

Engineering Laboratory

National Institute of Standards and Technology

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Smart Grid: U.S. National Policy

- "It is the policy of the United States to support the modernization of the Nation's electricity [system]… to achieve…a Smart Grid."

- *Congress, Energy Independence and Security Act of 2007*

One Hundred Tenth Congress
of the
United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Thursday, the fourth day of January, two thousand and seven

An Act

To move the United States toward greater energy independence and security, to increase the production of clean renewable fuels, to protect consumers, to increase the efficiency of products, buildings, and vehicles, to promote research on and deploy greenhouse gas capture and storage options, and to improve the energy performance of the Federal Government, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Energy Independence and Security Act of 2007".

www.gpo.gov/fdsys/pkg/BILLS-110hr6enr/pdf/BILLS-110hr6enr.pdf

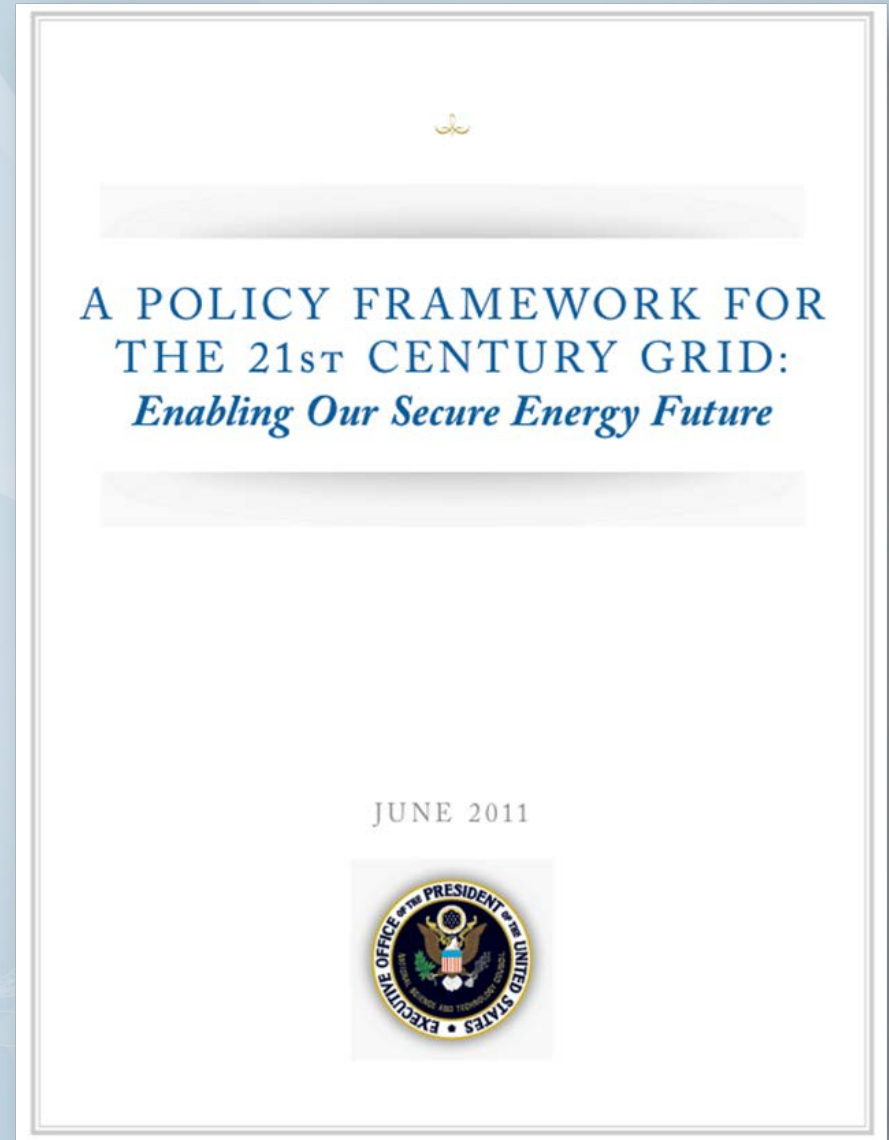# **Standards:** An Important Foundation

The Energy Independence and Security Act directs NIST

"to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"

- Congress directed that the framework be "flexible, uniform, and technology neutral"

Cooperation: Key to Success

"A smarter and more secure grid will require sustained cooperation among the private sector, state and local governments, the Federal Government, consumer groups, and other stakeholders."

A POLICY FRAMEWORK FOR THE 21ST CENTURY GRID:
Enabling Our Secure Energy Future

JUNE 2011

http://www.whitehouse.gov/ostp

Progress: An Evolving Smart Grid Landscape

- An estimated 65 million smart meters will be installed nationwide by 2015
- Electricity suppliers have committed to making Green Button energy use data accessible to more than 50 million homes and businesses
- DoE/ARRA projects that deployed automated feeder switches are reporting up to 56% shorter and 11-49% less frequent outages with fewer affected customers
- Through ARRA investments, more than 1,000 networked PMUs will be deployed by the 2014-2015 time frame
- The rate of deployment of photovoltaic arrays grew by 41% in 2013 with PV providing 12.1 GW system-wide at the end of 2013

NIST Smart Grid Framework and Roadmap

NIST Special Publication 1108

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

Office of the National Coordinator for Smart Grid Interoperability

NIST • National Institute of Standards and Technology • U.S. Department of Commerce

Release 1
January 2010

NIST Special Publication 1108R2

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0

Office of the National Coordinator for Smart Grid Interoperability, Engineering Laboratory
in collaboration with
Physical Measurement Laboratory
and
Information Technology Laboratory

NIST • National Institute of Standards and Technology • U.S. Department of Commerce

Release 2
February 2012

NIST Special Publication 1108R3

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

Smart Grid and Cyber-Physical Systems Program Office and Energy and Environment Division, Engineering Laboratory

in collaboration with
Physical Measurement Laboratory
and
Information Technology Laboratory

NIST • National Institute of Standards and Technology • U.S. Department of Commerce

- **Release 3 – Draft posted for public comments**
- **April / May, 2014**
- **www.nist.gov/smartgrid**

Framework Contents

Draft Release 3 - Table of Contents

Executive Summary

1   Purpose and Scope

2   Smart Grid Visions

3   Smart Grid Interoperability Panel (SGIP)

4   Standards Identified for Implementation

5   Architectural Framework

6   Cybersecurity Strategy

7   Framework for Smart Grid Interoperability T&C

8   Cross-Cutting and Future Issues

Chapter 4: Standards Identified for Implementation

Jerry FitzPatrick **gerald.fitzpatrick@nist.gov**

Leader, Applied Electrical Metrology Group

Physical Measurements Laboratory

National Institute of Standards and Technology

National Institute of
Standards and Technology
U.S. Department of Commerce

Purpose of Chapter 4 – Standards Identified for Implementation

- EISA 2007 assigned NIST the responsibility of coordinating development of a smart grid interoperability framework, including model standards and protocols

- Table 4-1 is a list of standards and protocols identified as supporting interoperability of the smart grid
  - Guiding principles for identifying standards for implementation included
  - Includes requirements documents and guidelines

