

NIST Special Publication 1108r4

**NIST Framework and Roadmap
for Smart Grid Interoperability
Standards, Release 4.0**

Avi Gopstein
Cuong Nguyen
Cheyney O'Fallon
Nelson Hastings
David Wollman

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.1108r4>

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

NIST Special Publication 1108r4

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0

Avi Gopstein, Cuong Nguyen, Cheyney O’Fallon, and David Wollman
*Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory*

Nelson Hasting
*Applied Security Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.1108r4>

February 2021



U.S. Department of Commerce
Wynn Coggins, Acting Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1108r4
Natl. Inst. Stand. Technol. Spec. Publ. 1108r4, 239 pages (February 2021)
CODEN: NSPUE2

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.1108r4>

Key Messages – NIST Smart Grid Interoperability Framework

Interoperability — the ability to exchange information in a timely, actionable manner — is a critical yet underdeveloped capability of the power system. Significant grid modernization has occurred in recent years, but the proliferation of technology and associated standards has only modestly improved interoperability.

The expansion of distributed energy resources and other technologies, along with changing customer expectations, have complicated the interoperability challenge. This revision of the NIST Smart Grid Interoperability Framework uses evolving technology and power system architectures as context for describing a new set of interoperability perspectives.

Distributed and customer-sited resources figure prominently in the future smart grid, as do intelligent distribution systems and other key integrators. As society modernizes the physical mechanisms by which we produce, manage, and consume electricity, strategies for system operations and economic structure will diversify. This diversification will benefit from — and eventually rely upon — enhanced interoperability.

The benefits of interoperability are broad and reach all stakeholders at all scales. Interoperability is a hedge against technology obsolescence, maximizes the value of equipment investments by increasing usage for secondary purposes, and facilitates combinatorial innovation by allowing coordinated small actions across diverse stakeholders and devices to have grand impacts. The interoperability value proposition can be realized in any system domain, from the utility to the customer and beyond.

Interoperability requires a cybersecurity approach that manages risk while opening new communication interfaces. The desired outcomes for the grid and the information exchanges that must be protected will have to be considered in concert and will benefit from a structured approach to system security. New interfaces can benefit from existing security processes.

Testing and certification is a critical enabler of smart grid interoperability. However, the current industry focus on certifying conformance to individual standards is only the first step on the pathway to assuring interoperability for devices or systems, and cannot provide interoperability without significant additional effort.

Interoperability Profiles are a proposed solution to the interoperability challenge. Built upon concepts of physical and informational interoperability and drawn from existing standards, these Profiles describe a subset of requirements that — when implemented and verified through testing and certification — would ensure interoperability across devices and systems.

Acknowledgements

This Framework is the result of an ongoing collaborative effort involving many individuals and organizations across industry, academia, and government. Through six public workshops and additional presentations, more than 300 attendees and speakers provided invaluable feedback which helped ensure that this document reflects a broad set of stakeholder perspectives regarding the issues surrounding smart grid interoperability.

The authors would like to thank Christopher Greer for his invaluable guidance, support, and extensive reviews throughout the Framework development process. This document is far better for his contributions.

Many others have provided important ideas and facilitated processes that are the foundations for this Framework. The contributions of the following individuals were especially noteworthy and appreciated: Jason Allnutt, Dhananjay Anand, Paul Boynton, Danielle Byrnett, Christopher Irwin, Konstantina Di Menza, Amimul Ehsan, Thomas Linn, Jeffrey Marron, Eric Simmon, Aaron Smallwood, Ravi Subramaniam, Jeffrey Taft, Christopher Villarreal, and Kerry Worthington.

Several organizations were instrumental in providing or otherwise managing the stakeholder engagement activities critical to obtaining early-stage feedback. Members of the NIST Smart Grid Advisory Committee reviewed and provided valuable feedback on many early-stage drafts and spoke at NIST workshops. Meetings hosted by the National Association of Regulatory Utility Commissioners, the Public Utility Commissions of Atlanta, California, Indiana, and Rhode Island, and the Smart Electric Power Alliance provided in-person opportunities to maximize stakeholder engagement.

Table of Contents

Key Messages.....	i
Acknowledgements.....	ii
List of Figures.....	vii
List of Tables	viii
List of Acronyms	ix
 1. Purpose and Scope	 1
1.1. Overview and Background.....	1
1.2. The Role of Interoperability.....	3
1.2.1. The interoperability value proposition	3
1.2.2. The empowered consumer	5
1.2.3. Interoperability and customer value.....	6
1.2.4. Utility and Other Benefits	7
1.2.5. Interoperability and environmental sustainability.....	8
1.3. Framework Content and Structure	10
1.3.1. The role of grid architecture.....	10
1.3.2. Updated models.....	11
1.3.3. A common language for the grid.....	11
1.3.4. Tools to facilitate interoperability	11
1.4. Use of this Framework	11
 2. Models for the Smart Grid	 12
2.1. NIST Smart Grid Conceptual Model	12
2.1.1. Conceptual model updates	14
2.1.2. Conceptual model domains	15
2.1.3. Other services and financial markets	17
2.2. Communication Pathways Scenarios.....	17
2.2.1. Graphic conventions.....	18
2.2.2. The legacy communication pathways scenario	19
2.2.3. High-DER communication pathways scenario	20
2.2.4. Hybrid communication pathways scenario	23
2.2.5. Microgrid communication pathways scenario	24
2.3. An Ontology for the Smart Grid.....	25
2.3.1. The NIST framework for cyber-physical systems	26
2.3.2. The aspects of a modern electrical grid.....	27
2.3.3. Aspects and concerns of the electrical grid.....	29
 3 Operations.....	 30
3.1 Interoperability for Utilities	32
3.1.1 System composition and constructivity.....	32
3.1.2 Hedging against obsolescence.....	33
3.2 Interoperability for New Technology	34
3.2.1 Changing physics at the edge of the system.....	34

3.2.2	Changing supply and demand technology	36
3.2.3	Alternating and direct current interactions.....	37
3.2.4	Electric vehicles and a changing infrastructure.....	38
3.3	Evolving Control Schemes.....	38
3.3.1	Utility-driven control schemes.....	39
3.3.2	Emerging customer-driven control schemes	40
3.3.3	System devolution.....	42
3.4	Emerging Interoperability Requirements.....	42
3.4.1	Requirements for metrology, observability, and controllability	43
3.4.2	Trustworthiness.....	47
3.5	Interoperability for Customer Empowerment	48
3.6	Future Work	49
4	Economics	50
4.1	Economics of the Conventional Utility	51
4.1.1	Functions of electric utilities	51
4.1.2	Cost structures.....	52
4.1.3	Ratemaking	52
4.2	Evolution of the Distribution Utility.....	53
4.2.1	Changes to utility organizational structure.....	53
4.2.2	Performance-based regulation.....	54
4.2.3	Economics of changing operations	55
4.3	Factors Affecting — and Benefits From — Interoperability	56
4.3.1	Interoperability and specificity.....	57
4.3.2	Interoperability and customer empowerment.....	57
4.3.3	Complexity and cost structures	58
4.3.4	Trust and assurance	60
4.3.5	Testing and certification.....	61
4.4	Economics and Challenges of Certification Institutions.....	61
4.4.1	Challenge: consumer demand	62
4.4.2	Challenge: interdependence and accountability	63
4.4.3	Challenge: concentration of market power	63
4.4.4	Challenge: consumer vigilance	63
4.5	Interoperability Benefits.....	63
4.5.1	Minimizing transaction costs	63
4.5.2	Creating value	64
4.6	Conclusion and Future Work.....	66
5	Cybersecurity.....	67
5.1	Securing Organizations.....	69
5.1.1	NIST cybersecurity framework core functions	69
5.1.2	NIST cybersecurity framework core categories and subcategories	71
5.1.3	Cybersecurity profiles	72
5.1.4	Cybersecurity framework profile for the smart grid	74

5.2	Securing Information Exchange	77
5.2.1	Known system interfaces and categories.....	77
5.2.2	New system interfaces.....	78
5.2.3	Assessing security requirements of new interfaces.....	80
5.3	Additional Cybersecurity Resources	82
5.4	Conclusions and Future Work	83
6	Testing and Certification	85
6.1	The Role of Testing and Certification	86
6.1.1	Testing and certification value	86
6.1.2	Current practice	87
6.2	Levels of Interoperability	87
6.3	Types of Testing Processes.....	89
6.3.1	Conformance and interoperability testing	90
6.3.2	Interoperability tests	90
6.3.3	Certification regimes	91
6.4	Current Smart Grid Testing Initiatives	92
6.4.1	Testing support.....	92
6.4.2	Catalog of standards	92
6.4.3	Catalog of test programs	93
6.4.4	Reference interoperability procurement language	94
6.5	Towards Interoperability Profiles	95
6.5.1	Interoperability profiles.....	95
6.5.2	Example of an interoperability profile	96
6.5.3	Interoperability profiles work plan.....	98
6.5.4	Open source test tool development	99
6.6	Conclusions and Future Work	100
7.	Conclusion.....	101
Appendix A – Smart Grid Conceptual Model Domains	104	
A.1 - Customer Domain	104	
A.2 - Markets Domain.....	107	
A.3 - Service Provider Domain.....	110	
A.4 - Operations Domain	113	
A.5 - Generation Including DER Domain.....	116	
A.6 - Transmission Domain	119	
A.7 - Distribution Domain	121	
Appendix B – Mapping CPS Aspects and Concerns to the Electrical Grid.....	123	
Appendix C – Inverter and DER Functions	153	
Appendix D – The Core Set of Electric Industry Roles.....	158	
Appendix E – Cost Recovery, Rate Design, and Regulation.....	160	

Appendix F – Distribution Platforms and Markets.....	163
Appendix G – Smart Grid Cybersecurity Profile Subcategory Prioritization and Considerations Matrices.....	165
G.1 – Identify Function.....	165
G.2 – Protect Function.....	172
G.3 – Detect Function.....	180
G.4 – Respond Function.....	183
G.5 – Recover Function	186
Appendix H – Logical Interface Categories from NISTIR 7628.....	187
Appendix I – Types of Information Exchange Between Entities in the High-DER Example.....	190
Appendix J – List of Reviewed Smart Grid Interoperability Standards	202
References	209

List of Figures

Figure 1 – Installed photovoltaic price trends over time	2
Figure 2 – Interoperability across scales.....	5
Figure 3 – Customer and consumer benefits from the smart grid.....	7
Figure 4 – Updated NIST smart grid conceptual model	13
Figure 5 – Legacy communication pathways scenario	20
Figure 6 – High-DER communication pathways scenario	22
Figure 7 – Hybrid communication pathways scenario	24
Figure 8 – Microgrid communication pathways scenario.....	25
Figure 9 – CPS framework domains, facets, and aspects	27
Figure 10 – Example electrical waveform distortions observed in NIST experiments	36
Figure 11 – Representation of utility direct load control programs.....	41
Figure 12 – Representation of utility voluntary load curtailment programs.....	41
Figure 13 – Smart meter accuracy under high harmonic waveform loads	44
Figure 14 – Example smart meter measurement accuracies for highly distorted waveforms	45
Figure 15 – Wide area precision time requirements in power systems	46
Figure 16 – State-level absolute and per-customer electricity consumption trends	54
Figure 17 – Data standardization stimulates innovation.....	59
Figure 18 – Sustained outages by AMI penetration and wind speed.....	65
Figure 19 – Cybersecurity Framework core functions	70
Figure 20 – Applying the cybersecurity core to develop risk profiles.....	73
Figure 21 – Example of cybersecurity Considerations for the electrical system.....	75
Figure 22 – Smart Grid Profile excerpt.....	76
Figure 23 – Logical Interface Reference Model "Spaghetti Diagram" from NISTIR 7628 ...	78
Figure 24 – Example logical interfaces in a High-DER architecture	80
Figure 25 – Logical interface categories (LICs) for the High-DER example.....	81
Figure 26 – Mapping cybersecurity framework subcategories to NERC CIP requirements..	83
Figure 27 – Levels of interoperability conceptual diagram	88
Figure 28 – Testing and certification development process	89
Figure 29 – Interoperability standards and associated testing and certification	94
Figure 30 – Potential implementation combinations for IEEE 1547-2018.....	96
Figure 31 – California Rule 21 interoperability profile implementation.....	97
Figure 32 – Interoperability Profiles clarify implementation requirements	98
Figure 33 – Overview of the Customer domain.....	104
Figure 34 – Overview of the Markets domain	107
Figure 35 – Overview of the Service Provider domain	110
Figure 36 – Overview of the Operations Domain.....	113
Figure 37 – Overview of the Generation Including DER Domain	116
Figure 38 – Overview of the Transmission domain.....	119
Figure 39 – Overview of the Distribution domain.....	121

List of Tables

Table 1 – Domains and roles/services in the smart grid conceptual model.....	16
Table 2 – Domain descriptions and graphical color representation.....	18
Table 3 – Communication pathways diagrams symbol descriptions.....	18
Table 4 – Cybersecurity Framework functions and categories.....	71
Table 5 – Cybersecurity Framework subcategory examples	72
Table 6 – Certification regime characteristics (illustrative)	92
Table 7 – Typical application categories in the Customer domain.....	106
Table 8 – Typical applications in the Markets domain.....	109
Table 9 – Typical applications in the Service Provider domain	112
Table 10 – Typical applications in the Operations domain	114
Table 11 – Typical applications in the Generation Including DER domain.....	118
Table 12 – Typical applications in the Transmission domain	120
Table 13 – Typical applications within the Distribution domain	122
Table 14 – Mapping CPS Aspects and Concerns to the electrical grid	123
Table 15 – Inverter and DER functions: mandatory, autonomous, and market-based	153
Table 16 – Identify function subcategory prioritization and considerations	165
Table 17 – Protect function subcategory prioritization and considerations.....	172
Table 18 – Detect function subcategory prioritization and considerations.....	180
Table 19 – Respond function subcategory prioritization and considerations	183
Table 20 – Recover function subcategory prioritization and considerations.....	186
Table 21 – Logical Interface Categories from NISTIR 7628	187
Table 22 – Information exchanges in Figure 24 High-DER example	190
Table 23 – List of standards reviewed for testing and certification availability.....	202

List of Acronyms

AC	Alternating Current
ADMS	Advanced Distribution Management System
AGC	Automatic Generation Control
AMD	Amendment
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
B2B	Business-to-business
BACNet	Building Automation and Control Networks
BAS	Building Automation System
BES	Bulk Energy System
BTM	Behind the Meter
C&I	Commercial and Industrial
CapEx	Capital Expenditures
CBM	Condition-Based Maintenance
CCA	Community Choice Aggregation
CEA	Consumer Electronics Association
CFL	Compact Fluorescent Lamp
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CIS	Customer Information System
CIS CSC	Center for Internet Security Critical Security Controls
CME	Chicago Mercantile Exchange
COBIT	Control Objectives for Information Technologies
ComEd	Commonwealth Edison
COS	Catalog of Standards
CoTP	Catalog of Test Programs
COTS	Commercial Off-the-Shelf
CPS	Cyber-Physical Systems
CPUC	California Public Utilities Commission
CSR	Customer Service Representative
CTA	Consumer Technology Association
CVR	Conservation Voltage Reduction
DC	Direct Current
DCS	Distributed Control System
DDC	Distributed Data Collector
DER	Distributed Energy Resources
DERMS	Distributed Energy Resource Management System
DG	Distributed Generation

DLC	Direct Load Control
DMS	Distribution Management System
DNP	Distributed Network Protocol
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DRMS	Demand Response Management System
DSO	Distribution System Operators
ECp	Electrical Connection Point
EMI	Electromagnetic Interference
EMIX	Energy Market Information Exchange
EMS	Energy Management System
EPRI	Electric Power Research Institute
EPS	Electric Power System
ERCOT	Electric Reliability Council of Texas
ESI	Energy Services Interface
ESP	Energy Service Provider
EUMD	Energy Usage Metering Device
EV	Electric Vehicles
EVSE	Electric Vehicle Supply Equipment
FDEMS	Facilities DER Energy Management System
FERC	Federal Energy Regulatory Commission
FLISR	Fault Location, Isolation, and Service Restoration
FSGIM	Facility Smart Grid Information Model
GHG	Greenhouse Gas
GIS	Geographic Information System
GMLC	Grid Modernization Laboratory Consortium
GNSS	Global Navigation Satellite System
GOOSE	Generic Object Oriented Substation Events
GPS	Global Positioning System
GWAC	GridWise Architecture Council
HAN	Home Area Network
HVAC	Heating, Ventilation, and Air Conditioning
ICAP	IEEE Conformity Assessment Program
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IEC	International Electrochemical Commission
IED	Intelligent Electronic Devices
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IoT	Internet of Things
IOU	Investor Owned Utility
IP	Internet Protocol
IPRM	Interoperability Process Reference Manual
IRM	Interface Reference Model
ISA	International Society of Automation
ISO	Independent System Operators
ISO	International Organization for Standardization
IT	Information Technology
ITCA	Independent Testing and Certification Authority
ITU	International Telecommunication Union
kWh	kilowatt-hour
LAN	Local Area Network
LED	Light Emitting Diode
LIC	Logical Interface Categories
LMS	Load Management System
MDMS	Meter Data Management System
MIB	Management Information Base
MISO	Midcontinent Independent System Operator
MQTT	Message Queuing Telemetry Transport
MWh	Megawatt-hour
NAESB	North American Energy Standards Board
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NYMEX	New York Mercantile Exchange
O&M	Operating and Maintenance
OASIS	Organization for the Advancement of Structured Information Standards
OCPP	Open Charge Point Protocol
OGC-GML	Open Geospatial Consortium – Geography Markup Language
OMM	Operation, Maintenance and Monitoring
OMS	Outage Management System
OPC-UA	Open Platform Communications Unified Architecture
OpenADR	Open Automated Demand Response
OSI	Open Systems Interconnection
OT	Operational Technology
PCC	Point of Common Coupling

PEV	Plug-in Electric Vehicles
PF	Power Factor
PICS	Protocol Implementation Conformance Statement
PII	Personally Identifiable Information
PIM	Performance Incentives Mechanisms
PJM	PJM regional transmission organization
PMU	Phasor Measurement Units
PUC	Public Utilities Commission
PV	Photovoltaics
PWG	Public Working Group
RBAC	Role-based Access Control
REP	Retail Energy Provider
ROCOF	Rate of Change of Frequency
ROE	Return on Equity
ROI	Return on Investment
RTO	Regional Transmission Organizations
RTU	Remote Terminal Unit
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SCED	Security Constrained Economic Dispatch
SEP	Smart Energy Profile
SEPA	Smart Electric Power Alliance
SIPS	System Integrity Protection Schemes
SNMP	Simple Network Management Protocol
SOC	State of Charge
SOS	Systems of Systems
SPI	Sensitive Personal Information
T&C	Testing and Certification
TBLM	Transmission Bus Load Model
TI	Time Intervals
TOU	Time of Use
TSS	Test Suite Specification
UCAIug	Utility Communications Architecture International Users Group
VAR	Volt-ampere reactive
Volt-Var	Voltage-reactive power mode for inverter/DER control
VPN	Virtual private network
VVO	Volt/VAR Optimization
WAMS	Wide Area Management System
WAN	Wide Area Network
WAPOD	Wide Area Power Oscillation Damping

WASA	Wide-area Situational Awareness
Watt-PF	Active power-power factor mode for inverter/DER control
Watt-Var	Active power-reactive power mode for inverter/DER control
WMS	Work Management System
XMPP	Extensible Messaging and Presence Protocol

1. Purpose and Scope

It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system ...The National Institute of Standards and Technology shall have the primary responsibility to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems.

Energy Independence and Security Act of 2007 [1]

The United States power system encompasses more than 7,000 power plants [2] feeding a distribution system with 6,000,000 miles of wire serving 150,000,000 customers [3]. This immense system, integrated into every aspect of modern life, has provided inexpensive, reliable power for decades. It is also in the midst of a dramatic transformation that changes everything from how energy is produced¹ to how it is consumed [5].

The electrical grid is the tightly coupled system that manages and delivers power from where and how it is generated to where — and how — it is consumed. The Nation needs an electrical grid that is adaptable, secure, reliable, resilient, and can accommodate changing loads, generation technologies, and operating business models. Grid modernization will bring new capabilities and economic opportunity to utilities and customers through improved access to data, cyber security protections, and power flow control, but will also require new physical and informational capabilities to observe and manage the system and its emerging and increasingly complex dynamics [6]. Interoperability is the crucial enabler of these needed capabilities.

1.1. Overview and Background

Technological advances are transforming the electric grid. Over the last decade, the United States has experienced large increases in the deployment and use of nontraditional energy resources [7]. As the installed costs for technologies like solar photovoltaics (PV) continue their dramatic decline (see **Figure 1**), deployments are expected to rise significantly [8]. But generation is only one part of the system, and the largest category of distributed energy technologies in use today — demand response — is focused on optimizing electricity consumption rather than production [9]. And as the capabilities of modern power electronics expand, new sources of essential reliability services are emerging [10]. The power grid will become more resilient as these capabilities are deployed across a broadening range of applications and scales [11].

¹ In the year 2000 the United States produced more than 200 times as much electricity from oil than from solar energy. Over the next 15 years solar power generation grew by almost 30% annually while oil-based generation fell by nearly 9% per year; by 2015 the amount of electricity generated from both resources were similar. In the years since solar generation grew at nearly 40% per year while oil generation continued to decline, so that in 2018 nearly 3 kWh of solar power were generated for each kWh of oil-fueled electricity [4].

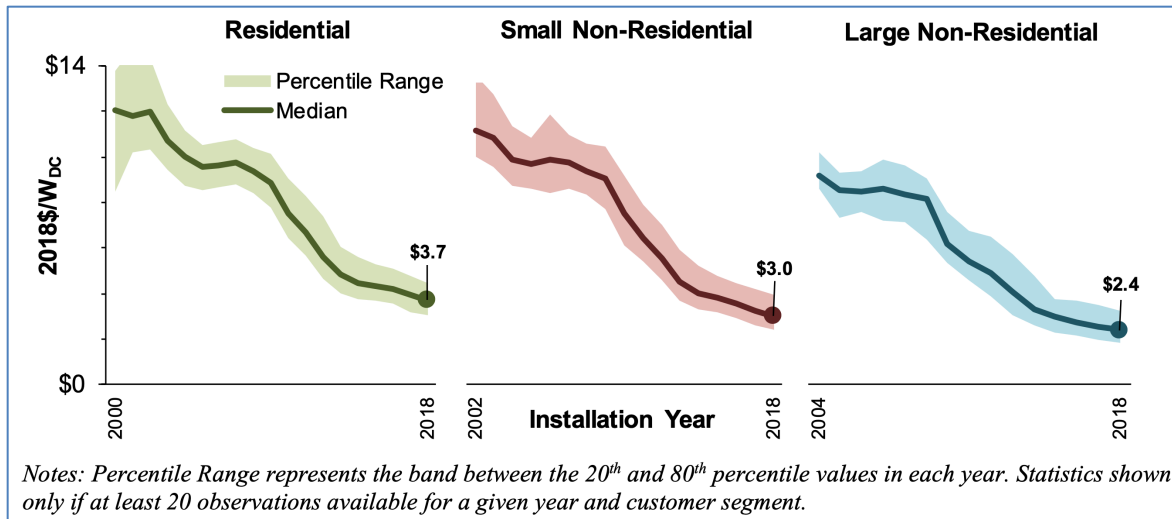


Figure 1 – Installed photovoltaic price trends over time [12]

Through a virtuous cycle of improving technology, increasing deployments, and declining costs, contract prices for utility-scale solar power have declined more than 80% since 2010 [13], with low prices for wind and solar energy found in every region of the U.S. electric grid [13, 14]. Global renewable energy auction volumes broke records in 2020 despite some delays due to Covid-19, and annual deployments are forecast to continue growing through 2025 [15]. Beyond inexpensive electricity supply, improving energy efficiency and demand management technologies are saving utilities and customers millions of dollars through coordinated action of customer-sited and distributed energy efficiency resources [16, 17]. These economic conditions induce power system stakeholders to incorporate new technologies and modernize.

The modular and scalable nature of modern energy technologies [18] also allows for distributed implementations of grid capabilities which have historically been provided through large and centralized utility infrastructures. These changes, combined with - regulatory changes that have altered the historic guarantee for a utility's return on capital investment, have over time reduced the unit size of newly deployed generation [6] and allowed generation and demand management capabilities to expand toward the grid edge [19]. This evolving set of resources and capabilities are conventionally referred to as Distributed Energy Resources (DERs).

Because electricity is perishable, most power is delivered at the time it is generated.² The supply, transmission, distribution, and consumption of electricity in the system are therefore closely coupled, and must be actively coordinated [21]. This requires the coordinated sensing, measurement, and control of devices and systems spread across the grid. Fortunately, the cost of sensors has declined even more rapidly than the cost of energy technologies, and the growth of sensing and network enabled energy devices and systems is unleashing dramatic opportunities to improve our ability to understand and operate the power grid [22]. Interoperability is the key to unlocking this potential.

² Energy storage provides temporal flexibility and has an increasing role in the system. However, the scale of energy storage deployments of all kinds remains small compared to the grid's net generating capacity [20].

1.2. The Role of Interoperability

These [interoperability] protocols and standards shall further align policy, business, and technology approaches in a manner that would enable all electric resources, including demand-side resources, to contribute to an efficient, reliable electricity network.

Energy Independence and Security Act of 2007

In our work, we define interoperability as the capability of two or more networks, systems, devices, applications, or components to work together, and to exchange and readily use information — securely, effectively, and with little or no inconvenience to the user.³ The smart grid will be a system of interoperable systems; that is, different systems will be able to exchange meaningful, actionable information in support of the safe, secure, efficient, and reliable operations of the grid [24]. As the number of devices and systems used on the electrical grid continue to multiply [25], the interoperability requirements become more complex and the path to achieving interoperability becomes more challenging.

1.2.1. The interoperability value proposition

Modern energy systems rely on an increasing array of sophisticated controls and information exchanges which are managed across diverse operational and economic systems [26]. Interoperability is therefore key to maximizing the benefits of technology investments. Yet because it is not easy to directly quantify the value of seamlessly exchanging a single bit of information in a complex system like the electrical grid, the value of interoperability is most often thought of in the context of what is avoided: the expensive and time consuming set of activities necessary for one-off integrations of incompatible systems [27]. Indeed, anecdotes abound regarding the expense and functional limitations associated with integrating equipment designed to conform to the same interoperability standard [28]. For equipment designed to dissimilar standards, the challenges of achieving the intended functionality can become difficult to overcome.

Beyond minimizing system integration costs, grid interoperability also creates new value throughout the smart grid. As tens of billions of dollars are spent annually on communications-capable electrical devices and software, the transition from isolated and siloed capabilities to interconnected systems will engender tremendous economic and operational opportunities across society [22]. Empowering consumers to better manage their energy consumption is but one of the growing set of capabilities that interoperability enables, which together will impact every aspect of how electricity is produced and managed and provide fundamentally new and different value propositions.

Beginning with individual sensors and devices found in the home, **Figure 2** depicts how the impacts of interoperability can change with the scale of interaction. Each level of the

³ While the IEEE definition of interoperability [23] provides that interoperability is the “ability of two or more systems or components to exchange information and use the information that has been exchanged,” we extend that in our work to ensure that use is secure, effective, and poses little or no inconvenience to the user.

diagram represents a new set of interactions and information exchanges which can lead to new value opportunities. These include:

Local: Interoperability between individual sensors, energy consuming devices, and system controllers can allow residential, industrial, and commercial customers to better monitor their energy demand (or production), and manage consumption according to their specific needs.

Proximal: Interoperability at the community level would create opportunity by allowing customers to interact with and potentially provide services to their neighbors, aggregators, or distribution utility. Specific community and local reliability needs could be met by better local management of power flow and quality issues in the system.

Regional: Interoperability at the regional level would improve situational and state awareness for utilities, system operators, and regulators, allowing for more efficient operation and improved long-term planning. Physical interactions between the electrical system and the local environment (e.g., managing surface water [29]) could be better managed, as well.

Global: At the societal scale, interoperability will enable expanded access to modern energy services, economic development, and environmental stewardship [30].

While interoperability — or lack thereof — is often considered an issue that must be addressed for utilities to maximize return on investment for specific system assets [31],

Figure 2 describes a different general concept: that interoperability *creates* value by overcoming the designed specificity of energy devices connected to the grid. Breaking this asset specificity would allow systems purchased to perform one set of tasks the ability to contribute to an entirely different set of applications by sharing information with a new set of actors. Value accrues as it flows from local to global levels; for example, as smart load and DER management at the house contribute to proximal voltage stability and regional balance of load to renewable energy sources.

Interoperability is therefore a tool to unlocking new value across the power system. The benefits can accrue at any scale, and for assets owned by any stakeholder. Some of the most intriguing implications relate to the role of the energy consumer.

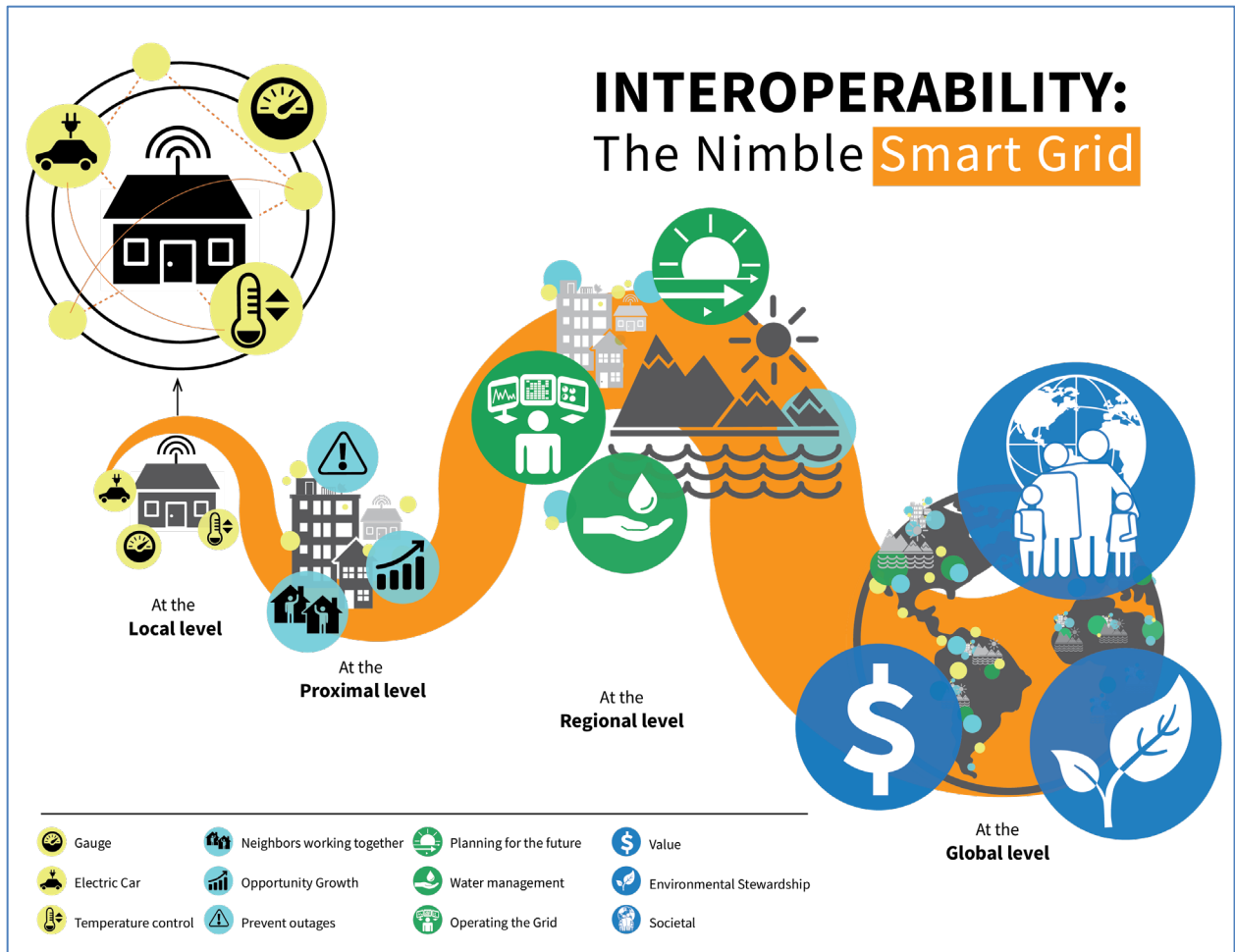


Figure 2 – Interoperability across scales

1.2.2. *The empowered consumer*

The power grid was for decades modeled as a simple set of interactions [32]. With simplicity born of a need for computationally tractable approaches to manage the system, these models codified the relationships between grid actors in similarly simple terms. In this paradigm generators produce electricity that is fed to and consumed by customers, and everything on the system is well characterized with behaviors that are both linear and consistent in their response.

Changing technologies have upended these assumptions. The new power grid is increasingly dynamic [33], few devices interact with the grid in the straightforward linear manner of old [34], and customers have long-since evolved into providers of resources that actively support grid health [35]. Indeed, expanding capabilities and falling costs for small-scale energy technologies have allowed customers and other actors to emerge as entirely new classes of asset owners.

The empowered energy consumer who can actively manage their interactions with the power grid is therefore one of the key elements of this Framework. Empowered by integration of new physical and informational capabilities, consumer devices can manage load, produce power, and otherwise support grid health⁴ in ways which defy the historical customer-utility relationship. As consumer and third-party assets gain capability to respond to economic opportunity beyond the traditional tariff structure, the relationships between asset owners and electric utilities will evolve.

The empowered consumer's expanding set of roles are depicted in **Figure 2**, where devices deployed in the home enable a diverse set of interactions and outcomes. Similar developments will also occur with commercial and industrial devices and systems.

1.2.3. Interoperability and customer value

An empowered energy consumer has many opportunities to obtain value and can optimize their interactions with the broader energy system to maximize their preferred benefit. Complementary to the concepts explored in **Section 1.2.1** where the value of interoperability flows outward from technologies in the home to the local community and beyond, interoperability also allows customers to identify and prioritize interactions optimized to yield a desired outcome.

Widespread interoperability will enable interested energy customers to tailor their activities towards preferred value classes, such as the financial, environmental, reputational, and other benefits illustrated in **Figure 3**. The variety of smart grid benefits ensures that stakeholders with diverse priorities can identify and pursue the subset of opportunities that most resonates with their objectives. Commercial and industrial customer priorities may differ from those of residential consumers, as illustrated by the revenue and reputational value classes in **Figure 3**. Customers could also focus their interactions on metrics related to a single benefit, such as selling power back to the grid or improving local air quality, thereby gaining more direct feedback and perceived value from each action.⁵

The value of opportunities brought to the customer through the smart grid is limited only by the extent of system interoperability and the pace of innovation. Further discussion on this issue is found in **Section 4**.

⁴ For example, by providing reactive power or voltage support along a distribution feeder.

⁵ While each customer action likely produces multiple benefits, the ability to track metrics for specific benefits is an important mechanism for promoting transparency and stimulating customer action.

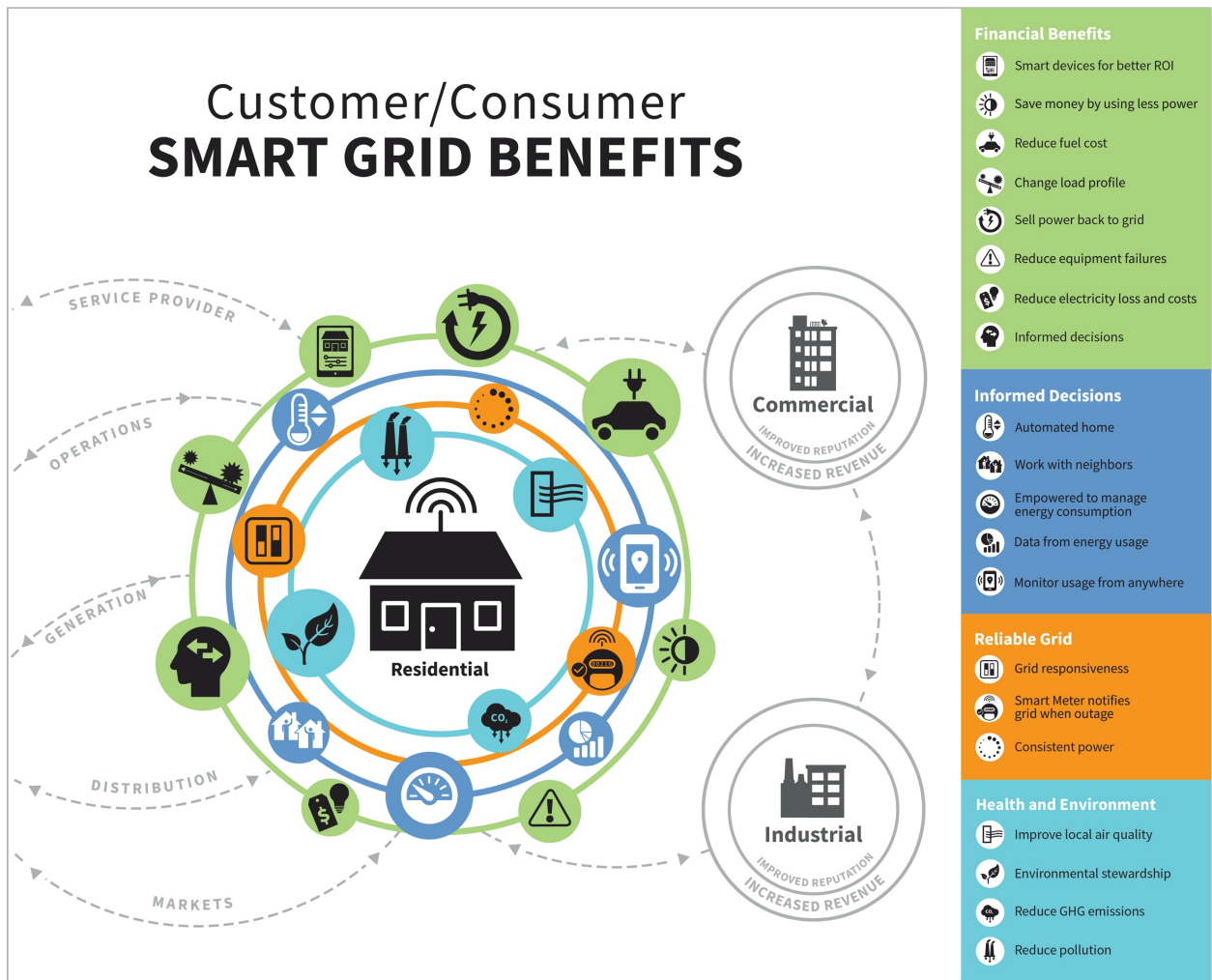


Figure 3 – Customer and consumer benefits from the smart grid

1.2.4. Utility and Other Benefits

Interoperability benefits are often reciprocal in nature and can accrue to multiple parties through diverse interactions. While **Figure 2** depicts a value stream emanating from customer-sited devices, utility investments in interoperable equipment would likely have similarly far-reaching impacts and provide value to a broad range of stakeholders.

Recent NIST work has shown that utility-based interoperability investments improve system resilience, an effect which is conservatively estimated to provide billions of dollars in economic benefit during natural disasters and potentially savings lives [36]. This resilience benefit is different from the operational efficiencies traditionally cited as justification for utility-based interoperability investments [37].

The scope of benefits are only just beginning to be understood for utility or third-party interoperability investments that enable platforms for innovative grid management, such as through transactive market signals or peer-to-peer services [38].

1.2.5. Interoperability and environmental sustainability

Energy and environmental concerns are inextricably linked [39]. The long-standing prioritization of resource development policies over environmental protection policies [40] is being rebalanced to enhance consideration of environmental and other impacts [41, 42]. Because greenhouse gas emissions from fossil fuel energy consumption is the primary driver of climate change and associated environmental impacts [43], policies to reduce greenhouse gas emissions in the energy sector are being proposed and implemented from local [44] to global [45] scales.

President Biden has committed the United States to rejoining the world's governments in pursuing the goals of the Paris Climate Agreement [46], an action supported by governors and leaders of nearly 200 U.S. states, counties, and cities who are similarly committed to advancing energy and climate policies that will continue progress towards the Paris Accord goals [47, 48].

Driven by the fact that electricity and heat production activities emit more greenhouse gases worldwide than any other economic sector [49], climate policies tend to prioritize new deployments of low-carbon power generation [50]. This is true in the United States as well, with 37 states and the District of Columbia having established renewable energy goals [51]. Expanding clean energy capacity is important, but the positive environmental impact of doing so is tempered by the fact that new energy resources have historically supplemented rather than displaced existing infrastructures and energy technologies [52].

A recent analysis by the International Energy Agency has determined that continued operation of the world's currently built power systems would ensure global temperature rise exceeds the targets of the Paris Accord unless there is significant change to how existing electric grids are managed [53]. Realizing the environmental sustainability objectives of nearly all the world's governments therefore requires that power systems break from century-old practices and instead operate with new strategies focused on integrating clean energy and distributed technologies into systems designed under different requirements.

Power systems require significant and continued investment [54], and must become substantially more flexible [55] to maximize the environmental benefits of renewable and clean energy investments. Coordination across the electrical system, from the generator to end-use devices, is necessary to accommodate the inherent variability of demand and some renewable resources [56, 57], and also the operational uncertainty that emerges as distributed technologies migrate control schemes towards the system periphery (see **Section 3.3.3**).

The functions of interoperability are primarily about information exchange and physical compatibility between elements of a broader system, capabilities that directly improve grid flexibility and are described throughout this Framework. Yet the benefits of flexibility do not accrue uniformly throughout the system, but instead are specified through the details of coordinated action. In that way, distributed assets could be managed to promote renewable energy absorption, or to lessen feeder congestion, or to improve interfaces with other infrastructures.

It is within this context that the environmental benefits of an interoperable smart grid are understood:

Better integration of utility-scale clean energy technologies: Renewable energy resources are relatively diffuse [58] and therefore inherently more distributed when compared to legacy energy technologies. Some renewable resources are more variable [59] than conventional resources, while nuclear is comparatively inflexible [60]. As the grid changes with these technologies, utilities that previously managed against relatively few large-scale contingencies must now operate within a growing set of complex uncertainties [61]. An interoperable smart grid facilitates the communication and information exchanges critical to improving system flexibility through dynamic operations. This flexibility is necessary to best integrate clean and distributed energy resources into power systems, and to maximize the potential for displacing high-polluting resources in grid operations [62].

Compounding environmental benefits of customer-sited resources: Physical losses in power generation, transmission, and distribution mean most of the energy used to produce electricity never reaches the customer [63-65]. The compounding effects of these losses, which are highest during periods of peak demand [66], mean a greater percentage of electricity produced from customer-sited resources will become useful work when compared to more remote installations [67, 68]. Interoperability is a key enabler of the highly distributed system architectures and grid services⁶ that can best utilize a broad array of customer-sited clean and efficient energy resources to reduce upstream greenhouse gas emissions.

Avoiding infrastructure upgrades: Electric grids are built to handle rarely achieved peak demand, reflecting a design philosophy that leaves system capacity significantly underutilized for most of the year but which — in combination with an aging system and changing loads — requires distribution system upgrades costing more than \$50 billion annually [69]. Referred to as non-wires alternatives, coordinated energy efficiency and DER deployments enabled by an interoperable smart grid can cost-effectively defer or supplant these capacity upgrades [5]. Already successfully deployed in New York [70], these strategies avoid the embodied emissions associated with fabrication and installation of new grid infrastructure [71]. Furthermore, the capital savings alone from deferring infrastructure upgrades is estimated at \$10 billion annually [72, 73], resources which could be redirected towards clean energy goals and support more extensive long-term emissions reductions.

Decarbonizing connected infrastructures: Increasing electrification of energy infrastructures in the transportation, industrial, and buildings sectors is required to achieve sustainability targets [55]. Doing so will require interdependencies and information exchanges between previously distinct systems and actors. An interoperable smart grid capable of integrating diverse resources and technologies would provide an enabling platform for these interactions.

⁶ For example, conservation voltage reduction

1.3. Framework Content and Structure

This Framework document reflects the results of the ongoing technical work of the National Institute of Standards and Technology (NIST) in the area of smart grid interoperability, and builds on prior Framework versions [24, 74, 75]. This revision examines the impacts changing grid technologies will have on four key areas, and the associated evolution of grid interoperability requirements. The four areas are:

- Grid Operations
- Cybersecurity
- Grid Economics
- Standards Testing & Certification

The impact of interoperability on the emerging trends in each of these four focus areas is explored, and roadmaps for research, standards, and other technical work to advance interoperability in the smart grid are described.

1.3.1. *The role of grid architecture*

Grid architecture is the highest level description of the complete grid, and is an important tool to understand and define the many complex interactions that exist in the electrical system [76]. The relationships between technology, regulatory policy, and economic opportunity that govern interactions throughout the grid also guide the evolution of grid architectures.

While early grids were similar in a broad enough range of characteristics that they could generally be described by a single architecture,⁷ today's environment is far more heterogeneous. Vertically integrated utilities with conventional tariff structures remain the standard for large portions of the country, whereas other regions have embraced diversified asset ownership,⁸ market-driven operations, and unconventional or non-wires alternatives to traditional electricity supply [78].

This Framework uses multiple grid architectures described by the U.S. Department of Energy (DOE) [79] as inspiration for use cases to explore the different types of interactions one could expect to see in the electrical grid. No single architecture is deemed the correct architecture, and the use cases employed herein are abstractions of the detailed DOE architecture descriptions intended to elucidate specific system characteristics.

⁷ For example, vertically integrated utilities with conventional generation (e.g., steam cycle, hydropower, or reciprocating engine), and unidirectional power flows from generator to radial distribution networks that fed customers with similar characteristics.

⁸ For example, through distribution system operators (DSOs) [77].

1.3.2. Updated models

The NIST Smart Grid Conceptual Model is used to build a high-level and scalable understanding of the different physical and informational interfaces across the smart grid. In this Framework the Conceptual Model is updated to reflect evolving interface trends across the grid. The logical model of legacy systems from the previous Framework has been updated to explore interface characteristics across multiple grid architectures.

1.3.3. A common language for the grid

Diversifying architectures complicates an already challenging space. As roles, responsibilities, and interfaces evolve across architectures, opportunities for miscommunication increase significantly — especially as companies engage in multiple locations and similar equipment is utilized in substantially different architectures.

Interoperability depends on a consistent understanding of the language used to describe capabilities and requirements for devices, systems, and actors. To facilitate this common understanding of the language of the grid, NIST has applied a cyber-physical systems ontology [80] to the smart grid.

1.3.4. Tools to facilitate interoperability

Achieving interoperability is a complex challenge towards which compliance to individual communications or data model standards will yield limited progress. To maximize the benefits new devices and systems can bring to the electrical grid, NIST has developed an approach to interoperability that depends on co-optimization of standards requirements related to the physical function, communications protocols, and information models.

Referred to as an interoperability profile, this approach to coordinated application of requirements which may span multiple standards is described.

1.4. Use of this Framework

The results of NIST’s ongoing technical work reflected in this Framework document should assist smart grid stakeholders in future decision making. The ideas expressed in this work are foundational to information exchange and interoperability concerns across the smart grid, have gone through a full vetting process, and are expected to stand the “test of time” as the building blocks for emerging power sector issues.

It is important to note that standards for electrical grid technologies are not static — as technology evolves, so too will the relevant standards. Standards undergo continuing revisions to add new functionalities, integrate with legacy standards, harmonize/align with overlapping standards, and remedy shortcomings that are discovered as their implementations undergo interoperability testing. Standards are also deprecated when no longer useful. The concepts and gaps described in this Framework provide a foundation to guide this process moving forward.

Key Messages – Models for the Smart Grid

Models aid our understanding of interoperability and other smart grid concerns, and facilitate common language and communication across stakeholders. Evolution in technology and grid architecture in recent years requires an update of these tools.

The NIST Smart Grid Conceptual Model reflects technology and platform-driven capabilities emerging in the Customer and Distribution Domains, as well as the structural reorganization of a system that is more reliant on distributed resources.

Communication Pathways Scenarios are presented to help stakeholders examine how interface requirements might change with different system architectures or control strategies. These scenarios are not mutually exclusive and allow users to visually examine interoperability considerations that might arise through decisions on technology, operations, or economic structure.

Communications challenges increase with grid complexity, which adds risk to everything from stakeholder engagement to equipment procurement. An ontology for the smart grid is introduced to provide reference language that can be used to clarify communications.

2. Models for the Smart Grid

Several models have been developed by NIST to describe interoperability concerns in the smart grid. In this version of the Framework, these models are updated and expanded to reflect emerging power system trends. An ontology for the smart grid is also described, which can be used to model functional and requirements descriptions for actors and equipment across the grid.

2.1. NIST Smart Grid Conceptual Model

The NIST Smart Grid Conceptual Model describes the overall composition of electric grid systems and applications. It is meant to provide a high-level view of the system that can be understood by many stakeholders. Originally introduced in 2010 [74], the Conceptual Model is updated with each Framework revision. The Smart Grid Conceptual Model update in this document (see **Figure 4**) reflects large increases in the number and types of distributed energy resources (DERs) used throughout the grid, the increasing importance and automation of distribution systems, new customer interactions and assets, and the role of service providers in the distribution system.

Smart Grid Conceptual Model

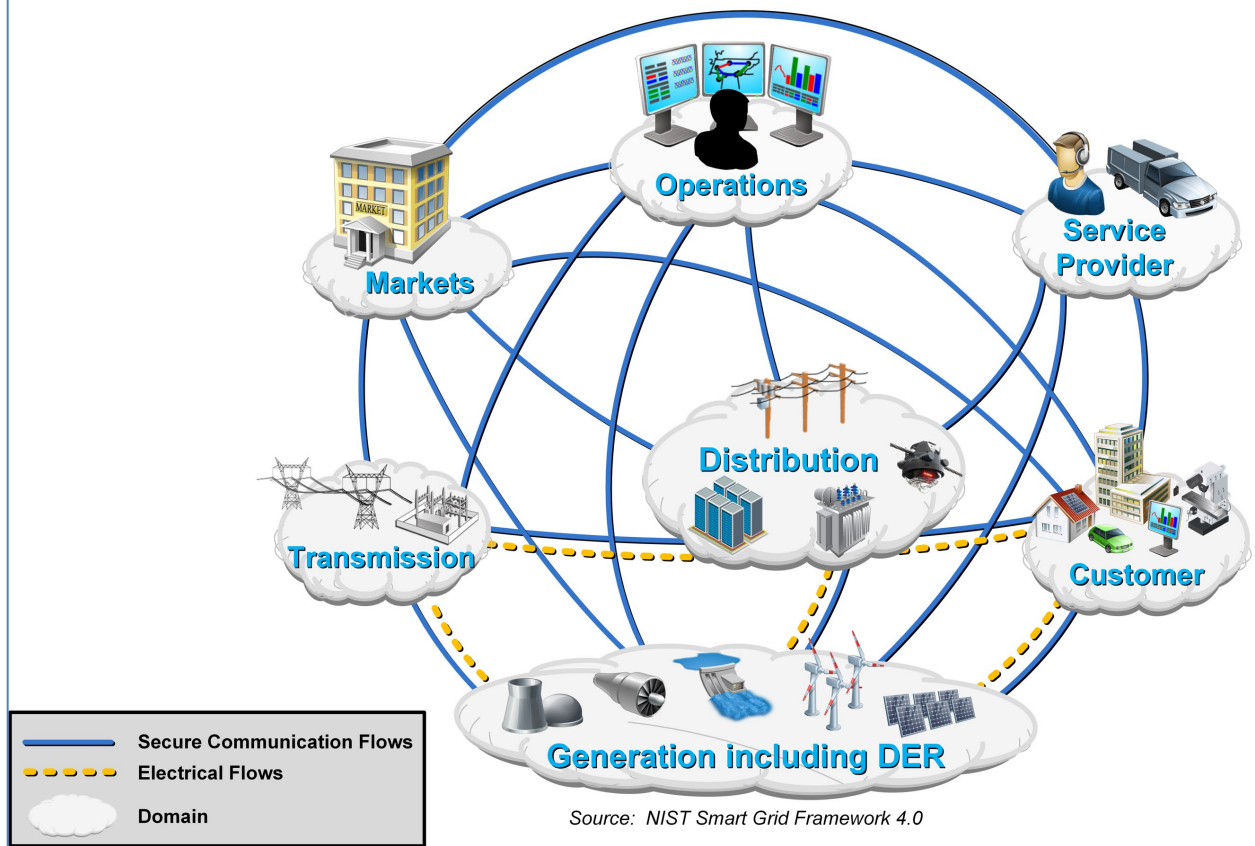


Figure 4 – Updated NIST smart grid conceptual model

The key Framework concepts derived from the updated Conceptual Model remain broadly similar to those of previous editions. First, the roles and responsibilities for actors and equipment in the electrical grid are a function of the domain in which they are applied. Through this lens we understand that functions required of grid equipment will likely change depending on the grid context, or domain, in which it is used.⁹ Benefits associated with equipment, resource, or action will similarly vary with domain and other context.

Second, the Conceptual Model reinforces the contrast between the growing complexity of information exchange necessary to operate the grid, and the relatively straightforward physical exchanges of energy that actually are the grid. Producing or consuming electricity still relies on relatively few and simply physical connections, even as energy technologies diversify across the system and grid dynamics become less certain. Conversely, grid communications and data complexity are exploding as people leverage the proliferation of low-cost power electronics, sensors, and microchips to support grid operations through coordinated actions of small-scale and distributed devices — coordination that was once the

⁹ For example, a photovoltaic system installed at a single-family house may have significantly different operating parameters than ones installed at commercial facilities or used for bulk power generation.

exclusive purview of large generators in close proximity.¹⁰ Whether to expand coordination of the high voltage system¹¹ or to prolong the life of existing distribution infrastructure,¹² information flows are increasing everywhere across the grid.

2.1.1. Conceptual model updates

While the high-level concepts contained in the NIST Smart Grid Conceptual Model have proven robust with time, the grid is also changing rapidly. The Conceptual Model and its derivatives have been updated to reflect many changes throughout the system and explore the associated impact on system interoperability requirements. These changes include:

Generation Domain

Changing scale — the domain name has been updated to *Generation including DER* to explicitly acknowledge the growing diversity in scale and utilization of grid resources.

Technology diversity — the number and types of generation technologies has been expanded, to reflect the growing diversity of U.S. generation assets [7].

Physical siting — the *Generation including DER* domain has been elongated to represent the geographic and topological diversity of included technologies. Icons representing large scale generation technologies are physically closer to the *Transmission* domain, and smaller scale or more modular technologies are physically closer to the *Distribution* and *Customer* domains.

Customer participation — resources provided by the customer, whether generation or demand management, are included as one of the many resource options available in the *Generation including DER* domain (see **Figure 37**).

Distribution Domain

Expanding role — the *Distribution Domain* has been made larger and placed more centrally within the Conceptual Model to reflect the growing responsibilities distribution systems have for optimizing grid function.

Improved sensing — sensing in distribution systems (represented by the icon of an overhead line fault detection device) is important to improving state awareness, a prerequisite for optimizing grid function.

Controllability and intelligence — computer servers represent the growing availability and use of real-time data for intelligent control of distribution grids.

¹⁰ For example, while energy imbalances between supply and demand used to only be managed by dispatching one of two large generators, today the same imbalance could also be addressed through the coordinated actions of many customers and their devices.

¹¹ For example, the Western Energy Imbalance Market [81]

¹² For example, the Brooklyn Queens Demand Management Project [78]

New actors — historically the province of distribution utilities, service providers and other actors are increasingly providing equipment to and services for the distribution grid as indicated by the new link between the *Distribution* and *Service Provider Domains*.

Customer Domain

Distributed operations — with active energy management possible at the grid edge, operations, control and automation enter the customer domain as represented by the computer monitor replicated from the *Operations Domain*.

Customer diversification — from multi-family dwellings to commercial and industrial facilities and campuses, the *Customer Domain* has been updated to reflect many types of customers served by and interacting with the electrical grid and energy markets.

Even with these updates, the high-level Conceptual Model shown in **Figure 4** is useful only for exploring the electrical and communications flows *between* grid domains. Much innovation occurs *within* the grid domains, the exploration of which improves understanding of the relationships between technology, communications, and interoperability. The Conceptual Model therefore includes detailed domain-specific examinations of smart grid roles, technologies, services, and information exchange, which are described in **Section 2.1.2** and **Appendix A** – Smart Grid Conceptual Model Domains.

Underlying the Conceptual Model is a legal and regulatory framework that governs many aspects of the electrical grid. These regulations apply to actors and applications, and to their interactions, throughout the system and enable the implementation and management of policies and requirements that keep the power system safe, reliable, and cost effective while maximizing the public good. Organizations that adopt these regulations exist at several levels, from federal agencies to public utility commissions at the state and local levels.

The transition to a modern grid introduces new regulatory considerations, which may transcend jurisdictional boundaries and require increased coordination among federal, state, and local lawmakers and regulators. The Conceptual Model is intended to be a useful tool for regulators at all levels to assess how best to achieve public policy goals that, along with business objectives, motivate investments in modernizing the nation's electric power infrastructure.

2.1.2. Conceptual model domains

Each domain — and its sub-domains — in the Conceptual Model describe smart grid conceptual roles and services. They include types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing tasks to achieve system goals, such as: customer and demand response management, distributed generation aggregation, and outage management. Services are performed by one or more roles within a domain. For example, corresponding services may include home automation, distributed

energy resource (DER) and customer demand response, load control, and wide-area situational awareness (WASA).

Each of the seven NIST Smart Grid Conceptual Model domains is described in **Table 1**.

Table 1 – Domains and roles/services in the smart grid conceptual model

	Domain	Roles/Services in the Domain
1	Customer	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own sub-domain: residential, commercial, and industrial.
2	Markets	The facilitators and participants in electricity markets and other economic mechanisms used to drive action and optimize system outcomes.
3	Service Provider	The organizations providing services to electrical customers and to utilities.
4	Operations	The managers of the movement of electricity.
5	Generation Including DER	The producers of electricity. May also store energy for later distribution. This domain includes traditional generation sources and distributed energy resources (DER). At a logical level, “generation” includes those traditional larger scale technologies usually attached to the transmission system, such as conventional thermal generation, large-scale hydro generation, and utility-scale renewable installations usually attached to transmission. DER is associated with generation, storage, and demand response provided in the customer and distribution domains, and with service provider-aggregated energy resources.
6	Transmission	The carriers of high voltage electricity over long distances. May also store and generate electricity.
7	Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

To enable smart grid functionality, the roles in a particular domain often interact with roles in other domains, as shown in **Figure 4**. Moreover, as system complexity increases and communications and interoperability expand operational control beyond the locational specificity of physical connections, it is likely that organizations will contain components of multiple domains. For example, the Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs) in North America have roles in both the markets and operations domains. Similarly, a distribution utility is not entirely contained within the distribution domain — it is likely to contain roles in the operations domain, and perhaps also the markets domain as economic signals become more dynamic across the system. Vertically integrated utilities will have roles in many domains.

Detailed descriptions and diagrams for each of the NIST Conceptual Model Domains are provided in **Appendix A – Smart Grid Conceptual Model Domains**.

2.1.3. *Other services and financial markets*

With its visual representation of domains, interfaces, and electrical and communications flows, the Conceptual Model supports a collective understanding of the actors, roles, and responsibilities needed to ensure effective day-to-day grid operations and control. The Model is an aid to understand how transitioning to a smart, interoperable grid may modify the expectations and roles of different system components or contributors. For example, with the updated Generation including DER, Operations, Distribution, and Customer Domains, the Conceptual model helps clarify emerging concerns and opportunities associated with the introduction of new customer-sited resources and increasingly distributed operations.

The Conceptual Model focuses on the key considerations of interfaces and interoperability and does not identify every possible concern related to the grid. For example, the financial roles defined in the Markets Domain are directly relevant to operations through pricing strategies or other economic activities that serve as proxies for system control signals. The roles of construction and associated financial services that are critical to the buildout of new grid infrastructure — but do not influence day-to-day operations and control — are included.

The Conceptual Model does not need to explicitly include every function related to the grid to maintain its value to help organize disparate stakeholders and provide a common conceptual foundation to advance interoperability. The Model allows extended concerns to be identified and understood in its context, thereby providing support for policy and planning activities from regional planning to resource adequacy assessments.

2.2. **Communication Pathways Scenarios**

The updated Smart Grid Conceptual Model provides a high-level set of descriptions adequate to include the broad set of evolving trends in the smart grid. Yet interoperability requirements derive from specific system and device interfaces that are not sufficiently characterized by such high-level depictions. In this section, another set of model diagrams — communication pathways diagrams — are provided wherein the domain structure of the Conceptual Model is used to facilitate a more detailed examination of system interfaces.

The Communication Pathways Scenario diagrams are an update and diversification of earlier mappings drawn to provide a visual reference for legacy applications and logical interfaces within the context of the Conceptual Model. Published in earlier Frameworks, the legacy applications mappings depicted an overarching architecture and provided a static perspective on the range of system and device interfaces. Building on the emerging diversity of grid architectures and associated system interfaces, the logical application model drawing has been updated into a series of Communication Pathways Scenario diagrams to depict specific interfaces and conceptual issues inspired by the DOE's reference grid architectures (see **Section 1.3.1**).

The architecturally inspired scenarios include:

- Legacy Communication Pathways Scenario
- High-DER Communication Pathways Scenario
- Microgrid Communication Pathways Scenario
- Hybrid Communication Pathways Scenario

These scenarios are not mutually exclusive. Rather, they represent views of the grid emphasizing various aspects. For example, many actors such as smart meters and advanced distribution systems appear in multiple reference models.

2.2.1. Graphic conventions

Each Communication Pathways Scenario diagram uses a common set of graphical conventions. For each diagram, colored boxes represent Conceptual Model Domains (see **Table 2**), and symbols are used to define actors, gateways, communications paths, and networks (see **Table 3**).

Table 2 – Domain descriptions and graphical color representation

Domain	Domain Role/Service	Color Code
Operations	The managers of the movement of electricity.	Blue
Markets	The operators and participants in electricity markets i.e. Independent System Operators (ISOs), Regional Transmission Organizations (RTOs), and Distribution System Operators (DSOs).	Purple
Distribution	The distributors of electricity to and from customers.	Light Brown
Transmission	The carriers of bulk electricity over long distances.	Maroon
Generation	Generators of electricity. Includes older generation sources such as coal and other carbon-based fuels, nuclear, hydro as well as distributed energy resources (DERs) such as wind and solar.	Plum
Customer	Residential, commercial, and industrial entities that use, produce, or store energy and interact with utilities, aggregators, and markets.	Orange
Service Providers	Billing, Information Technology (IT), finance, procurement, regulatory and aggregation functions performed for electric grid stakeholders.	Green

Table 3 – Communication pathways diagrams symbol descriptions

Symbol Name	Description	Symbol
Comm. Network	A communication network carries analog and digital information from a physical location to other locations	
Roles and Actors	Roles comprise specific business activities and actors can perform multiple activities.	
Gateway Role	Role that represents a border of the communication network.	
Comms. Path	A communications path shows the route that information flows within a Domain.	
Comms. Path Changes Owner/Domain	A communications path that shows the route that information flows between domains and in some cases between the owners of the information.	

The complexity of some scenario diagrams demands a simplified approach to portraying certain interfaces. When a communication pathway would likely interact with all domain or sub-domain actors in a similar manner, one pathway is drawn that terminates at the (sub-) domain boundary rather than cluttering the diagram with redundant individual communication pathways to each actor. Although prevalent in all scenarios, this technique is most evident in the High-DER Scenario through the simplified interactions of the operations sub-domains with the “Operational Enterprise Service Bus” actor, and also in the simplified interactions of the Internet with each of the domains in **Figure 6**.

2.2.2. *The legacy communication pathways scenario*

The Legacy Communication Pathways Scenario (see **Figure 5**) depicts the Conceptual Model mapping to the overarching electric grid architecture from the previous revision of the NIST Interoperability Framework [24]. It serves as a baseline mapping that also depicts a structure representative of current electric grid systems. Domains and sub-domains show logical groupings of systems and applications. For example, transmission systems such as an Energy Management System (EMS) are shown in the transmission operations sub-domain within the operations domain.

The model also shows information flows and communications paths between systems. Communications paths describe interfaces where standards may be helpful in defining the required protocols and characteristics of information exchange, although the depiction in this diagram of any single communication pathway is not in-and-of-itself an indication that NIST supports standardization of that interface.

Sub-domains in the Legacy Scenario are shown to identify typical groupings within the utility business sector. The particular collection of elements (network, roles, actors, and gateway role) helps define a business¹³ or department¹⁴ in an illustrative fashion without being exhaustive.

¹³ For example: RTO/ISO, Utility Provider, or Third-Party Provider

¹⁴ For example: Transmission Operations, Distribution Operations

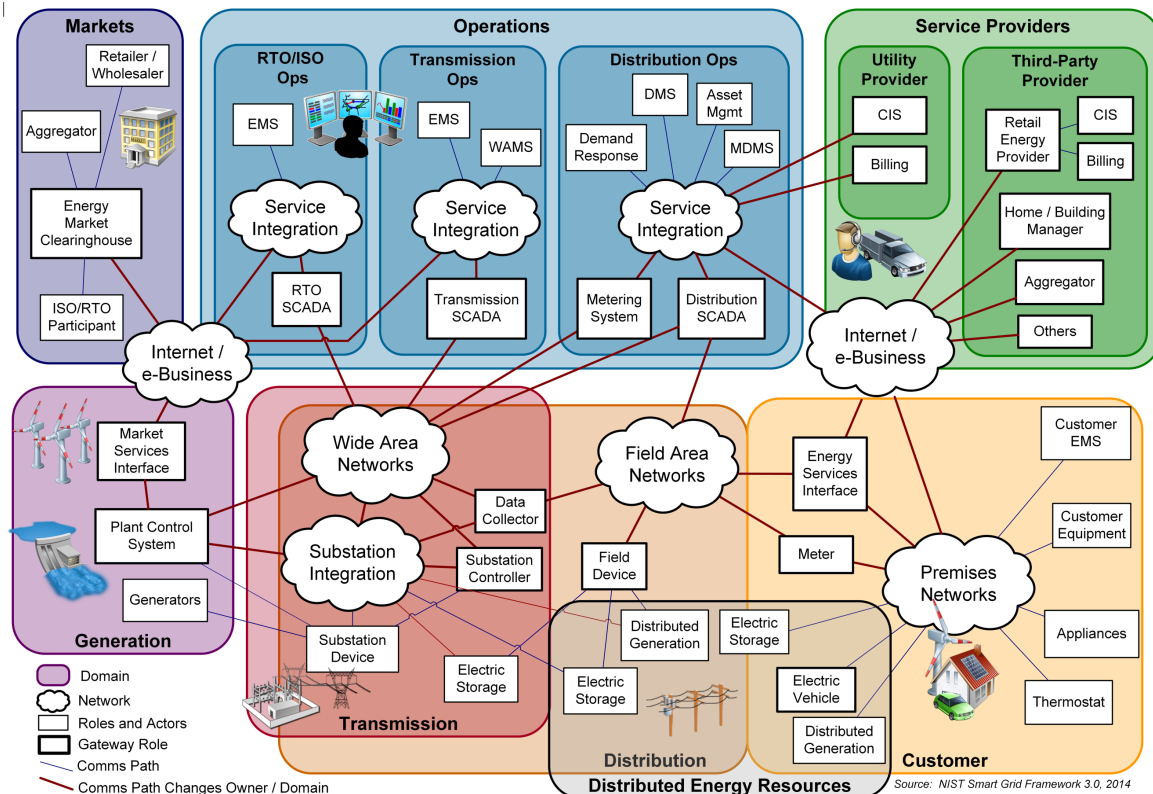


Figure 5 – Legacy communication pathways scenario

2.2.3. High-DER communication pathways scenario

The High-DER Communication Pathways Scenario (see **Figure 6**) represents current and future grids with DERs providing large amounts of power. In the future, market management functionality may be performed at both the distribution and transmission levels, and market makers such as Distribution System Operators (DSOs) will need to optimize for both economic factors and reliability.

As described in **Section 1.1**, large increases in the number of DERs have occurred and are now much more common in electric grids. The contributions DER assets provide will transform over the coming years as new policy complements advancing technology. The Federal Energy Regulatory Commission's (FERC) recent Order 2222 [82] removes barriers to market access that prevented DERs from competing on a level playing field with conventional resources providing a range of grid services [83].

Distributed energy technologies are therefore not a special class of generation assets, but a typical asset that can use power generation or demand response to participate in balancing supply and demand in the electrical grid. Accordingly, DER assets can reside in numerous domains with numerous operational strategies. Some examples include:

Utility-owned DER assets: These assets reside in the Generation Domain and prioritize supporting conventional markets and grid infrastructure.

Customer-sited DER assets: These assets reside in the Customer Domain and may prioritize local or non-utility services or operational strategies over utility priorities. Although sited at the customer premises, these assets may be controlled by customers, third party aggregators, or utilities.

The High-DER Scenario in **Figure 6** depicts a paradigm where market signals can be sent over the Internet to both distribution utilities or DSOs and to customers who own DERs. In this way, non-utility assets can participate and respond to the same market or other economic incentives as conventional resources. These capabilities are key enablers of many fundamentally new strategies for grid operations including transactive energy [38].

The colocation of customer-sited resources and loads — including demand response — means non-utility DERs could provide multiple services traditionally delivered through utility-owned assets.¹⁵ Importantly, the internet connectivity of DERs in this scenario means the device owner/operator could choose whether to optimize function around local concerns or those of a more regional or global nature.

¹⁵ For example, DERs such as solar photovoltaic or demand response can reduce peak demand during the mid-part of the day while an energy storage asset can supply reactive power.

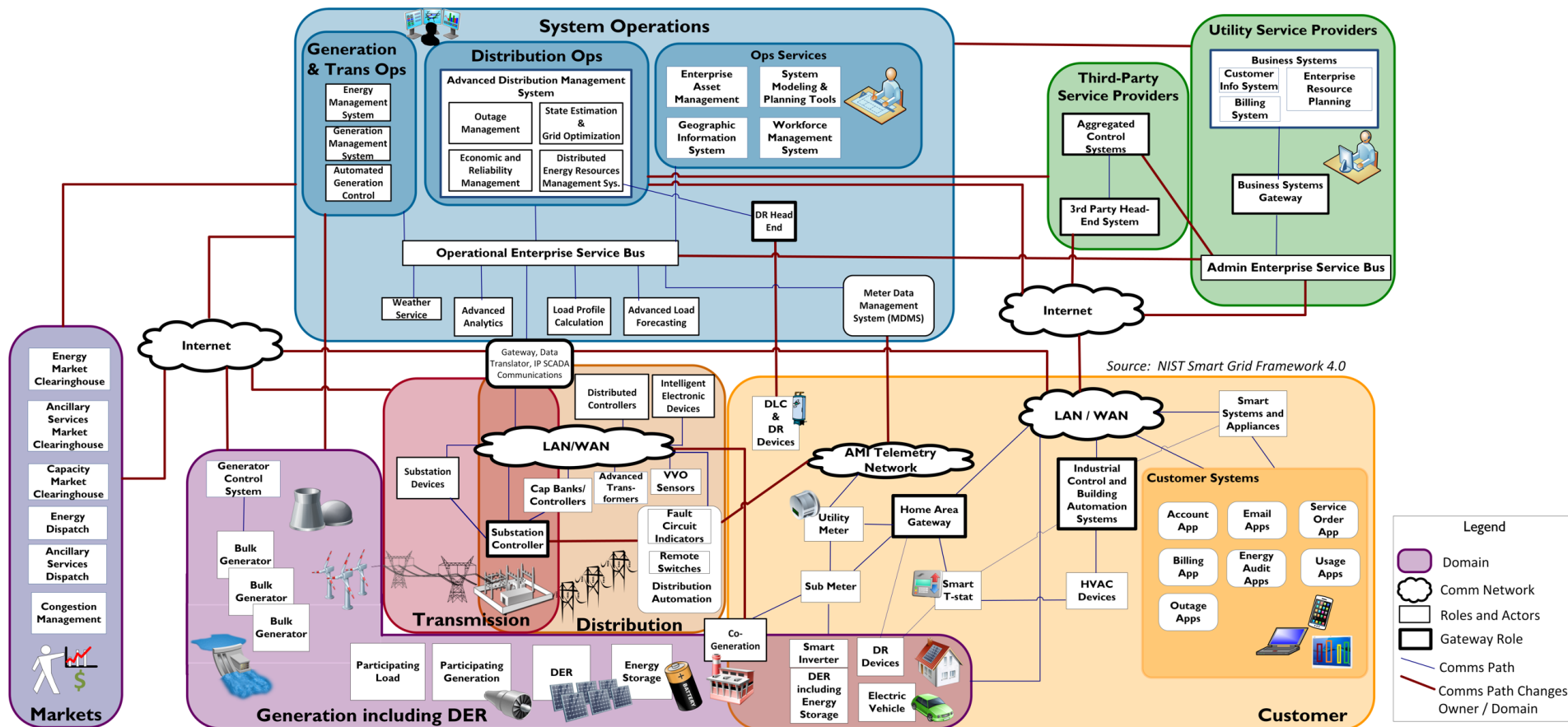


Figure 6 – High-DER communication pathways scenario

The multiple communication pathways for many actors and gateways are another important aspect of this model. While many communication pathways in these scenario diagrams are intended to aid in exploring the characteristics of specific interfaces, the diversity of interfaces and control loops depicted in **Figure 6** instead highlight the complexity of interfaces for single actors, and the possibility for multiple redundant communication loops to yield conflicting information.

Other points of interest for the High-DER Scenario include combining the *RTO/ISO Ops* and *Transmission Ops* sub-domain functions from the Legacy Scenario into a combined *Generation & Trans Ops* sub-domain. This is done to highlight how market functions in the High-DER Scenario may operate at different levels with fewer restrictions than those of the Legacy Scenario *RTO/ISO Ops* grouping.¹⁶

For this model, the *Gateway, Data Transfer, and IP SCADA Communications* role is placed across the system operations, transmission, and distribution domains, as this aligns with actual deployment and operation. Similarly, the *Cogeneration* actor is placed across the customer, distribution, and generation including DER domains because the scale and specifics of each cogeneration deployment will determine the physical and functional domain alignment.

2.2.4. Hybrid communication pathways scenario

The Hybrid Communication Pathways Scenario shown in **Figure 7** is inspired by the reference model for distribution grid control in the 21st century [84]. It depicts a high DER environment with centralized, distributed (non-centralized) and edge functionality. Grid control devices are in the Transmission and Distribution Domains. This diagram is called the Hybrid Communication Pathways Scenario because it depicts a hybrid approach to operational communications that uses both public and private communication pathways.

This diagram depicts several concepts worth noting. The first is that each domain has its own edge, so the term grid-edge device immediately becomes context specific. For example, while a customer's grid-edge device may be an appliance that actively manages energy consumption, the edge of a distribution utility's grid is the smart meter behind which the entire customer domain resides. Further, the edge of the transmission grid may be the phasor measurement unit or intelligent electronic device positioned at a substation behind which exist the entire distribution and customer domains. This concept is also applied to distributed assets which lie in between the centralized systems and edge devices.

Another important concept in this diagram is one of parallel communications infrastructures. While the dedicated operational communications network and pathways between the operations domain and actors in the distribution and transmission domain implies a proprietary communications infrastructure, unseen are the implied internet communications interfaces with each of the remaining actors in the scenario. While a DER, electric vehicle, or remote controllable appliance could be expected to be managed by a system operations

¹⁶ In the Legacy Scenario *RTO/ISO Ops* functions are limited to cross-region functions on the bulk power system.

domain actor in a high DER environment, it is not necessary that those operational communications utilize the same operational communications network as utility-owned critical infrastructure.

A final concept worth noting is that market actors need not be classified as centralized infrastructure. While the classic model of an aggregator may be to bundle distributed resources for sale into centralized markets [85], aggregators can work in decentralized or local markets as can other market actors.

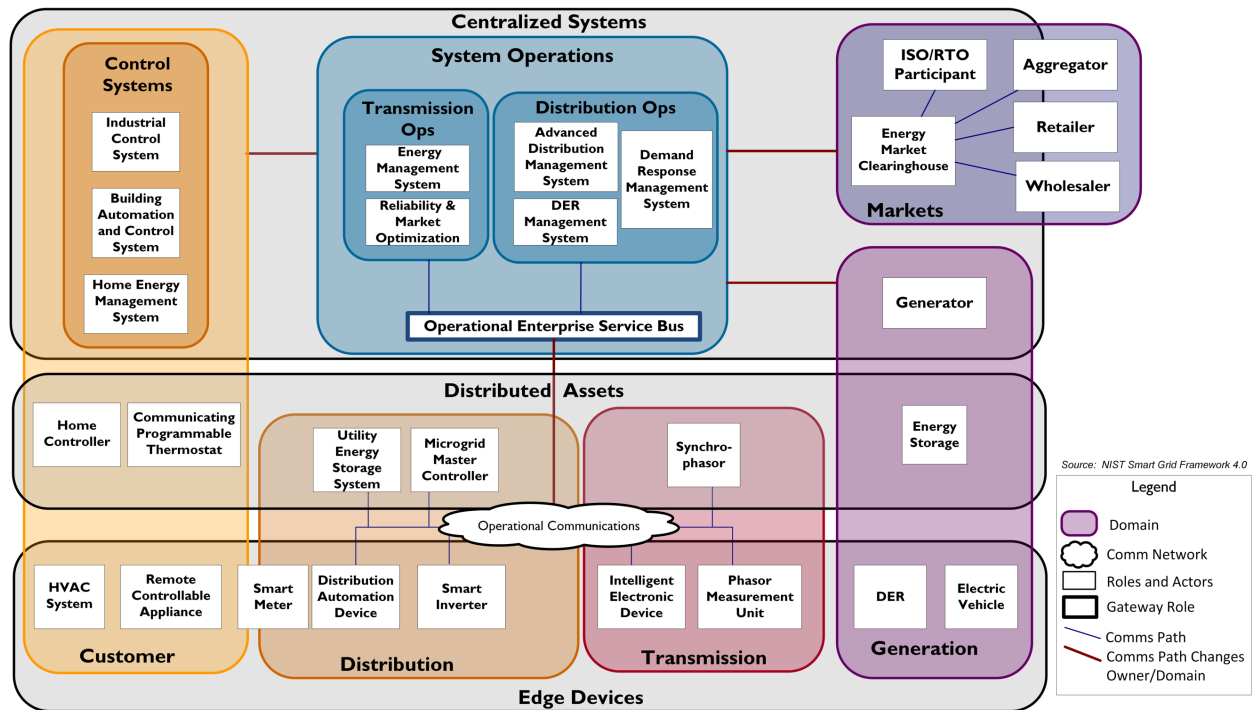


Figure 7 – Hybrid communication pathways scenario

2.2.5. Microgrid communication pathways scenario

Microgrids vary in scope ranging from a single premise to those including substations. Ownership and control of microgrids varies, with some owned and operated by consumers and some controlled by utilities that may or may not also own the microgrid. The Microgrid Communication Pathways Scenario depicts two example microgrids, one managed and controlled by a customer, and one managed by a utility.

Microgrids have the ability to isolate the circuits under their control from the main electrical grid. Modern microgrids can also be optimized to support overall grid health or provide specific grid services when operating while connected to the main electrical grid. Although managed by different entities, both types of microgrids are used primarily to improve reliability. In particular, microgrids are often deployed in situations where mission critical functions require power to be available at all times.