- Guidance to standards for all SG stakeholders

Criteria for Inclusion

- *Relevancy*
  - Improve reliability, security and efficiency of the Smart Grid
  - Dynamic optimization of grid operations and resources, with full cyber-security
  - Deployment and integration of distributed resources and generation, including renewable resources.
  - Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
  - Deployment of "smart" technologies
  - Integration of "smart" appliances and consumer devices.
  - Deployment and integration of advanced electricity storage and peak-shaving technologies
  - Provision to consumers of timely information and control
  - Development of standards for communication and interoperability of appliances and equipment
  - Lowering of unreasonable or unnecessary barriers to adoption
- *Community Acceptance*
- *Deployment Suitability*
- *Interface Characterization*
- *Document Maintenance*

How to Use Table 4-1

- Table is divided into 4 sections:
  - *Standards and Specifications*
  - *Cross-cutting standards*
  - *Requirements and Guidelines*
  - *Cybersecurity*

- Grouped by families of standards

How to Use Table 4-1 (cont'd)

No.	Standard	Application	Comments	Included in SGIP Catalog of Standards?	SG Conceptual Architecture Domains
29	IEC61850-90-5 http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument CSWG Report : http://members.sgip.org/apps/group_public/document.php?document_id=2633&wg_abbrev=cosd CoS : http://sgip.org/Member-Dashboard	Synchrophasor data transmission	This technical report is a part of the IEC 61850 series of standards that adds a method for exchanging synchrophasor data between PMUs, PDCs, WAMPAC (Wide Area Monitoring, Protection, and Control) systems, and between control center applications. The data, to the extent covered in IEEE C37.118.2 - 2011, is transported in a way that is compliant to the concepts of IEC 61850. This document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.	Y	Transmission, Distribution

How to Use Table 4-1 (cont'd)

Link to SSO website

No.	Standard	Application	Comments	Included in SGIP Catalog of Standards?	SG Conceptual Architecture Domains
29	IEC61850-90-5 http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument CSWG Report : http://members.sgip.org/apps/group_public/document.php?document_id=2633&wg_abbrev=cosd CoS : http://sgip.org/Member-Dashboard	Synchrophasor data transmission	This technical report is a part of the IEC 61850 series of standards that adds a method for exchanging synchrophasor data between PMUs, PDCs, WAMPAC (Wide Area Monitoring, Protection, and Control) systems, and between control center applications. The data, to the extent covered in IEEE C37.118.2 - 2011, is transported in a way that is compliant to the concepts of IEC 61850. This document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.	Y	Transmission, Distribution

How to Use Table 4-1 (cont'd)

Link to cybersecurity review

No.	Standard	Application	Comments	Included in SGIP Catalog of Standards?	SG Conceptual Architecture Domains
29	IEC61850-90-5 http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument CSWG Report : http://members.sgip.org/apps/group_public/document.php?document_id=2633&wg_abbrev=cosd CoS : http://sgip.org/Member-Dashboard	Synchrophasor data transmission	This technical report is a part of the IEC 61850 series of standards that adds a method for exchanging synchrophasor data between PMUs, PDCs, WAMPAC (Wide Area Monitoring, Protection, and Control) systems, and between control center applications. The data, to the extent covered in IEEE C37.118.2 - 2011, is transported in a way that is compliant to the concepts of IEC 61850. This document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.	Y	Transmission, Distribution

How to Use Table 4-1 (cont'd)

Relevant SG Architectural Domains

No.	Standard	Application	Comments	Included in SGIP Catalog of Standards?	SG Conceptual Architecture Domains
29	IEC61850-90-5 http://webstore.iec.ch/webstore/webstore.nsf/artnum/033549!opendocument CSWG Report : http://members.sgip.org/apps/group_public/document.php?document_id=2633&wg_abbrev=cosd CoS : http://sgip.org/Member-Dashboard	Synchrophasor data transmission	This technical report is a part of the IEC 61850 series of standards that adds a method for exchanging synchrophasor data between PMUs, PDCs, WAMPAC (Wide Area Monitoring, Protection, and Control) systems, and between control center applications. The data, to the extent covered in IEEE C37.118.2 - 2011, is transported in a way that is compliant to the concepts of IEC 61850. This document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.	Y	Transmission, Distribution

How to Use Table 4-1 (cont'd)

Link to SGIP CoS search

No.	Standard	Application	Comments	Included in SGIP Catalog of Standards?	SG Conceptual Architecture Domains
29	IEC61850-90-5 http://webstore.iec.ch/webstore/webstore.nsf/artnum/03354 9!opendocument CSWG Report : http://members.sgip.org/apps/group_public/document.php?document_id=2673&wg_abbrev=cosd CoS : http://sgip.org/Member-Dashboard	Synchrophasor data transmission	This technical report is a part of the IEC 61850 series of standards that adds a method for exchanging synchrophasor data between PMUs, PDCs, WAMPAC (Wide Area Monitoring, Protection, and Control) systems, and between control center applications. The data, to the extent covered in IEEE C37.118.2 - 2011, is transported in a way that is compliant to the concepts of IEC 61850. This document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.	Y	Transmission, Distribution

How to Use Table 4-1 (cont'd)

What's new in R3.0?

- A column was added identifying the relevant Smart Grid Conceptual Architecture domain
  - Bulk generation, transmission, distribution, operations, service providers, customer
- The number of implemented standards has increased from 37 to 74
  - Standards are still grouped as "families of standards", but parts have a separate numbered entry
- Standards added:
  - Synchrophasors: IEC61850-90-5, IEEE C37.118.1, IEEE C37.118.2
  - Event data: IEEE C37.239
  - Energy Services Provider Interface: NAESB REQ-21
  - Third party access to Smart Meter Data: NAESB REQ-22
  - OASIS Energy Interoperation
  - Coexistence for broadband power line carrier: NISTIR 7862
  - PAP18 transition from SEP 1 to SEP 2.0
- Standard updated:
  - DNP3: IEEE 1815-2012 replaced IEEE 1815-2010

Chapter 5: Architectural Framework

David Wollman david.wollman@nist.gov

Deputy Director, Smart Grid and Cyber-Physical Systems Program Office

Engineering Laboratory

National Institute of Standards and Technology

National Institute of Standards and Technology
U.S. Department of Commerce

Highlights – Architectural Framework

- How to use Framework?

- What is new?
  - International coordination (European Smart Grid Coordination Group SG-CG)
  - Conceptual reference model improvements
  - Smart Grid Architecture Methodology (SGAM)
    - comprises the original NIST conceptual domain architecture, EU-M490 Reference Architecture, IEC 62357 and the combined reference model

Architectural Goals for Smart Grid

- Options (support broad range of tech options, legacy/new)
- Interoperability (incl. standard interfaces)
- Maintainability (safe/secure/reliable throughout lifecycle)
- Upgradeability (enhance systems, remain operational)

- Innovation
- Scalability
- Legacy
- Security
- Flexibility
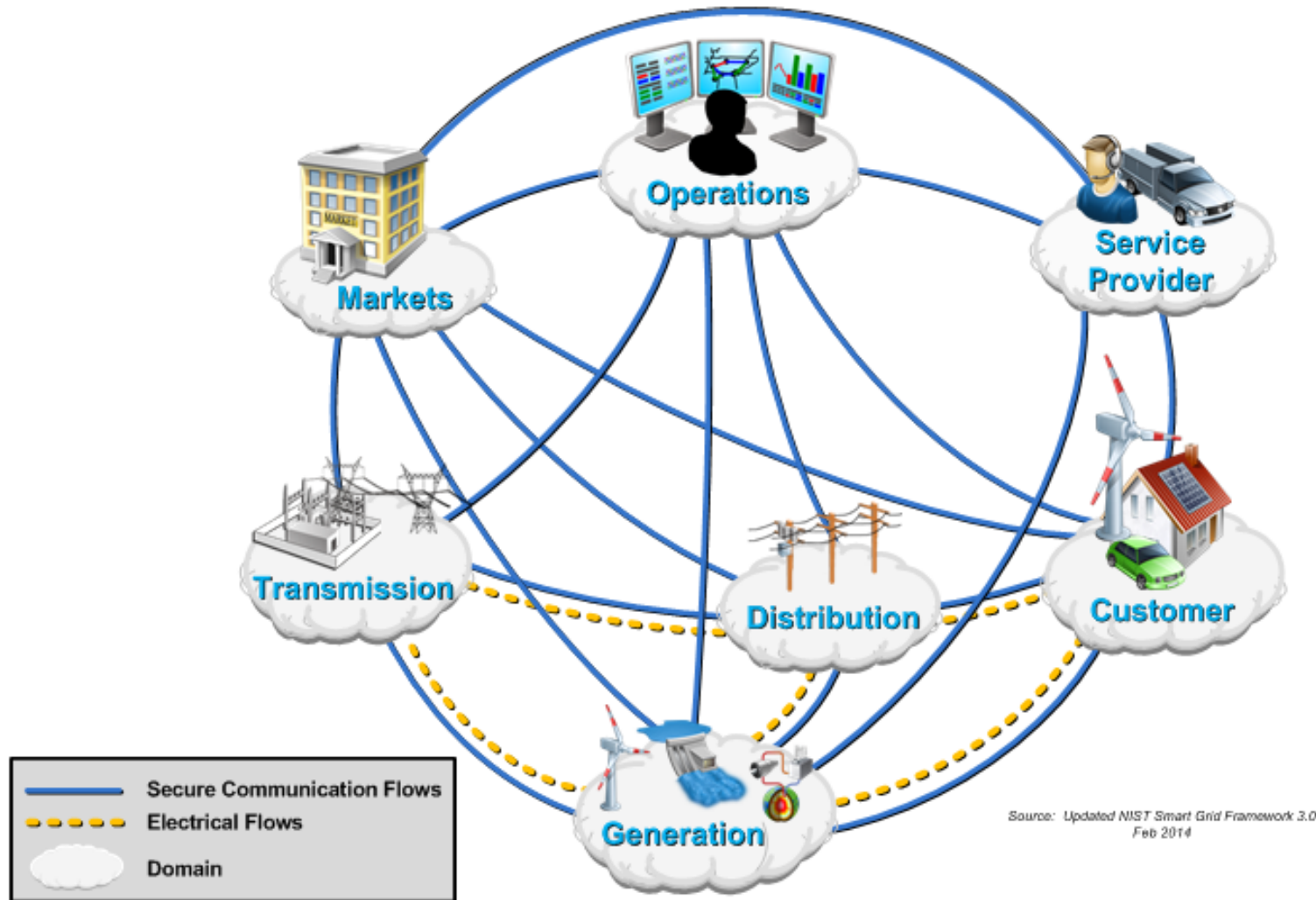- Governance
- Affordability

**Figure 5-1. Interaction of Roles in Different Smart Grid Domains through Secure Communication**

NIST Smart Grid Domains

Source: NIST Smart Grid Framework 1.0 Sept 2009

Legend:
- Secure Communication Flows
- Electrical Flows
- Domain

Source: Updated NIST Smart Grid Framework 3.0 Feb 2014

- NIST Framework Release 1 and 2

- Draft Release 3 for Public Comments

NIST Smart Grid Domains

Source: NIST Smart Grid Framework 1.0 Sept 2009

Source: Updated NIST Smart Grid Framework 3.0 Feb 2014
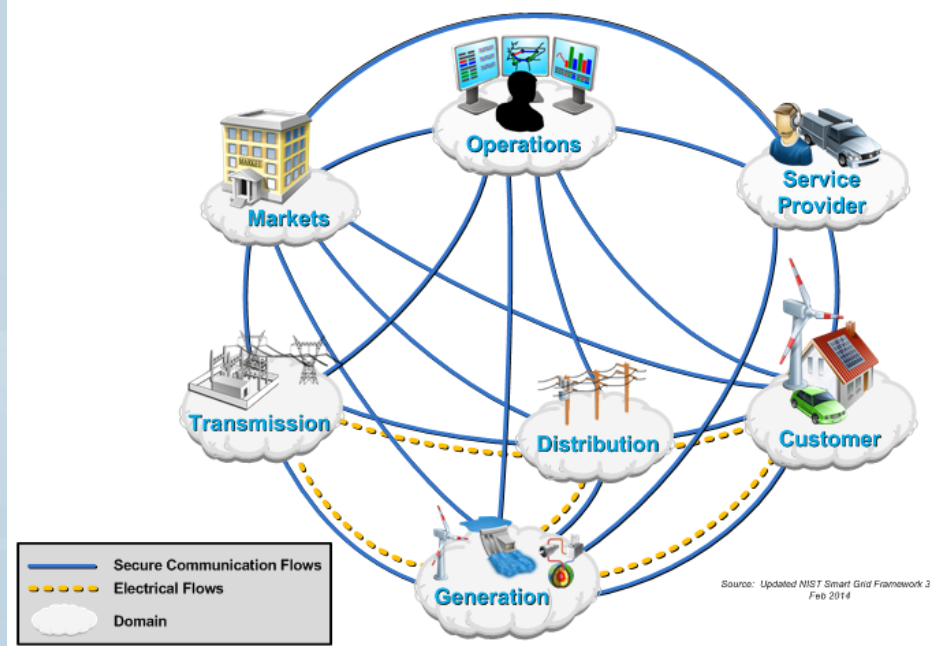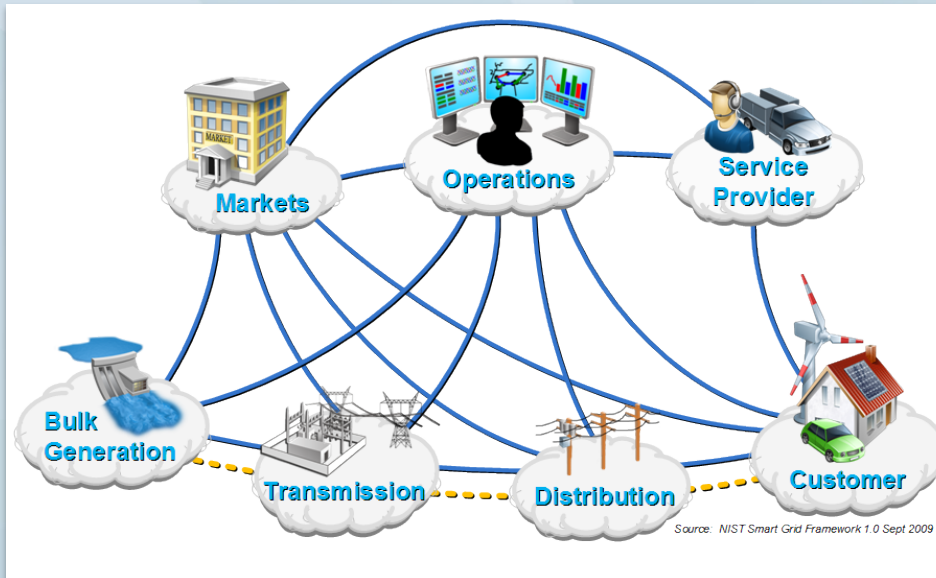
- NIST Framework Release 1 and 2
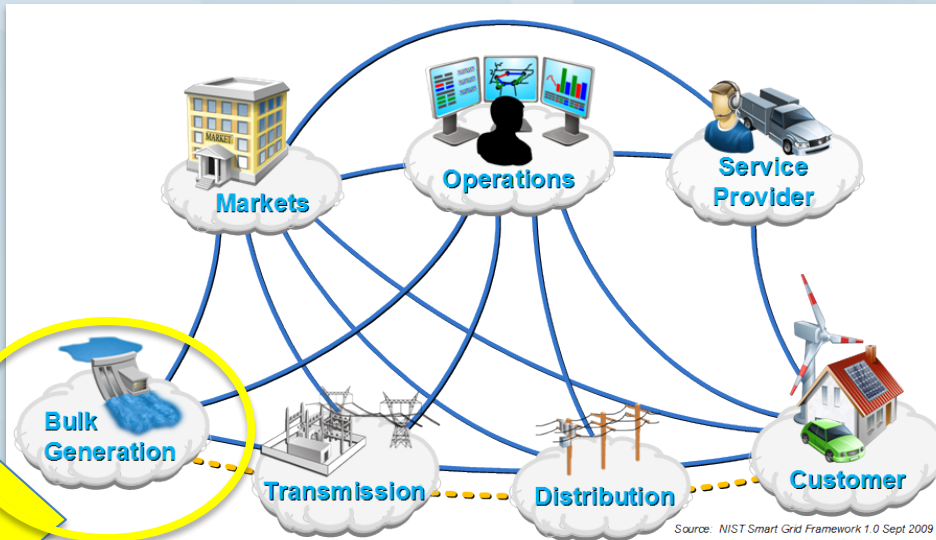
Bulk Generation → Generation