The principal difference between the customer- and utility-managed microgrids is in determining which communication pathways change domains and/or transition between assets with different owners. Communication pathways that change owner or domain — colored brown in **Figure 8** — are more likely to benefit from interoperability standardization.

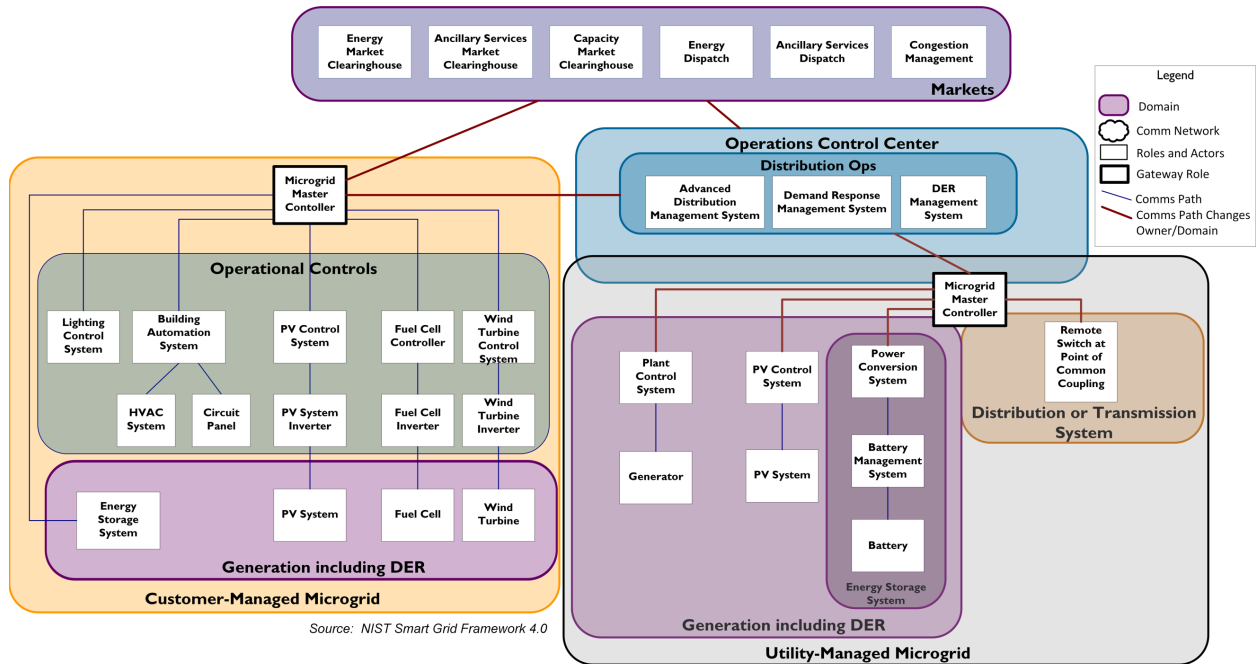


Figure 8 – Microgrid communication pathways scenario

2.3. An Ontology for the Smart Grid

The electrical grid is an impossibly large and complex system that has been called the greatest engineering achievement of the 20th century [86]. Beyond the sheer scale of the infrastructure, electrical grids are complex systems of systems (SoS) in which mechanical, electro-mechanical, and electronic control devices must all work together in near-real time with human oversight and intervention to produce and manage the electricity critical to modern society [3].

And yet despite this complexity, the language we use to describe the grid is often obtuse and lacks the clarity necessary to describe the specific capabilities that enable a complex SoS to operate.¹⁷ Even the term interoperability belies the complex series of interactions and requirements necessary to exchange actionable information (see **Section 6** –Testing and Certification).

¹⁷ For example, popular media will use catch-all phrases like “intelligent grid” [87] to describe any number of complex interactions and developing system capabilities, and the term “grid modernization” on the regulatory arena can mean anything from advanced metering to utility business model reform to microgrids and demand response [88].

A common understanding of the relationship between individual component capabilities and the functions of the broader electrical system could improve our ability to communicate between stakeholder groups regarding objectives, concerns, and strategies for grid modernization. Yet any pursuit of a common set of terms, or ontology,¹⁸ for the electrical grid must address the fact that the grid is not an isolated system. Indeed, electricity is the preferred energy carrier for modern society, and as a key enabling critical infrastructure the grid serves a great number of other systems — including many that are life-critical [21]. The electrical grid is therefore but one domain in the broader universe of cyber-physical systems.

Current design and management approaches for these broader systems are often domain-specific, resulting in redundant efforts that lack the robust, formal methods for design, evaluation, verification, and validation. Any ontology developed for the electrical grid should be consistent with those ontologies already developed for other cyber-physical systems; doing so would improve interactions and enable co-optimization of the grid with the other systems it serves.

2.3.1. *The NIST framework for cyber-physical systems*

Relying on engineered interactions between physical and computational components also means the electrical grid is a cyber-physical system, and because the grid only works when numerous systems operate in parallel¹⁹ the electrical grid is actually a multi-layered cyber-physical SoS. The design and engineering of advanced cyber-physical systems such as the smart grid can be so complex that existing approaches for performance prediction, measurement, management, and assurance are often inadequate.

NIST’s Framework for Cyber-Physical Systems [80] provides a useful analysis methodology and template for developing ontologies to describe key features of cyber-physical systems (CPS). Facets and Aspects are core concepts to this methodology.

Facets are inclusive of all system engineering processes (conceptualization, realization, and assurance), and can be thought of as “modes of thinking” about a CPS.

Aspects are groupings of stakeholder concerns along functional, business, human, trustworthiness, timing, data, composition, boundaries, and lifecycle concerns.

As seen in **Figure 9**, the CPS Framework’s methodology provides holistic concern-driven input to guide the development of the set of activities and artifacts, regardless of the specific systems engineering approach used. In this implementation, the *Domains* represent different application areas of CPS,²⁰ including smart grid (Energy).

¹⁸ An ontology is a set of concepts and categories in a subject area or domain that shows their properties and the relations between them [89].

¹⁹ For example, the transmission SoS is operated in parallel to the distribution system, which is also a SoS whose components include system operators, switches, distribution lines, and advanced inverters.

²⁰ The logical relationship between the “domains” in **Figure 9** and the Smart Grid Conceptual Model domains which describe roles and services within the grid is that changing the CPS application domain (e.g., from energy to healthcare)

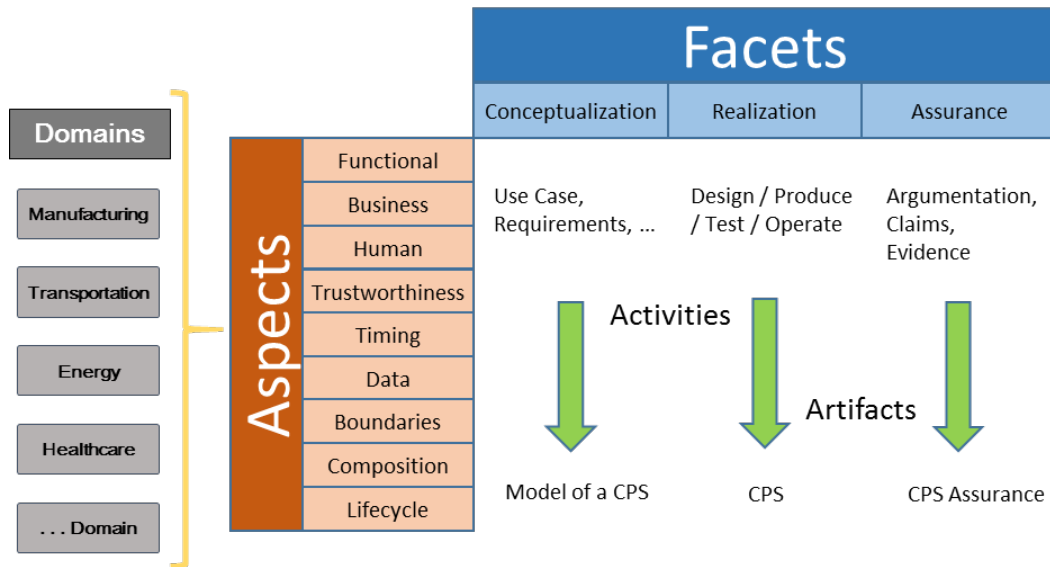


Figure 9 – CPS framework domains, facets, and aspects

2.3.2. The aspects of a modern electrical grid

An electrical grid is an energy-domain application of a CPS, so the aspects of a CPS shown in **Figure 9** also apply to the grid. A modernized electrical grid aligns to the cyber-physical framework's aspects as follows:

Functional — Concerns about function, including sensing, actuation, control, and communications, accurately describe grid modernization issues. For example, one grid modernization functional aspect concern relates to the impact that incorporating DERs on electrical distribution grids will have on the sensing, control, and communications requirements of existing systems.

Business — Concerns about enterprise, time to market, environment, regulation, cost, and other business areas. For the electric grid, a key business aspect concern involves the ability to design markets to optimize energy costs as many locations transition from regulated monopoly markets.

Human — Concerns about human interaction with and as part of a CPS. An important human aspect concern is whether human-in-the-loop system operators will be able to effectively manage a grid with potentially millions of new distributed generation devices not under their direct control.

Trustworthiness — Concerns about trustworthiness of CPS including security (cybersecurity and physical security), privacy, safety, reliability, and resilience. Addressing these concerns, including understanding and managing

fundamentally alters participant roles and procured services within that system, just as the *Distribution* to the *Markets* domains of the Smart Grid Conceptual model have different participant roles and procured services.

their interrelationships, is fundamental to the electric grid. Thus the trustworthiness aspect should be considered as a key driver for grid modernization, including through its impact on development of grid architectural principles.

Timing — Concerns about time and frequency signals, including the generation and transport of time and frequency signals, timestamping, managing latency, and timing composability. Timing aspect concerns reflect the real-time nature of electricity generation, transmission, distribution, and use, and have long been addressed by the electric industry through many existing electrical grid timing standards.²¹

Data — Concerns about data interoperability including fusion (situational awareness), data definitions (metadata), privacy, quality, type, and identity. Data interoperability is a key concern of the electric grid as evidenced by international standards such as IEC-61850 which defines configuration data for electric substation Intelligent Electronic Devices (IEDs). In addition, data accuracy, timeliness, and availability are crucial to data analytics ability to improve grid operation.

Boundaries — Concerns related to topological, functional, and organizational demarcations and interactions. For electrical utilities, a persistent boundary aspect concern is the friction between organizational siloes that must be integrated in order to maximize the operational efficiency of the grid. Examples include the boundaries between Information Technology (IT) and Operational Technology (OT) organization groups.

Composition — Concerns related to the ability to construct new systems from existing CPS systems. For electrical utilities, a current composability concern is how to effectively replace newly constructed control systems that combine Outage Management System (OMS) and Distribution Management System (DMS) features. Another key composition aspect concern is the ability to integrate utility control systems with user-owned and controlled DER assets.

Lifecycle — Concerns related to the management and maintenance of CPS systems and components throughout their lifecycle, including design, deployment, operation, enhancement, and ultimately disposal. For electrical utilities, lifecycle concerns include the need to maintain system and component performance time periods as expectations of system lifetimes are often measured in decades rather than years.²² Another lifecycle concern is the need to manage increased repetitive usage of grid control devices such as tap changes which may need to operate much more frequently to control voltage changes induced by modern loads and distributed generation. A

²¹ For example, IEEE 1588-2008 *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems* [90]

²² The average age of power plants is over 30 years [91].

further lifecycle aspect concern is how to upgrade firmware in existing devices to support new features such as the ability of advanced inverters to control voltage and frequency.

2.3.3. *Aspects and concerns of the electrical grid*

The CPS Framework “aspects” and “concerns” apply to all cyber-physical domains and can be mapped to a modern electric grid. The first step in this mapping is to evaluate the grid context for the existing set of CPS concerns, and if necessary to clarify the description of the CPS concern in the context of the electric grid. The results of this exercise are presented in **Table 14** of **Appendix B**. CPS concerns relate directly to system performance, and the domain-driven context for these concerns characterizes the relationship between the concern and system function.

The relationships between these concepts form the basis of a system ontology. In **Table 14**, the “Architecture Significance” column provides some examples of how each concern relates to activities or emerging trends in power systems as well as changes that could arise as new architectures are introduced. The architecture significance column therefore may help clarify the importance of CPS concerns to the electrical grids of today and tomorrow.

Key Messages – Operations

The use of open standards to achieve interoperability is key to optimizing utility operations as new devices, systems, equipment, and technologies are increasingly used within the context of an aging electric grid.

Customers will expand their participation in grid operations and control schemes, both obtaining additional value from and contributing new resources to the system.

The ongoing transition from analog to digital energy technologies alters the physical dynamics at the edge of the system and has implications for operations. This emerging physical context affects system observability requirements and operational schemes, meaning issues of physical interoperability require attention as a complement to the traditional concerns of informational interoperability.

Interoperability is a principal enabler of system control schemes that can manage and rely on the active participation of distributed resources while empowering customers to provide solutions across numerous scales. Operational trustworthiness emerges as a requirement for grid modernization.

Interoperability allows utilities, system operators, and other grid participants to select and implement high-priority capabilities from a menu of available operational strategies. Customer-focused and utility-centric control strategies are therefore no longer mutually exclusive.

3 Operations

[The Framework shall be] *designed to accommodate traditional, centralized generation and transmission resources and consumer distributed resources, including distributed generation, renewable generation, energy storage, energy efficiency, and demand response and enabling devices and systems.*

Energy Independence and Security Act of 2007

Electric power systems serve populations spanning communities, nations, and even continents. They are naturally complex due to the large number of physical connections whose states are determined through a combination of individual choices, environmental conditions, the status of neighboring connections, and even the unknowable. Indeed, it is impossible to know all aspects of a complex system at any one time, and this is especially true for the electrical grid [92]. Yet the system functions despite this complexity, and over

time several strategies have emerged which allow the grid to be operated in a deterministic manner.

Chief among the strategies to simplify operations was averaging uncertainties within the system. At the turn of the last century when Samuel Insull electrified Chicago, he did so by building ever-larger generators and incorporating more neighborhoods into the utility's service territory in a virtuous cycle of physical and economic efficiency [93]. Ancillary benefits to Insull's economic efficiencies include physical momentum provided to the grid by thousands of pounds of spinning steel in each large-scale generator, and a smooth electricity demand curve determined by the collective behavior of millions [21]. Expansive service territories and physically imposing generators mask grid complexity by averaging out and riding-through physical uncertainty within the system, thereby making operation of large-scale electrical systems tractable.

As technology and regulatory policy have evolved, so too have the constraints within which the grid must be optimized. From 1978 onward, public policy in the United States has required utilities to purchase electricity from the most economically efficient producers [94]. This altered the financial calculus for investing in large-scale generators, as did emerging innovations in thermal cycle and energy conversion technologies that could yield similar or higher energy production efficiencies with smaller-scale and modular technologies and investments. As energy technologies migrate toward efficiency models governed by semiconductors²³ and information technology,²⁴ the forces of technological change driving technology towards the edge of the system are similarly driving change in the strategy for — and structure of — utility operations [95].

Even as information exchange becomes an increasingly critical part of the electrical grid, our ability to quantify interoperability and its operational impacts remains limited. The challenge of quantifying interoperability benefits is well documented [96], and indeed our own definition of interoperability is functional in nature (see **Section 1.2**)²⁵ and cannot be characterized with a static metric or measurand. Understanding the evolving role interoperability has in smart grid operations therefore requires examining a range of functional contexts. It is from these functional contexts that it becomes possible to characterize the importance of, and future requirements for, the exchange and use of information across the grid.

²³ The efficiency of a solid-state transformer or inverter is governed by semiconductor switching, battery storage efficiency is governed by chemistry at the electrode, and photovoltaic efficiency is governed at the photonic scale.

²⁴ Exchange of operational information allows for regular and more efficient redispatch of system resources [95].

²⁵ Earlier in this report we define interoperability as the capability of two or more networks, systems, devices, applications, or components to work together, and to exchange and readily use information.

3.1 Interoperability for Utilities

3.1.1 System composition and constructivity

Expanded use of DERs and other new technologies, as described in the communication pathways scenarios (see **Section 1**), will have impacts throughout the electricity system — including the Bulk Power System — and require utilities to integrate more refined observation and control at the edge of their respective systems [97]. But even without technology advancement, product lifecycles and evolving safety requirements [98] demand integration of new devices and systems into the existing grid. Utilities therefore cannot escape the challenge of integrating new equipment into their existing systems, which typically involves significant effort and expense [27].

In 2016 the DOE described the lessons learned from nearly \$8 billion in public and private smart grid investments. While a majority of these funds (\$4.4 billion) supported advanced metering infrastructure (AMI) deployment, significant investments were also made in distribution grids (\$2.2 billion), customer systems (\$0.8 billion), and the transmission system (\$0.5 billion). The DOE concluded that integration of new and legacy systems was a constant challenge for nearly all utilities, and that turnkey solutions for these integration issues were generally not available. The Department also noted that customized testing, coding, and systems development was often required to achieve the interoperability necessary for utility operations [99].

Although specific interoperability costs and value metrics are difficult to quantify, utilities and equipment manufacturers have reported to NIST that their costs for integrating non-interoperable equipment and systems ranges from \$140 million to \$1 billion per year per firm [28]. The scale of these outlays indicates an interoperability value proposition that could exceed even the upper estimates of \$10 billion in interoperability-derived annual savings [31] that is potentially achievable in the U.S. electric power industry.

The savings described above are for point-to-point system integration [27], which are similar in form to the interoperability challenges faced when a utility interconnects new and legacy systems through back-end integration, or when a utility tries to integrate power system components of various types and configurations into a common system.²⁶ Standards-based interoperability approaches have been identified as a key opportunity to mitigate these costs [27, 96].

²⁶ This concern is called “constructivity” in the ontology of the smart grid (see **Appendix B** – Mapping CPS Aspects and Concerns to the Electrical Grid).

3.1.2 Hedging against obsolescence

The electric grid is aging. From generators²⁷ to transformers and other parts of the system,²⁸ a substantial portion of grid assets have either reached the end of their planned lifetimes or are technically obsolete [101]. Additionally, research has suggested the challenges and costs of dealing with the aging of smaller commodity units that make up the majority of the electrical grid might be substantially higher than those associated with the major equipment classifications described above [102].

Aging infrastructure presents a particularly challenging task to the electric utility: how to manage grid assets which have reached the end of their designed operating life but are still in use. These aged but functional assets were specified decades earlier for a likely very different grid and set of operating conditions. Equipment which achieves longer-than-planned functionality also tends to be over-specified for the original task [102], and it is up to the utility to determine if these technically obsolete — but still functional — assets bring enough value to the system to warrant the ongoing investment necessary to extend their functional and economic lifetimes.

Informational requirements in the smart grid era compound the challenge of extending asset lifetimes, as the functionality of modern equipment is often inextricably linked with its ability to communicate with the broader system. The task of interfacing information technology systems from different eras can quickly become an exercise in developing custom interfaces — physical and informational — and the over-specificity of decades past which allowed the device to operate longer than anticipated may also inhibit efforts to adapt device communications to anything beyond the originally intended function and interface.

It is well known that standards-based interoperability requirements are key to maximizing equipment capabilities in the smart grid [26], and to reducing the effort and expense of integrating new equipment into legacy systems [27]. Given the extensive availability of standards for mapping between communications protocols and/or information models [103], deriving today's interoperability specifications from open standards²⁹ may give firms the opportunity of easily mapping these specifications to future standards as smart grid equipment and informational requirements evolve. In essence, adopting open standards avoids over-specification of information technology requirements and is a mechanism for utilities to hedge against the limitations and expenses inherent in developing customized interfaces required for lifecycle extensions of assets that would otherwise become obsolete.

²⁷ More than 6,000 generators representing 35 percent of all grid-tied generating capacity are more than 40 years old [20].

²⁸ Seventy percent of power transformers and transmission lines are more than 25 years old, and 60 percent of circuit breakers are more than 30 years old [100].

²⁹ Open standards are nonproprietary and involve a consensus-driven approach to establishing the requirements.

3.2 Interoperability for New Technology

The number and types of technologies used throughout the power grid are evolving rapidly (see **Section 1**), with emerging system compositions upending many traditional operating strategies. Observations of power quality and other functional metrics [104] enabled by increasing sensor deployments [22] reveal an urgent need to improve our understanding of the emerging interactions between grid technology, equipment, and operations.

While it is clear the ongoing transition from analog circuitry to semiconductor technology throughout the grid will have some impact on the control schemes and waveforms of alternating current, the absence of historic observability for distribution system power quality means we do not know *a priori* whether new measurements are indicative of worsening system performance or merely reflect migration from functional states of years past which yielded similarly challenging — albeit unobserved — characteristics. These emerging datasets engender questions regarding the causes and long-term trends of the observed phenomena, and the implications for interoperability in future smart grids.

3.2.1 *Changing physics at the edge of the system*

The electric grid emerged in an analog world, in which common circuit elements yielded smooth operational characteristics that in turn afforded substantial flexibility in system operations. In this early environment, the alternating current likely resembled a smooth sinusoidal waveform that could be used whether in its ideal form or not.³⁰ The latter point is important because most analog electrical equipment continues functioning reasonably well even as grid conditions deviate from ideal, which has always provided some measure of operational flexibility.

For example, the current-voltage relationship for an ideal resistor is a straight line. This simple characteristic means that by using Ohm's law we can state that when circuit voltage increases, the power through a resistor increases in a smooth and quasi-linear³¹ fashion. Similarly, the power through a resistor decreases when circuit voltage decreases. The behavior is predictable, and the resistor still functions — albeit with slightly modified performance outputs — even as circuit conditions deviate from normal.

Incandescent lightbulb filaments are resistors,³² examination of which can aid our conceptual understanding of the relationship between the physics and operational flexibility of analog grids.³³ When an incandescent bulb receives more or less voltage than intended, it will

³⁰ The term “likely” is inserted here because the metrology equipment necessary to observe waveform characteristics was not, at the time, deployed on the electric grid.

³¹ The relationship between voltage and power is not purely linear because power rises with the square of voltage. However, the relationship between voltage and power for analog circuits is a smooth function that can be approximated as a linear relationship for small voltage differentials.

³² Although not an “ideal resistor,” under grid conditions lightbulb filaments are a useful proxy for the ideal resistor described in the previous paragraph.

³³ Although the current-voltage-resistor relationship described by Ohm's law applies to direct current electric circuits, purely resistive elements do not affect the phase of an alternating current circuit and so the direct current relationships described still apply, albeit with impedance substituted for resistance.

simply glow more brightly or dimly than it would at the standard voltage rating. Indeed, this phenomenon is the basis for the term “brownout,” which occurs when utilities reduce the electrical voltage provided to customers (usually as part of emergency actions to match available supply and demand). The voltage reductions during brownouts reduce power consumption while still providing customers with some minimum level of electrical service, and the analog characteristics of the incandescent bulb continue to provide a reduced level of functionality under sub-optimal conditions.

Other analog circuit elements also have response characteristics that allow for continued use under sub-optimal conditions. Inductive motors, for example, can operate at suboptimal circuit voltages and frequency, albeit with reduced efficiency which may minimize device usefulness under degraded conditions.³⁴ Yet inductive motors and loads are designed to continue operations through suboptimal grid conditions [105] and regularly do so.

The smooth physics of analog circuitry does not apply to modern semiconductor-based electronics. That the electrical conductivity of a semiconductor changes with environmental conditions is the very essence of that material class, and it is through control of these parameters via transistors that semiconductors become computationally powerful. The ability to precisely control conductivity in transistors³⁵ is also what makes semiconductor-based power electronics valuable to the electric grid.

Yet the binary nature and fast switching capabilities of transistors and diodes in semiconductor based (solid-state) power electronics introduce functional step-changes to normal operations which change the physical dynamics of the grid. While the benefits from high electrical efficiency and discrete controllability are immense, the very nature of this switching creates minute but very sharp step-changes in the aggregate waveform which can manifest as nonlinear and transient interactions³⁶ with the rest of the system.

As different as the strategies are for managing analog circuit elements (e.g., resistors, inductors, and capacitors), even more diverse are the integration requirements and operational strategies for managing semiconductor-based systems. Solid-state power electronics are scalable and modular, which provides meaningful opportunity to improve efficiency and control throughout the distribution system. This is especially true at the system edge where customer technologies are diversifying and gaining new energy management capabilities. Changes to grid physics associated with the transition from analog to digital (or solid-state) components warrants examination as stakeholders seek to understand evolving interoperability requirements for observing and controlling the grid.

³⁴ Because of phase interactions between inductive loads and alternating current circuits, under highly stressed grid conditions it may be possible for motors or other inductive loads to contribute to system failure in a way that resistive loads do not.

³⁵ Diodes are also used in semiconductor-based electrical loads and can be designed to have switching characteristics similar to transistors, albeit with switching characteristics driven by voltage thresholds. However, transistors provide the optimal controllability.

³⁶ For example, simultaneous switching of large numbers of diodes can produce a current inrush which induces a magnetic field that can affect the impedance of the very wires through which that electricity is flowing [106].

3.2.2 Changing supply and demand technology

The introduction of distributed generation is often cited as a prominent source of power quality issues in distribution grids [107-110]. It seems logical that a grid originally designed for unidirectional powerflows from centralized generating facilities outward could buckle under the stress of incorporating generation and active power management technologies at the customer site. As generation capabilities have changed, uncertainty over the impacts of these technologies has also emerged.

Solar inverters provide an interesting case-study on the changing capabilities of generating technologies. In 2003 IEEE published standard 1547, the first grid interconnection standard for distributed resources. Most commonly applied to inverter-based generation, the evolution of this standard and inverter capabilities provides an interesting case-study in the accelerating evolution of technology on the grid. The original IEEE standard mandated just one actively controlled capability — the ability for distributed resources to de-energize (turn off) when grid voltages or frequencies deviated from a narrow operational range [111]. Just fifteen years later more than 35 new DER functions had been identified (see **Appendix C – Inverter and DER Functions**), some of which have become mandatory through California Rule 21 and the 2018 revision of IEEE 1547.

The confluence of dramatically expanding DER capabilities with grid management schemes that historically modeled customers as passive system loads [112] would seem to buttress the argument that distributed generation could be the primary source of power quality issues and emerging dynamics on the distribution grid. Yet distributed solar generation accounted for only 0.7 % of total U.S. generation in 2018 [113, 114], and so it is important to consider whether there may be other more ubiquitous causes for the emerging grid dynamics.

Importantly, the transistors and diodes changing the physics of the power grid (see **Section 3.2.1**) exist in all forms of solid-state power electronics, and not just inverters and other generation assets. Research has shown that the power electronics in CFL and LED lightbulbs can severely affect local electrical waveforms, a phenomenon which does not occur for incandescent bulbs. When combined with other circuit elements, including switches and/or dimmer controls, the distortions can appear extreme (see **Figure 10**, [115]).

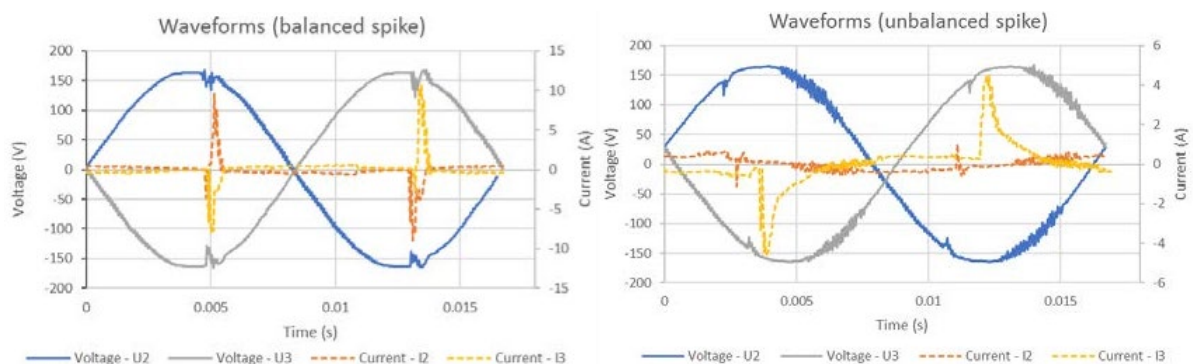


Figure 10 – Example electrical waveform distortions observed in NIST experiments

Considering the ubiquity of semiconductor-based power electronics in both existing technologies³⁷ and emerging devices, the major driver affecting the declining power quality of our electric grids [116] may in fact be changes in how electricity is consumed rather than the oft-cited emergence of distributed generation. That grid performance can be materially affected by energy consumption comes as no surprise — after all, supply and demand has been balanced in real-time since the grid's inception. It is, however, the emerging and uncontrolled interaction³⁸ of modern devices with the grid through nontraditional physical mechanisms³⁹ that demands a sharper focus on the physical aspects of system interoperability.

3.2.3 *Alternating and direct current interactions*

The revolution in solid-state power electronics described above has led to a proliferation of direct current (DC) devices and systems. More than just battery-driven electronics, DC equipment and appliances already permeate our homes and businesses⁴⁰ and are becoming available for all manner of end-use applications [117].

The benefits of using DC systems in buildings include lower capital and installation costs, improved energy efficiency, and a reduced physical footprint which enables more flexible design. Combining DC building systems to utilize a common transformer or other DC power source would compound gains to yield dramatic efficiency improvements and simplify building design constraints [118], especially when DC energy sources such as solar PV or battery electric storage are available onsite.

Expansion of DC technologies into applications and services traditionally served by alternating current (AC) technology can be extremely beneficial, as DC-ready appliances typically operate at or above the highest energy efficiency levels of their conventional AC counterparts [117] and provide greater functional controllability. Extensive DC technology deployment could also impact utility operations at the grid-edge and even limit the efficacy of traditional AC system management techniques,⁴¹ but may also alter customer service requirements and potentially allow utilities to relax their operational constraints.

Utility-scale distribution grids will continue AC operations even as the foothold for DC technology grows. Expanding use of DC technology in devices, systems, and even

³⁷ For example: computers, televisions, mobile device chargers, and variable speed electric motors/fans, among others.

³⁸ These interactions are not governed by a centralized dispatch or even an adaptable control algorithm, but instead by the fundamental characteristics of the energy consumption that are unique to each device or class of devices.

³⁹ Not only can energy consumption introduce harmonic distortion to the local circuit, but distortion of the baseline supply waveform amplifies the device-introduced distortions [116]. This could create a feedback mechanism accelerating grid performance degradation and warrants further study.

⁴⁰ Every computer, flat panel display, or device that has a rechargeable battery is a DC device.

⁴¹ Conservation Voltage Reduction (CVR) is one management technique that is rendered ineffective by DC devices and systems. Utilities employ CVR to reduce energy demand by lowering circuit voltage and corresponding power consumption through the relationship described in **Section 3.2.1**. However, the power electronics in most DC devices readily convert all manner of AC waveforms to the required DC voltage and current, and so would continue to function and consume energy normally and without adjustment during a CVR event.

microgrids highlights the need to better understand the effects physical interoperability between DC and AC systems will have on control theory and operational practice.

Standards for DC systems and microgrids are only now emerging for modern energy applications, and will need to be developed further as these technologies penetrate the marketplace.

3.2.4 Electric vehicles and a changing infrastructure

Sales of electric vehicles (EVs) in the United States increased 49% annually on average from 2010-17, [119] and the more than 1 million electric vehicles on the road by the end of 2018 are a major driver of change within the electric industry [120]. Although projections about future growth in EVs vary widely, even the more conservative growth estimates have implications for future grid operations, economics, and markets.

Growing electricity demand for vehicle charging will bring additional revenue to generators, system operators, and utilities alike, while also benefiting customers through reduced transportation fuel costs. But increased residential load from EV battery chargers will also require controlled/managed charging to mitigate potential peak load conditions on distribution transformers and feeders, while still providing owners with timely recharging capabilities.

Managed charging programs for EVs are offered by utilities and third-party service providers and successfully adjust peak loads to lessen infrastructure risks [121]. This can be accomplished through a variety of control schemes and communication mechanisms, including direct control (local or remote), rate design offerings, or through market signals.

The data and communications requirements necessary to support managed charging and vehicle-to-grid interactions are being developed and standardized through an interoperability profile. For more on this topic, please see **Section 6**.

3.3 Evolving Control Schemes

Grid management techniques devised more than a century ago, and described earlier in this chapter, have worked admirably. But the change in grid economic systems over the past forty years, and the technological advancements which have occurred over the same timeframe, are changing how the system is controlled. Where averaging away complexity and uncertainty was originally a benefit that enabled scale, doing so today omits economic opportunity and diminishes the available solution space within which utilities can optimize their operations.

And so while the characteristics of the grid are changing in an uncertain way (see **Section 3.2.1**), the mechanisms for controlling the grid and operating the grid are also evolving. The next two sections examine how different control schemes can affect organizational concepts and system interoperability requirements.

3.3.1 Utility-driven control schemes

The modern electrical grid is managed through a series of physical operations and economic optimizations designed to keep the system running at greatest efficiency while minimizing the chance of disruption. These functions can be triggered through automated process, operator dispatch, or economic signal. The interoperability requirements associated with each operation will change with the temporal, spatial, and topological constraints for the function.

For the utility, architecture and operations need to accommodate both new and legacy devices in an evolving environment which is being rapidly influenced by policy and market decisions. Any of the dimensions mentioned above can be used to organize system function to aid our examination of the associated interoperability requirements. Below is an illustrative listing of some near- and medium-term grid functions that could be developed to mitigate some of the uncertainty and operational challenges emerging in the grid, grouped by implementation time-constant.

60Hz+ (sub-cycle)

Real power stabilization
Reactive power stabilization
Power flow control
Microgrid islanding
Dynamic distribution reconfiguration

<5 minutes (sub-dispatch interval)

Frequency regulation
Local optimization
Congestion management

5-15 minutes (linked to dispatch cycle ahead)

Dynamic line and transformer ratings
Dynamic topology management
Flexibility ramping
Forecast driven SCED⁴²
Bulk power real-time redispatch
Real-time energy imbalance and settlement

>15 minutes (intra-day and day)

Upstream Volt/VAR control
Security-constrained unit commitment

Although not a comprehensive set of grid functions, the above listing is indicative of the diversity of functions and grid services that are or could soon be regularly provided across the system. Grouping along the temporal dimension provides an intuitive understanding of some interoperability requirements, such as data timeliness, and allows us to evaluate these functions in relation to conventional market structures. Other dimensions along which these functions must also be understood include topological,⁴³ control mechanism,⁴⁴ and economic,⁴⁵ as each of these considerations drive a number of interoperability requirements.

⁴² Security Constrained Economic Dispatch

⁴³ Will the service be provided in the bulk or distribution grids, or on the customer side of the meter?

⁴⁴ Will the function be controlled through utility dispatch or automated algorithm?

⁴⁵ Will the service value be determined by fixed tariff, market settlement, or some other dynamic approach?

As we consider the above list of possible grid functions, it is clear that the majority of fast-acting opportunities are at the edge of the system. A future grid state that could incorporate and benefit from these — or similar — capabilities will rely on innovation in resource flexibility, power electronics, distributed intelligence, and adaptive protection [97]. Changes of this magnitude will expand the awareness requirements for the distribution utility, which would benefit from increasing observability into customer-sited resources to maximize the value of these emerging grid-edge functions and services [97].

3.3.2 *Emerging customer-driven control schemes*

Value creation in the grid was once as predictable and unidirectional as the powerflows. But an interoperable smart grid allows value to be created in and flow between domains in new and potentially unexpected ways. The traditional system operations architecture had very little impact on customers other than through the economic and reliability metrics for the provided electric service.

As consumers move to being active participants in the operation of the grid, the architecture of the operational systems can influence how and why consumers choose to change from being simply a service delivery point. As illustrated in **Figure 2**, DERs and other capabilities available at the customer site and the periphery of the grid can dramatically impact utility, regional, and even societal goals.

One example of this is in Hawaii, where distributed resources — including large quantities of customer-sited generation — are growing very rapidly. On four islands serving more than one-third of the state's electricity customers, distributed resources will soon have larger aggregate generating capacity than conventional centralized generation resources [122]. The value propositions of distributed generation in Hawaii span numerous scales and beneficiaries, including reducing systemwide electricity costs,⁴⁶ achieving state policy goals including renewable portfolio standards, and reducing pollution and other emissions from conventional generation in environmentally sensitive locations [123].

While value can flow extensively from the customer domain outward, it also flows extensively from an interoperable smart grid to the customer. As demonstrated in the Hawaii example and illustrated in **Figure 3**, emerging schemes focused on maximizing customer engagement and asset utilization can yield benefits from financial, through reliability, to environmental. Yet the control schemes to maximize these value propositions are emerging in real-time, and indeed the economic structures and operational capabilities necessary to properly and fully stimulate these functions and value streams may not be available today.

Interoperability requirements are a necessary precursor to modern grid operations strategies seeking to maximizing the efficacy of growing equipment and technology investments across the system. Because DER physical actions have an inherently local effect on the grid, care should be taken to ensure that local conditions or utility concerns are not undermined if the value sought is further afield. These requirements will have to be refined as new technologies emerge and grid functionality expands.

⁴⁶ Most Hawaiian electricity is generated using oil for fuel, which carries with it a high cost of generation.

Incorporating customer resources in utility control schemes A Minnesota electric cooperative case study

Utility and customer focused control schemes are not mutually exclusive and are regularly combined in utility operations. Just as the High DER and Microgrid Communication Pathways Scenarios in this Framework highlight direct communications with customer sited assets (former) or management systems (latter), utilities regularly incorporate customer-owned assets as operational resources through demand management programs.

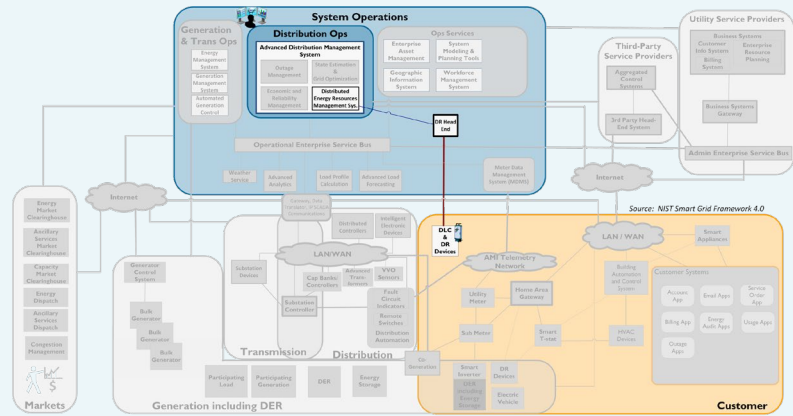


Figure 11 – The NIST High DER Communication Pathways Scenario, highlighting a representation of utility direct load control programs

Electric cooperatives in Minnesota utilize a number of customer-focused control schemes to complement conventional electricity supply and grid management technologies. For example, Great River Energy's 28 distribution cooperatives serve 700,000 customers [124], 200,000 of which participate in demand response programs [125] totaling 400 MW capacity equal to 12 % of the cooperative's generation resource [126]. The customer-sited load management program leverages technologies ranging from interruptible water heaters to irrigation pumps to microgrids. The distribution cooperatives employ a variety of control schemes to initiate the load curtailment, from direct load control techniques used to cycle customer-owned water heaters and air conditioners as illustrated in the High DER

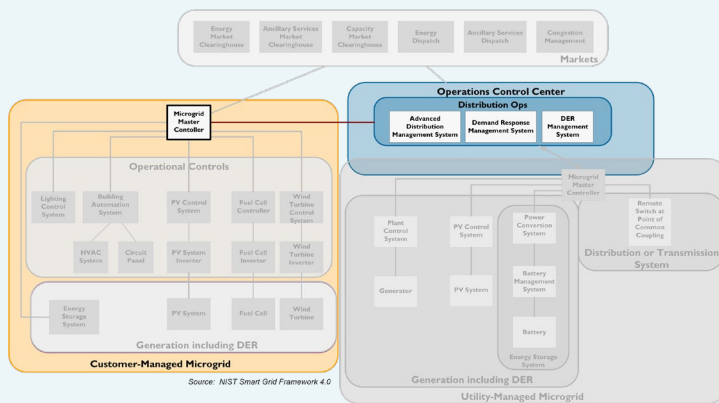


Figure 12 – The NIST Microgrid Communication Pathways Scenario, highlighting a representation of utility voluntary load curtailment programs for industrial and commercial customers

Communication Pathways Scenario (see **Figure 11**), to calling on campus microgrids to self-supply and reduce system load in an approach which mirrors the customer-owned microgrid illustration in the Microgrid Communication Pathways Scenario (see **Figure 12**).

Incorporating customer-sited resources and control schemes into their conventional electricity supply model has saved Minnesota electric cooperatives millions of

dollars, with load management programs at Dakota Electric yielding economic efficiencies exceeding 8% of total revenue [127]. These benefits are achieved even as several of the resources are infrequently called upon [128]. Improvements in control theory and interoperability could further empower customers and yield significantly greater benefits.

3.3.3 System devolution

Observation and control capabilities are extending to the edge of all grid systems. Enabled by declining technology costs [22] and occurring in every smart grid domain — as exemplified in the Hybrid Communication Pathways Scenario (see **Section 2.2.4**) — the need to manage expanding capabilities and faster response times means grid control has begun migration toward system peripheries.

The introduction of automated protection schemes for substations and other equipment necessitated the dispersal of certain actuator controls. Where system operations once relied almost exclusively on phone calls and other interpersonal dispatches from centralized operations centers, modern protection decisions and corresponding actuations must occur in the sub-cycle timeframe (<15ms). These actions are now made automatically in response to local conditions by equipment that uses logic and governance structures sanctioned by a central authority or operations center.

More than just a function of protection schemes, control devolution⁴⁷ is progressing regardless of system architecture as optimization strategies evolve to incorporate and rely upon the local actions of DERs and other technologies. Campuses as microgrids, automated building management systems, and emerging distribution level market platforms all rely on devolution of grid control systems that empower local actors to provide value to system operations. More work is required to understand the evolving interoperability requirements associated with the devolution process.

3.4 Emerging Interoperability Requirements

Physical interactions with the grid now entail a dynamism governed by both the physical conversion of electrical energy into work, and the application for which that energy has been harnessed. The resultant feature-space from these physical interactions may — depending on the operational objectives — require development of new observational techniques or control strategies, which in turn could drive associated informational interoperability requirements.

Where interoperability has historically been considered an informational challenge [24], the unique physical interaction each device has with the electric grid (see **Section 3.2.2**) elevates the importance of physical interoperability alongside the conventional information-based aspects of interoperability. Emerging interactions between end-use devices and the grid — intended or otherwise — mean our understanding of physical interoperability must evolve to include functional aspects and be much more than the design of the physical connections.⁴⁸

⁴⁷ Traditionally defined as the transfer of power or authority from centralized government to local institutions, the term *devolution* is employed here to describe the emerging independence of localized control actions that affect device and system interactions with the power system.

⁴⁸ For example, socket and plug design.

3.4.1 *Requirements for metrology, observability, and controllability*

State awareness⁴⁹ is at the heart of grid operations. Whether through central operations or distributed local control, knowing the operating status and conditions of the grid and connected assets provides context for control actions and economic signals alike. This is true even for automated devices, where at a bare minimum knowledge of whether the grid is up or down and whether grid following or grid forming functions are needed is required for safe operations.

Measurement is a prerequisite for state awareness, and a fundamental requirement for optimizing any cyber physical system — the electric grid included. The measurement parameters must be properly designed to capture the physical phenomena of interest, which becomes more challenging as the physical interactions of devices with the grid become more dynamic and complex (see **Section 3.2.2**).

⁴⁹ Also called the “States” functional concern in CPS ontology, see **Appendix B** – Mapping CPS Aspects and Concerns to the Electrical Grid.

SMART METER ACCURACY

UNDER HIGH HARMONIC WAVEFORM LOADS

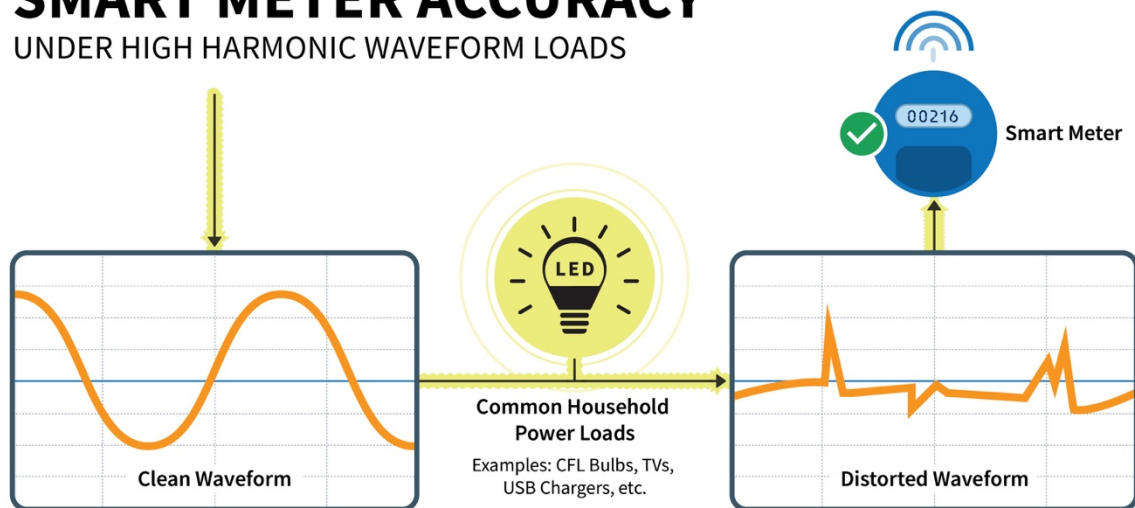


Figure 13 – Smart meter accuracy under high harmonic waveform loads

Perceptions that smart meters are grossly inaccurate have impeded progress towards achieving the benefits that could be realized with deployment. One 2016 study [129] stated that more than half of the smart meters evaluated had measurement errors near 500 percent, indicating the likelihood of overbilling. News media reports around the world cited the study[130-132], as have groups and individuals who oppose smart meter deployments [133, 134].

Many have drawn erroneous conclusions about smart meter accuracy because of this study, especially because the smart meters tested were not built to the latest standards. For example, U.S. smart meters must comply with the American National Standard for Electricity meters, ANSI C12.20-2015 [135], published in 2017. It “is the most ambitious and significant update to the standard since its inception in 1998,” stated NIST’s Shannon Edwards, Chair of ANSI C12 Subcommittee 16. It “addresses the challenges of metering in the 21st-century environment head-on,” as the standard includes harmonic waveform testing to ensure metering accuracy with distorted loads.

NIST subsequently developed a testbed to examine the effects of harmonic distortions on smart meter measurements, similar to those in the 2016 study [115]. NIST’s tests used eight U.S. smart meters manufactured since 2015 and in compliance with the ANSI standard. NIST’s tests showed meters designed to accommodate the harmonics described in the updated ANSI standard have very good accuracy,⁵⁰ thus proving that measurement accuracy can be achieved even for the most complex emerging system dynamics.

⁵⁰ Three meters showed variations only within the test uncertainty, or almost 0 percent error. Of the meters exhibiting measurable error, single meters exhibited maximum errors of -1 percent, -2 percent, and +2 percent, while two meters

Fortunately, the challenges posed by the emerging system and waveform complexity do not preclude proper measurement. The NIST research that produced the highly distorted waveforms in **Figure 10** and described in the text box above also demonstrated that smart meters designed to meet the ANSI C12.20-2015 accuracy requirements [135] were broadly able to do so (see **Figure 14**, [115]). It is clear that measurement accuracy is possible under even the harshest of conditions, but achieving the required accuracy requires an understanding of emerging system and waveform characteristics.

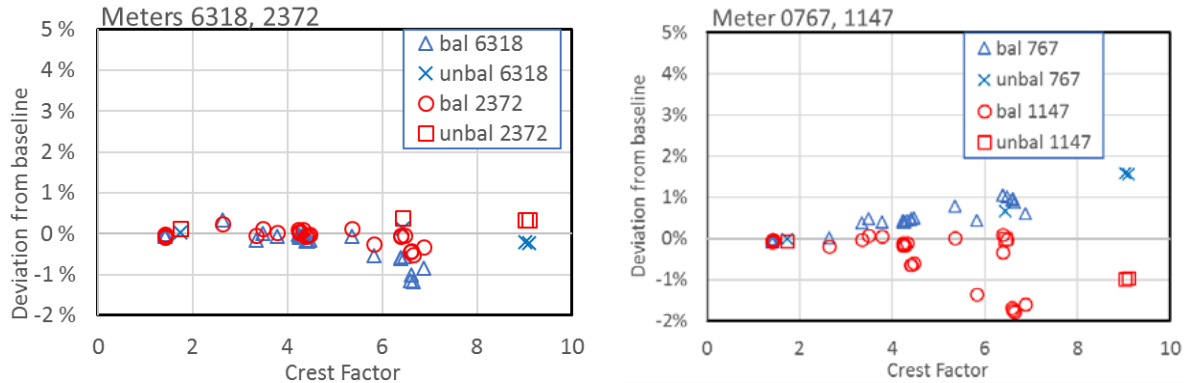


Figure 14 – Example smart meter measurement accuracies for highly distorted waveforms

But measurement alone does not yield observability, which is a prerequisite for state awareness. Observability is achieved through the coordinated and timely evaluation of diverse measurements across the system, a fundamentally different endeavor from making individual measurements. As described in **Section 2.3.2** and **Appendix B**, a number of system functional concerns must be addressed to achieve state awareness, including: sensing, measurability, communication, monitorability, and uncertainty, among others.

Well-designed requirements can yield measurability, observability, or other system capabilities. But the requirements associated with each concern are not constant across function, and evolve with physical and application context. For example, phasor measurement units (PMUs) typically measure line voltage 10,000 times or more per second, yet only report the phase data 30 to 60 times per second. This is because of the different sample rate requirements necessary for directly measuring electrical dynamics and that for observing much slower acting system dynamics and state changes.

Similar to the difference between temporal requirements for measurement and observability, the requirements for system control tend again to be orders of magnitude less stringent. This is especially so for centrally dispatched control signals, which tend to focus on timescales from minutes to hours.

exhibited maximum errors of +4 percent. No meter tested exhibited errors within two orders of magnitude of those found in the 2016 study.

Time requirements for measurement, observability, and control: A case study of oscillation damping in the Western Interconnect

As grid operations complexity has increased, questions have emerged over timing requirements for the system. Monitoring and control schemes derived for emerging grid applications and large geospatial areas have developed particularly stringent requirements for time awareness. The availability of satellite and network-based timing signals has led some to conclude that these accuracy requirements are easily achieved despite the technical challenges with doing so, and the introduction of communications standards premised on virtually unlimited bandwidth and minimal latencies (e.g., IEC 61850) compound this perception. But the difference in timing requirements for measurement, observability, and control applications are often misunderstood.

In 2017 NIST published a workshop report on Timing Challenges in the Smart Grid [136], in which expert consensus was developed around required time accuracy and precision for different applications and communication events in modern power systems (see **Figure 15**). Of note is that stated timing requirements for everything from measurement applications to communications events were all more stringent than a millisecond, with some requirements more than a thousand-fold more precise.

Application	Time Accuracy Requirement
Traveling Wave Fault Detection and Location	100 to 500 ns
Synchrometrology (synchrophasors) Wide Area Protection Frequency Event Detection Anti-Islanding Droop Control Wide Area Power Oscillation Damping (WAPOD)	Better than 1 μ s
Line Differential Relays	10 to 20 μ s
Sequence of Events Recording	50 μ s to ms
Digital Fault Recorder	1 ms
Communication Events	
Substation Local Area Networks (IEC 61850 GOOSE)	100 μ s to 1 ms
Substation Local Area Networks (IEC 61850 Sample Values)	1 μ s

Figure 15 – Wide area precision time requirements in power systems

Around the same time, researchers were conducting the first full-scale experiments on damping wide-area oscillations in the Western Interconnect of the U.S. grid. Using distributed PMU measurement data – which have timing accuracy requirements of 1 microsecond (10^6 Hz) for data acquisition – the scientists developed oscillation damping schemes [137] utilizing control signals which update at only 60Hz [138]. Further study on communications requirements for the same application indicated system damping could be achieved with latencies of up to 0.5 seconds [139].

This example – where timing accuracy and latency requirements span five orders of magnitude across measurement, observability, and control – demonstrates the importance of properly deriving requirements from both application and function. Additional research is required to fully characterize application- and function-specific timing requirements for power systems.

3.4.2 Trustworthiness

Trustworthiness in the grid is often viewed from a cybersecurity perspective. It is generally understood to be whether devices or systems can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats [140]. This information-driven understanding of trustworthiness is inadequate for the electric grid, where nested hierarchical architectures and control systems create an operational paradigm wherein it is impossible for each higher-layer grid system to validate the activity of each subordinate edge device that impacts its operations.

This is particularly important for the electric grid as edge devices, or field level nodes, continue to gain energy production and management capabilities. Field nodes can actively communicate with sibling nodes, and therefore develop coordinated actions that amplify the impact of control actions by individual field nodes on the superior system. This highlights the importance of developing a rigorous approach to operational trustworthiness.

This is why the aspects of a modern electrical grid described in **Section 2.3.2** highlight that trustworthiness for a cyber physical system includes physical security, reliability, and resilience in addition to the typical informational trustworthiness concerns. For the electric grid, the reliability and resilience concerns are critical to developing the interoperability requirements for lower level systems and edge devices. From **Appendix B – Mapping CPS Aspects and Concerns to the Electrical Grid**:

Trustworthiness → Reliability: Concerns related to the ability of the grid, or components within a grid, to deliver stable and predictable performance in expected conditions.

Trustworthiness → Resilience: Concerns related to the grid, or components within a grid, to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.

Were the CPS definition of trustworthiness achieved in the grid, the interoperability requirements for subordinate systems or nodes could be limited to initial operational status — likely determination upon connection — and subsequent status updates only when the operational state changes. If complete trustworthiness is achieved, field nodes might never require exposure to the system operator. This trusted ideal is in marked contrast to the input NIST received during a recent set of workshops, wherein some participants emphasized that utilities may need to continuously monitor all DERs on a system — including those contained within customer-owned microgrids — to ensure the utility can manage contingency operations [97].

The reality of operational trustworthiness will likely fall somewhere in between the full-trust and zero-trust options described above. Trustworthiness of a device or system node, and the related effects interactions among many nodes will have on operational trustworthiness for

the system, must be better characterized before interoperability requirements can be properly established.

Testing and certification are mechanisms to improve trustworthiness across the system. For a detailed discussion on these issues, please see **Section 6 – Testing and Certification**.

3.5 Interoperability for Customer Empowerment

The future grid will benefit from — and require — innovation spanning all domains. As noted in **Section 3.3.1**, resource flexibility, power electronics, distributed intelligence, and adaptive protection are all necessary for future utility control schemes. These and other technical innovations will also profoundly impact the customer, as new capabilities will enable the motivated customer to realize substantial benefits from new interactions with the grid.

But the many benefits illustrated in **Figure 3** cannot all be achieved through technology alone. Indeed, most of the benefits can accrue only after the customer becomes engaged with physical, information, or market systems outside the home, and these benefits accrue more rapidly as interoperability increases. Three primary ways customers and grid operations benefit from interoperability include [95]:

Breaking asset specificity: Consumer devices are often packed with extra capabilities in an effort to improve convenience or enjoyment. Interoperability allows harnessing of these extra capabilities to improve energy operations. For example, a thermostat's sole function is to control the temperature in a building. Remote access was added for customer convenience, and interoperability across organization and platform now allows thermostats to be enrolled in numerous energy management schemes allowing customers and utilities to co-optimize their comfort, infrastructure, and operational priorities.

Market access: Barriers to market entry have historically been large in the electricity space, where wholesale market entry required asset scales not typically achieved at the customer level. Interoperability decreases integration costs and enables asset aggregation, which expands market access for customers and the pool of market resources for utilities to utilize. Aggregation may also improve the bargaining position of customer-sited assets vis-à-vis other stakeholder groups, thereby improving profitability.

Reduce transaction costs: Full interoperability largely eliminates the cost of executing a transaction. The result is that small-scale transactions executed by or among customers can be utilized to optimize their engagement with the system.

Importantly, combining interoperability benefits creates a virtuous cycle wherein opportunity grows with additional capability. For example, using interoperability to break the asset specificity of a thermostat allows customers to enroll in utility managed direct load control or demand response programs. Using interoperability to facilitate market access through

aggregation allows customer-sited thermostatically controlled demand response resources to bid into wholesale electricity markets in addition to engaging utility direct load control programs.

By stacking interoperability benefits as described above the customer is able to pursue the best value opportunity. Doing so not only ensures optimal return on the customer's investment, but also ensures customer resources contribute to addressing the most important system needs.⁵¹

Reducing transaction costs allows for smaller and more frequent transactions, which will allow development of new market structures to enable optimization at the system edge where utility control schemes typically have little — if any — visibility or control. The benefits of this are not yet fully understood, but could be significant given that substantial efficiency and economic benefits have been realized in electricity systems even when market transactions are used to optimize only a small percentage of system generation [141].

3.6 Future Work

In general, the role, benefits, and beneficiaries of interoperability require further study and elucidation. Characterization of the ancillary benefits from interoperability investments that cross system and domain boundaries is a particular need.

Interoperability requirements and metrics should derive explicitly from the physical requirements and constraints of specific applications and interfaces. In some instances, this may require transitioning away from interface abstraction and towards establishing specific interoperability profiles that describe a constrained set of implementation options. For a deeper exploration of this issue, please see **Section 6**.

The relationship between interoperability and the changing physics introduced by semiconductor technologies and new system configurations requires deeper understanding. Interoperability requirements could derive from the need to measure and/or observe phenomena that are not currently considered during conventional grid operations, and also the need for automated or dispatched control to manage the system effects.

Emerging interfaces between DC and AC systems in the smart grid should be factored into research to expand our understanding of system optimization and control theory. The industry would benefit from developing some standards around DC systems and microgrids and their interfaces with the broader AC grid, while taking care to avoid unnecessary or over-specification.

As active control pushes towards the system edge and sibling field nodes communicate and coordinate activity, emergent behavior issues as well as the relationship between bulk-level market signals and local operations need study. Clarifying the relationship of interoperability to control strategies that can manage these potential behaviors would be beneficial.

⁵¹ This assumes economic incentives are properly aligned with system need.

Key Messages – Economics

Interoperability is key to the economics of the future grid. The traditional means of ratemaking and cost recovery are under strain as growth in distributed energy resources and changing customer capabilities alter traditional economic dependencies.

Reducing information asymmetry through interoperability helps ensure the technical and economic benefits from grid modernization flow across smart grid participants and accrue to all stakeholder classes. Interoperability is therefore a critical enabler of customer empowerment and value creation.

Interoperability can minimize transaction costs and entry barriers to market participation, thereby facilitating the creation of new participatory and economic opportunities across the system and enabling customer choice as they seek to integrate their equipment into the system's value network.

Interoperability reduces limitations caused by asset specificity, and in this way facilitates combinatorial innovation and value stacking which can improve stakeholder value propositions across the sector.

4 Economics

The electric grid exists to serve the energy needs of a dynamic economy. The growth of the sector over the last century and the success of its stakeholders in realizing improvements while operating continuously are evidence of the system's efficacy. Electrons are incredibly high-quality energy carriers that can be used for any application. The breadth of this applicability contributes to the sector's capacity for value creation and broad attractiveness. As households and firms have responded strategically to energy related incentives and the economy has oriented itself around the electric grid, this infrastructure is increasingly critical to the continuity and growth of modern civilization.

The inseparable linkage between electric infrastructure and economic growth does not mean the relationship must remain unaltered. Technology, policy, and stakeholder expectations each affect the strategies by which the system is optimized, and the economics of value creation. Increasing interoperability will enable changes toward more cooperative and collaborative operating strategies for the electric power sector at a time when society expects and needs it to contend with all hazards while delivering on myriad new value propositions.

The challenges confronting the electric grid are manifold. With new problems comes the inevitable call for new problem-solving capacity. This combination of challenges and

solutions adds complexity to the power system discussed throughout this Framework. Acknowledging that “every increase in complexity has a cost” [142], this chapter presents a discussion of the central role for interoperability in ameliorating such costs and adding new value to the system. Through improving interoperability, the core mission of serving the energy needs of a diverse and dynamic set of customers will be ever-more achievable.

4.1 Economics of the Conventional Utility

4.1.1 *Functions of electric utilities*

The electric industry in the United States is both highly diverse and highly fragmented. It consists of a mix of entities, ranging from heavily-regulated utilities whose profitability and system investments are determined through public hearings and dockets with utility commissions, to those which operate competitively in deregulated markets. Utilities include investor-owned utilities, quasi-governmental entities, municipalities, and cooperatives. In total there are more than 3,000 utilities spread across the 50 states. Some are regulated by state or federal regulatory commissions. Others are overseen by government entities, or in the case of cooperatives managed as not-for-profit entities for their members by their governing boards.

In addition to utilities, there are numerous companies that participate in the competitive generation sector, either as their core business or, in the case of co-generators, as a byproduct of their core business activities. The emergence of DERs which may be owned by utilities, competitive or collective entities, or individuals — and also the incorporation of demand response resources into conventional energy markets — complicates the supply-side economics. Finally, there are competitive electric service providers that serve as intermediaries between customers and markets, providing energy services to customers or as aggregators of loads and/or services to markets.

The function of any given utility typically includes three services: generation, transmission, and distribution. In states that have restructured, the investor-owned utility has sold off its generation assets to a third-party owner, and the transmission system is operated by a Regional Transmission Operator (RTO) or Independent System Operator (ISO). Additionally, those states may also allow customers to choose a competitive supplier to provide their electricity needs, which leaves the monopoly as the “poles and wires” company responsible for distributing the electricity to end use customers.

In other states, vertically integrated utilities, which own generation, transmission, and distribution assets, operate as regulated monopoly providers of electricity to end-use customers. Some vertically integrated utilities are in organized wholesale markets, operated by an ISO or RTO, and others operate in less structured markets.

While this portrayal of the industry as complex and fragmented is accurate, there is also a high level of consistency in the value provided by each group based upon the overall role that they play within the industry. The Smart Grid Conceptual Model is useful in defining this

core set of industry roles, and is described further in **Appendix D – The Core Set of Electric Industry Roles**.

4.1.2 Cost structures

Utility costs are typically differentiated between capital and operating and maintenance (O&M) costs. In general, capital costs earn a higher return on equity (ROE) than O&M costs [143]. The ROE is set by the regulator during the rate case or during a separate cost of capital proceeding. Examples of capital costs include construction of new infrastructure, like a power plant, transmission line, or substation. Examples of O&M costs include maintenance costs for power lines, operational efficiencies, or utilization of software as a service or cloud-based services.

Due to this structure, utilities earn more profit via capital projects than O&M projects, which impacts utility investment strategies. This becomes important when considering interoperability, as it may be competing against a capital project which earns a higher ROE.

Costs are also treated as either long-term and variable, or short-term and fixed. Costs that are treated as variable are recovered through the variable component of the rate and recovered through volumetric charges. Treating certain costs as fixed allows the utility to have greater certainty in recovery of those costs, as the regulator considers costs associated with those investments as necessary for service provision. This has a significant impact on the rate design and bills as a high fixed charge, while providing the utility greater certainty on the recovery of its authorized revenue requirement. This means fewer costs are recovered in the variable rate. When variable rate cost recovery diminishes per this relationship, the price signal to customers is muted and limits the ability of the customer to invest in technologies to lower their bills.

4.1.3 Ratemaking

Review of utility costs is traditionally based on least cost ratemaking. This means that the utility is to spend the least amount of money needed to provide safe and reliable electricity service, plus a rate of return (i.e., profit). As the utility industry grew, the ability of the utility to scale large assets was a preferred means of meeting utility service obligations, and so large capital investments were regularly considered least-cost.

Additionally, the early models of utility economics focused on the societal goods of expanding access and increasing electricity use. This meant that, by expanding the rate base, utilities could recover their costs across more kilowatt hours and provide sufficient electricity to an expanding set of customers.

Because utilities generate revenue through electricity sales, they are incentivized to sell more electrons. During the 1970's, however, some states began experimenting with a different way of setting rates via a mechanism called decoupling. Decoupling is a means by which a utility's revenue requirement and profit is not driven by sales, but by the authorized revenue requirement set by the regulator. In other words, the utility is guaranteed to recover its

authorized revenue requirement regardless of how much (or how little) electricity the utility sells. Decoupling allows utilities to maintain profitability even while encouraging lower consumption, for example through improving customer efficiency. However, decoupling does not address the profit incentive towards increasing capital expenditures.

This discussion of utility cost structures and ratemaking is intended to provide high-level economic context for the examination of interoperability costs, benefits, and value that follows. Additional information on ratemaking, cost recovery, and rate design is found in **Appendix E – Cost Recovery, Rate Design, and Regulation**.

4.2 Evolution of the Distribution Utility

The electricity network exists to provide customers with access to electricity to power their lives and industry. As described in the Operations section of the Framework (**Section 3**), the integration of modern technologies and resources means the electricity system is embarking on a substantial evolution towards a two-way delivery system with the capability of relying on local resources to meet system needs. This will result in the distribution utility taking on additional roles that it has not fulfilled in the past, including more detailed modeling of the distribution system, customer demand, and optimization and utilization of resources located either at the customer site or close thereto.

4.2.1 Changes to utility organizational structure

Distribution utility operations are changing with increasing DER adoption. Whereas in the past the distribution system delivered electricity to end use customers, the distribution grid must now be organized and operated to handle two-way electricity flows. The emerging power flow complexity hints at an underlying transition in domain function and actor role. Where distribution utilities were built to service customers who were purely consumers of electricity, utilities may now be the recipients of services provided by customers, or even the facilitator of the exchange of services between customers.

Just as two-way electricity flows complicate system operations, system economics become similarly more challenging. Where utility cost recovery has historically been manageable through simple tariff structures consisting of energy and demand charges (see **Appendix E**), the economics of cost recovery will have to change as technology allows customers to self-supply energy or locally develop and exchange services.

Evidence has also emerged in recent years of an ongoing disruption of the historic linkage between energy consumption and economic growth. Although absolute electricity consumption continues to rise across the country (see **Figure 16**),⁵² the decoupling of economic and societal outputs from energy consumption has yielded a flattening (and even a decline) of per-capita electricity consumption across the country [144]. The effect on account-level consumption has been stark, with average customer consumption in 39 states

⁵² Analysis of Energy Information Administration form 861M data indicates that absolute electricity consumption has risen in 49 of 50 U.S. states

and the District of Columbia — representing nearly 80 percent of electricity demand in the United States — declining since 2010 (see **Figure 16**).⁵³ This dynamic of declining per-customer consumption has eroded the reliability of the sector’s historical cost-recovery approach and raised concerns over optimal utility function [145] and tariff structures [146] for the future.

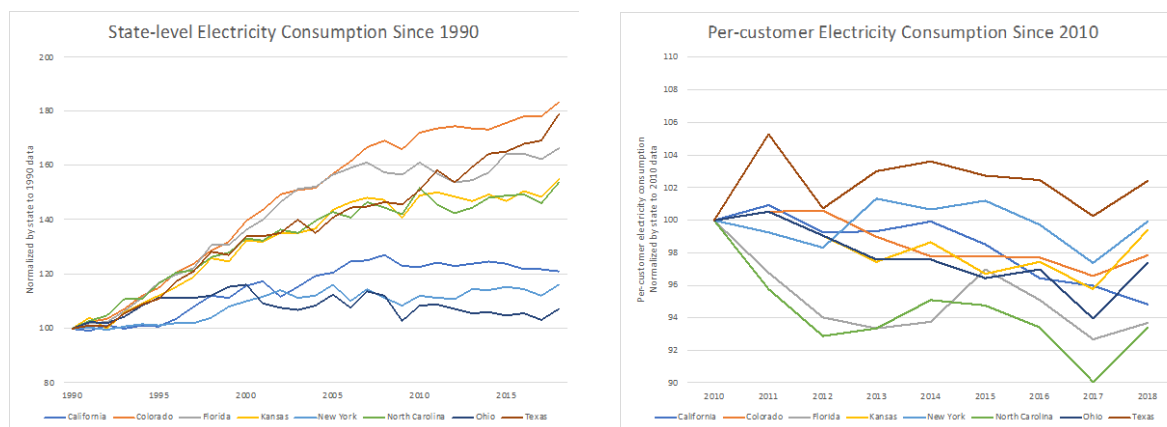


Figure 16 – State-level absolute and per-customer electricity consumption trends

There are many ways to describe the future organizational and operational structures of the electric utility, but a commonly used term is that of the distribution system operator (DSO) [77]. Although some might correlate the DSO terminology to the introduction of independent market operators to the distribution system, this need not be the case. In this report — as elsewhere [147] — the term DSO is used to describe a system where utility functions will necessarily expand beyond those conventionally provided by the historic utility.

No single business model or market function is implied through our use of the DSO term. Yet as has been described throughout this Framework, the DSO must provide some additional capabilities which allow the system to utilize and optimize resources other than those owned by monopoly utilities in servicing customers and other market participants. This, in turn, impacts the utility business model.

4.2.2 Performance-based regulation

As the utility business model evolves, so too must the mechanisms by which utilities recover costs. One approach is to move to a performance-based ratemaking scheme. This type of regime provides utilities with additional revenue for achieving certain performance metrics, such as enhanced reliability, faster integration of DERs, or customer satisfaction rates. This type of cost-recovery is intended to offset the capital bias inherent in cost-of-service ratemaking (see **Appendix E – Cost Recovery, Rate Design, and Regulation**).

⁵³ Per customer electricity consumption in 2018 was lower than in 2010 for AK, AL, AR, AZ, CA, CO, CT, DC, DE, FL, GA, HI, ID, IL, IN, KS, KY, MA, MD, MI, MN, MO, MS, MT, NC, NE, NH, NJ, NY, OH, PA, RI, SC, TN, UT, VA, VT, WA, WI, and WY, representing 78.5% of national electricity demand.

4.2.3 *Economics of changing operations*

While the physical aspects of changing utility operations are discussed extensively in **Section 3**, the relationship between the economics and physical operation of a system with expanding capabilities warrants examination. With expanding distribution utility functionality, modernizing business models, and DER proliferation, the mechanisms used to ensure optimal deployment of grid resources can be expected to change.

For example, in California the distribution resource planning process includes analyses, by line segment, of the hosting capacity as well as the value of DER on the grid at that location. Distributed resources, including demand response and non-wires alternatives, can therefore be sited in specific locations where it can be expected to provide greater optimization of the grid as a whole. More broadly, through incorporation of economic signals linked to spatial, temporal, and topological optimization constraints, incentives will exist to locate and utilize DER where it provides the greatest value to the grid — including to customers.

Developing economic mechanisms to optimize DER deployment and utilization will likely increase overall asset utilization, and create a virtuous cycle where legacy infrastructure can be maintained for a longer service life. For example, deployment of demand response and/or energy storage resources may prove to be a more economical solution to alleviate an overcapacity constraint on a feeder or substation — as opposed to a more traditional approach of rebuilding infrastructure to increase capacity. These non-wires alternatives are regularly employed as alternatives to distribution system construction investments [148]. Placing resources closer to the load they serve can additionally be expected to reduce overall cost and physical energy losses of delivering energy to customers.

Identifying locational net values for DER, including possible development of locational marginal pricing and distribution-level energy markets for energy and other grid supporting services, can be expected to effectively flatten the load, increase the utilization of existing assets, and broaden the participation in energy market or optimization services. Participation would expand directly through individual DER ownership, and indirectly with the participation of aggregators and energy service providers.

The same distribution-level incentives can help ensure all market participants are equitably compensated for the energy and services they provide while ensuring physical compatibility of the DER with local operating considerations. This is an especially important consideration as customers connected to the distribution system gain access to wholesale markets⁵⁴ and are presented with an ever-increasing range of energy investments⁵⁵ that offer the potential for economic value previously unavailable to them and independent of the local utility.

A discussion of some specific utility organizational and operational structures is found in **Appendix F – Distribution Platforms and Markets**.

⁵⁴ For example, through FERC Order No. 2222.

⁵⁵ For example, community solar or storage projects, energy management systems, demand response programs, or customer owned and sited DER technologies ranging from solar panels to electric vehicles and home energy management tools.

4.3 Factors Affecting — and Benefits From — Interoperability

The electric power sector stands on the precipice of a period of great “combinatorial innovation” just as expectations of and within the industry are changing rapidly.⁵⁶ Increasing technical and organizational modularity within the sector have opened opportunities for innovation by incumbents and new entrants. Recent developments are consistent with past historical experiences in which a “set of technologies comes along that offers a rich set of components that can be combined and recombined to create new products” [150]. Modular and distributed energy resources, coupled with entrepreneurial capabilities and encouraged by an awakening customer base, promise to remake the structure of electricity markets and value creation.

The current influx of information and communications technology (ICT) to the electric grid has brought with it organizational perspectives and processes for the accelerated development and deployment of new technologies. Other sectors extensively impacted by ICT exhibit rapid rates of technological adoption, one of the major drivers of which has been a relaxing of the requirement for detailed modeling and analysis prior to technology adoption [151]. While electric utilities cannot forgo the economic analysis to justify equipment expenditures or the detailed examination of operational models prior to technology adoption, customers accustomed to the ICT-enabled conveniences of digital service offerings available in other sectors have formed new expectations about the electric services they consume.

Electric utilities face significant uncertainty with respect to their future operating environment (see **Section 3**). Managers (and regulators) are therefore concerned with the pursuit of no-regrets moves that will pay off regardless of how the uncertainty is ultimately resolved. Cost-cutting initiatives are prototypical examples of such regret-free strategies [152]. One important source of uncertainty in the electric power sector has to do with the cost of integrating new technology with the legacy grid and ensuring interoperability.

Uncertainty over integration costs may provide an impetus for investment in smart grid research, development, and deployment activities as firms seek to uncover actual cost structures through exploratory efforts. However, a lack of consensus regarding which standards are most important for interoperability — or even how to select requirements to achieve interoperability through existing standards (see **Section 6**) — may constrain the set of no-regrets moves and constitute a barrier to investment in distributed energy resources and other emerging technologies. In the near term, as system integration is pursued in an ad hoc manner, a high-degree of solution specificity is to be expected.

⁵⁶ Invention entails the integration of existing concepts, devices, and systems to deliver new capabilities. The rate of invention reflects the readiness of ease with which these parts can form new and useful amalgams. Combinatorial innovation occurs when a diverse collection of components becomes ripe for synthesis, and market actors rapidly succeed at creating and improving many and varied value propositions through the novel recombination of these parts [149]. Greater interoperability should catalyze combinatorial innovation within the electric power sector.

4.3.1 *Interoperability and specificity*

The complexity of the electric power sector value chain is increasing with the proliferation of specific solution implementations for a range of new operational challenges, especially DER and customer-owned asset integration. Asset specificity often results from efforts to meet technical or regulatory requirements and meaningfully contribute to the value chain. Increasing specificity leads directly to rising transaction costs as the technology stack supporting transactions becomes more diverse and complicated to maintain. Specificity may then act as a barrier to more extensive utilization of devices and systems.

Interoperability offers a strategy set through which to reduce “specificity barriers” and engender an environment conducive to combinatorial innovation by all stakeholders. Highly specific solutions to electric grid challenges are present on both the demand and supply sides of electricity markets. Consequently, interoperability strategies can improve stakeholder value propositions across the sector.

4.3.2 *Interoperability and customer empowerment*

On the demand side of electricity economics, interoperability is crucial to customer empowerment. A variety of concerns affect customer opportunity in the legacy grid, among which interoperability can help address:

Information asymmetry: Enhancements to interoperability should reduce informational imperfections that can afflict electricity markets and manifest as pricing conditions that favor producers — who may have an informational advantage — over consumers or third-party service providers [95]. Interoperability enhancements should reduce information asymmetry and better inform customers about their own electricity-use decisions and technological investments. This in turn should allow for improved economic return on these actions and likely improve technology adoption outcomes.

Value stacking: Customer assets that often sit idle due to lack of outside options for application could be matched with new opportunities as interoperability increases and barriers to providing grid services fall. Capacity utilization and thus the value proposition of economically efficient customer assets⁵⁷ will generally increase with the level of interoperability that exists between those assets and the rest of the electric grid.⁵⁸

⁵⁷ Unlike merchant generators or utility-owned grid equipment, customers generally purchase assets primarily for priorities or to provide functions other than grid services. With overnight capital allocations justified for other purposes and fuel costs generally negligible for distributed renewable and demand response resources, customer assets may have very low marginal costs and can often generate value at modest grid services pricing.

⁵⁸ Some assets that are no longer efficient when opened to competition from newly interoperable grid resources will be dispatched with decreasing frequency. The nature of this compositional shift in grid value networks will be determined by the details and dynamics of interoperability investment.

Customer choice: Interoperability improvements can reduce barriers to entry and transaction costs paid by customers as they seek to integrate their equipment into the sector's value network. Absent an environment that allows universal access to the full range of opportunities, customers may be required to select devices and systems for feasibility of integration rather than the operational or economic value propositions they offer.

4.3.3 *Complexity and cost structures*

The electric power sector is confronting a complexity problem. Operational fragmentation and increasing specificity of assets means the process of producing and delivering electricity to customers has more — and more varied — stakeholders than ever. Regulatory status varies across the value chain, and coordinating value-adding activities in a manner that is consistent with customer expectations and regulatory requirements is costly. In many cases, it simply costs too much to make the fragments of the grid interoperate effectively. This lack of interoperability is the primary barrier of consequence to realizing the potential for combinatorial innovation in the electric power sector.

Interoperability investments will reduce, though not eliminate, some barriers to sectoral entry. Though some incumbents may be slow to embrace interoperability,⁵⁹ support for greater standardization in pursuit of lower interoperating (transaction) costs is expected as the benefits become manifest.

As interoperability improves and entry barriers are reduced, more participants are likely to enter the sector, which may bring additional capital investment resources to the electric grid. This is especially important as investment requirements for the grid are expected to rise substantially in the coming decades [153]. Interoperability improvements may therefore relax two important binding constraints⁶⁰ on the electric grid: the constraint on capital available for investment, and the feasible set of investment opportunities for smart grid assets.

As an attribute of the electric grid, interoperability is challenging to achieve because it places requirements on the systems and components of multiple organizations which have to coordinate strategies while remaining in compliance with antitrust law. Institutions and mechanisms that make such coordination less costly and more dynamic will prove valuable to electric grid stakeholders. However, organizations investing in smart grid technologies need mechanisms to provide assurance that their equipment is fit for purpose and will work as intended and expected. Interoperability testing and certification programs will need to fill the role of such mechanisms (see **Section 6** – Testing and Certification).

⁵⁹ Numerous factors affect the maturation of interoperability strategies across the sector. To the extent that integration costs are considered capital expenditures, utilities face perverse incentives to avoid minimizing integration outlays that increase the rate base.

⁶⁰ A third important constraint is the regulatory construct which, at times, prevents grid investment. While non-utility investments may reduce customer costs, the relationships between these and regulated investments requires clarification.

Creating value through data interoperability

Consumers are benefiting from the emergence of new service providers offering innovative services from energy savings to clean power installation. The lack of consistent data access strategies, however, fragments customers of the nation's 3000+ electric utilities into smaller markets. This increases transaction costs for accessing data and creates information asymmetries between utilities and external companies. Each of these challenges can lead to market failures that undermine business models and limit the emergence of new energy services. On the other hand, data interoperability reduces complexity, lowers development and operating costs, and increases the size of accessible markets for service providers. Interoperability therefore enables a vibrant marketplace of new firms offering innovative value propositions.