- Draft Release 3 for Public Comments

Architecture methodology

SGAM:
Smart Grid
Architecture
Methodology

Fig 5-5. SGAM iterations, layers, and planes

Architecture methodology

GWAC & SGAM Alignment with TOGAF

Architecture methodology
Architecture layers and iteration levels
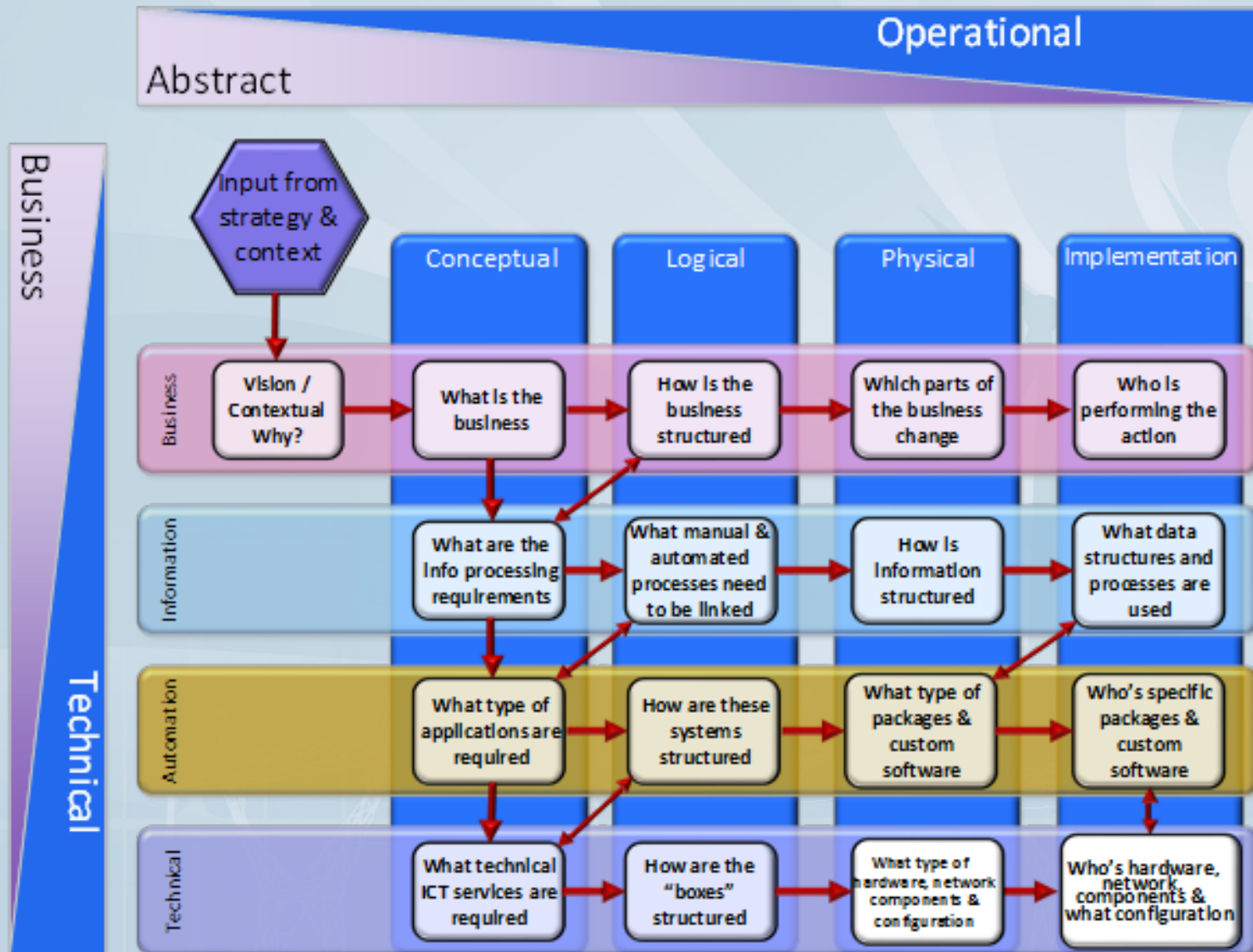
NIST Conceptual Architecture mapping to Matrix