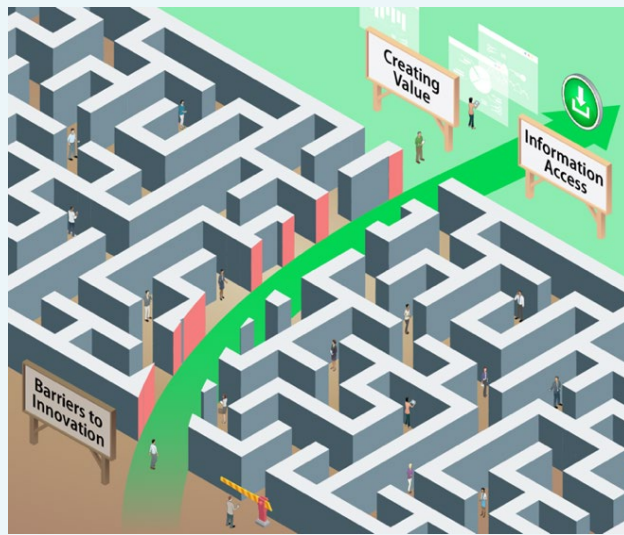


Figure 17 – Data standardization stimulates

Several communities have pursued standards-based data access policies to stimulate the creation of new energy services for their residents. The City of Fort Collins, Colorado has partnered with UtilityAPI to offer customers the option of securely and efficiently sharing their data through the Green Button Connect interoperability and access framework [154]. To date, 16 organizations have aligned their data processes with City requirements to offer new customer services [155]. A similar directory for Silicon Valley Clean Energy, which also uses standards-based data access solutions, lists 92 firms [156]. And in 2017 Pacific Gas and Electric Company began a pilot program in which customers could grant third-party service providers access to standardized meter data in exchange for guidance on energy savings opportunities [157]. This small pilot has already saved customers more than 50 million kilowatt-hours [158].

Consistent and standardized data access can also increase customer compensation for their participation in demand response or virtual power plant services. OhmConnect, which aggregates customers and bids their demand reductions into wholesale markets, has stated in regulatory filings that the company has higher marketing and management costs — and lower customer benefits — in utility territories that lack standardized data access programs [159]. Logical Buildings, a third-party aggregator in New York, leverages access to standardized smart meter data in its GridRewards program to inform the compensation customers receive for reducing electricity consumption during utility event days [160, 161].

Open data access lowers barriers to entrepreneurship and facilitates competition that empowers customers through greater choice. The value of standardized data access can accrue broadly across stakeholders, although implementation variability that reduces interoperability dissipates these benefits. The value of standardized data access would be maximized for all parties through development of certification programs for standards conformance that could better ensure commonality across implementations and service territories (see **Section 6**).

4.3.4 *Trust and assurance*

Realizing an interoperable grid to enable growth in valuable services requires surmounting numerous challenges. Stakeholders must be able to trust that the electric grid on which modern society is built will continue to be reliable; such trust can be built on assurance. One working definition of assurance is “our estimate of the likelihood that a system will fail in a particular way” [162], which falls within the CPS trustworthiness concerns of reliability and resilience described in **Section 3.4.2** and **Appendix B – Mapping CPS Aspects and Concerns to the Electrical Grid**.

Previous trustworthiness discussions in this Framework focused on the effects operational trustworthiness would have on informational — and thus interoperability — requirements. Here, trust and assurance are examined from the perspective of the risk that components or systems will not be able to interoperate. Assurances that reduce the expected costs of integration improve the value proposition of investment options, encouraging more rapid and extensive technological adoption.

The interoperability assurances needed to accelerate adoption of smart grid technologies vary with the specific technology considered and the stakeholders in whom trust must be cultivated. There will always be costs associated with obtaining this assurance, although systematic approaches to achieving desirable assurances will prove more cost effective than ad hoc alternatives. The gap between these approaches will likely widen over time as interoperability strategies mature and evaluative organizations learn by doing.

Some might worry that movement towards standards will diminish product and service differentiation or limit innovation. Yet vendors can in fact differentiate their products and earn increased markups over marginal costs on products for which they can supply the necessary interoperability assurances to address their customers integration challenges. Implementers might willingly trade ballooning integration cost structures for set testing and certification costs.

Integration costs place an upper bound on an organizations’ willingness to pay for the testing and certification programs designed to obviate implementation barriers.⁶¹ Electric sector organizations can choose to opt in to employing assurance mechanisms that demonstrably reduce integration costs relative to in-house approaches. As the cost of systems integration rises with complexity, the opportunity for assurance mechanisms to create value will improve. As only about one in five smart grid interoperability standards currently has an independent testing and certification program [103], entry into this space is needed (see **Section 6 – Testing and Certification**).

⁶¹ As described in **Section 3.1.1**, the costs to utilities and equipment manufacturers for integrating non-interoperable equipment ranges from \$140 million to \$1 billion per year per firm.

4.3.5 Testing and certification

Stakeholders across the electric power sector can generally agree that greater assurances with respect to equipment and system performance are needed [28], yet it is unclear how to share the burden — and benefits — of overcoming interoperability challenges. Testing and certification programs can reduce barriers to interoperability. Identifying and mitigating the barriers to these efforts is a necessary step towards achieving this goal.

The fixed costs associated with developing a testing and certification program can be considerable. Markets for specific testing and certification services must be sufficiently large to induce entry by testing and certification organizations. However, the electric power sector's high levels of specificity and complexity have yielded a large enough number of interoperability relevant standards that the certification market for each is relatively thin. Thus, developing testing and certification programs remains relatively unlikely.

Two approaches to increasing the availability of testing and certification services include reducing complexity of implementation and diminishing the barriers to entry. The development of interoperability profiles can help accelerate development of the testing and certification programs through reducing implementation complexity (see **Section 6.5.1**). An interoperability profile can define a subset of a given standard or set of standards on which stakeholders have agreed to focus their efforts. The crucial tradeoff in this approach is one that reduces degrees of freedom in implementation for decreased integration cost.

Another approach to increasing the availability of testing and certification programs is to develop affordable tools such as test harnesses⁶² that can be employed by stakeholders to troubleshoot common implementation problems. This can free testing and certification organizations to focus their efforts on the most vexing system integration problems facing the sector.

4.4 Economics and Challenges of Certification Institutions

Achieving high levels of interoperability can be very costly.⁶³ That interoperability is difficult to quantify (see **Section 1.2.1**) does not mean it is unachievable, but rather calls for advances in the sector's measurement capabilities. And while interoperability can be hard to measure directly, the concepts of increasing transaction and integration costs are far more tangible. A low level of interoperability is prevalent in the market for smart grid solutions in part because utilities and other implementing stakeholders have a limited ability to discern between high and low interoperability options before they undertake systems integration efforts. This means that vendors are incompletely compensated for engaging in costly efforts that could improve the interoperability of their products.

⁶² Open-source test harnesses were identified as important interoperability enablers during NIST workshops [28]

⁶³ High levels of interoperability are required for the maintenance and ongoing integration of old and new systems across the grid, as well as for the delivery of new services. Interoperability in electrical systems typically derives from extensive systems integration work that entails trial and error, learning by doing, uncertainty, and unpredictability. The strategic and context specific nature of these efforts implies that lessons learned are generally incompletely communicated between stakeholders, increasing the likelihood for costly duplication of work.

A situation in which buyers, suppliers, and regulators lack all the information necessary to make an informed decision is known as imperfect information. Furthermore, as vendors and implementors likely possess different amounts of information regarding the ultimate quality and value of a system to be integrated, information asymmetry also afflicts the market for smart grid solutions. Both of these informational problems have a chilling effect on investment — especially in regulated commodity environments — that can hinder grid modernization.⁶⁴

While smart grid investments are demonstrably capable of providing operational benefits to electric grid stakeholders, uncertainty and costly systems integration efforts are dissipating an unacceptable portion of the potential gains. Testing and certification programs “mostly exist in order to deal with failures caused by asymmetric information” [164]. They can help quantify the interoperability of prospective solutions, informing stakeholders of relative costs, reducing uncertainty, and rewarding vendors that work to reduce systems integration costs with additional business. Firms that are unable or unwilling to pursue strategies that meet implementers needs for lower integration costs through greater interoperability will encounter a competitive disadvantage as these costs are brought into the light. In the long run, the informational improvements offered by third-party testing and certification programs will reduce the influence of actors whose lack of interoperability dissipates value [165].

While third-party testing and certification programs are not silver-bullet solutions for improving interoperability, thoughtful design and expansion of such institutions will be net-beneficial to grid modernization. Past experience argues for the presence of five features that support reliable third-party certification programs: consumer demand, brand competition, interdependence, concentration of market power, and consumer vigilance [166]. These prerequisites are largely satisfied in the market for smart grid interoperability testing and certification services. However, efforts to improve outcomes may want to focus on areas where these prerequisites are not always met in full.

The following discussion explores a number of challenges that testing and certification programs must overcome to remedy information asymmetry, and reasons that these potential pitfalls should ultimately prove surmountable.

4.4.1 Challenge: consumer demand

Grid modernization will require massive expenditures by thousands of utilities and a rising group of service providers. Therefore, there will likely be sufficient consumer (in this case, utility and service provider) demand for third-party certification of the many systems that are envisioned to constitute the smart grid of tomorrow. The need for these services should induce entry into the certification market, especially if certification becomes either a regulatory or procurement requirement.

⁶⁴ An example of investment constrained by imperfect information or information asymmetries are the numerous rejections by state regulators of utility applications for deploying smart meters [163].

4.4.2 Challenge: interdependence and accountability

Market spoilage can occur when poor quality products or services persist long enough to affect customer value perception. In a testing and certification environment, certifications that do not adequately guarantee interoperability can affect not only the reputation of the certification agency, but left unchecked could damage the opportunities for competing firms as customer expectations decline.

The nature of ensuring interoperability between diverse systems means testing and certification programs most likely enjoy a sufficient degree of interdependence to hold each other accountable for poor performance. If the certifications provided by one firm prove unreliable to others in the process of providing upstream or downstream certification, these third-party certifiers will have an incentive to discipline the bad actors.

4.4.3 Challenge: concentration of market power

Large numbers of firms acting in diverse regulatory and economic regimes raise the expense and complexity for achieving accountability, regardless of the objectives [167]. While many firms operate in the electric power sector, market power can be concentrated for certain functions. For testing and certification, the concentration of market power within a relatively few organizations makes enforcement of the above described discipline necessary to achieve accountability less costly and more credible.

4.4.4 Challenge: consumer vigilance

The critical nature of the business of electric utilities virtually assures the customer vigilance necessary to make testing and certification programs successful. If poor certification services are responsible for electric service outages, utilities will find out and action will be taken to prevent further interruption to a sector that is a fundamental input to the modern economy and is substantially compensated based upon service reliability. Any third-party testing and certification programs that develop a reputation for failing stakeholders will undoubtedly be eliminated by market forces.

4.5 Interoperability Benefits

Grid modernization benefits will be substantial and sweeping. Interoperability is foundational to ensuring that new technologies can be cost-effectively integrated with the legacy system. It is also foundational to ensuring that diverse, distributed, and decentralized stakeholder groups can realize the anticipated benefit streams of grid modernization.

4.5.1 Minimizing transaction costs

Transaction costs are the costs of running an economic system, and high transaction costs are known to impede or completely block the formation of markets [168]. The ongoing rise of modular and distributed generation and delivery technologies has brought with it an emphasis

on employing aggregates and composites of these systems for integration with the electric power system. One consequence of this modularity and combinatorial innovation is that transaction costs increasingly constitute system level production costs. Greater interoperability will drive down transaction costs for the electric power sector, thereby allowing the creation of new market opportunities to obtain value for system stakeholders.

Improvements to technical and organizational interoperability will enable the dynamic assembly and reconfiguration of optimal value chains in accordance with changing conditions, opportunities, and threats to operation. The subsequent increase in available options and improvement in flexibility will drive efficiency gains in the dispatch of generation, transmission, and distribution segment assets in service of customer needs.

Interoperability will place downward pressure on information, integration, coordination, and transaction costs, opening up new value propositions. Some resource pairings for which coordination would presently prove uneconomic will — through greater interoperability and improved cost structures — be able to serve customers more frequently, leading to higher capacity utilization. Rising trading volume in services provided between increasingly interoperable nodes of the grid can fortify thin markets and provide liquidity that is attractive to other potential market participants. The presence of a virtuous cycle between new entry and market liquidity may further accelerate grid modernization.

The fall in transaction costs will lead less efficient combinations of resources to be foregone to the benefit of operators and their customers. Some resources that might otherwise have been rendered obsolete will be able to continue providing services due to the improved marketability of their offerings that comes with lower transaction costs. Old assets may also be repurposed in line with the changing requirements of grid operators and those they serve. By extending the useful life of the existing generation fleet and delivery assets, construction of new resources for which capacity utilization is expected to be low may be avoided.

Lower transaction costs will also enable smaller distributed resources to compete in the provision of energy and ancillary services, which could induce an accelerated pace of adoption for these emerging technologies. With time, such decentralization may reduce the criticality of any individual asset contributing to the grid, improving the resilience of the grid against diverse hazards. A grid with more options from which operators may choose could realize lower production costs while proving to be more reliable.

4.5.2 Creating value

To the extent that greater interoperability can reduce the cost of integrating new systems with the existing grid, modernization efforts may unleash new opportunities for sales growth. Electric vehicles are one clear opportunity for the electric grid to achieve growth through improving interoperability with increasingly ubiquitous transportation assets. Interoperability enhancements that improve observability and control of electric vehicle charging will make it operationally easier and more profitable for utilities and service providers to coordinate grid assets to meet customer needs.

Interoperability Benefits: A case study on resilience

Interoperability benefits are regularly framed by assessments of system integration or resource development costs, this Framework included. Yet the definition of interoperability provided in this Framework – the ability of two or more networks, systems, devices, applications, or components to work together, and to exchange and readily use information... with little or no inconvenience to the user – means the most important benefits accrue across systems rather than to any specific device or actor. Because system-level characteristics are rarely the result of single procurements, the relationship of interoperability requirements or investments with traditional econometrics will be challenging to describe.

Grid resilience is an inherently system-level characteristic that is developed through years-long and often complex procurement and operational reform strategies. Resilience is also difficult to quantify, as any metric necessarily involves assessment of the counterfactual outages or other system disturbances which would have otherwise occurred but are instead avoided through improved system capability. In one recent example, a utility has claimed that smart grid investments yielded 13 million fewer outages and \$2.6 Billion in associated societal savings through an eight-year grid modernization initiative [169]. That a utility in general does not simultaneously exist in multiple divergent states of preparedness typically limits validation of estimates such as these.

Large-scale physical insults to the grid such as those which occur through severe weather events provide an opportunity for quasi-experimental validation of these typically counterfactual benefits analyses. For example, NIST recently studied the effect of Hurricane Irma windspeed on utility outage performance [36]. Using utility-level smart meter deployment rates as a proxy for interoperability investments, and accounting for variation in wind-speed, building stock, and other factors, NIST was able to evaluate the outage performance of each Florida county.

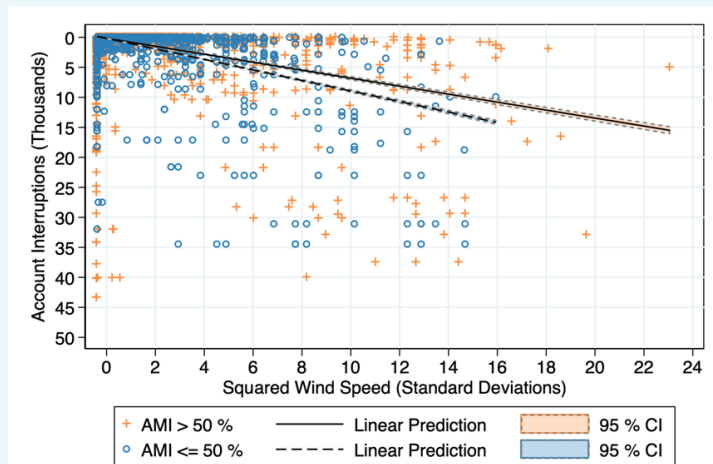


Figure 18 – Sustained outages by AMI penetration and wind speed

The results indicate that utilities which are heavily invested in smart grid interoperability capabilities should expect to see, on average, nearly 10 percent fewer additional outages for each standard deviation increase in wind speed than would those utilities that had not made any interoperability enhancing investments (see **Figure 18**, [36]). Examination of outage performance for neighboring counties with significantly different interoperability investment indicators confirmed this expected over- and under-performance relationship and provides validation of claimed resilience benefits. The NIST research indicates the societal economic benefit from smart grid interoperability investments was likely in the billions of dollars range for this single event.

Greater interoperability can also encourage flexibility among electricity consumers. For most of the electric power sector's history, customers were relatively unresponsive to the fluctuating cost of serving a load because the price paid by most consumers was static and did not reflect underlying costs. Interoperability enhancements can reduce the transaction costs associated with dynamically communicating information on operating costs and conditions to relevant stakeholders, and therefore increase the price responsiveness of end customers. These relatively elastic consumers will be better equipped to shift their consumption patterns to account for price variability, which will improve capacity utilization for existing generation assets [170].

The opportunities for the exercise of market power by generation owners also falls with the increasingly elastic demand interoperability engenders. Prices will therefore move towards competitive equilibrium levels as interoperability improves.

4.6 Conclusion and Future Work

With more than 3,000 utilities in the United States, the importance of interoperability to the utility, marketplace, and customer cannot be overstated. While specific requirements and functions will always be made at the local level, as the rollout of any given investment will not be uniform across the country or state, a foundation of interoperability and open standards provides the building blocks for successfully meeting system needs.

Interoperability is a key component of ensuring the technical and economic benefits from grid modernization flow across stakeholder interests throughout the evolution of the electricity system. Utilities are investing in substantial updates to their infrastructure, and customers are increasingly seeking to achieve additional savings and benefits from investments in DER. Interoperability driven by open standards can help lower transaction and implementation costs associated with DER and other investments.

Interoperability provides benefits that are often lost in the larger context of a utility rate case. However, investments without consideration of interoperability will limit the ultimate reach of a technology, may be more expensive than necessary, and may not enable a grid that is ready and capable of integrating and optimizing the new resources coming to the distribution system. The costs associated with the absence of interoperability are growing as our distribution systems become more advanced and customers seek to realize greater savings from their investments. Effective testing and certification programs will assist in showing these savings, but regulators should ensure that interoperability is an identified component of any utility investment.

Key Messages – Cybersecurity

New technologies, changing resources, and expanding stakeholder participation carry with them a growing cybersecurity risk. To realize the benefits of an interoperable smart grid, security practices will have to evolve beyond strategies of physical isolation or other overly restrictive access regimes.

Understanding and mapping institutional cybersecurity capabilities and processes to the outcomes we seek in a smart grid will help an organization position itself to manage cybersecurity requirements at the device or interface level. The Cybersecurity Risk Profile for the Smart Grid presented in this section and Appendix G provides a structured approach to assessing organizational readiness for cybersecurity.

Cybersecurity protections at the device or system level need not be newly invented even as new technologies and interfaces are introduced to the system. New interface characteristics can be mapped to the existing set of logical interface categories, thereby facilitating protection through known standards and best practices likely already employed for other legacy system interfaces.

5 Cybersecurity

In the traditional electrical grid power flows in one direction — from centralized generation facilities, through transmission lines, and finally to the customer via distribution utilities. As electric utilities incorporate new technologies and accommodate changing customer expectations, the basic structure of the grid remains broadly consistent with the first electric systems built more than a century ago. The centralized design has historically brought efficiencies in facilities and operations, but the criticality of centralized assets has also made the grid vulnerable to both malicious actions and natural disasters.⁶⁵

As demands on the power system evolve and come in conflict with the physical constraints of decades-old infrastructure, the operational and economic solutions brought by new technologies gain prominence. While the distributed nature of many new technologies diminishes the criticality of any single asset, the informational capabilities inherent to these devices carry vulnerabilities that were unknown to the historical grid.⁶⁶

⁶⁵ For example, the Northeast Blackout of 2003 affected 50 million people and was initiated when a grid operator was unable to respond to the failure of the Eastlake Unit 5 generator and the Stuart-Atlanta 345 kV transmission line in Ohio [171].

⁶⁶ Grid communications are increasingly based on conventional “Information Technology (IT)” approaches, leaving them more vulnerable to attacks from hackers with IT expertise.

The large number of non-utility stakeholders and increasing number of devices connected to the grid means that — even in the best of circumstances — secure operations can no longer be guaranteed by a single organization or security department. The utility must instead rely on engineering strategies⁶⁷ and cybersecurity risk management and mitigation techniques⁶⁸ to better ensure secure operation. Furthermore, the integration of modern technology with legacy infrastructure via custom-designed interfaces and unique feature-sets can complicate vulnerability assessments and exacerbate the challenge of protecting power systems.

Protecting the electrical grid against cyber-attack also carries a set of constraints that precludes use of some common IT security strategies. For example, when an IT system is under attack best practice often involves quickly disconnecting or otherwise isolating affected devices from the network, but that approach may not be possible in power system operations where hastily disconnecting control systems could trigger blackouts or other catastrophic system failures.

Securing the grid can seem an impossible challenge given the extensive diversity of organization, actor, and equipment, but cybersecurity issues are not insurmountable and can be mitigated. A successful approach to cybersecurity consists of many techniques that involve processes as well as technology solutions. Minimizing organizational and device exposure to threats promotes system security but requires a structured approach to characterizing cybersecurity risks and managing the system's protection and recovery schemes.

The complexity of achieving cybersecurity stems from the fact that no single action can ensure systemwide security. Much like the smart grid, where new system-level capabilities are most often realized through the aggregated impact of many discrete investments and technology choices, achieving cybersecurity requires utilities to address a wide-ranging set of issues from general IT policies to techniques used to secure specific physical assets and interfaces.

A structured approach to assessing cybersecurity risk is critical to appropriately prioritizing actions that will have the greatest impact on securing the utility and its assets. Below we describe approaches to assessing organizational risk through the application of the NIST Framework for Improving Critical Infrastructure Cybersecurity [172] and evaluating the new interfaces and associated cybersecurity requirements introduced by emerging system architectures.

⁶⁷ For example, system configurations that rely on gateways, network segmentation, and security perimeters.

⁶⁸ For example, those described in the NIST Cybersecurity Framework core and including authentication, access control, key management, network monitoring, and security logs.

5.1 Securing Organizations

The modern electrical grid should be safe, reliable and resilient, yet cybersecurity threats have exploited the increasing complexity and connectivity of this critical infrastructure [173, 174]. A resilient grid must therefore withstand cyber events in addition to the known hazards, human errors, hardware failure, and software bugs that occur in the system. The NIST Framework for Improving Critical Infrastructure Cybersecurity (the Cybersecurity Framework) is a key part of a systemic process organizations can use to identify, assess, and manage cybersecurity risk. Through this process, utilities and other grid organizations can prioritize those activities that can best manage cybersecurity-related risk while aligning with their unique environment, requirements, and budgetary considerations.

The Cybersecurity Framework consists of three main components:

Cybersecurity Framework Core⁶⁹ – Provides a catalog of desired cybersecurity activities and outcomes⁷⁰ using common language. The Core guides organizations in managing and reducing their cybersecurity risks.

Framework Implementation Tiers – Provide context on how to view cybersecurity risk management, and help organizations assess the functionality and repeatability of their risk management process.

Framework Profiles – Used to identify and prioritize opportunities for improving cybersecurity at an organization through customization of Core outcomes.

5.1.1 NIST cybersecurity framework core functions

The Cybersecurity Framework Core is built around five concurrent and continuous Functions illustrated in **Figure 19**. Used to analyze an organization's entire risk management portfolio, when considered together these five Functions provide a high-level, strategic view of the organization's cybersecurity risk management approach.

⁶⁹ Elements of the Cybersecurity Framework – including Core, Implementation Tiers, Profile, Function, Category, and Subcategory – are normally capitalized and will be capitalized throughout this document.

⁷⁰ The word “outcomes” is used because the Cybersecurity Framework focuses on the “what” not the “how.” In other words, the emphasis is on the cybersecurity outcomes that the organization wants to achieve, but not how they will achieve them.

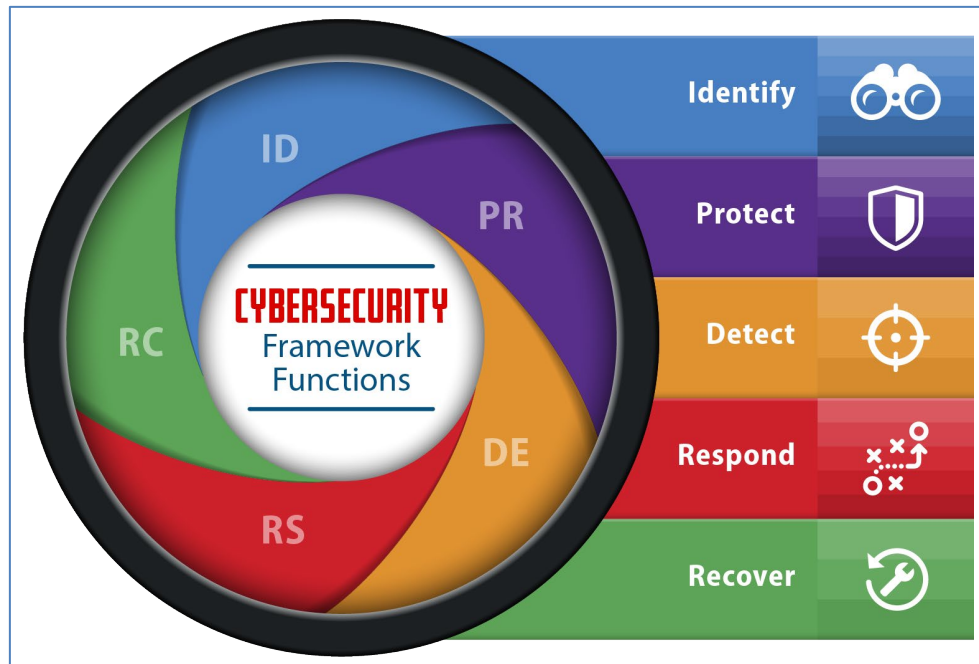


Figure 19 – Cybersecurity Framework core functions

The five cybersecurity functions are:

Identify – Develop the organizational understanding to manage cybersecurity risk of its systems, assets, data, and capabilities. The activities in the Identify Function are foundational to an organization’s assessment of cybersecurity risks and allow organizations to focus and prioritize their cybersecurity efforts consistent with its risk management strategy and business needs.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect Function support the ability to defend against a potential cybersecurity event and limit or contain its impact.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to limit and contain the impact of a potential cybersecurity event.

Recover – Develop and implement the appropriate activities/plans to maintain resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity event.

These Functions align with existing methodologies for incident management and help elucidate the benefits of cybersecurity investments. When considered together, the Functions provide a high-level, strategic view of the lifecycle and management of cybersecurity risk within an organization, and provides a structured approach to evaluating cybersecurity outcomes.

5.1.2 NIST cybersecurity framework core categories and subcategories

The Cybersecurity Framework organizes the five cybersecurity Functions (Identify, Protect, Detect, Respond, and Recover) into subdivisions, or Categories, that can be used to group similar cybersecurity activities that support a particular Function. **Table 4** shows the five Functions divided into the 23 Categories of cybersecurity activities.

Table 4 – Cybersecurity Framework functions and categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The Cybersecurity Framework provides an additional level of granularity by further dividing the 23 Categories of cybersecurity activities into 108 Subcategories, each defining a desired outcome. These Subcategories provide a list of outcomes that — if achieved — would increase the likelihood that an organization could successfully optimize its cybersecurity

posture relative to its risk tolerance. **Table 5** provides an example of two Cybersecurity Framework Subcategories aimed at managing supply chain risk within the Identify Function.

Table 5 – Cybersecurity Framework subcategory examples

Function	Category	Subcategory	Informative References
Identify (ID)	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9

The final element of the Cybersecurity Framework are the informative references provided next to each subcategory. As shown in **Table 5**, these references are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that provide practical suggestions for how to achieve the desired outcomes for each Subcategory. Based upon cross-sector guidance received during the Cybersecurity Framework development process and therefore not explicitly related to power sector activities, the informative references provide a launchpad for users seeking to gain knowledge on existing guidelines and best practices for achieving the cybersecurity subcategory outcomes.

The [Cybersecurity Framework Core](#) is available online in an easily accessible spreadsheet format [175].

5.1.3 Cybersecurity profiles

Creating a Cybersecurity Profile translates the outcomes of the Cybersecurity Framework Core into a prioritized set of actions an organization can use to better position itself against cyber threats. This process aligns the Cybersecurity Framework Functions, Categories, and Subcategories with the organization's business requirements, risk tolerance, and resources.

The Framework Core provides structure for understanding an entity's cybersecurity posture and risk through rigorous examination of systems or components. This function is illustrated in **Figure 20**, where smaller versions of the multi-colored shutter aperture from **Figure 19**, and representing the NIST Cybersecurity Framework core functions, are overlaid on devices or systems that might be examined to develop a cybersecurity risk profile.



Figure 20 – Applying the cybersecurity core to develop risk profiles

The boundaries for these examinations are flexible. The Core can therefore be used to evaluate cybersecurity concerns over a range of scenarios, from reviewing protection strategies for individual assets and organizations, to characterizing the cybersecurity posture for infrastructures that derive functionality from the connected systems of multiple organizations.

The prioritization of the Subcategory outcomes will vary from one organization or infrastructure to the next because each organization has unique requirements including risk tolerance and budget. It is this prioritization that is the essence of a Cybersecurity Framework Profile.

A great benefit of a Cybersecurity Framework Profile is that it provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services [172]. Similar to the ontology provided in this Framework (see **Section 2.3**), the comprehensive considerations of a Cybersecurity Framework Profile offer organizations and their partners a language and methodology to help ensure new products or services meet critical security outcomes. This is

especially important in the electrical grid, where power system owners and operators rely on and interact with an ever-increasing community of active participants and third-party service providers.

5.1.4 *Cybersecurity framework profile for the smart grid*

To facilitate development of a common cybersecurity language and methodology for the power sector, NIST created a cybersecurity risk profile for the smart grid (Smart Grid Profile) based upon the Cybersecurity Framework [176]. In the Smart Grid Profile, the five cybersecurity functions are examined through the lens of power system owner/operators, and cybersecurity outcomes are evaluated for relevance against the following four high-level business objectives:

Maintain safety: Safety is an overarching concern of power system management seeking to minimize the impact to human life, equipment, and the environment from cybersecurity risks.

Maintain power system reliability: Reliability is the ability to deliver stable and predictable power in expected conditions or, in case of power system failure, the ability to restore normal operational service.

Maintain power system resilience: Resilience is the ability of power systems to withstand instability, unexpected conditions or faults, and gracefully return to predictable, but possibly degraded, performance.

Support grid modernization: This requirement supports integration of smart technologies with the traditional grid by managing cybersecurity risks to power systems, including integrity and timeliness of data and control commands.

The Smart Grid Profile is designed to be broadly applicable to the electricity sector and is intended to help power system owners/operators prioritize cybersecurity activities based on the high-level business objectives described above. As shown in **Figure 21**, the Profile also describes considerations for each Subcategory which highlight challenges that may be encountered as organizations attempt to achieve the Subcategory outcomes.

The list of cybersecurity considerations for power system owner/operators is one of the most valuable components of the Smart Grid Profile. These context-specific descriptions of issues relevant to the desired cybersecurity outcomes of the Core yield an accessible baseline of language and understanding about power system cybersecurity. It is hoped this common foundation will improve dialogue across stakeholder communities regarding cybersecurity risks, mitigation strategies, and investments.

Function (ID) Identify
Category (AM) Asset management
Subcategory (1) Physical devices and systems within the organization are inventoried
Subcategory (2) Software platforms and applications within the organization are inventoried

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
ID	Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	Knowing hardware assets is critical for maintaining safety, reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets ¹⁰ need to be known and understood. As modernized grids become more distributed, power system owners/operators need to be accountable for all distributed assets that they own.
		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	Knowing software assets is critical for maintaining reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. This especially applies to modernized assets because the sophisticated logic that they execute is driven by software.

Figure 21 – Example of cybersecurity Considerations for the electrical system

The ubiquitous nature of an electric grid on which all of modern society depends combined with the broad-reaching nature of the grid operator objectives previously described yield a Smart Grid Profile in which most Subcategories are deemed relevant to one or more of the business objectives. While this lack of meaningful differentiation among Subcategories would provide little value to an organization attempting to prioritize security investments, several benefits accrue to industry from this effort.

First and foremost, the Smart Grid Profile describes power system-relevant Considerations for each cybersecurity Subcategory in the Cybersecurity Framework. This baseline of issues related to grid cybersecurity provides a common reference language upon which cybersecurity discussions can be had and gives a shared context for establishing cybersecurity requirements and investments. The easily accessible outcomes and considerations of the Profile can smooth interaction across organizations or stakeholder communities, including with state regulators who are often charged with approving utility cybersecurity investments.

Another benefit of a Smart Grid Profile — in which the significant majority of cybersecurity outcomes are relevant to each of the examined objectives — is the insight gained from the few instances where Framework Subcategories were *not* deemed relevant to most or all of the examined objectives. Given the broad nature of objectives evaluated for this Profile, a universal determination of non-relevance may indicate a structural constraint that is unique to the power sector.

The PR.AC-6⁷¹ Subcategory is an excellent example of how a Profile can highlight the interplay between important cybersecurity outcomes and system constraints. The outcome for PR.AC-6 is that identities are proofed, bound to credentials, and asserted in interactions. Yet the Smart Grid Profile does not prioritize PR.AC-6 as a cybersecurity outcome relevant to grid operator objectives (see **Figure 22**).

Function (PR) Protect
Category (AC) Identity management, authentication and access control
Subcategory (6) Identities are proofed and bound to credentials and asserted in interactions

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		PR.AC-5	PR.AC-5	PR.AC-5	PR.AC-5	Network segmentation is an important tool for containing potential incidents (safety, reliability), and limiting damage from incidents (resilience). Grid modernization efforts should consider segmenting networks from the design stage into operations (e.g., DER devices could be segmented to limit exposure to the rest of the power system infrastructure).
		PR.AC-6	PR.AC-6	PR.AC-6	PR.AC-6	In the power system, the safe delivery of reliable power is paramount. For this reason, there may be situations (e.g., emergency maintenance or need to restore power) in which the binding and proofing of credentials may interfere with safety, reliability, and resilience. Power system owners/operators will need to consider any risks introduced if identities are not proofed and bound to credentials and if those credentials are not required for certain user actions.

Figure 22 – Smart Grid Profile excerpt

Identity proofing is a well-known contributor to system-level cybersecurity, and a host of well-regarded best practices exist to achieve that capability [177], so the designation of this cybersecurity outcome as not relevant to the grid should be viewed skeptically. Further examination of the Profile considerations for the PR.AC-6 subcategory indicates the mutual assistance strategies employed by utilities following natural disasters and other significant disruptions present a structural constraint against achieving this outcome through conventional identity proofing and credentialing approaches. In short, requiring identities be proofed and bound to credentials prior to interacting with the system would inhibit a utility's ability to recover from major disruptions.

A consequence of the structural constraint to achieving the cybersecurity outcome in PR.AC-6 is that utilities will have to devise alternate strategies for controlling access to systems and devices. Utilities will also have to address any risks that may be introduced by an alternate credentialing and access control scheme. The identity management, credentialing, and access considerations for utilities will evolve with the system's architecture, and will become more complex as autonomous devices owned by organizations other than the utility play ever-increasing roles in system operations.

⁷¹ This notation indicates this is the sixth Subcategory for the Identity management, authentication, and access control (AC) Category under the protect (PR) Function of the Cybersecurity Framework.

The full set of Smart Grid Profile Considerations is described in [176] and duplicated in **Appendix G – Smart Grid Cybersecurity Profile Subcategory Prioritization and Considerations Matrices**. The original Smart Grid Profile publication also includes a mapping of the NERC Critical Infrastructure Protection (CIP) v5 regulations to the Cybersecurity Framework v1.0 Subcategories (see **Section 5.3**).

5.2 Securing Information Exchange

Information cybersecurity is primarily associated with information exchange interactions⁷² between entities⁷³ and is a critical aspect of power system operations and security. The impacts of cybersecurity breaches — whether deliberate or inadvertent — may affect both physical and cyber operations of the grid.

5.2.1 Known system interfaces and categories

Identifying the entities⁷³ involved with information exchanges in power systems operations is the first step towards understanding cybersecurity issues for the grid. To facilitate this understanding, the 2014 NIST publication *Guidelines for Smart Grid Cybersecurity* (NISTIR 7628) [178] included a composite diagram of grid entities that exchange information within and across each of the seven smart grid Conceptual Model domains (see **Section 2.1** and **Appendix A – Smart Grid Conceptual Model Domains**). By mapping these information exchanges — called logical interfaces — to the composite diagram of grid entities, the guidelines found in NISTIR 7628 described where, at a high level, the smart grid would need to provide security (see **Figure 23**).

Yet knowing *where* security is needed is of limited value, as location information alone does not provide details on the requirements of *what* needs to be done to enhance security. To understand the latter, the NISTIR 7628 [178] defined a set of logical interface categories (LICs) based on attributes that could affect grid cybersecurity requirements.

Because many of the individual logical interfaces have similar security-related characteristics, grouping interfaces into LICs with similar characteristics is a means to simplify the identification of appropriate security requirements. In that way, the hundreds of individual interfaces drawn in **Figure 23** can be grouped into 22 representative LICs, from which broadly applicable cybersecurity requirements can be derived (see **Appendix H – Logical Interface Categories from NISTIR 7628**).

⁷² Although information cybersecurity also addresses stored data, NIST's smart grid program focus is on interoperability and securing associated information exchanges.

⁷³ Entities consist of — but are not limited to — users, systems, devices, network or communications nodes, etc.

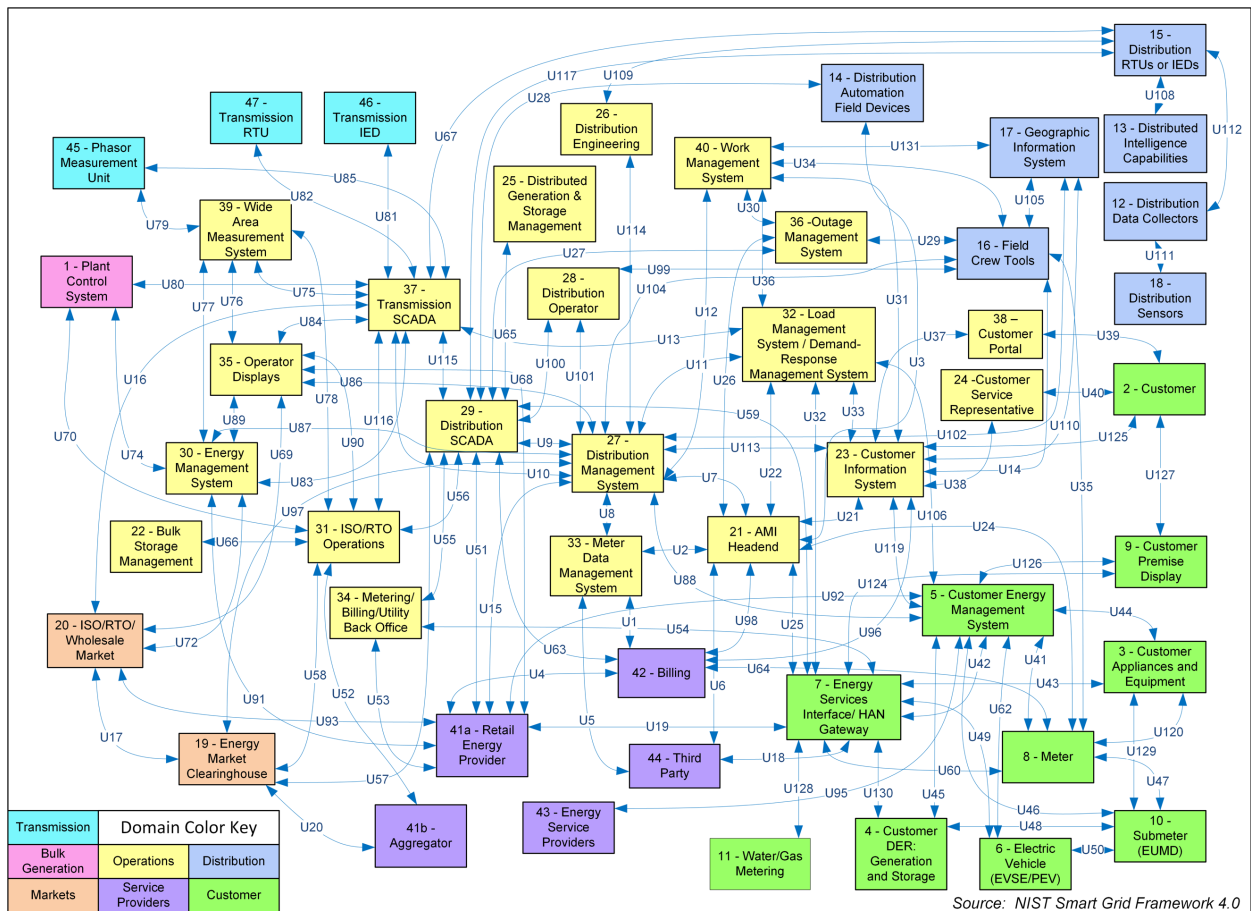


Figure 23 – Logical Interface Reference Model "Spaghetti Diagram" from NISTIR 7628

5.2.2 New system interfaces

The modern grid will be more heavily dependent on information exchange than the legacy grid. As DERs and other innovations are used more extensively across the grid (see **Section 2.2.3**), the set of entities involved with information exchanges in power system operations will expand and new communications interfaces will evolve. It is useful, therefore, to explore how portions of the **Figure 23** logical interface diagram — which contains high-level representations of current power system operations domains — can be expanded to provide more detailed cybersecurity requirements for emerging interfaces.

To explore the cybersecurity implications of introducing new technologies and architectures to the grid, we updated the NISTIR 7628 logical interface diagram found in **Figure 23** to include examples of the new equipment and information exchanges that could be expected for future High-DER penetration grids. A representation of the new power system entities and logical interfaces for a High-DER architecture is shown in **Figure 24**, where Uxx-labeled blue interface arrows are the same as those originally shown in NISTIR7628 and Dxx-labeled red interface arrows are newly introduced interfaces for the High-DER example.

From the High-DER example shown in **Figure 24**, we understand that a modernized grid would likely have to accommodate at least three new types of communications interfaces, including:

New interfaces for new entities: As new entities are introduced to the grid the number of communications interfaces and pathways will increase dramatically. For example, extensive penetration of distributed resources requires introduction of a Distributed Energy Resource Management System (DERMS) into the grid operations domain (**Figure 24**, box 25). This DERMS would likely have different data and communications requirements than legacy systems, and new communications linkages are required throughout the rest of the system.

New interfaces between subsystems: As the physical capabilities of grid-connected systems advance, logical interface requirements between equipment subsystems will evolve. The customer-sited DER asset, electric vehicle asset, and the utility-scale DER or cogeneration asset have been split to reflect the different logical interface requirements between asset controllers (**Figure 24**, boxes 4a, 4c, and 6a) and the equipment (**Figure 24**, boxes 4b, 4d, and 6b) connected to the grid physically consuming or supplying electrons.

New interfaces for legacy systems: As new capabilities are introduced to conventional grid assets, information will have to be exchanged with and between legacy systems. Both the utility-scale DER or cogeneration asset and the facility energy management system interface directly with the utility supervisory control and data acquisition (SCADA) system via a new logical interface (**Figure 24**, red lines D03 and D04). Additionally, where Aggregator interfaces in NISTIR 7628 were constrained to energy providers and markets (**Figure 23**, box 41b and blue lines U20 and Uaa), Aggregators interact with new actors in the High-DER scenario and the logical interfaces increase accordingly (**Figure 24**, red lines D08, D52, and D92).

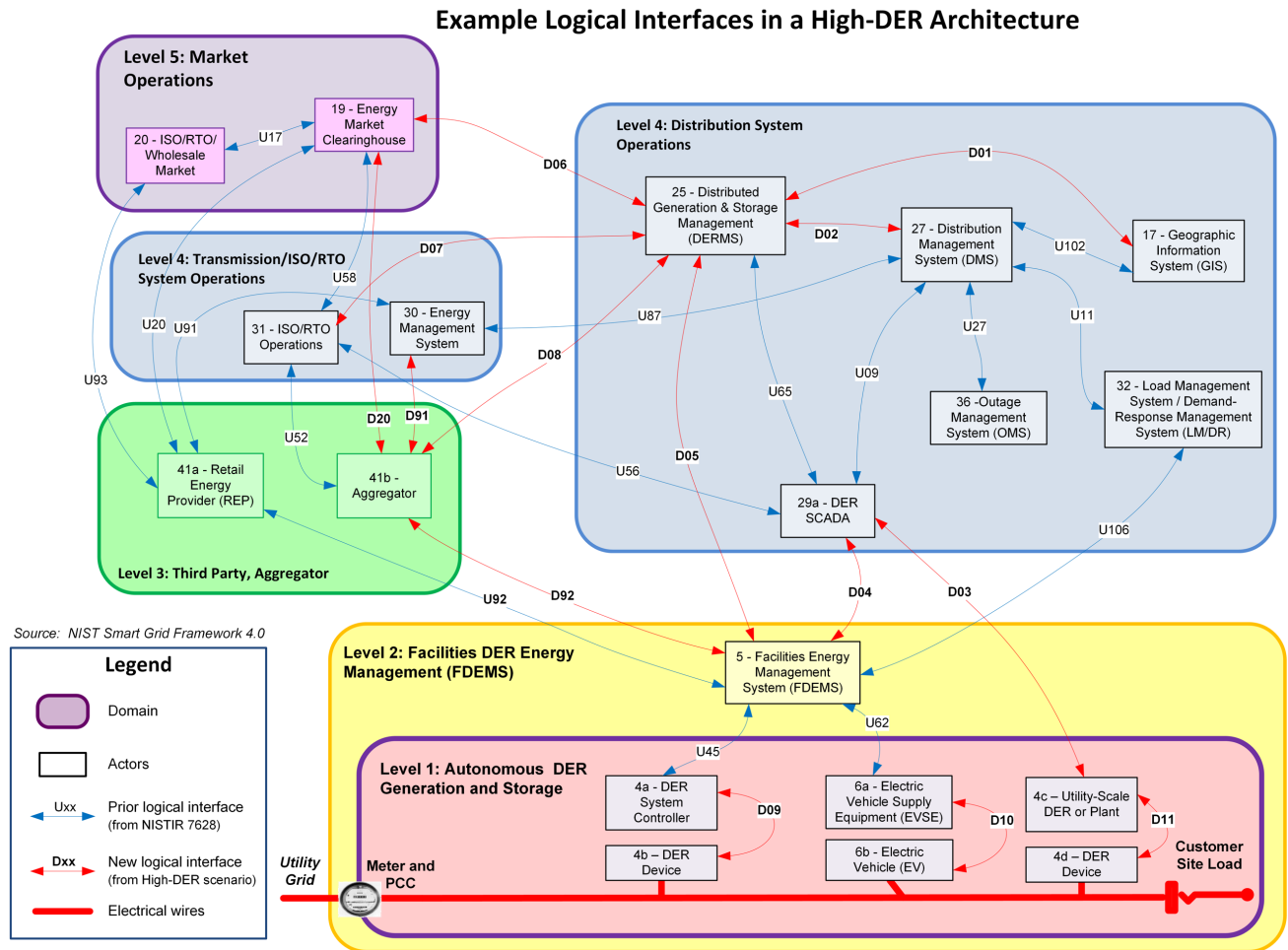


Figure 24 – Example logical interfaces in a High-DER architecture⁷⁴

5.2.3 Assessing security requirements of new interfaces

New or changed logical interfaces may require new cybersecurity precautions. The High-DER example identifies nearly a dozen new interfaces (**Figure 24**, thin red lines), and the changing characteristics of the system itself may alter the communications and cybersecurity requirements for previously established interfaces.⁷⁵

To assess the cybersecurity requirements for the High-DER example, the new and updated interfaces were evaluated against the LICs found in NISTIR 7628. Each of the new interfaces for High-DER example could be mapped to an existing LIC, meaning the cybersecurity requirements for protecting communications interfaces within this new architecture can be derived — at least in part — from those described in the current NISTIR 7628.

⁷⁴ To ease examination, this figure includes only those entities requiring new logical interfaces for this high-DER example.

⁷⁵ Detailed information on each of the interfaces in **Figure 24** is provided in **Appendix I**.

The complete evaluation of each information exchange in **Figure 24** is provided in **Appendix I**, and the LIC interface mapping is shown graphically in **Figure 25**. It should be noted, however, that not all of the conventional approaches for responding to and coping with cybersecurity attacks that were described in NISTIR 7628 will map directly to evolving grid architectures.

For example, the High-DER scenario depicts a power system that relies on increasing communications between, and coordinated management of, diverse assets to provide essential grid services. As the criticality of DERs to system operations increase, it may not be plausible to abort communications and potentially cease device operations in response to cyberattacks as was described in NISTIR 7628 for several LICs in conventional system architectures. Even so, mapping emerging interfaces to existing LICs and the associated NISTIR 7628 cybersecurity guidance provides a foundation upon which the cybersecurity of emerging grid architectures can be built.

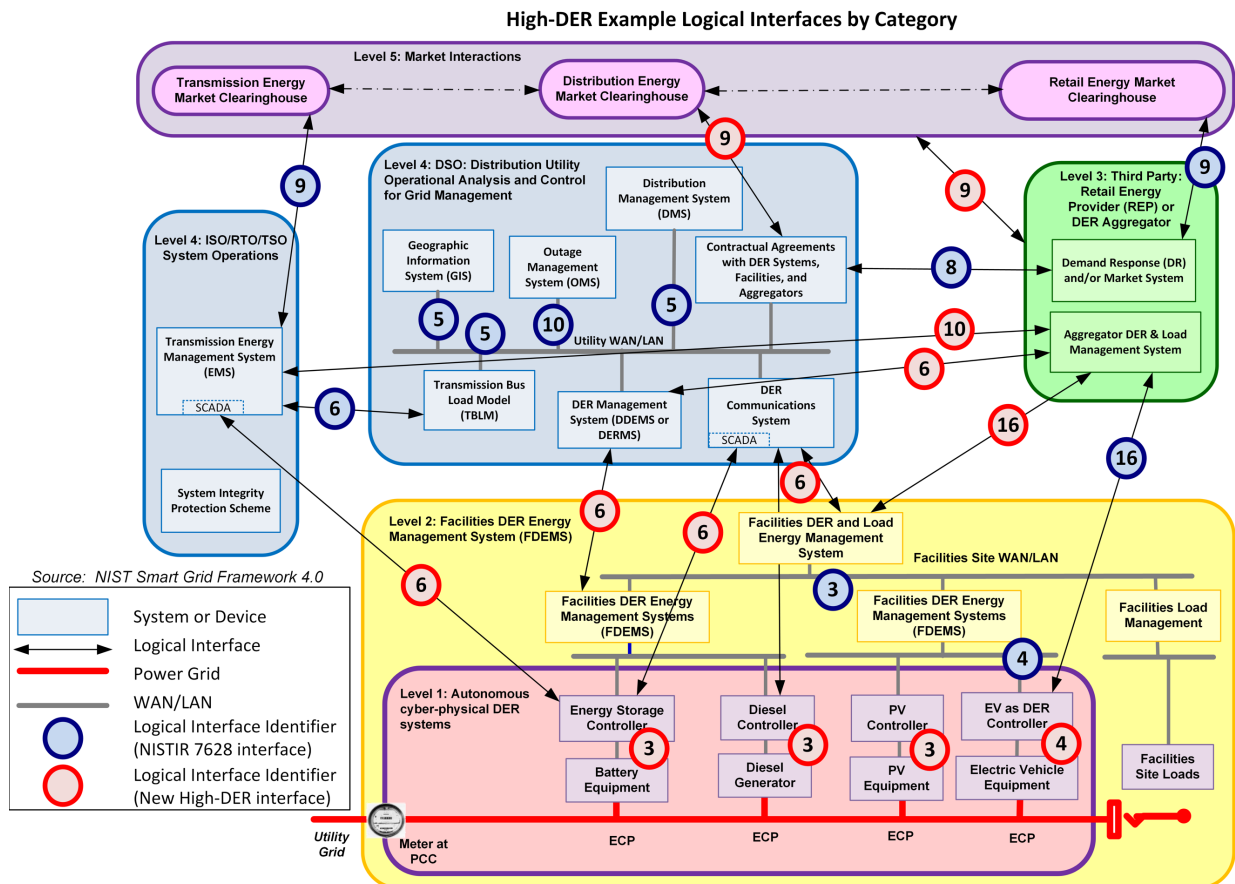


Figure 25 – Logical interface categories (LICs) for the High-DER example

5.3 Additional Cybersecurity Resources

Cybersecurity requirements for the Nation's high-voltage transmission system⁷⁶ are overseen by the Federal Energy Regulatory Commission (FERC), and developed and enforced by the North American Electric Reliability Corporation (NERC) through a series of Critical Infrastructure Protection (CIP) standards [179]. From the adoption of its first cybersecurity standard in 2004 [180], NERC CIP has evolved into a collection of current and future standards subject to enforcement [181].

While the CIP standards provide detailed and regularly updated cybersecurity requirements for transmission system stakeholders, enforcement of these standards is constrained to the bulk electric system⁷⁷ (BES) and there is no nationwide analog for distribution grids. While FERC engages state and industry partners to address cybersecurity issues through voluntary initiatives, the Commission does not have authority to directly impose cybersecurity obligations on entities outside FERC's BES jurisdiction [182].

Analysis of realistic potential failure scenarios provides insight into common cybersecurity threats, vulnerabilities, and mitigations. By also characterizing the potential impacts of a cyber event, scenario analysis can be useful for a range of organizational responsibilities from risk assessment to security testing. The National Electric Sector Cybersecurity Organization Resource [183], led by the Electric Power Research Institute (EPRI) with funding from DOE, has defined a set of cybersecurity failure scenarios that span each of the NIST Smart Grid Conceptual Model domains and is a useful complement to requirements- and standards-driven cybersecurity processes [184].

The Cybersecurity Framework and NISTIR 7628 have been recognized as useful tools for characterizing and reducing cybersecurity risk [179, 182, 184]. NIST's special publication on security and privacy controls for information systems [140] provides a risk assessment methodology that can be adapted for any type of system. But no single document or organization can provide a comprehensive understanding of the cybersecurity risks and best practices that must be addressed throughout the power system. The valuable resources described in this section and elsewhere are each unique in scope and purpose, and provide complementary information and guidance on cybersecurity practices.

NIST and collaborators have developed numerous analyses to help clarify and map the alignment between these and other cybersecurity guidance documents and standards. Of particular interest has been alignment between the Cybersecurity Framework and NERC CIP, and in 2020 NERC and NIST collaborated to develop an updated mapping between the most recent versions of these resources. This tool is available for download [185].

⁷⁶ Transmission elements or power sources operating at 100 kV or higher are considered high-voltage.

⁷⁷ The high-voltage transmission system is commonly referred to as the bulk electric system.

Function	Category	CSF SubCat ID	Subcategory	CIP ID	NERC CIP
DETECT (DE)	Anomalies and Events (AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2	DE.AE-2: Detected events are analyzed to understand attack targets and methods	CIP-007-6-R4	CIP-007-6 R4: Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.
DETECT (DE)	Anomalies and Events (AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2	DE.AE-2: Detected events are analyzed to understand attack targets and methods	CIP-008-5-R1	CIP-008-5 R1: Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.
DETECT (DE)	Anomalies and Events (AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-2	DE.AE-2: Detected events are analyzed to understand attack targets and methods	CIP-008-5-R2	CIP-008-5 R2: Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.

Figure 26 – Mapping cybersecurity framework subcategories to NERC CIP requirements

Designed as an informative reference to help users examine the relationships between the cybersecurity best practices described in the NIST Framework and the cybersecurity requirements detailed in the NERC CIP standards, the mapping tool details which Framework subcategories relate to which CIP requirements — and why. As shown in **Figure 26**, a single Framework subcategory can relate to multiple CIP requirements. A single CIP requirement can similarly map to numerous Framework subcategories. The mapping tool provides lookup and pivot tables to help users examine these relationships.

Effective cybersecurity guidance must be regularly updated, and a commitment to making that guidance accessible is equally important. Both the NIST Cybersecurity Framework and the NERC CIP standards have been updated⁷⁸ in recent years. NERC has made the Framework/CIP spreadsheet mapping tool available to the public on NERC’s “One-Stop Shop” webpage for its Compliance, Monitoring and Enforcement Program [185]. NIST has also completed a mapping of the Cybersecurity Framework v1.1 to the EPRI failure scenarios for advanced metering infrastructure, distributed energy resources, and distribution grid management [184], which will be published in an upcoming NIST report.

5.4 Conclusions and Future Work

The smart grid brings new information technology capabilities to electric infrastructure, and as this occurs the number of communications interfaces will grow substantially. No single mitigation method can guarantee security and organizations will be best served by taking complementary approaches to assess and manage risk at multiple levels within the system.

Even as the number of communication interfaces grows, the fundamental cybersecurity requirements for each interface – and the attendant obligations on their managing organizations – are likely to be consistent with known requirements. This Framework describes two complementary approaches to risk management, one at the organizational level and the other at the device interface level.

Creation of a Cybersecurity Risk Profile for the Smart Grid (see **Section 5.1.4**) provides a structured methodology and common reference language for evaluating organizational cybersecurity posture while facilitating communication across organizational boundaries and

⁷⁸ NIST Cybersecurity Framework has been updated to version 1.1 [172], and some NERC CIP standards are in their eighth revision while others are just being introduced [181].

smart grid domains. The description of grid-specific subcategory considerations allows utilities or other grid organizations to assess their own security posture and prioritize cybersecurity outcomes that best match their organizational need.

But complex infrastructures with multiple actors like the power system are difficult to fully characterize in a single Cybersecurity Profile. Utilities and other grid stakeholders may therefore choose to create multiple profiles to characterize cybersecurity outcomes for specific interactions, functions, or other organizing principles within the system. Multiple profiles can also be developed to examine differences between present and desired cybersecurity states, where the identified gaps can provide a foundation for an organization's cybersecurity roadmap.

Examining the emerging set of logical interfaces as new technologies take root in the power system (see **Section 5.2.2**) provides some confidence that the basic cybersecurity requirements described by existing LICs will be relevant for new interfaces as well. However, it is similarly likely that cybersecurity response guidance may require updating to capture emerging functionality and system criticality of these technologies (see **Section 5.2.3**). Mapping new interfaces to existing LICs should therefore facilitate the effective application of category-driven protection schemes to the evolving grid, and also identify gaps in this approach where updated cybersecurity guidelines and/or protection schemes would be useful.

While the Cybersecurity Risk Profile and interface category-driven risk management approaches are useful, the complexity inherent in crafting new Profiles or mapping LIC protection schemes may require expertise not available to every organization. This complexity, combined with the manifold security requirements to which firms must adhere and the diversity of options available in the marketplace, can create a confusing environment for securing grid systems. This is why stakeholder feedback to NIST has repeatedly focused on the value of cybersecurity case-studies that can be used to create tangible implementation guides, as well as a need for updated mappings between the latest versions of cybersecurity requirements and analysis guidelines.

As grid architectures evolve, so too will communications network architectures. The transition from brokered to brokerless communications, expanding use of publicly accessible tools and infrastructures, and increasing dynamism of customer participation with the system all indicate a need for improved identity management infrastructure for grid connected devices.

Finally, interoperability in the system will only be achieved if openly available standards are used across many utilities and vendors. The use of open standards to achieve interoperability also means significant numbers of devices and systems will likely be more visible and potentially accessible to malicious actors than in the past. Interoperability requirements and standards must therefore include security requirements, including data protection and attack detection, and an ability to respond to the threat and recover from disruption

Key Messages – Testing and Certification

Testing and certification is a critical enabler of grid modernization with benefits to industry ranging from operational trustworthiness to investor confidence. Yet the availability of testing and certification programs is limited.

Smart grid standards often include many user-selected options. This optionality typically allows for non-interoperability even among products conforming to the same standard. This means that the current industry focus on certifying conformance to individual standards is inadequate to assure interoperability.

Interoperability Profiles that describe the communications protocol and data model requirements necessary to achieve a specific set of physical functions are possible solutions to the interoperability challenge.

Interoperability profiles are not new standards, but instead describe a subset of requirements from existing standards that—when implemented and verified through testing and certification—would ensure interoperability across devices and systems.

6 Testing and Certification

The modern electric grid is often described as a “system of systems” (SOS) spanning multiple technology domains, involving thousands of organizations, and hundreds of standards (see **Section 2.3**). Smart grid devices, systems and applications require extensive data exchange and need well-defined interfaces to transfer and translate this data between points across the grid. Interoperability is necessary to provide seamless functional performance across systems that enables many benefits of the smart grid.

Test programs are needed to ensure products are developed in a manner where standards implementation enhances interoperability. While standards promote interoperability, the breadth and flexibility of implementation options for each standard means that interoperability is not guaranteed. Reducing the complexity involved with implementing a standard would also simplify the associated testing requirements to validate conformance and give a clearer indication of device or system capability upon certification.

This chapter provides an overview and benefits of testing and certification (T&C) for smart grid standards and describes benefits, gaps, and required work to address the longer-term implementation challenges in maintaining a robust T&C ecosystem for system and device. The development and use of Interoperability Profiles is proposed as a mechanism to advance

interoperability while simplifying evaluation requirements, thereby facilitating and further enhancing T&C efficiency and efficacy.

Interoperability Profiles (see **Section 6.5.1**) describe a subset of a standard — or group of standards — for implementation that would reduce the degrees of freedom available for implementing standards by the device supplier, implementor, and system owner. By clarifying interoperability functions, the interoperability profile would narrow performance gaps that hinder interoperability and streamline the set of device functions that must be evaluated for effective certification.

6.1 The Role of Testing and Certification

Testing and Certification (T&C) programs provide common processes that are used to demonstrate conformance with a standard [186]. When accepted and used across industries, these testing and certification processes support interoperability between devices and systems that span equipment vintage and manufacturer. Completing a T&C program allows vendors to offer products certified to a standard, and affords customers a level of trust that products will work as intended when deployed.

Standardized interface and performance requirements are necessary for modernizing the grid as new technology integrates with legacy grid systems [187, 188]. Well-defined interface requirements enable creation of adaptors and gateways that allow new equipment to interact with existing systems to extend useable service life. Performance requirements are critical to ensure the deployed equipment has the necessary capability or can be upgraded to accommodate future applications.

The value of certification programs increases as the number of devices grows through economies of scale for both manufacturers and test program operators. As the range of technologies and their uses continue to evolve, grid operations become commensurately more complex. Certification programs, therefore, become essential to ensure the reliable performance of grid components in this increasingly dynamic environment.

6.1.1 Testing and certification value

As described in **Section 4.3.5**, the T&C value proposition benefits all grid stakeholders. The following list describes how these benefits accrue to principal classes of grid stakeholders:

Customers⁷⁹ benefit by ensuring standards and performance requirements are implemented appropriately and consistently across purchased equipment, which eases integration of new products and services with existing infrastructure and operations [189].

⁷⁹ Here the term “customers” is used to describe the individual or firm that purchases equipment. While a customer could be the electricity consumer who purchases appliances or other residential-scale smart grid technology, a customer could also be a utility that purchases equipment appropriate only for use on the bulk or distribution power systems.

Manufacturers and Vendors benefit from the establishment of clear performance requirements, which reduces implementation costs for new standards [190]. T&C programs ensure product certification occurs in a neutral environment and creates a level playing field for participants, which can facilitate market access and reduce entry barriers for all — including new entrants.

Regulators benefit because interoperability T&C maximizes the benefits of new grid technology investments they approve through regulatory proceedings [186, 191].

6.1.2 *Current practice*

NIST worked with sector experts to create best practice guidelines for the development of T&C programs for smart grid systems and devices. The foundational products are the Interoperability Process Reference Manual (IPRM) standard [186] and accompanying User's Guide [192]. The IPRM standard defines a process by which industry stakeholders may procure, test, and assert interoperability between disparate vendors of smart grid products built to specific standards. It includes practical guidance on requirements and recommendations for general test policies, test suite specifications, test profiles, interoperability T&C authority technical programs, governance, laboratory qualification, and process improvements.

The IPRM standard defines an entity, the Interoperability Testing and Certification Authority, that serves as test program operator. Ideally, there should be an Authority to certify interoperability for each smart grid standard for which a T&C program is required.

Testing and Certification is an important aspect of the technology product development and deployment lifecycle. Unfortunately, T&C is often overlooked because of the added costs to equipment manufacturers for completing and maintaining product certification, the limited availability of appropriate test programs (see **Section 6.4.3**), and the lack of qualified testing organizations to perform the tests. These are among the main reasons for the persistent gap in the availability of testing programs for smart grid standards and interoperability.

6.2 **Levels of Interoperability**

There are many levels of interoperability, each with its own industry definitions. This is important for T&C because most standards, tests, and certifications have been created by industry to deliver a desired function and interoperability level.

One way to define the interoperability level is through the Open Systems Interconnection (OSI) 7-layer model [191]. This approach provides a method for defining interoperability within and across communications system levels. Another method for defining interoperability is the GridWise Architecture Council (GWAC) interoperability stack concept [193], which describes interoperability from a functional approach.

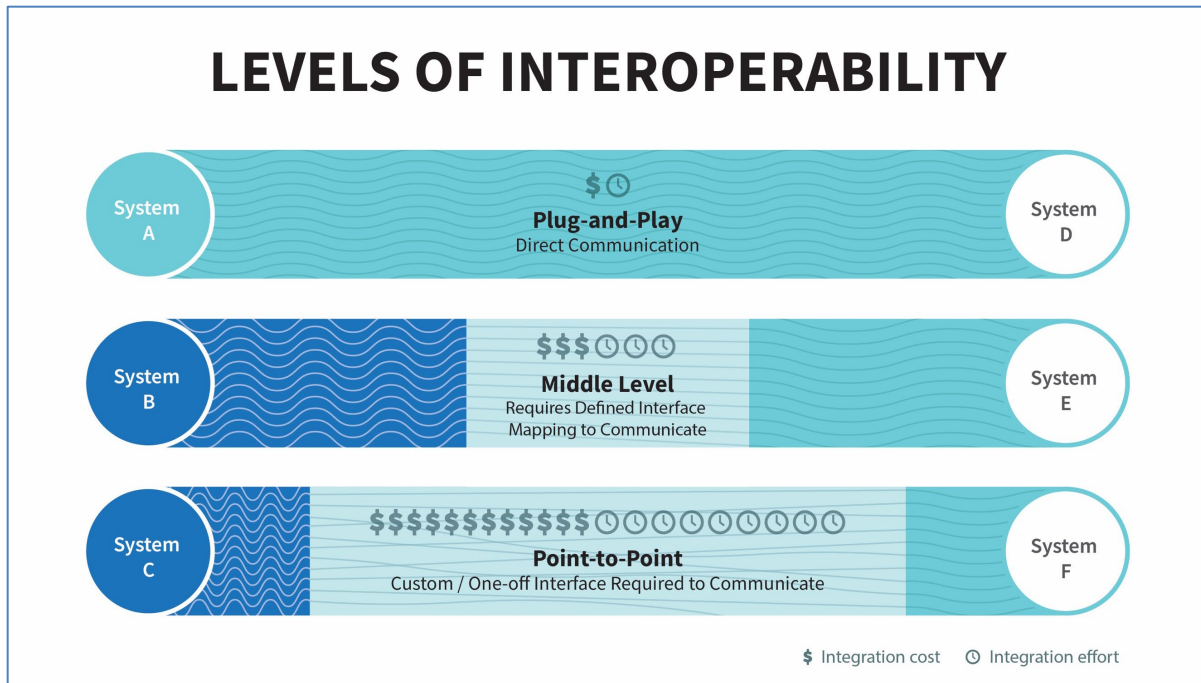


Figure 27 – Levels of interoperability conceptual diagram

A practical way to characterize interoperability is through the integration concept. From plug-and-play on one end of the spectrum to point-to-point integration on the other, each interoperability level describes the ease with which communication can be achieved across devices or systems, and the time and expense associated with overcoming any communications gaps. **Figure 27** provides a cartoon representation of three interoperability levels, where plug-and-play allows for direct communication at little expense to the device operator and point-to-point integration requires development of custom interfaces that take considerable time and money to develop.

There are a few examples of plug-and-play interoperability in the electric grid. One example is the compatibility between electric vehicles and public charging stations. When the station and vehicle support the same plug type and charging protocol, charging begins as soon as the two are connected regardless of the fact that the vehicle and charging systems are owned by different actors.⁸⁰

The middle interoperability level — where devices require integration efforts to work with the rest of the system — is more common. Substation equipment is a useful example due to the two dominant standards in this arena. A utility could have an existing substation designed around the DNP3 communications protocol [195] but wants to incorporate new piece of equipment with specific functionality supported by the GOOSE communications protocol [196]. This difference in designed-to communications protocols means the new device will not be able to communicate with the rest of the substation without specific

⁸⁰ Even with the plug-and-play interoperability that exists between electric vehicles and public charging stations [194], communications between the charging station and grid operators and markets remains highly constrained and interoperability is limited to the physical exchange of energy.

integration efforts. However, this integration issue can be addressed with the IEEE 1815.1-2015 standard which provides a mapping between GOOSE and DNP3 that a gateway can use to translate between the two communication protocols [197]. A gateway conforming to IEEE 1815.1-2015 would therefore allow the new device to interoperate with the rest of the substation.

Point-to-point integration is often referred to as a custom one-off solution. This type of integration is needed when integrating new equipment to existing systems that implement proprietary or obsolete communications protocols. This is a common problem in the electric grid due to the long service life of most grid equipment [91] and the need for older equipment to communicate with newer systems to enable new functionalities as part of grid modernization. This scenario will lead to a custom integration solution where the communication mapping between existing and new systems will need to start from scratch and cannot rely on a published standard. This type of integration is time-consuming and costly.

6.3 Types of Testing Processes

Developing testing and certification programs involves many processes, the steps for which are shown in **Figure 28**. Because the designed interoperability level for each product is a function of technical and business considerations, not every product or standard will complete all of the steps.

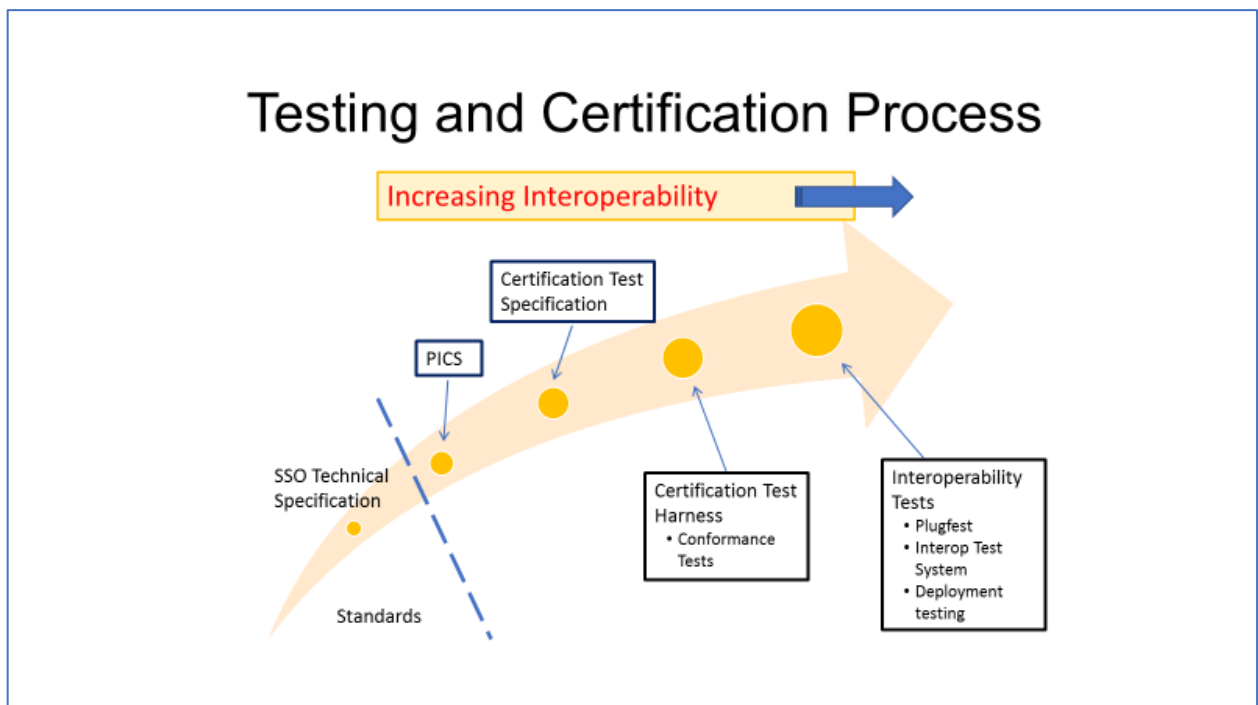


Figure 28 – Testing and certification development process

6.3.1 Conformance and interoperability testing

Conformance testing ensures products conform to requirements detailed in a standard or other specification. Interoperability testing ensures that products from different vendors can communicate and exchange actionable information in the same system. Conformance testing does not guarantee interoperability because standards often include multiple options manufacturers can choose from to meet a requirement. Standards contain these implementation options to be flexible, but this optionality introduces significant product and systemwide variability that can inhibit interoperability.

Interoperability testing is more complex than conformance testing since manufacturers must agree to a common list of requirements to enable the products to work together. This is generally referred to as an implementation agreement and is an essential element of an interoperability test program. From these agreed upon requirements, an industry stakeholder group develops the protocol implementation conformance statement (PICS) for the test plan.

Implementing Agreements define a common interpretation of a standard which includes a specific subset of requirements from the original standard [192].

Protocol Implementation Conformance Statement (PICS) enables the development of a test plan from the requirements identified in the implementing agreement.

This process often leads to an implementation profile for a standard which serves as the basis for interoperability testing requirements. As discussed later in this chapter, the development of interoperability profiles may offer a way to identify a subset of requirements common to a specific implementation of a standard, thereby minimizing the differences between implementations of a standard for a common application.

6.3.2 Interoperability tests

An example of interoperability testing in the final step of **Figure 28** above is a plugfest. An interoperability plugfest is an event where different vendors and stakeholders gather to conduct testing of a standard or specification. The goal of a plugfest is to determine if devices from different manufacturers are able to communicate and exchange information as specified in the requirements, and to show incompatibilities when interoperability is not achieved. A successful plugfest requires participation from equipment manufacturers, test support personnel, and witnesses.

Reports from recent plugfests, such as the 2017 IEC 61850 plugfest, indicate the value of these activities. The final report for this event identifies communication issues that occurred among devices due to their varied implementation of certain aspects of the IEC 61850 standard. In one case a device had its network domain

address hardcoded and could not be dynamically changed to different values as required by tests. The device therefore failed the communication test [198].

Industry recognized the importance of plugfests in specifying product procurement requirements [199]. A purchaser can potentially require vendors to participate in plugfests to demonstrate the interoperability of their products. Plugfests also provide an avenue for vendors to showcase products and capabilities to potential customers, since utility staff can participate in the event as witnesses.

Interoperability testing is important because it can expose compatibility issues for devices from different vendors operating within a closed system. In this way, interoperability testing provides information manufacturers can use to refine their products, and also helps implementers avoid previously known integration issues.

The key takeaway on conformance and interoperability testing is that they are both necessary to enable interoperability of smart grid devices and systems.

6.3.3 *Certification regimes*

Three certification types described in the IPRM standard are first party, second party, and third party. **Table 6** provides a broad illustration of performance metrics related to the different certification types.

First-party certification is when a manufacturer attests that a product meets the standard's requirements. This type of certification, often called self-certification, is common in industry.⁸¹ In first-party certification, the purchaser relies on the manufacturer developed test plan.

Second-party certification is when a user tests and certifies a product to verify that it meets the standard's requirements. This type of certification relies on the user's own test plan, which could include specific requirements based on their existing systems and is not scalable because it is difficult for other users to take advantage of this testing. In the smart grid it is often the utility that serves this role.

Third-party certification is done through an independent authority that includes a certification body and associated test lab. Third-party certification has public test plans, which facilitate transparent audit and evaluation of the testing implementations. Third-party certification by fully vetted and independent testing authorities is one of the best means to deliver interoperability.

⁸¹ An example of first party certification is the ANSI C12 family of standards for electric meters [200]. The meters are mostly procured with the manufacturer's certification of conformance to the C12 standard.

Table 6 – Certification regime characteristics (illustrative)

	Speed	Transparency	Independence
First Party	High	Low	Low
Second Party	Medium	Medium	Medium
Third Party	Low	High	High

6.4 Current Smart Grid Testing Initiatives

NIST is involved in a number of initiatives designed to support development of testing and certification regimes across the sector, a few of which are described below.

6.4.1 Testing support

Testing events and test program formulations are important catalysts for building a robust testing ecosystem. However, these activities are often done by volunteers with limited support from organizers. More support is needed to drive these activities to success and further develop the smart grid testing and certification ecosystem beyond the current nascent stage. NIST works with the community in developing test protocols for conformance assessment,⁸² and also participates in testing activities such as plugfests.⁸³

6.4.2 Catalog of standards

Each prior version of this Framework included a listing of smart grid-relevant standards, requirements, and guidelines identified through a consensus-driven stakeholder engagement process. In the 2010 Framework [74], context for the enumerated standards was provided through discussion of relevant applications and needed improvements. By the 2014 Framework [24], the contextual information grew to include capability descriptions and mappings to the Smart Grid Conceptual Model domains and other standards catalogs. At the same time, in just four years the number of standards included in the listing grew from 25 to 72.

Expansion of the standards landscape has continued apace since the 2014 Framework [103]. This fact, along with the growing range and amount of contextual information provided for each entry, would have limited the usefulness and usability of periodically published static lists of smart grid standards. NIST has therefore worked with industry⁸⁴ to develop the SEPA Catalog of Standards (COS) [203], an online version of the smart grid-relevant standards lists published in prior Frameworks. The COS is publicly accessible, allows for navigation using NIST Smart Grid Conceptual Model domains and other parameters, and is updated regularly through a consensus-based and transparent process.

⁸² For example, NIST staff is working on a test suite specification (TSS) for the utility power profile for precision timing protocol (IEEE C37.238 and IEC 61850-9-3), which will serve as the basis for the testing program the IEEE Conformity Assessment Program (ICAP) will operate [201].

⁸³ NIST staff have developed test harnesses for, and participated in, interoperability plugfests such as the UCAlug hosted 2017 IEC 61850 Interoperability Plugfest [202].

⁸⁴ Through the Smart Electric Power Alliance's Testing and Certification Working Group

6.4.3 *Catalog of test programs*

The COS provides curated and useful information on standards relevant to smart grid development and deployment [203]. The COS does not, however, include information on associated test programs for these standards. A lack of readily accessible information on the availability of T&C programs is a barrier to further adoption and limits the interoperability benefits to industry that these techniques could provide.

To address this information gap, NIST conducted a landscape analysis on the availability of T&C programs for smart grid standards [103] and determined that T&C programs are available for only a small percentage of interoperability standards (see **Figure 29**). The analysis also revealed there is a significant challenge in finding test programs even for those with expert industry knowledge and awareness, and that industry would benefit from a repository that contains information on available test programs.