Input from strategy & context

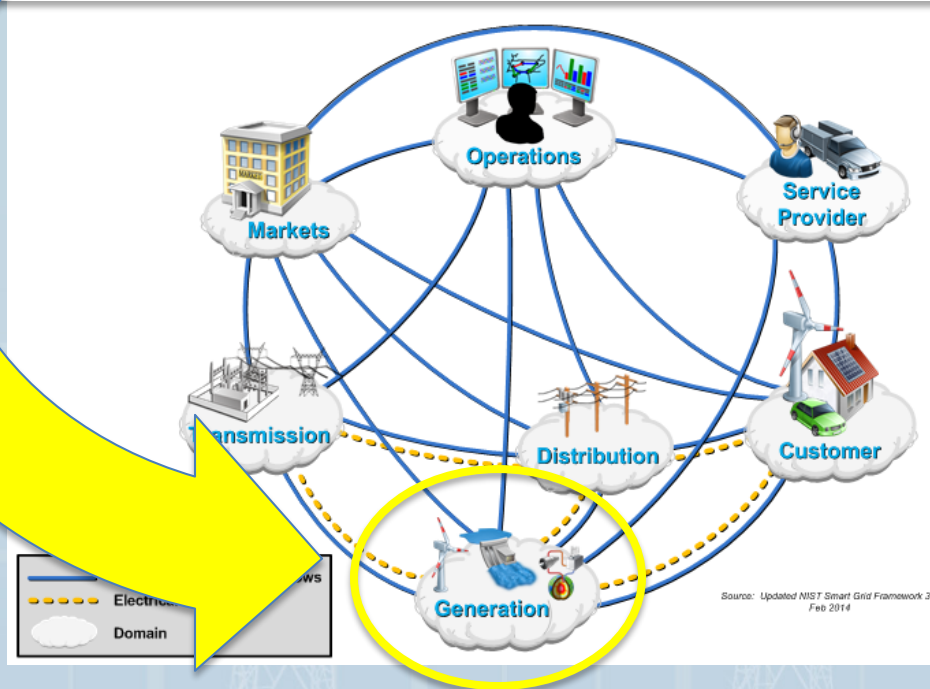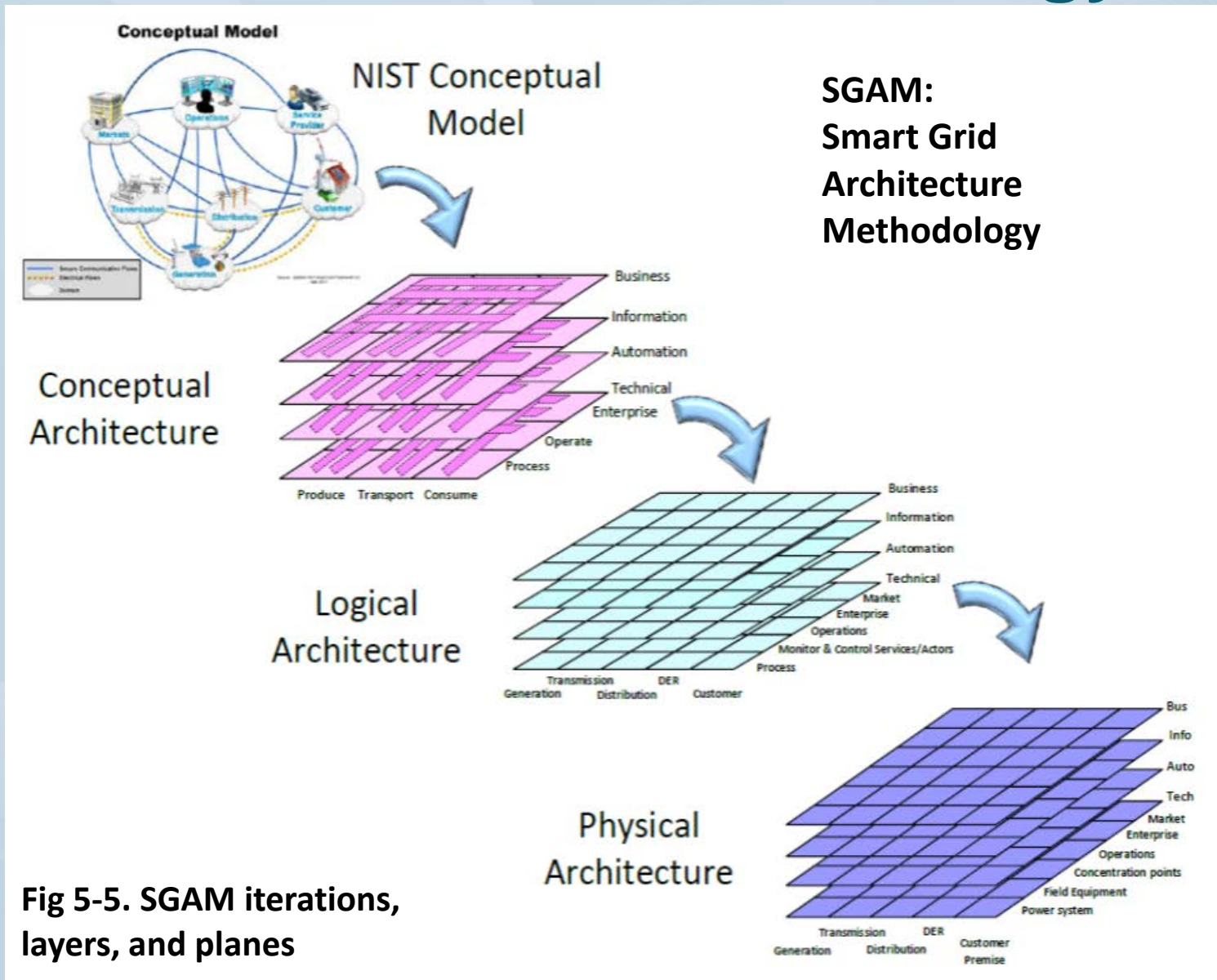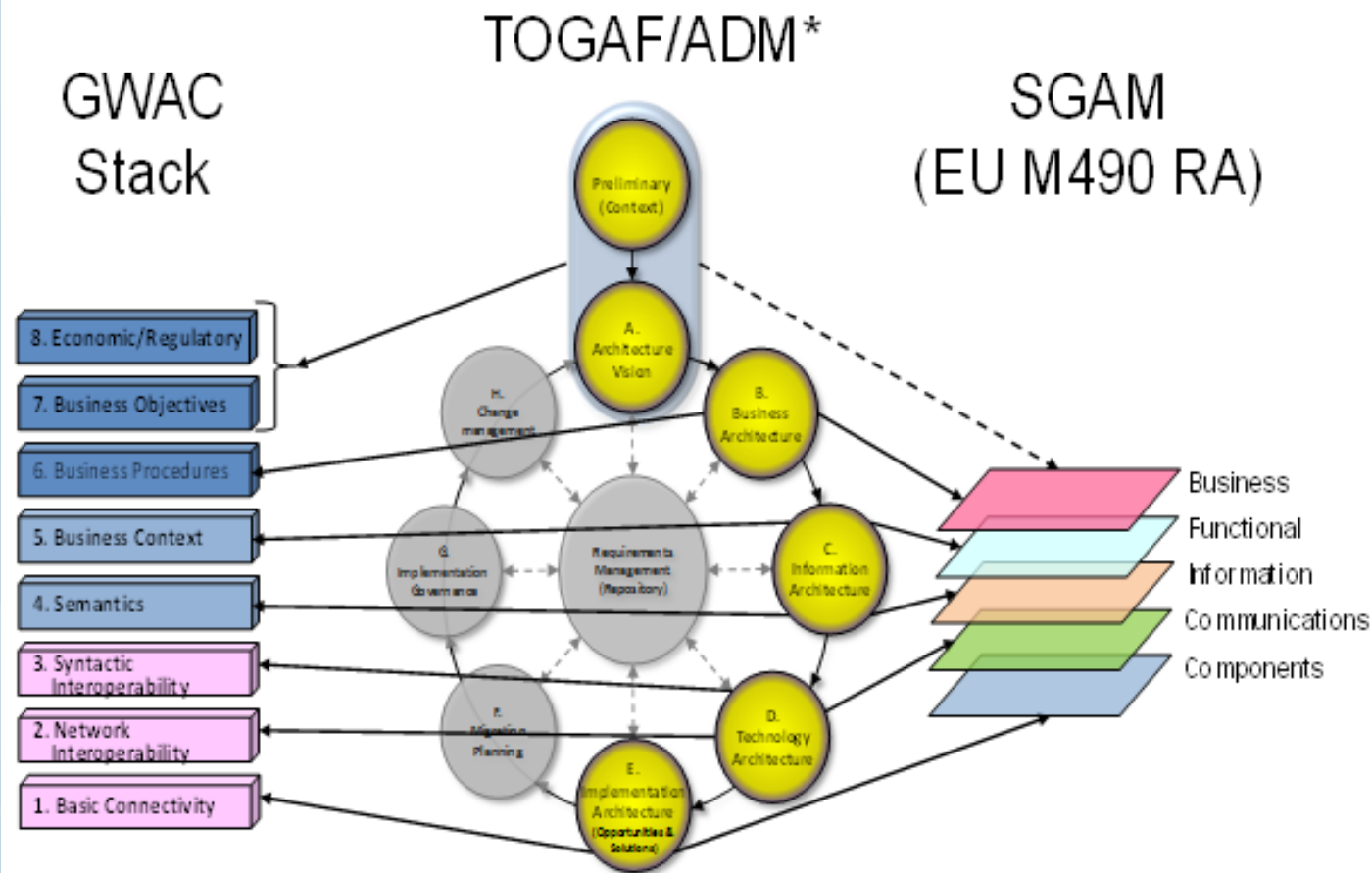**NIST Conceptual Architecture SGiP 1.0**

	Conceptual	Logical	Physical	Implementation
Business	Vision / Contextual Why? → What is the business	How is the business structured	Which parts of the business change	Who is performing the action
Information	What are the info processing requirements	What manual & automated processes need to be linked	How is information structured	What data structures and processes are used
Automation	What type of applications are required	How are these systems structured	What type of packages & custom software	Who's specific packages & custom software
Technical	What technical ICT services are required	How are the "boxes" structured	What type of hardware, network components & configuration	Who's hardware, network, components & what configuration

30

Architecture methodology

Figure 5-7. Logical Model of Legacy Systems Mapped onto Conceptual Domains for Smart Grid Information Networks

Semantic Framework – Future Direction

Toward a canonical semantic model for the smart grid

MultiSpeak

CIM

ETSO-E eMix

Operations

Service Provider

Markets

OpenADR (DR)
Green Button (EUI)
WXXM (Weather)

Transmission

Distribution

Customer

Source: NIST Smart Grid Framework 1.0 Sept 2009

Generation

61850

FSGIM
SEP 2.0
C12.19

ICCP

DNP

EI/EMIX/WSCAL

32
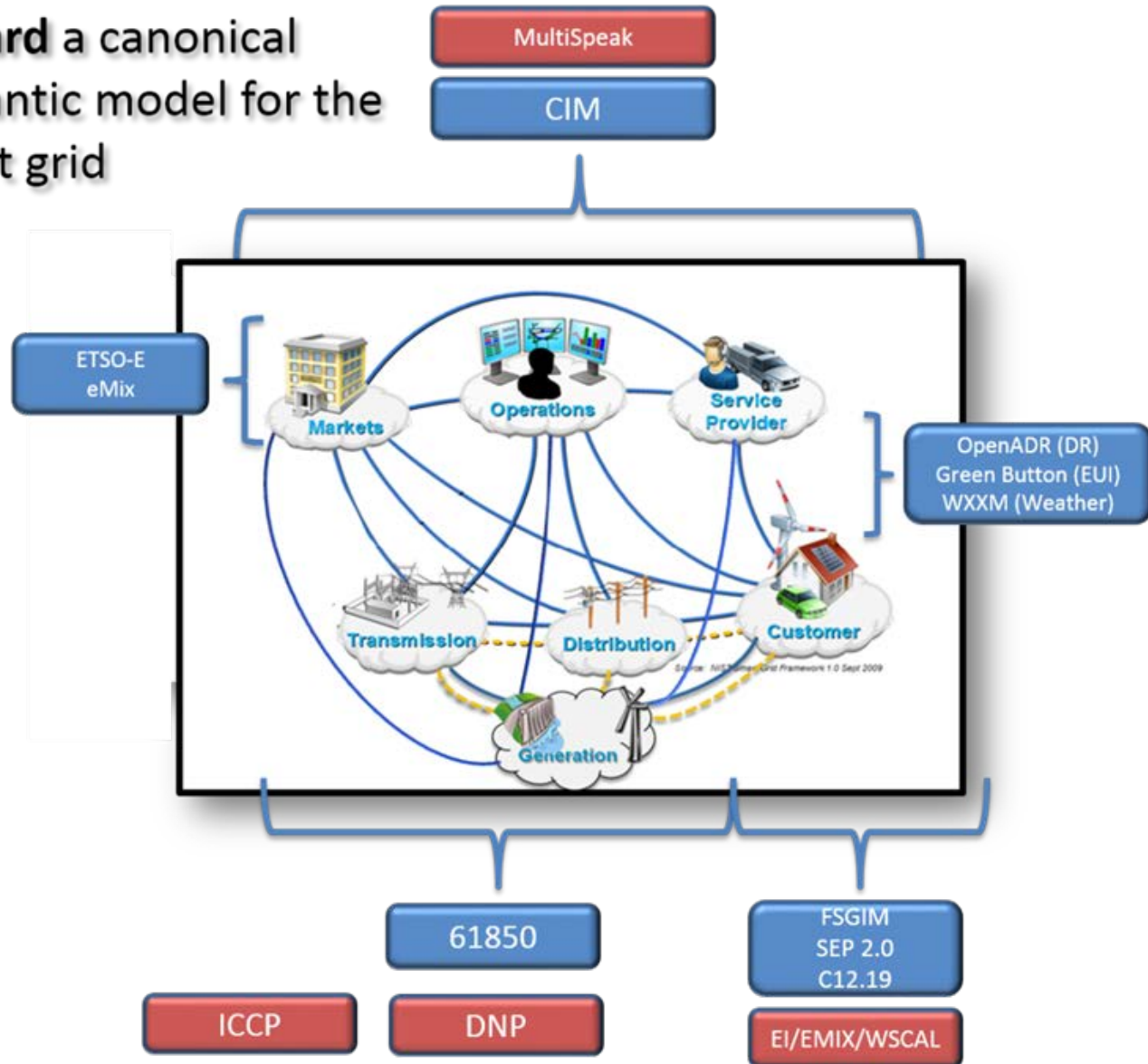
Architectural Framework – Highlights

- SGIP SGAC: Int'l coordination
  - EU: SG-CG
- SGAM
  - Smart Grid Architecture Methodology
- Domains
  - Bulk Generation
    ➡ Generation
- Future work
  - Semantic Framework, …