In response to its findings, NIST is working with industry⁸⁴ to create a Catalog of Test Programs [204]. There are several industry test programs that are beneficial to interoperability of smart grid systems and devices, and a comprehensive directory of available test programs will provide value to the stakeholder community. Such a catalog provides guidance to equipment purchasers on whether reference test programs are available, and also provide visibility for test program operators — potentially increasing their usage.

Built from the information generated during the NIST landscape analysis, the Catalog provides a directory of industry test programs that support assessments against interoperability standards. It is a one-stop, publicly accessible resource to support utilities and vendors as they seek to identify available device testing resources. This initiative will regularly update the Catalog, and is expected to foster collaborations between test programs and labs thereby expanding coordination across the T&C ecosystem.

The complete list of interoperability standards evaluated for NIST's T&C landscape analysis is found in **Appendix J** – List of Reviewed Smart Grid Interoperability Standards [103].

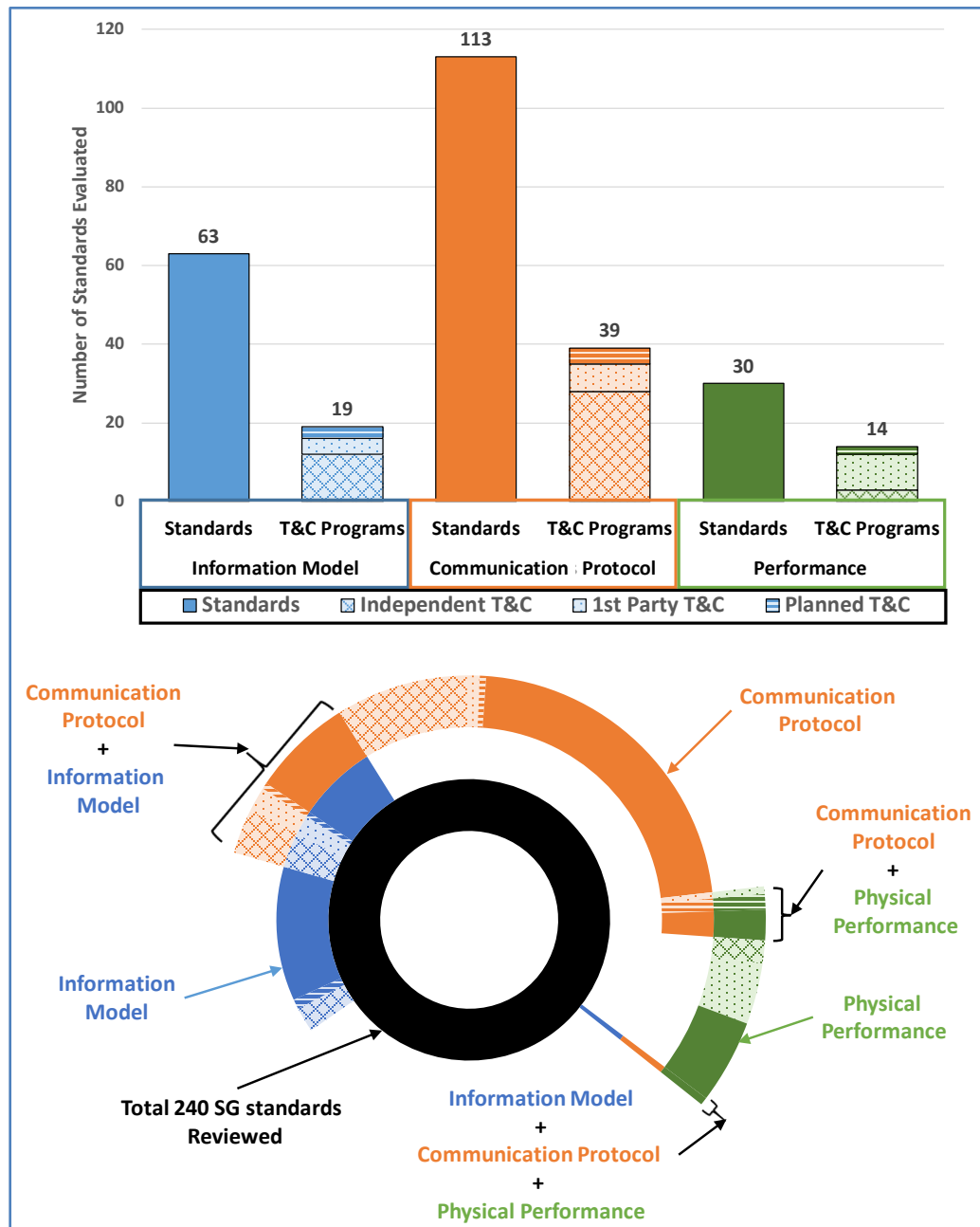


Figure 29 – Interoperability standards and associated testing and certification

6.4.4 Reference interoperability procurement language

Procurement language is crucial to specifying product interoperability requirements so that integration issues can be addressed and mitigated before deployment. It is more efficient for customers to develop interoperability requirements at the purchasing stage than it is to deal with integration issues after products are delivered. Failure to reference specific interoperability requirements in the procurement language increases the chances that the resulting product will not be interoperable with other equipment or systems.

A challenge in this space is that technical requirements for acquisitions by utilities and other customers are often focused on the functional specifications of the systems to be purchased, and do not include appropriate descriptions for the interoperability requirements. One solution is to develop reference language so that it is readily available to specify interoperability requirements during procurement.

NIST is partnering with SEPA and the DOE's Grid Modernization Laboratory Consortium (GMLC) to develop suggested guidelines for interoperability procurement language. This effort will develop a list of interoperability criteria and associated metrics that can be applied to stakeholder procurement language.

6.5 Towards Interoperability Profiles

As described previously, the latest landscape assessment reveals the availability of T&C programs for smart grid standards is quite limited (see **Section 6.4.3**). One opportunity to accelerate T&C program development is through the creation of interoperability profiles, wherein application-derived interoperability requirements are specified. Another is through the development of open-source test tools. Both approaches can provide stakeholders a greater sense of trust regarding device capability and performance.

6.5.1 *Interoperability profiles*

Interoperability Profiles reduce implementation and testing complexity by curtailing and clarifying the range of interoperability requirements to a well-defined subset of those available through standards. Once agreed upon by a user community, testing authority, or standards body, the Interoperability Profile would describe a subset of supported data types, logical nodes and elements, or services, and that subset would narrow interoperability gaps by reducing the available degrees of freedom for implementing standards by the device supplier, implementer, and system owner.

Interoperability Profiles would not replace or be considered standards, but instead would clarify standards-based interoperability implementation requirements for all stakeholders. Interoperability Profiles could therefore take many different forms based on the technology and underlying standards, and by defining the elements of the standard to be utilized for specific application environments would give all stakeholders greater confidence in asset functionality.

The basic set of elements for an Interoperability Profile include the asset description and associated physical performance specifications, communication protocol, and information model. The growing complexity of information models means that only a subset is likely to be necessary for any single application or piece of equipment. This can lead to interoperability failures when devices compliant to the same standard attempt to communicate different parts of the same data model. This communications failure could be

mitigated through the application of Interoperability Profiles that define implementations using a specific subset of the broader standard.

An Interoperability Profile with a narrow set of implementation requirements could be more easily tested for certification, and eventually could be listed by vendors that support it or could be used in procurement specifications by end users. This could facilitate the development and utilization of T&C programs and advance interoperability for smart grid equipment and systems.

6.5.2 Example of an interoperability profile

The core elements of the Interoperability Profile approach have already been successfully demonstrated for smart inverters. California Rule 21 [205] and IEEE 1547-2018 [206] both define the specifications for interconnection and interoperability of distributed energy resources with associated electric power system interfaces. The standards include physical performance specifications, communication protocols, and require data elements. While the physical performance specifications are similarly prescriptive, Rule 21 and IEEE 1547 employ different approaches to the requirements for communication protocols and data elements.

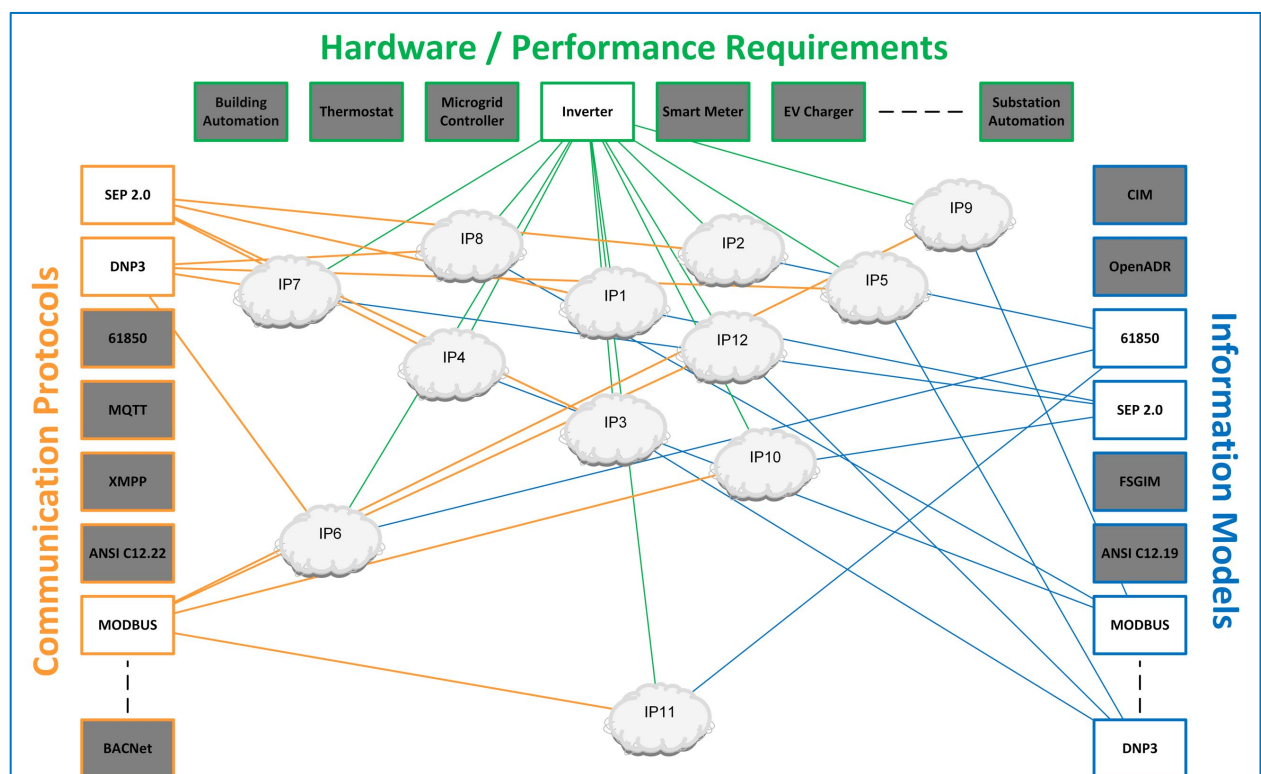


Figure 30 – Potential implementation combinations for IEEE 1547-2018

An inverter communicating via any one of three communications protocols (IEEE P2030.5, IEEE 1815, or Modbus) can conform to the IEEE 1547 standard.⁸⁵ The standard also defines required data elements but does not specify a particular information model, and section 10 of IEEE 1547 describes additional communications protocols and data models (including IEC 61850) that could also be used. The standard therefore offers numerous permutations of possible interoperability implementations, as shown in **Figure 30**.⁸⁶ While the inverter physical performance requirements are clear, the relatively large number of potential communications protocols and data model implementations could limit the ability to test for and certify device interoperability under the IEEE 1547 standard.

California Rule 21 also establishes rules for interconnection of inverter-based DER to the grid. While the physical specifications mirror those of IEEE 1547, Rule 21 specified IEEE P2030.5 as the required communication protocol and IEC 61850 as the required information model. The resulting combination is shown in **Figure 31**. This example demonstrates the application of an Interoperability Profile on existing standards by narrowing the degrees of freedom and complexity for implementing the required communication.

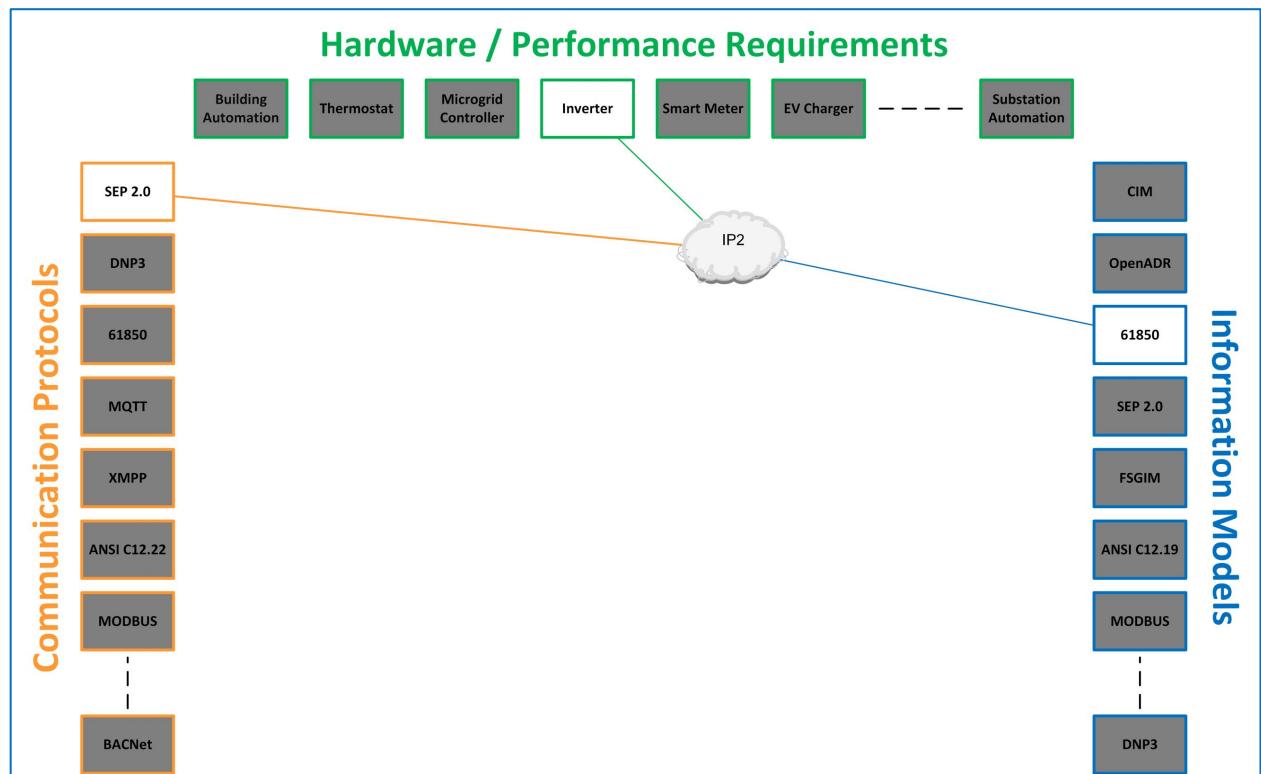


Figure 31 – California Rule 21 interoperability profile implementation

⁸⁵ According to the IEEE 1547-2018 standard, a DER will conform to the standard if it supports any one of three communications protocols, including: IEEE 2030.5 (Smart Energy Profile 2.0), IEEE 1815 (Distributed Network Protocol v3), and SunSpec Modbus. It is therefore possible for two DERs which conform to the IEEE 1547-2018 standard to be unable to communicate with each other because they support different communication protocols.

⁸⁶ The communications protocol and information model labels “SEP 2.0” and “DNP3” in **Figure 30** refer to the protocols and models defined in standards IEEE P2030.5 and IEEE 1815, respectively.

Rule 21 clarified inverter interoperability requirements, and an independent testing and certification program has been formed [207] that has since been adopted as a requirement by utilities and system operators in other regions of the country [208].

6.5.3 Interoperability profiles work plan

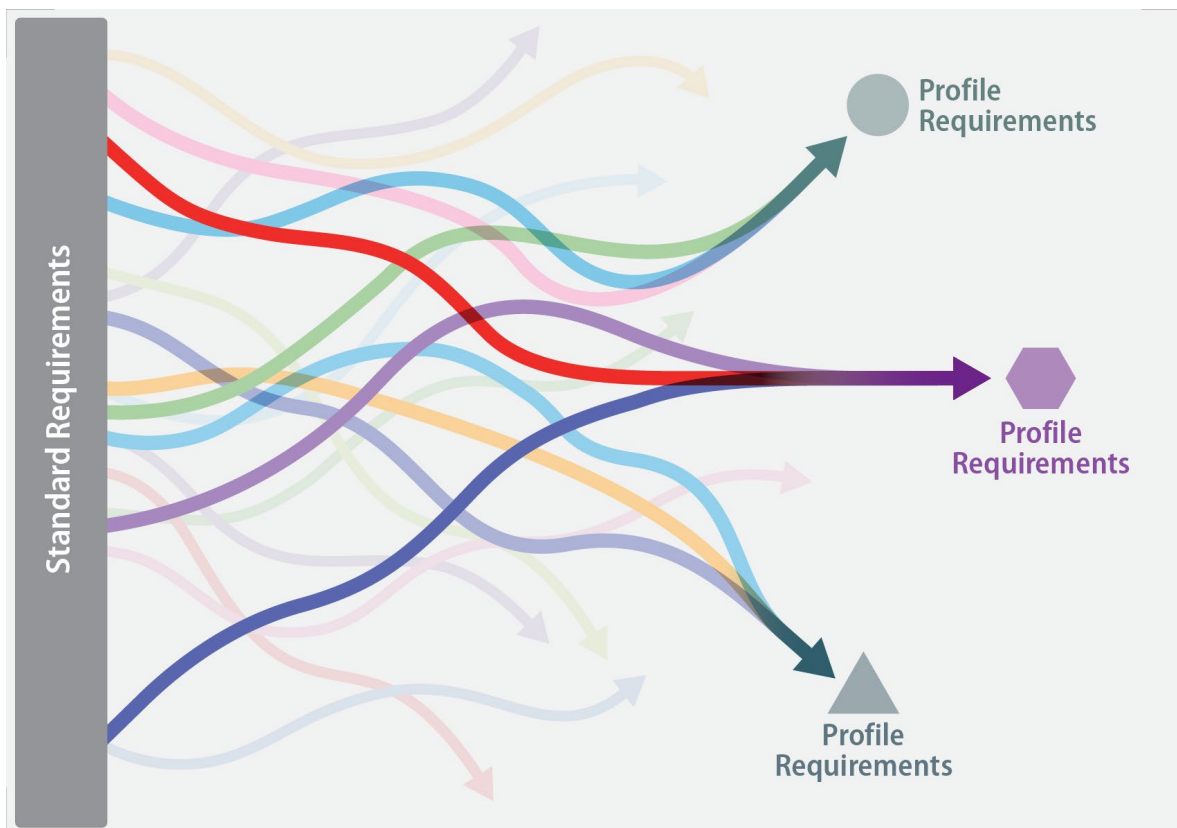


Figure 32 – Interoperability Profiles clarify implementation requirements

Originally described during a 2018 workshop [28], NIST has collaborated with industry and other stakeholders to refine the Interoperability Profile concept and content. As discussed in **Section 6.5.1** and visually represented in **Figure 32**, Interoperability Profiles draw from existing standards to clarify the requirements that will ensure interoperability to support specific functionality of grid-connected assets. The process for developing an Interoperability Profile includes selecting system interfaces and developing a use case to define functional requirements, and then creating a series of documents that describe specific interface requirements and provide implementation guidance.

Developing an Interoperability Profile first requires identifying an appropriate device or system interface. Interface selection will make or break the entire Profile and must present a clear and large enough value proposition to stimulate industry participation in the longer-term Interoperability Profile development process. Evaluation criteria for assessing the value

of any single interface include: industry interest, technological maturity and field deployments of the interface, and the existence of an ecosystem or other organization that can drive Interoperability Profile adoption. Interfaces that facilitate exchanges across smart grid Conceptual Model domains are particularly appropriate (see **Appendix A – Smart Grid Conceptual Model Domains**).

Following interface selection, a use case is developed to capture stakeholder requirements, describe the desired interface functions, provide a list of applicable standards, and identify relevant system actors. With an approach drawn from IEC methods [209], the use case provides an overview of the Interoperability Profile to be developed and is the guiding document for determining specific Profile requirements.

An application guide is created next, wherein the requirements set forth in the Profile use case are mapped to existing standards. This process of identifying relevant standards clarifies the basic structure for how the specific Interoperability Profile requirements will be met.

The Interoperability Profile is developed next, wherein the mapping in the application guide is used to specify standards-based implementation options to satisfy the original use case requirements. The Interoperability Profile will describe how to achieve the interoperability and functionality requirements of the use case by specifying the appropriate configuration options from each standard described in the application guide.

6.5.4 Open-source test tool development

A key component of the T&C process is the test harness, which is created by translated test cases into automated scripts that can be executed to evaluate interoperability functions. Test harnesses create efficiency by automating the test process, but creating test harnesses is often the costliest part of the test program and requires a different skillset than traditional standards development. This high development cost translates to high fees for using test harnesses, and industry has stated the overall cost for developing and using test harnesses is a significant barrier to entry for T&C programs [28].

Once a complete Interoperability Profile is available, the smart grid community can then assess the viability of developing the relevant test harness in an open-source environment. Similar to open-source software development, the community would be expected to develop and manage the tool. The benefit of this approach is that it would allow for broad participation in the test harness development process, and thereby reduce entry barriers for T&C activities.

Upon completion of open-source test tools, equipment manufacturers, customers, or independent test program operators could all have access to and benefit from the capability. This access to the test tool is, in turn, expected to accelerate innovation based upon the Interoperability Profile specifications.

6.6 Conclusions and Future Work

Meaningful interoperability across the power sector is difficult to achieve and — at this time — virtually impossible to ensure. Testing and certification programs are key to enhancing interoperability but are limited in availability and scope. Test programs must also evolve beyond their current practice focusing on standards-driven conformance assessment into a model that supports the types of tests which would better guarantee interoperability of device and system. Interoperability Profiles and open-source test harnesses are two tools that, if properly developed, would facilitate expansion of interoperability focused T&C programs.

Interoperability Profiles can constrain the wide-ranging implementation optionality inherent to most standards, and instead describe application-specific subsets of standard requirements that would reduce the degrees of freedom available to product designers and service implementors. Rather than constraining innovation, this reduced implementation subset would allow the community to purposefully combine selected parts of one or more standards that best support their selected application upon which innovation could flourish. A narrowed subset of implementation requirements should also enable the development of testing and certification regimes that would better assure interoperability capabilities.

The electric vehicle interface has been identified as one that would benefit from improved interoperability [97], and development of an initial Interoperability Profile for managed charging is underway. Creation of the first Interoperability Profile will further socialize the concept and provide an opportunity to refine the development process. There will need to be more Interoperability Profiles in the future, with several additional candidate interfaces already identified [97].

After creation of Interoperability Profiles, the development of open-source test harnesses would eliminate barriers to entry for interoperability testing efforts, and facilitate a rapid expansion of interoperability focused formalized T&C programs.

7. Conclusion

Interoperability remains a critical yet underdeveloped capability of the power system. Significant grid modernization has occurred in the years since the 2007 Energy Independence and Security Act was signed into law, but the proliferation of technology and associated standards complicated the interoperability landscape. The expanding use of distributed energy resources and other technologies has further expanded the interoperability challenge.

This revision of the NIST Smart Grid Interoperability Framework uses evolving technology and power system architectures as context for describing a new set of interoperability perspectives. Examined through emerging operational, economic, and cybersecurity challenges and opportunities, distributed and customer-sited resources figure prominently in the future smart grid — as do distribution systems and other key integrators.

Because interoperability requires shared requirements to enable information exchange between disparate systems, expanding the available communications toolset to facilitate common understanding across stakeholders is a priority of this Framework. Models that aid our understanding of interoperability and other smart grid concerns have been updated or newly introduced in the early sections of this Framework.

The NIST Smart Grid Conceptual Model is updated to reflect technology and platform-driven emerging capabilities in the Customer and Distribution Domains as well as the structural reorganization of a system more reliant on shared infrastructures and distributed resources. A series of Communication Pathways Scenarios help readers examine how interface requirements might change with different system architectures or control strategies. And an ontology for the smart grid is introduced that provides reference language which can be used to clarify communication between stakeholders.

The relationship between emerging physical interactions and grid operations becomes more important with the ongoing transition from analog to digital energy technologies. The emerging system dynamics provide critical context to the informational focus of prior Frameworks. Physical interoperability and trustworthiness are therefore established as critical complements to conventional (informational) interoperability concepts.

Interoperability is identified as a principal enabler of new system control schemes necessary to manage the active participation of distributed resources in a system undergoing the devolution of control authority, all while empowering customers to provide solutions across numerous scales. This expands the interoperability concept beyond the traditional utility-centric focus of interoperability as a mechanism to decrease system integration costs.

More than just a mechanism for measurement and control signals, interoperability is key to the economics of the future grid. The traditional means of ratemaking and cost recovery are under strain as growth in distributed energy resources and changing customer capabilities alter traditional economic dependencies and the role of the distribution utility.

As value propositions change throughout the grid interoperability can minimize transaction costs and minimize entry barriers to market participation, thereby facilitating the creation of new participatory and economic opportunities across the system. Interoperability is also key to ensuring the technical and economic benefits from grid modernization flow across smart grid Domains and stakeholder interests as the electricity system evolves, rather than accruing to single firms or stakeholder classes.

The value brought through introduction of ever-growing technologies and resources also carries with it a growing cybersecurity risk. Utilities and other organizations wanting to benefit from emerging interoperability-enabled opportunities will not be able to assure security by limiting connectivity through physical isolation or other overly restrictive access regimes. Instead, utilities and other stakeholder organizations will have to consider in concert the desired outcomes for the grid and the interfaces (and informational exchanges) that must be protected. The former lends itself to examination through institutional capabilities and processes, which if implemented properly will position a utility or other organization to achieve the latter.

This Interoperability Framework presents a Cybersecurity Risk Profile for the smart grid as a first step towards assessing organizational risk and establishing cybersecurity priorities. An updated assessment of logical interface categories in a High-DER scenario is also presented as a mechanism to improve our understanding of the cybersecurity requirements associated with new technology interfaces and provide a mapping to an existing set of category-driven guidelines.

Through all of this, testing and certification emerges as a critical enabler of grid modernization. The benefits to industry range from operational trustworthiness to investor confidence. But the optionality inherent to standards requirements generally allows for non-interoperability even among proper implementations. Therefore, the current industry focus on certifying conformance to individual standards is only the first step toward assuring interoperability of devices or systems.

The concept of an Interoperability Profile is proposed as one solution to the interoperability challenge. Built upon concepts of both physical and informational interoperability, an Interoperability Profile describes the communications protocol and data model requirements necessary to achieve a specific set of physical functions. Based on existing standards, these Profiles describe the subsets of requirements that, when implemented and verified through testing and certification, would ensure interoperability across devices and systems.

Much work must still be done to realize the smart grid interoperability promise. Case studies and practical guidelines that translate the abstractions of frameworks and other high-level interoperability requirements into actionable lessons will help stakeholders break through the sometimes-paralyzing uncertainty of highly complex systems and allow them to identify and act on strategies to advance smart grid capabilities.

Interoperability is more important today than ever before. Future grid operations, economics, and cybersecurity will demand vast interoperability improvements, and the customer will

depend on interoperability to achieve their objectives and obtain value from their investments no matter their specific priorities. The concepts laid out in this Framework provide a foundation from which the smart grid community and NIST can advance grid modernization and realize the full set of interoperability benefits and opportunities

Appendix A – Smart Grid Conceptual Model Domains

A.1 - Customer Domain

The customer is ultimately the stakeholder that the entire grid was created to support. This is the domain where electricity is consumed, but is increasingly a domain where electricity is actively managed and generated as well (see **Figure 33**). Actors in the *Customer* domain enable customers to manage their energy usage and generation. Some actors also provide control and information flow between the *Customer* domain and the other domains. The boundaries of the Customer domain are typically considered to be the utility meter and the energy services interface (ESI). The ESI provides a secure interface for utility- or service provider-to-customer interactions. The ESI in turn can act as a bridge to facility-based systems, such as a building automation system (BAS) or a customer's premise management system.

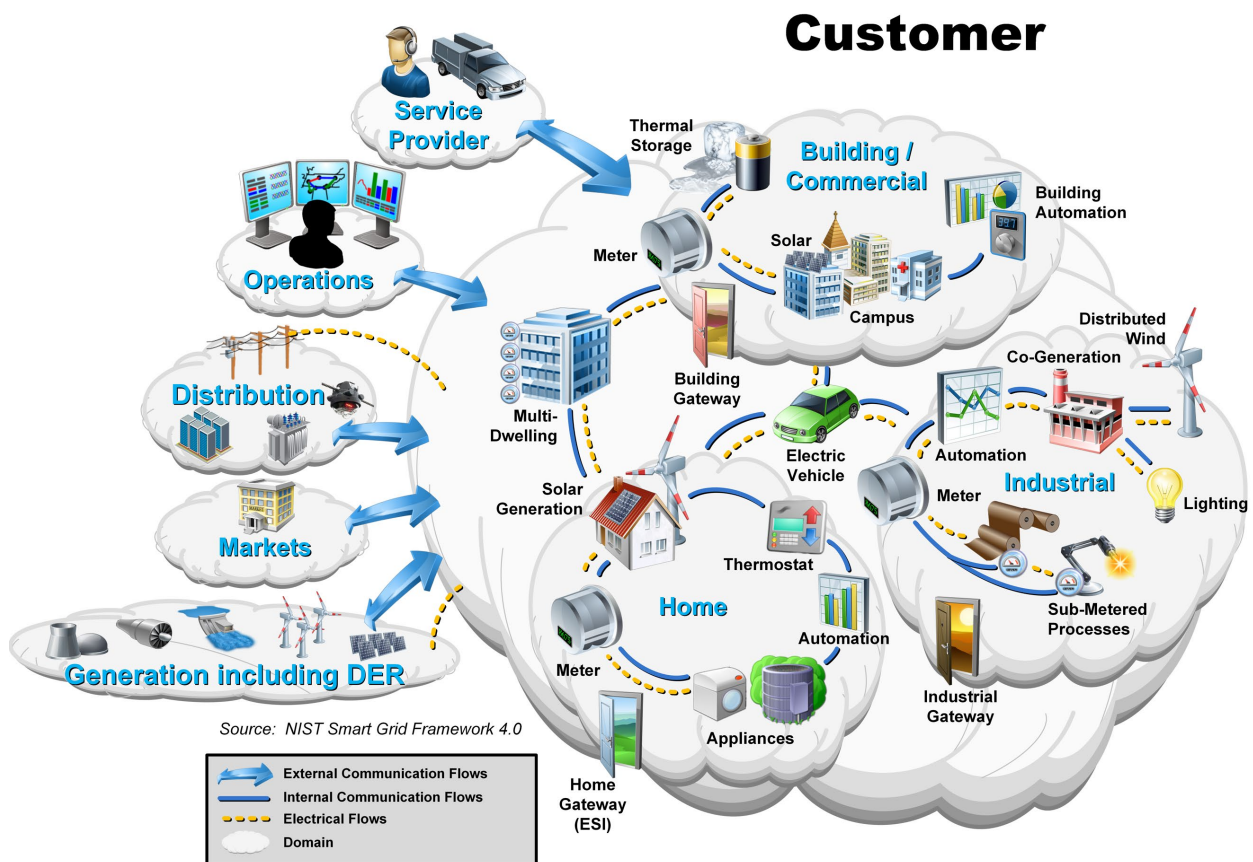


Figure 33 – Overview of the Customer domain

The Customer domain is usually segmented into sub-domains for home, building/commercial, and industrial. The energy needs of these sub-domains are typically less than 20kW of demand for a residence,^{87,88} 20-200 kW for commercial buildings, and over 200kW for industrial. Each sub-domain has multiple actors and applications, which may also be present in the other sub-domains.

Each sub-domain has a meter actor and includes an energy services interface (ESI), which is the primary service interface to the *Customer* domain. The ESI may reside at an end-device, in a premise-management system, in the meter, or outside the premises, and may communicate with other domains via the advanced metering infrastructure (AMI) or other means, such as the internet. The ESI provides the interface to devices and systems within the customer premises, either directly or via a home area network (HAN), other local area network (LAN), or some other mechanism in the future.

There may be more than one communications path per customer. Entry points may support applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems and the enterprise. They may provide auditing/logging for cybersecurity purposes.

In this revision, the *Customer* domain is electrically connected to the *Distribution* and *Generation Including DER* domains. This reflects the potential to connect, in a behind the meter fashion, up to the service rating of DER (up to 320A, nominally for single-phase services), as well as the potential for community energy storage and other DER connected to the distribution system. This diversity in scale and siting highlights a challenge in slotting DER into a specific role within the Conceptual Model, as DERs satisfy different needs depending upon the point of connection.

This *Customer* domain communicates with the *Generation including DER*, *Distribution*, *Operations*, *Market*, and *Service Provider* domains. Examples of typical application categories in the *Customer* domain are in **Table 7**.

⁸⁷ Most residences have either 100A or 200A service, or 24kVA and 48kVA maximum, respectively, at 240VAC. A single EV can introduce loads up to 2.4kVA (Level 1) or 19.2kVA (Level 2) when running at maximum output.

⁸⁸ Peak demand for large multi-family dwellings can exceed 1MW, although the per-residence energy consumption can be 60% less than that of single family homes [210].

Table 7 – Typical application categories in the Customer domain

Example Application Category	Description
Building or Home Automation	A system that is capable of controlling various functions within a building, such as lighting, temperature control and appliance usage.
Industrial Automation	A system that controls industrial processes such as manufacturing or warehousing. These systems have very different requirements compared to home and building systems.
Micro-generation	Includes all types of distributed generation including: solar, wind, and hydroelectric generators. This generation harnesses energy for electricity at a customer location. May be monitored, dispatched, or controlled via communications.
Storage	Means to store energy that may be converted directly or through a process to electricity. Examples include thermal storage units, and batteries (both stationary and electric vehicles)

A.2 - Markets Domain

Markets are where grid assets and services are bought and sold.⁸⁹ Some markets yet to be created may be instrumental in defining the smart grid of the future, particularly with DER and aggregated DER.⁹⁰ Entities in the *Markets* domain exchange price information and balance supply and demand within the power system (see **Figure 34**). The boundaries of the *Markets* domain include the edge of the *Operations* domain where control happens, the domains supplying assets (*Generation including DER, Transmission, and Distribution*), the *Service Provider* domain, and the *Customer* domain. In short, the *Markets* domain interfaces with all domains of the smart grid.

Communication flows between the *Markets* domain and the domains supplying energy are critical because efficient matching of production with consumption is dependent on markets or their proxies. Energy supply domains include the *Generation Including DER* — and more recently the *Customer* — domains. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protections (CIP) standards consider suppliers of more than 300 megawatts to be bulk generation; most DER is smaller and is typically served through aggregators.

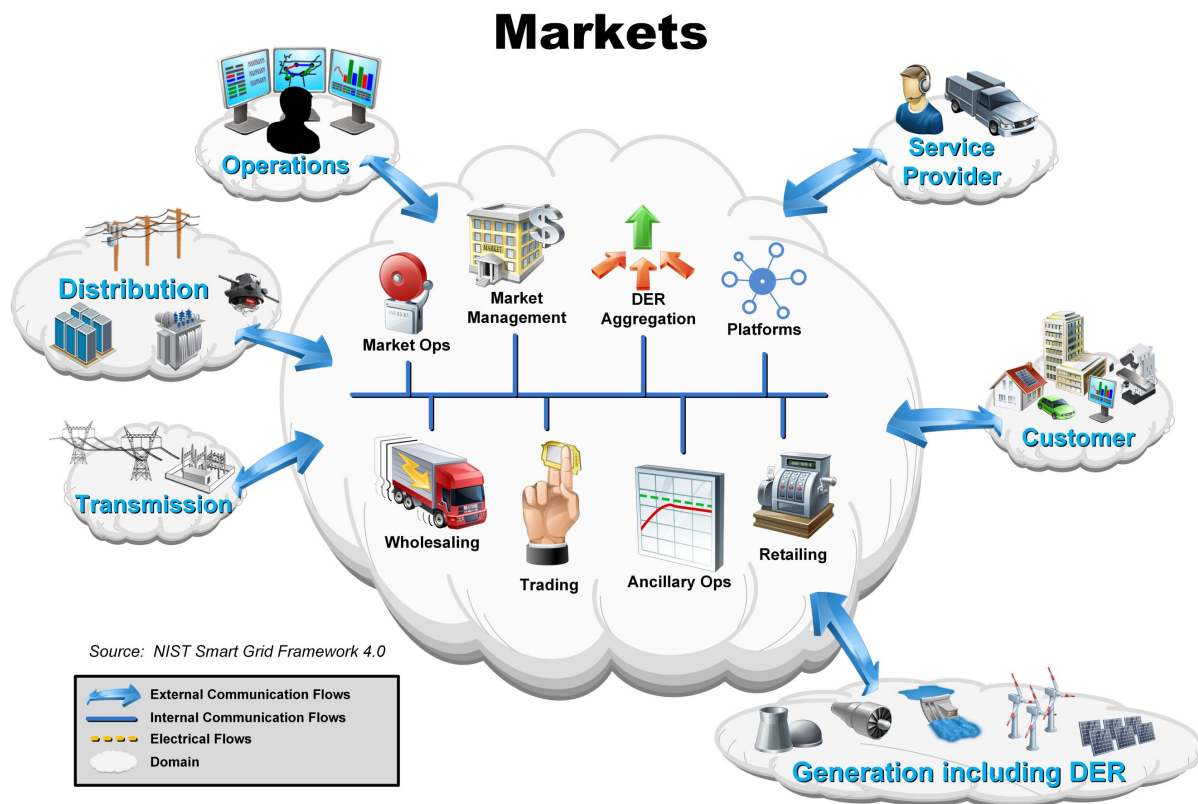


Figure 34 – Overview of the Markets domain

⁸⁹ Entities within the electric power sector have engaged in markets for inputs such as equipment, labor, and fuel since the outset of the sector's development.

⁹⁰ Some utilities utilize market concepts to determine the avoided operational and infrastructure costs associated with deploying DER on their grid.

DERs have an active and growing role in several wholesale markets through aggregation, and will participate to a greater extent as the smart grid becomes more interactive. Hyper-local markets based on peer-to-peer principles such as Transactive Energy have been demonstrated to work for a variety of applications and services, and appear poised to significantly expand the design and role of market interactions with the *Customer* domain. This is in addition to the active and growing role that DER, via aggregation, will have in wholesale markets.

This revision of the *Markets* domain introduces the “Platforms” icon to represent emerging opportunities for interactions among nontraditional grid actors to create value. Fundamentally markets are formed of sets of actors, which collectively establish the price of goods and services [211]. Advances in information and communication technologies have reduced the costs of coordinating and facilitating many types of trades, uncovering new economic opportunity as falling transaction costs improve the value propositions offered by entities at the edge of the grid. Organizational structures such as platforms are increasingly pivotal to the erosion of transaction costs and the formation of decentralized markets for services. The economic potential for the emergence of distribution level platforms is growing with the number and diversity of organizations attempting to pursue opportunities on the electric grid [33].

A major uncertainty remains the relationship between wholesale markets and distribution markets, including the information flows between market operators and participants at each level. The economic fundamentals and legal structures governing market activities and price levels in each market segment (retail and wholesale) co-evolve over time. That is, prices in distribution level markets influence wholesale prices, and vice versa.

Conventionally, prices are determined by rate designs and tariffs adopted by the applicable regulatory authority. These rates include flat rate, time of use rates, or other more dynamic rate designs, such as real time pricing. Rates are primarily a means by which the utility recovers its authorized revenue requirement. Furthermore, rates can also provide a signal to customers on when it is more or less costly to consume electricity thereby encouraging customers to shift consumption to other hours. Emerging technologies that can dynamically and autonomously interpret customer preferences while responding to signals of price, resource availability, and service provision will enable customers to adopt more active strategies for engaging with the electric grid.