Fig 5-4. Architecture layers and iteration levels

Chapter 6: Cybersecurity Strategy

Vicky Yan Pillitteri **victoria.yan@nist.gov**

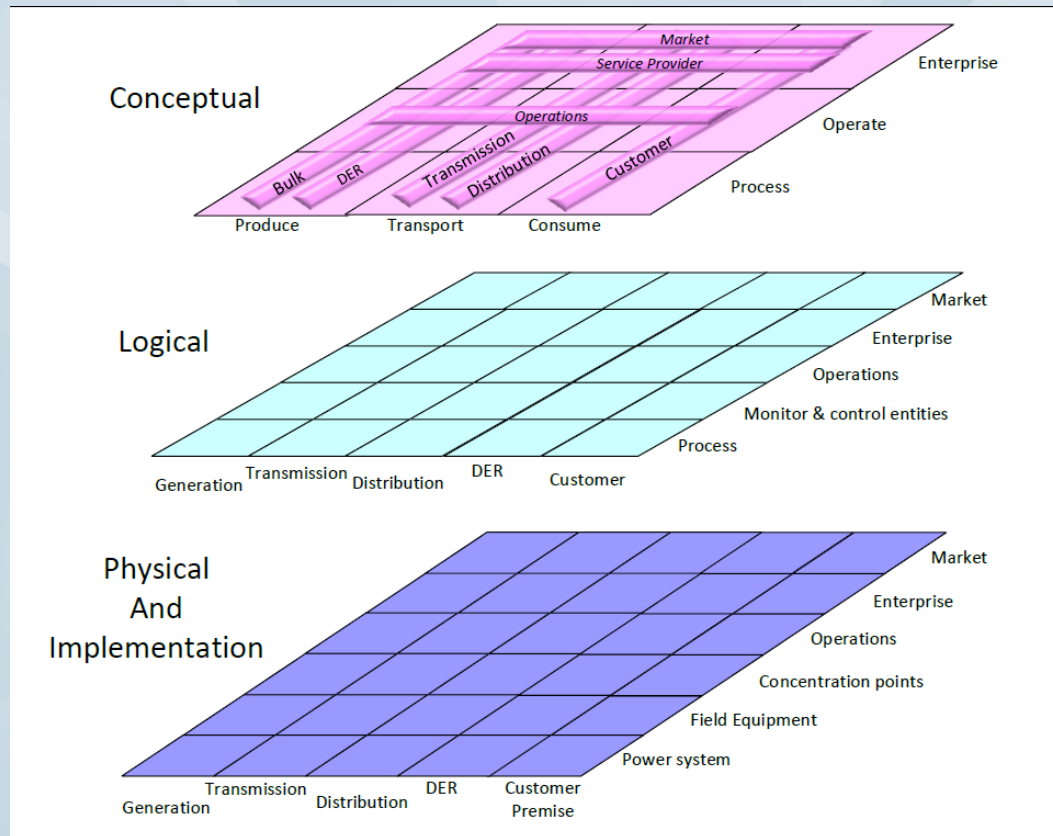Advisor for Information System Security

Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

What's New in the Cybersecurity Strategy

Updates on:

- NIST's role in the SGIP Cybersecurity Committee, including current subgroup activities
- Collaborative efforts across smart grid and energy sector stakeholders
- The *Framework for Improving Critical Infrastructure Cybersecurity*
- The upcoming release of NIST Interagency Report (IR) 7628, Rev. 1, *Guidelines for Smart Grid Cybersecurity*
- Companion documents to NISTIR 7628:
  - Guide for Assessing the High-Level Security Requirements in NISTIR 7628
  - NISTIR 7628 User's Guide
- Future NIST activities in smart grid

SGIP Smart Grid Cybersecurity Committee

- Provides recommended security requirements, updates NISTIR 7628, *Guidelines for Smart Grid Cybersecurity*
- Assesses standards against the high-level cybersecurity requirements and privacy recommendations in NISTIR 7628
- Identifies new smart grid-specific cybersecurity challenges
- Logical security reference model of the smart grid, and work towards a harmonized logical architecture and security architecture
- Subgroups:
  - Architecture, Cloud Computing, High-Level Requirements, Privacy, Risk Management Process Case Study, Standards
- Future developments:
  - Defense in Depth and Breadth White Paper
  - Risk Management Process Case Study White Paper
  - Smart Grid Cloud Cybersecurity Use Case and Guidance
  - Supply Chain Awareness Guide

Collaboration Across Stakeholder Community to Advance Cybersecurity

- Draft NIST Interagency Report 7628, Rev. 1, Guidelines for Smart Grid Cybersecurity

- SGIP White Paper: NISTIR 7628 User's Guide

- Framework for Improving Critical Infrastructure Cybersecurity

- Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

- DOE Electricity Subsector Cybersecurity Risk Management Process (RMP)

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

"It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties"

President Barack Obama
Executive Order 13636, *Feb. 12, 2013*

- The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work

For more information, visit: www.nist.gov/cyberframework
or email: cyberframework@nist.gov
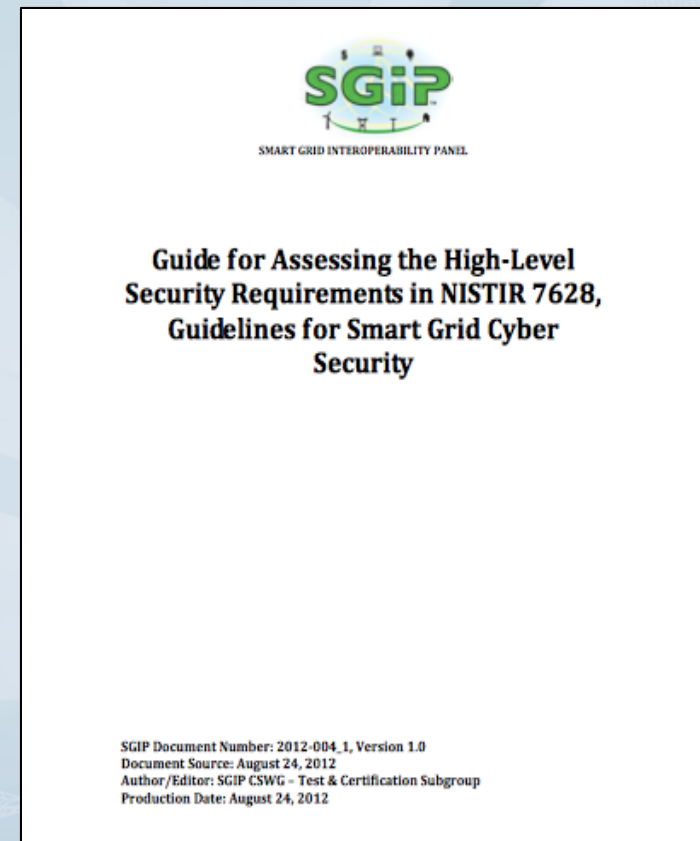
NIST Interagency Report 7628

- Published in August 2010, NISTIR 7628 Rev. 1 to released in Fall 2014
- NISTIR 7628 includes three volumes:
  - Volume 1: Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
  - Volume 2: Privacy and the Smart Grid
  - Volume 3: Supportive Analyses and References
- NISTIR 7628 provides:
  - An overview of the cybersecurity strategy used to develop the high-level cybersecurity requirements applicable to Smart Grid;
  - A tool for organizations that are researching, designing, developing, implementing, and integrating Smart Grid technologies—established and emerging;
  - An evaluative framework for assessing risks to Smart Grid components and systems; and
  - A guide to assist organizations as they craft a Smart Grid cybersecurity strategy that includes requirements to mitigate risks and privacy issues pertaining to Smart Grid customers and uses of their data.

NISTIR 7628

Guidelines for
Smart Grid Cyber Security:
Vol. 1, Smart Grid Cyber
Security Strategy, Architecture,
and High-Level Requirements

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director
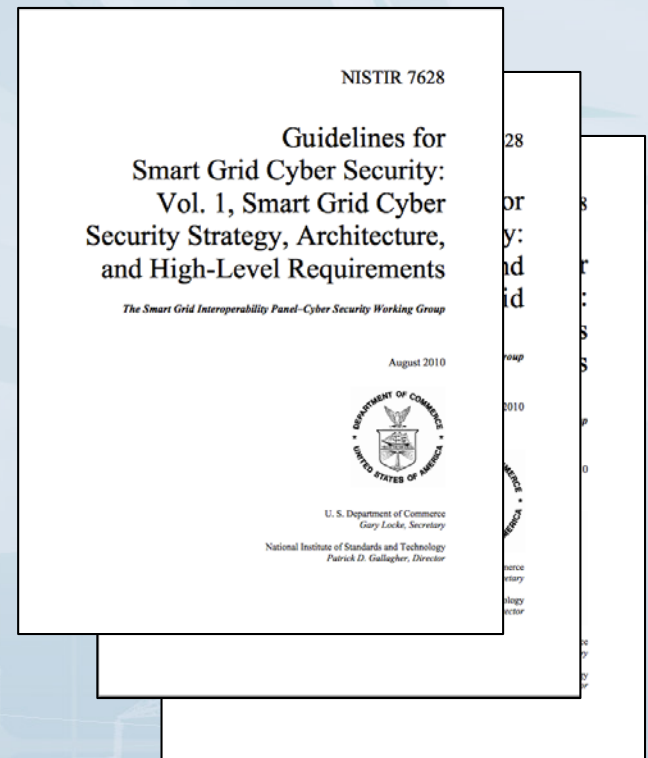
Guide for Assessing the High-Level Security Requirements in NISTIR 7628

- Guide for building effective security assessment plans

- Baseline set of procedures for assessing the effectiveness of security requirements in NISTIR 7628

- Provide a foundation to a security assessment based on NISTIR 7628

- Published in August 2012 under SGIP 1.0

  Available at: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/NISTIR_7628_Assessment_Guide-v1p0-24Aug2012.pdf

Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security

SGIP Document Number: 2012-004_1, Version 1.0
Document Source: August 24, 2012
Author/Editor: SGIP CSWG – Test & Certification Subgroup
Production Date: August 24, 2012

NISTIR 7628 User's Guide

- Recently published by the SGIP and available at www.sgip.org
- Provides an end-to-end implementation guide for Smart Grid Cybersecurity activities, including:
  - risk management process activities
  - identifying and selecting the appropriate high-level security requirements
  - references guidance to perform a gap assessment
  - create a plan to remediate identified gaps, and
  - develop a monitoring and maintenance plan

SMART GRID INTEROPERABILITY PANEL

NISTIR 7628 User's Guide

A white paper developed by the Smart Grid Interoperability Panel –
October 2013

Document Source: SGIP SGCC NISTIR 7628 User's Guide Subgroup
Author/Editor: Mark Ellison *et al*.
Production Date: October 25, 2013

Future Activities in the NIST Smart Grid Cybersecurity

- Continued technical leadership of the SGIP Cybersecurity Committee

- Design and develop a smart grid cybersecurity testlab as part of the NIST smart grid testbed facility; conduct cybersecurity research in relation to IEEE 1588, Precision Time Protocol

- Participate in the National Cybersecurity Center of Excellence Electricity Sector Use Case

Chapter 7: Framework for Smart Grid Interoperability Testing and Certification

Dean Prochaska   dean.prochaska@nist.gov

National Coordinator for Smart Grid Conformance

Smart Grid and Cyber-Physical Systems Program Office

Engineering Laboratory

National Institute of Standards and Technology

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

What's New

- Framework 3.0 includes an expanded section on testing and certification with the addition of significant new material

- IPRM Version 2 is the center piece of new material
  - Interoperability Process Reference Manual (IPRM) provides recommendations and best practices for test programs supporting Smart Grid standards

- Version 2 builds on the original IPRM transitioning from an informational to operational document

Operationalizing IPRM Version 2

- IPRM Version 2:
  - Describes the roles and responsibilities of an Interoperability Testing & Certification Authority (ITCA)
  - Describes processes for an ITCA to implement IPRM recommendations
  - Streamlines recommendations and requirements sections to aid in implementation
  - Expands content on cybersecurity testing considerations

Key Recommendations in IPRM V2

- All certification bodies and test labs operating programs associated with Smart Grid standards shall be accredited in accordance with globally recognized ISO standards
    - Certification Bodies – ISO/IEC Guide 65 accreditation
    - Test Laboratories – ISO/IEC Guide 17025 accreditation
- Nearly 40 additional technical requirements/best practices for the ITCA are specified to assure technical depth and sufficiency for end user needs addressing:
    - Explicit and transparent information on program requirements, processes, metrics, specific test environments
    - Detailed report documentation - procedures, profiles, results, product versions, caveats/limitations
    - Validated and traceable test tools and software
    - Qualitative evidence of interoperability – lack of reported problems or anecdotal information is insufficient

Development Guide

- A SGIP IPRM guidance document has been developed to support emerging ITCAs. It is intended to organize the IPRM's explicit and implicit requirements and suggested best practices for an ITCA into a roadmap to follow in launching its program.

Cross-Cutting and Future Issues

Chris Greer **chris.greer@nist.gov**

Director, Smart Grid and Cyber-Physical Systems Program Office

Engineering Laboratory

National Institute of Standards and Technology

Cross-cutting and Future Issues

- Electromagnetic disturbances and interference
  - SGIP Electromagnetic Interoperability Working Group
- Definitions of Reliability and Resilience of the Grid
- Implementability, Safety, Reliability, Resilience, and Impact of Framework Standards
  - SGIP Implementation Methods Committee (IMC) and implementation reviews
- Smart Grid research and development (R&D)

NIST Smart Grid Framework and Roadmap

- Models/tools for operations & planning

- Standards/protocols – performance, comms, data

- Control/mgmt architectures in distributed networks

- Evaluation methods for EE, DR, and DLC

- Communication/interconnection methods/technologies

- Models/topologies for security & resilience

- Cost-benefit & life cycle models

Foundations for Innovation

Strategic R&D Opportunities for the Smart Grid

Advancing measurement science and standards for smart grid technologies

March 2013

Report of the Steering Committee for Innovation in Smart Grid Measurement Science and Standards

Summary

Questions

Slides and audio recording will be posted soon on the NIST Smart Grid web site www.nist.gov/smartgrid.

For additional questions, please contact us at smartgrid@nist.gov.

For formal comments on the NIST Smart Grid Framework and Roadmap, please contact us at nistsgfwcmts@nist.gov.

NIST Smart Grid Framework and Roadmap

http://www.nist.gov/smartgrid/framework3.cfm