Communications for *Markets* domain interactions must be reliable, traceable, and auditable. Also, these communications must support e-commerce standards for integrity and nonrepudiation. As the percentage of energy supplied by small DER increases, requirements for the allowed latency in communications with these resources will have to be formally established.

The high-priority challenges in the *Markets* domain are: extending price and DER signals to each of the *Customer* sub-domains; simplifying market rules; expanding the capabilities of aggregators; ensuring interoperability across all providers and consumers of market information; managing the growth (and regulation) of retailing and wholesaling of energy;

providing access to actionable data about the customer and the grid to support these new technologies and resources; and evolving communication mechanisms for prices and energy characteristics between and throughout the *Markets* and *Customer* domains.

Table 8 – Typical applications in the Markets domain

Example Application	Description
Market Management	Market managers include ISOs for wholesale markets or New York Mercantile Exchange (NYMEX)/Chicago Mercantile Exchange (CME) for forward markets in many ISO/RTO regions. Markets can be used to identify transmission, resource, capacity, and other service needs. These markets may also treat non-traditional resources, like storage and demand response, similar to traditional dispatchable generation.
Retailing	Retailers sell power to end-customers and may in the future aggregate or broker DER between customers or into the market. Most are connected to a trading organization to allow participation in the wholesale market.
DER Aggregation	Aggregators combine smaller participants (as providers, customers, or curtailment) to enable distributed resources to participate in the larger markets.
Trading	Traders are participants in markets, which include aggregators for provision, consumption, curtailment, and other qualified entities. There are a number of companies whose primary business is the buying and selling of energy.
Market Operations	Market operations make a particular market function smoothly. Functions include financial and goods-sold clearing, price quotation streams, audit, balancing, and more.
Ancillary Operations	Ancillary operations provide a market to provide frequency support, voltage support, spinning reserve, and other ancillary services as defined by FERC, NERC, and the various ISOs. These markets normally function on a regional or ISO basis, although local implementations may become more prevalent as new capabilities continue to be introduced to the <i>Distribution</i> and <i>Customer</i> domains.
Platforms	A governance structure or mechanism for connecting potentially diverse organizations and actors that seek to create and deliver value through interaction (including interoperation).

A.3 - Service Provider Domain

Actors in the Service Provider domain perform services to support the business processes of power system producers, distributors, and customers (see **Figure 35**). These business processes range from traditional utility services, such as billing and customer account management, to enhanced customer services, such as management of energy use and home energy generation.

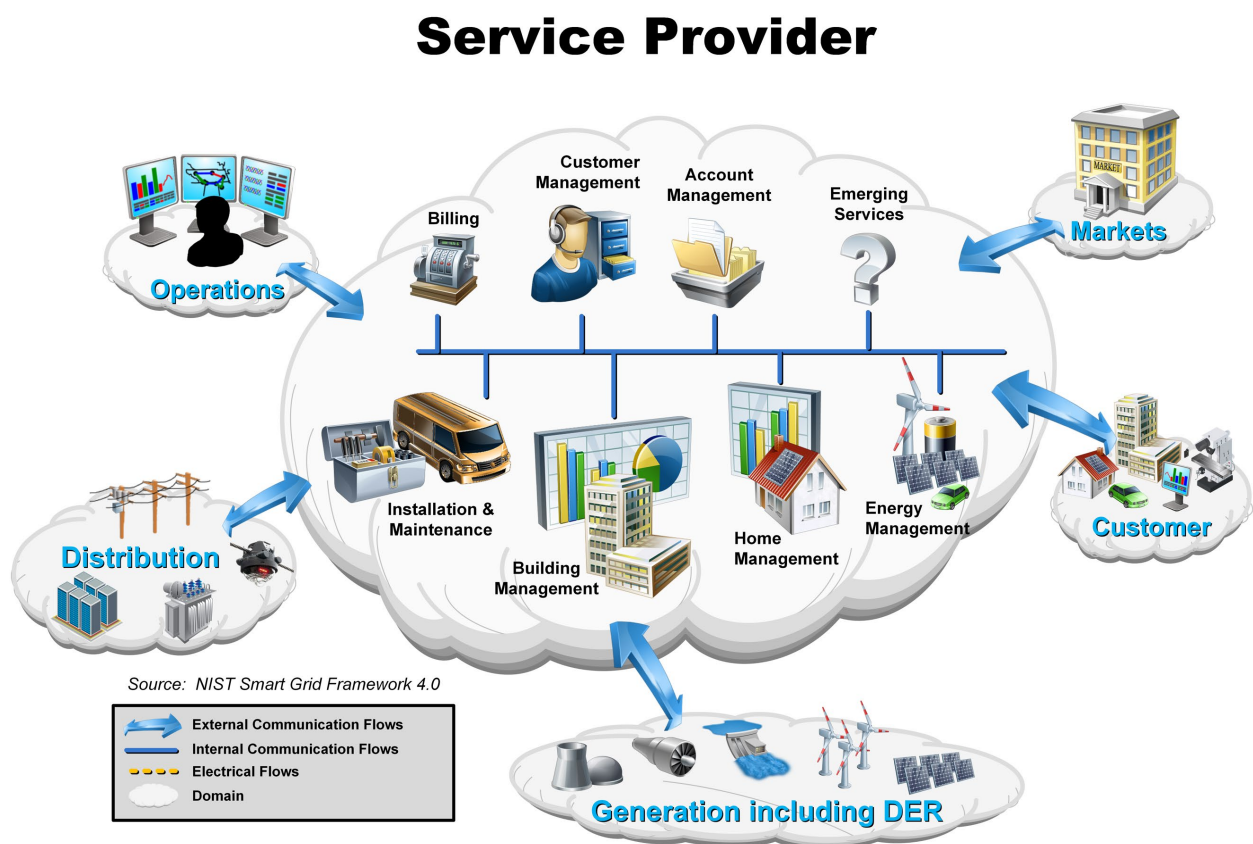


Figure 35 – Overview of the Service Provider domain

Service providers create new and innovative services and products to meet the requirements and opportunities presented by the evolving smart grid. Services may be performed by the electric service provider, by existing third parties, or by new participants drawn by new business models. Emerging services represent an area of significant new economic growth.

The priority challenge in the Service Provider domain is to develop key interfaces and standards that will enable a dynamic market-driven ecosystem while protecting the critical power infrastructure. These interfaces must be able to operate over a variety of networking technologies while maintaining consistent messaging semantics. The service provider must not compromise the cybersecurity, reliability, stability, integrity, or safety of the electrical power network when delivering existing or emerging services.

The *Service Provider* domain is updated here to include an explicit focus on system-level issues that keep the electrical grid running. Where earlier versions of the *Service Provider* domain focused on managing specific assets and functions for their customers,⁹¹ this revision reflects the expanding focus of third-party and other service providers towards co-optimizing energy and infrastructure requirements across multiple customers and value streams.⁹² The introduction of an energy management icon and communications flows with additional domains reflects the expanding service provider roles.

The *Service Provider* domain shares interfaces with the *Generation including DER*, *Distribution*, *Markets*, *Operations*, and *Customer* domains. Communications with the *Operations* domain are critical for system control and situational awareness; communications with the *Markets* and *Customer* domains are critical for enabling economic growth through the development of “smart” services. For example, the *Service Provider* domain may provide the interface enabling the customer to interact with the market.

The addition of communications to the *Distribution* and *Generation including DER* domains reflects the importance of higher DER penetration into utility portfolios, a condition that is likely under all regulatory and market structures given the scalability and rapidly declining costs of many distributed energy technologies [214]. Regardless of whether these new communication flows are from connecting directly to a single, large DER or to an aggregation of DERs behind an interface in the *Distribution* or *Customer* domains, these connections represent new challenges for system actors.

Some benefits to the service provider domain from the deployment of the smart grid include:

- The development of a growing market for non-utility providers to configure value-added services and products to customers, utilities, and other stakeholders at competitive costs;
- The decrease in cost of business services for other smart grid domains;
- A decrease in power consumption and an increase in power generation as customers become active participants in the power supply chain; and
- Better aligning consumption with service conditions, such as price or scarcity, and shifting consumption to optimize the operation of the electric grid.

⁹¹ For example, managing a building or facility for a commercial or residential customer, or certain functions such as customer account management for utility customers.

⁹² As value and benefits for third-party-managed DERs like storage are stacked, the focus and interactions of service providers will naturally expand beyond traditional single-customer relationships [212]. Furthermore, as third-party service providers assume larger roles in retail energy services, the provider’s responsibility to manage impacts on grid infrastructure will grow [213].

Table 9 – Typical applications in the Service Provider domain

Example Application	Description
Customer Management	Managing customer relationships by providing point-of-contact and resolution for customer issues and problems.
Installation & Maintenance	Installing and maintaining premises equipment that interacts with the smart grid.
Building Management	Monitoring and controlling building energy and responding to smart grid signals while minimizing impact on building occupants.
Home Management	Monitoring and controlling home energy and responding to smart grid signals while minimizing impact on home occupants.
Energy Management	Managing assets — often sited at multiple locations — to co-optimize for requirements and objectives at multiple scales and for multiple customers.
Billing	Managing customer billing information, including providing billing statements and payment processing.
Account Management	Managing the supplier and customer business accounts.

A.4 - Operations Domain

Actors in the *Operations* domain are responsible for the smooth operation of the power system. Today, the majority of these functions are the responsibility of a regulated utility (Figure 36).

The smart grid will enable more of these functions to be provided by service providers. No matter how the *Service Provider* and *Markets* domains evolve, there will still be functions needed for planning and operating the service delivery points of a regulated utility that owns and manages the electrical conductors, or wires, that make up the distribution system.

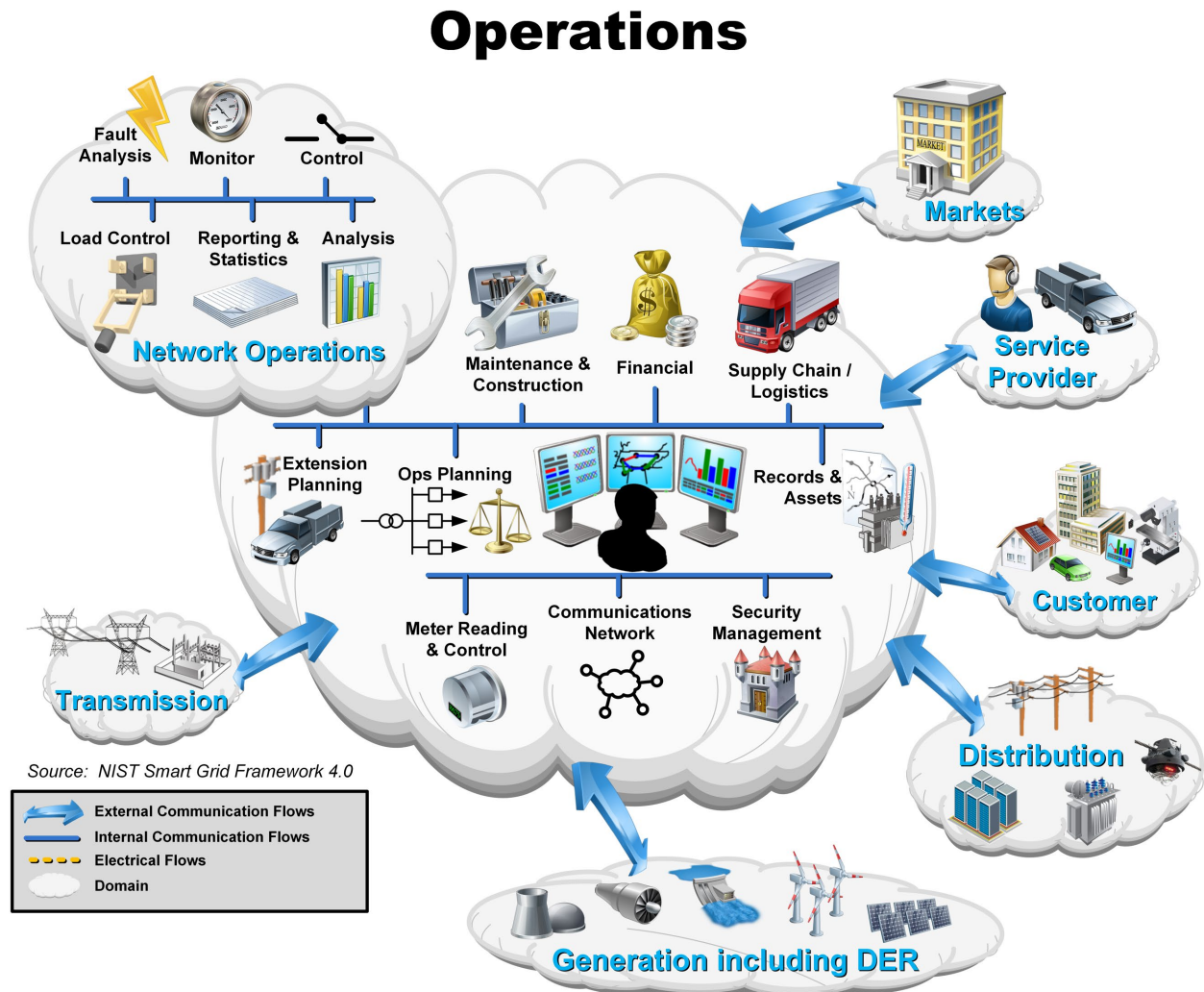


Figure 36 – Overview of the Operations Domain

Currently, at the physical level, various energy management systems are used to analyze and operate the power system reliably and efficiently. The *Operations* domain is updated here to include communication flows with the *Generation Including DER* domain to highlight the importance of resource awareness — including for DERs — in state awareness.

Representative applications within the *Operations* domain are described in (Table 10). These applications are derived from the International Electrochemical Commission (IEC) 61968-1 Interface Reference Model (IRM) for this domain.

Table 10 – Typical applications in the Operations domain

Example Application	Description
Monitoring	Network operation monitoring roles supervise network topology, connectivity, and loading conditions, including breaker and switch states, as well as control equipment status and field crew location and status.
Control	Network control is coordinated by actors in this domain. They may only supervise wide area, substation, and local automatic or manual control.
Fault Management	Fault management roles enhance the speed at which faults can be located, identified, and sectionalized, and the speed at which service can be restored. They provide information for customers, coordinate workforce dispatch, and compile information statistics.
Analysis	Operation feedback analysis roles compare records taken from real-time operation related with information on network incidents, connectivity, and loading to optimize periodic maintenance.
Reporting and Statistics	Operational statistics and reporting roles archive online data and perform feedback analysis about system efficiency and reliability.
Network Calculations	Real-time network calculations (roles not shown) provide system operators with the ability to assess the reliability and security of the power system.
Training	Dispatcher training roles (not shown) provide facilities for dispatchers that simulate the actual system they will be using.
Records and Assets	Records and asset management roles track and report on the substation and network equipment inventory, provide geospatial data and geographic displays, maintain records on non-electrical assets, and perform asset-investment planning.
Operational Planning	Operational planning and optimization roles perform simulation of network operations, schedule switching actions, dispatch repair crews, inform affected customers, and schedule the importing of power. They keep the cost of imported power low through peak generation, switching, load shedding, DER or demand response.

Maintenance and Construction	Maintenance and construction roles coordinate inspection, cleaning, and adjustment of equipment; organize construction and design; dispatch and schedule maintenance and construction work; and capture records gathered by field technicians inform and perform their tasks.
Extension Planning	Network extension planning roles develop long-term plans for power system reliability; monitor the cost, performance, and schedule of construction; and define projects to extend the network, such as new lines, feeders, or switchgear.
Customer Support	Customer support roles help customers to purchase, provision, install, and troubleshoot power system services. They also relay and record customer trouble reports.
State Estimation	A process by which Network Calculation algorithms are applied to real-time measured parameters across the electrical grid to produce the information necessary to operate and optimize the system.

A.5 - Generation Including DER Domain

Electricity generation is the process of creating electricity from other forms of energy and is the first process in delivering electricity to customers. This conversion may include a wide variety of primary energy resources and conversion technologies ranging from chemical combustion and nuclear fission, to flowing water, wind, solar radiation, and geothermal heat. As the primary electricity supply for the electrical grid, the *Generation Including DER* domain is electrically connected to the *Transmission* or *Distribution* or *Customer* domain, and shares communications interfaces with the *Operations*, *Markets*, *Transmission*, and *Distribution* domains.

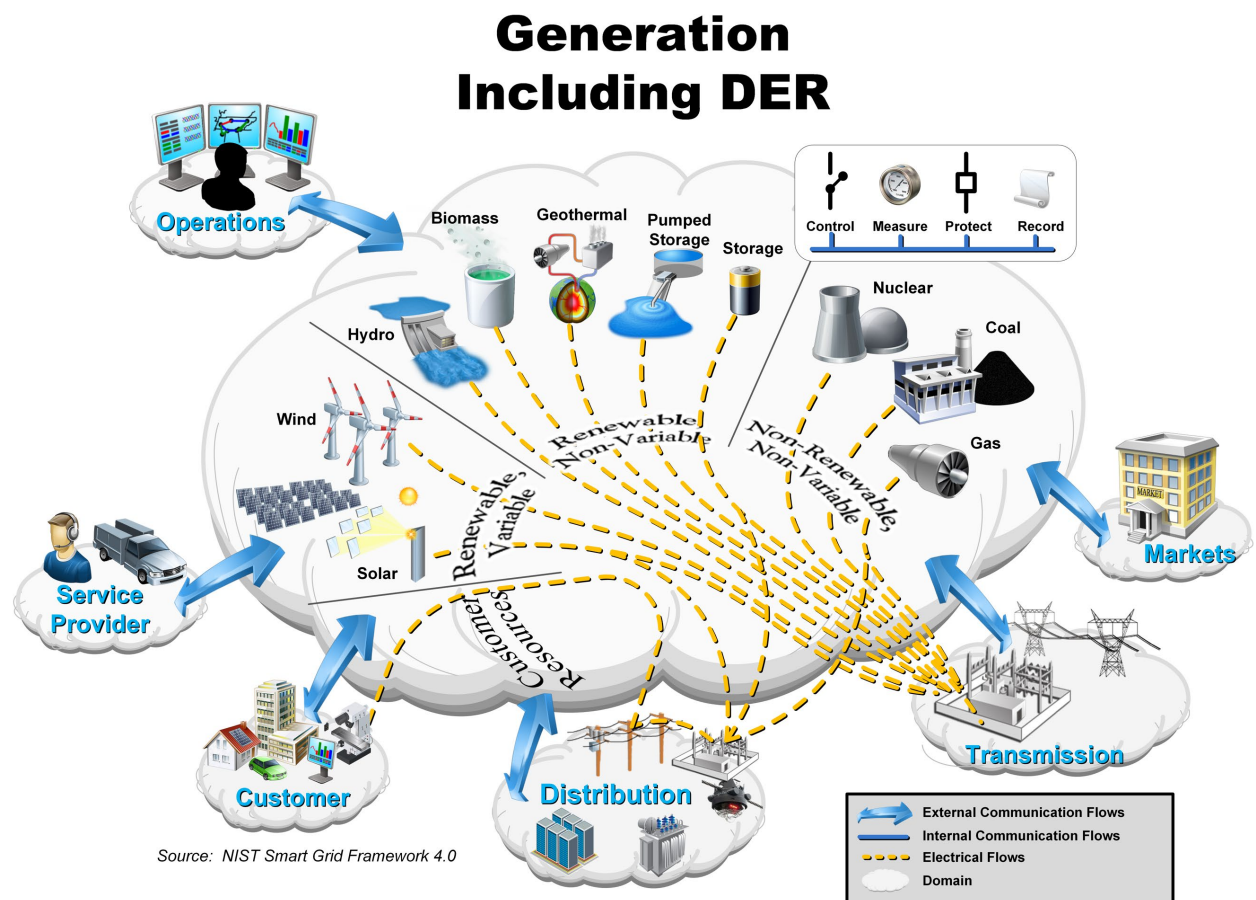


Figure 37 – Overview of the Generation Including DER Domain

Historically provided by large generators that fed only the high-voltage transmission system, the scalability and modularity of modern generating technologies alters the physical relationship and points of coupling between generation assets and the grid, as well as the distribution of generation assets. Accordingly, this domain has been updated to reflect direct electrical interconnection with the distribution system that smaller scale and distributed generation assets may utilize. The domain has also been renamed *Generation Including DER*.

Communications with the *Transmission* and *Distribution* domains are critical, because without a delivery mechanism, customers cannot be served. The *Generation Including DER* domain should communicate key performance and quality of service issues such as scarcity and generator failure. These communications may cause the routing of electricity from other sources, or trigger an increased reliance on customer-cited measures described below. A lack of sufficient supply is addressed directly (via *Operations*) or indirectly (via *Markets*).

For this revision, NIST has introduced a *Customer Resources* segment which includes an electrical flow that passes through the *Generation Including DER* domain to connect the *Customer* and *Distribution* domains. Aligning the *Customer Resources* electrical flow with the electrical flows from the broader set of generation resources is a visual indication of the growing participation of customer-sited generation resources in conventional settlement and dispatch processes. Initiating the customer resource in the *Customer* domain — which includes distributed generation, demand response, and other load-management technology — reflects the growing number of market structures which treat demand management similarly to generating capacity [215] and/or energy production [216]. Beginning the electrical flow in the *Customer* domain and terminating it on a secondary feeder in the *Distribution* domain highlights the unique physical conditions and control requirements for customer-sited resources when compared to conventional generation assets.

Communication are extremely critical to the increasingly pervasive DER at the bulk system and distribution levels, including behind-the-meter installations. The *Generation Including DER* domain has therefore been updated in this revision to explicitly identify necessary communications flows with the *Distribution*, *Customer*, and *Service Provider* domains. These external communications flows (shown as bidirectional arrows in **Figure 37**) represent the inter-domain communications flows previously drawn in **Figure 4**, and are not intended to describe specific interactions among roles or actors.

Evolving requirements for the *Generation Including DER* domain may include priorities such as controls for greenhouse gas emissions [217], increases in renewable energy sources [218], and provision of storage [219] to manage the variability of renewable generation or defer infrastructure obsolescence. To the extent that some of these goals require coordination across multiple domains, this complexity and associated interoperability requirements can be examined through the Conceptual Model communications flows. Roles in the *Generation Including DER* domain may include various physical actors, such as protection relays, remote terminal units, equipment monitors, fault recorders, user interfaces, and programmable logic controllers.

Examples of typical functions within the *Generation Including DER* domain that depend on communications flows and require interoperability are shown in **Table 11**.

Table 11 – Typical applications requiring interoperability in the Generation Including DER domain

Example Application	Description
Control	Performed by roles that permit the <i>Operations</i> domain to manage the flow of power and the reliability of the system. Currently a physical example is the use of phase-angle regulators within a substation to control power flow between two adjacent power systems.
Measure	Performed by roles that provide visibility into the flow of power and the condition of the systems in the field. In the future, measurement might be built into increasingly more discrete field devices in the grid. Currently, an example is the digital and analog measurements collected through the supervisory control and data acquisition (SCADA) system from a remote terminal unit and provided to a grid control center in the Operations domain.
Protect	Performed by roles that react rapidly to faults and other events in the system that might cause power outages, brownouts, or the destruction of equipment. Performed to maintain high levels of reliability and power quality. May work locally or on a wide scale.
Record	Performed by roles that permit other domains to review what happened on the grid for financial, engineering, operational, and forecasting purposes.
Asset Management	Performed by roles that work together to determine when equipment should have maintenance, calculate the life expectancy of the device, and record its history of operations and maintenance so it can be reviewed in the future for operational and engineering decisions.

A.6 - Transmission Domain

Transmission is the bulk transfer of electrical power from generation sources to distribution through multiple substations (see **Figure 38**). A transmission network is typically operated by a transmission-owning utility, Regional Transmission Operator or Independent System Operator (RTO, ISO respectively), whose primary responsibility is to maintain stability on the electric grid by balancing generation (supply) with load (demand) across the transmission network. Examples of physical actors in the *Transmission* domain include remote terminal units, substation meters, protection relays, power quality monitors, phasor measurement units, sag monitors, fault recorders, and substation user interfaces.

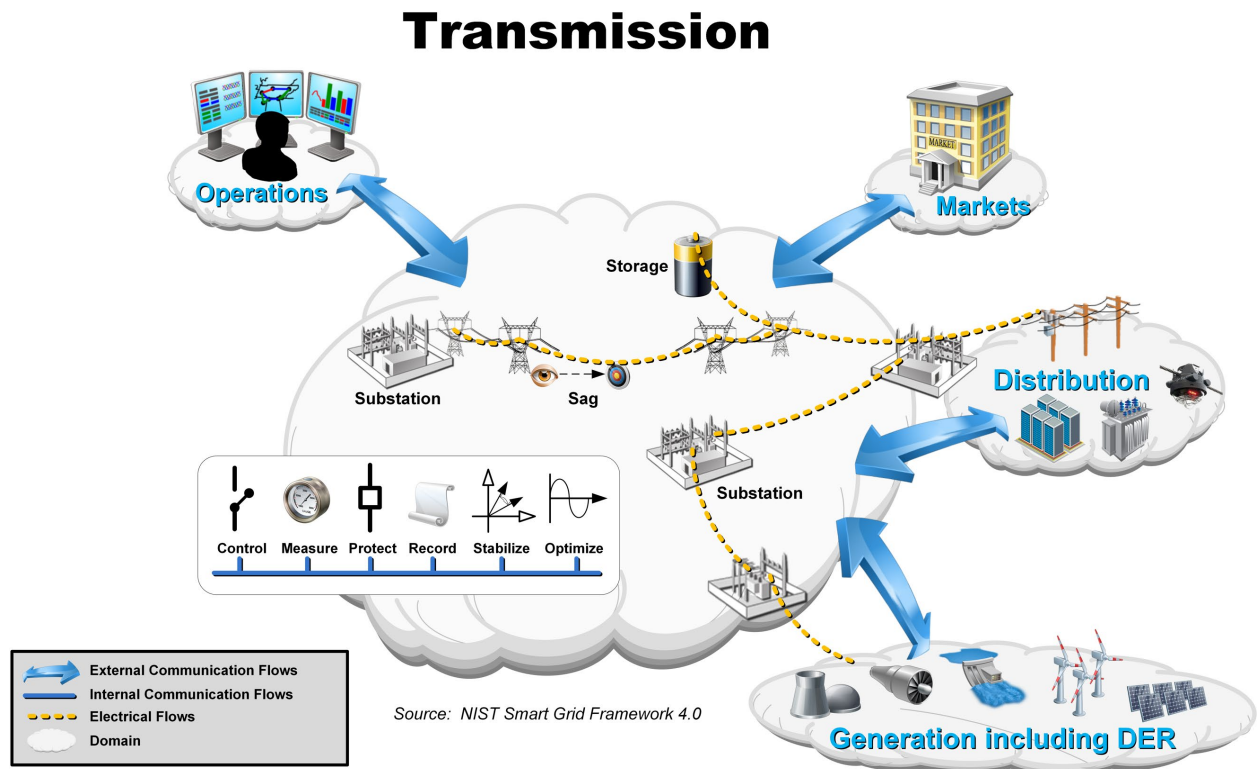


Figure 38 – Overview of the Transmission domain

Roles in the *Transmission* domain typically perform the applications shown in the diagram (**Figure 38**) and described in the table (**Table 12**). The Transmission domain may contain DER, such as electrical storage or peaking generation units.

Energy and supporting ancillary services (capacity that can be dispatched when needed) are procured through the *Markets* domain; scheduled and operated from the *Operations* domain; and finally delivered through the *Transmission* domain to the *Distribution* domain and ultimately to the *Customer* domain.

A transmission electrical substation uses transformers to step up or step down voltage across the electric supply chain. Substations also contain switching, protection, and control equipment. **Figure 38** depicts both step-up and step-down substations connecting generation

(including peaking units) and storage with distribution. Substations may also connect two or more transmission lines.

Transmission towers, power lines, and field telemetry (such as the line sag detector shown) make up the balance of the transmission network infrastructure. The transmission network is typically monitored and controlled through a SCADA system that uses a communication network, field monitoring devices, and control devices.

Table 12 – Typical applications in the Transmission domain

Example Application	Description
Substation	The control and monitoring systems within a substation.
Storage	A system that controls the charging and discharging of an energy storage unit to bridge temporal mismatches in supply, demand, and infrastructure capabilities.
Measurement & Control	Includes all types of measurement and control systems to measure, record, and control, with the intent of protecting and optimizing grid operation

A.7 - Distribution Domain

The *Distribution* domain is the electrical interconnection between the Transmission domain, the Customer domain, and the metering points for consumption, distributed storage, and distributed generation (see **Figure 39**). As does the *Generation including DER* domain, the *Distribution* domain may contain DER, such as electrical storage, peaking generation units, or other medium-scale assets such as community solar installations.

The electrical distribution system may be arranged in a variety of structures, including radial, looped, or meshed. The reliability of the distribution system varies depending on its structure, the types of configuration and control devices that are implemented, and the degree to which those devices communicate with each other and with entities in other domains.

Historically, distribution systems have been radial configurations, with little telemetry, and almost all communications within the domain was performed by humans. The primary installed sensor base in this domain was previously the customer with a telephone, whose call would initiate the dispatch of a field crew to restore power. Many communications interfaces within this domain have been hierarchical and unidirectional, although they now generally can be considered to work in both directions, even as the electrical connections are just beginning to support bidirectional flow. Distribution actors may have local inter-device (peer-to-peer) communication or a more centralized communication methodology. The use of higher speed communications to manage and optimize power flow and electricity generation and consumption in real time is an emerging concern for all stakeholders, particularly with higher penetration of DER (grid or behind-the-meter).

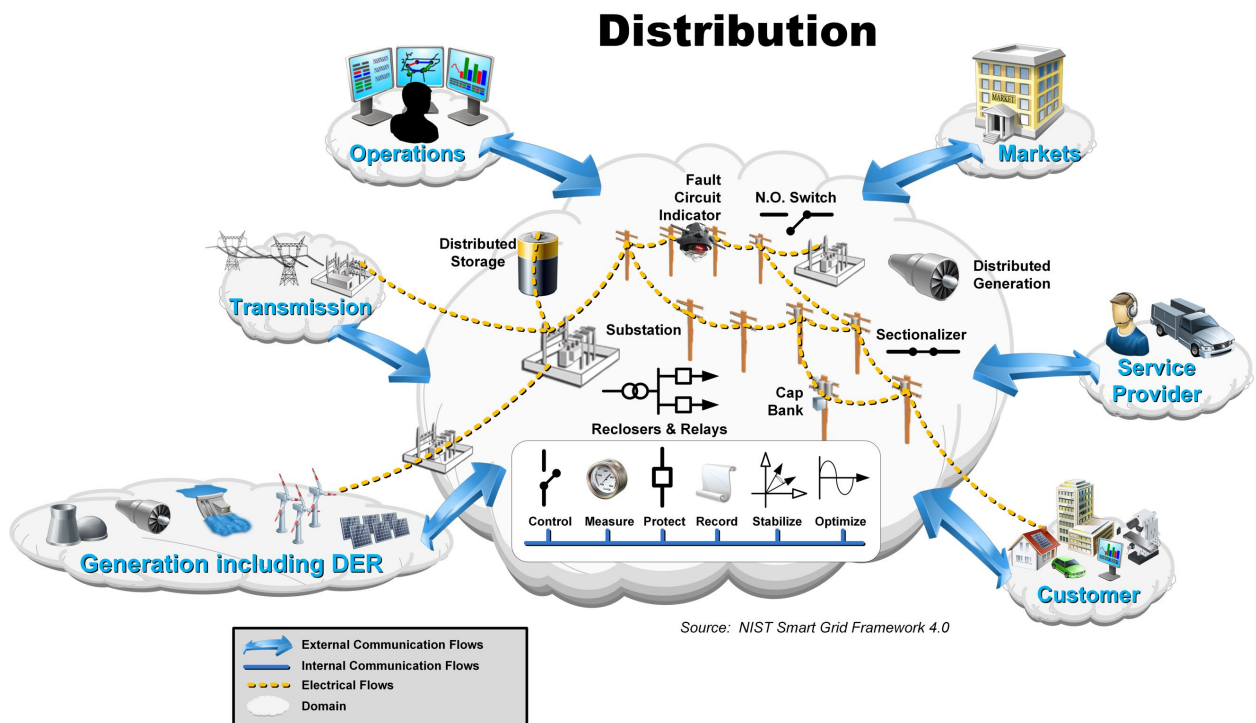


Figure 39 – Overview of the Distribution domain

In the smart grid, the *Distribution* domain will have increased sensing and control capabilities and communicate in a more granular fashion with the *Operations* domain in real-time to manage the complex power flows associated with new technologies, a more dynamic *Markets* domain, and other environmental and security-based factors. In general this dynamic indicates a need for improving distribution system observability and awareness, and the *Distribution* domain model in **Figure 39** has been updated to include additional sensing devices (e.g., fault circuit indicator) as well as domain operational functions (e.g., stabilize) which had been limited to the *Transmission* domain in previous Conceptual Models.

The *Markets* domain will communicate with the *Distribution* domain in ways that will affect localized consumption and generation. In turn, these behavioral changes due to market forces may have electrical and structural impacts on the *Distribution* domain and the larger grid. Under some models, service providers may communicate with the *Customer* domain using the infrastructure of the *Distribution* domain, which would change the communications infrastructure selected for use within the domain.

It should be noted that DER can be considered both a *Transmission* and *Distribution* asset, so the model has been updated to reflect this reality from the electrical and communications standpoints. Examples of typical application categories in the *Distribution* domain are in **Table 13**.

Table 13 – Typical applications within the Distribution domain

Example Application	Description
Substation	The control and monitoring systems within a substation
Storage	A system that controls the charging and discharging of an energy storage unit to bridge temporal mismatches in supply, demand, and infrastructure capabilities.
Distributed Generation	A power source located in the <i>Distribution</i> domain of the grid.
Non-Wires Alternatives	DER, either individually or aggregated, that are used to replace or defer distribution infrastructure upgrades.
Measurement & Control	Includes all types of measurement and control systems to measure, record, and control power flows, with the intent of protecting and optimizing grid operation.

Appendix B – Mapping CPS Aspects and Concerns to the Electrical Grid

This appendix presents the evaluation of grid context for the existing set of CPS concerns as described in **Section 2.3**. Note that the Description column in **Table 14** contains a summary of the concern as defined in the CPS framework, and has been included here verbatim from that document. The “Architecture Significance” column provides some examples of how each concern relates to activities or emerging trends in power systems, as well examples of changes that could arise as new architectures are introduced. The architecture significance column therefore may help clarify the importance of CPS concerns to the electrical grids of today and tomorrow.

Table 14 – Mapping CPS Aspects and Concerns to the electrical grid

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	Actuation	Concerns related to the ability of the CPS to effect change in the physical world.	• Geographic separation between power generation and its use requires sufficient electric transmission and improved bulk power control systems, including structural changes to existing systems to better manage the increasing fast grid dynamics and rising influence of distribution systems in bulk system operations.¹ In addition, the increased role of distribution grids requires greater coordination between premise, distribution, and bulk control systems and their operators. • Examples of new and anticipated control capabilities to address these power system actuation needs include better managing electric vehicle (EV) impact by monitoring and controlling EV chargers, and reconfiguring circuits using automatic circuit configuration, e.g. FLISR.	Ability to impact the power flow throughout the grid, including sources and load, by means of controlled, often remote, actuation of power systems equipment.	• To support overall grid system control through improved actuation capabilities, distribution systems are likely to need additional capabilities such as situational awareness and algorithms, previously needed only for transmission systems, e.g. state estimation. • To optimize distribution systems for new capabilities such as managed/smart EV charging and automatic circuit reconfiguration, projections of EV demand and generation levels and implementation of new Protection and Relay schemes that effectively respond to grid events are needed.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	Communication	Concerns related to the exchange of information internal to the CPS and between the CPS and other entities.	•Architecture concerns include sharing of infrastructure for communications.³³ • Legacy communications systems are widely deployed, trusted, tested, and represent billions of dollars of investment, thus transition to modern communications is likely to occur over an extended time period.	Exchange of information between internal and external networks including communications protocols, the communication network, and the exchange between interested parties.	• Additional sensors and wider-geographic area communications systems are needed to support the broad range of new functional communications requirements, including for enhanced situational awareness at the Distribution level. • Use of public communications networks will likely increase. • The addition of new distribution automation devices/intelligent electronic devices/meters will require more communications capabilities, e.g. higher bandwidth. •Architecture must support both rapid and slow transitions from legacy SCADA over IP devices/communications.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	Controllability	Ability of a CPS to control a property of a physical thing. There are many challenges to implementing control systems with CPS including the non-determinism of cyber systems, the uncertainty of location, time and observations or actions, their reliability and security, and complexity. Concerns related to the ability to modify a CPS or its function, if necessary.	• Controllability requires coordination of sensing, processing and acting. • Multiple inputs, including from multiple systems, are needed to inform control decisions. • Most grid control systems and hardware were not designed to accommodate large numbers of distributed energy resources (DERs). • More dynamic monitoring and control is needed to be able to respond to dynamic grid conditions.	Ability to control grid properties (sense, process and change); e.g., intentionally change a property.	• To provide the required controllability, distribution systems are likely to need situational awareness and algorithms previously only needed for transmission systems, e.g. state estimation. • Coordination of sensing and processing functions is needed to produce accurate control signals. • Architectures may need to support control applications that use multiple optimization factors including those based on carbon usage and market prices. • Architectures may need to support use of group commands (e.g., DNP3 settings groups) and third-party aggregator control of DERs. • Architecture support of faster input of sensor data from traditional SCADA devices and newer devices including phasor measurement units (PMUs) is needed.
Functional	Functionality	Concerns related to the function that a CPS provides.	• The constant evolution of the power system requires continual development and integration of new grid functionality. • Grid control functionality has expanded to include increased management of generation assets, including with diverse ownership, varying control capabilities, and distributed locations, all of which require different control functionality.	Ability to provide grid functions, e.g. control functions, sensing functions, service-related functions.	• Innovative grid technology is needed to facilitate development and implementation of a range of new grid functionalities, including in power markets, DERs, microgrids, Electric Vehicles, and others. • Architecture needs to support management of DERs with new control capabilities that differ from that of older types of generation.
Functional	Manageability	Concerns related to the management of CPS function.	• New functionalities are needed to improve effective management of an ever-changing portfolio of devices and systems that are deployed and operated at different grid levels.	Ability to develop and implement new functionality to manage change internally and externally to the grid.	• Communication topology views and key externally visible properties based on multi-tier distribution communications are needed for system control, substations, field operations, and Transmission/Distribution integration.⁷⁴

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	Measurability	Concerns related to the ability to measure the characteristics of the CPS.	• Changing dynamics of the grid require faster measurement of grid characteristics to gain visibility and situational awareness needed to enable active management instead of historically passive approaches, e.g. through physical inertia of generation. • SCADA systems typically report data at slow rates, e.g. once every 4 seconds, compared to new IoT control systems that can operate in the millisecond or microsecond timeframe. • Behind the meter (BTM) generation is typically not measured.	Ability to quantify a phenomenon / property against a known reference or fundamental definition.	• Architecture needs to support applications and sensors with a broad range of data rates. • Behind the meter (BTM) generation can be characterized through measurements with separate meters, or by using other techniques to estimate non-metered generation.
Functional	Monitorability	Concerns related to the ease and reliability with which authorized entities can gain and maintain awareness of the state of a CPS and its operations. Includes logging and audit functionality.	• Increasing complexity of bulk energy systems, combined with reduced operating margins, results in new and more complicated grid control issues⁸ and increased need for multi-tier situational awareness. • Additional visibility and monitoring, including to better forecast supply and demand, is needed to support increased deployment of prosumer systems, which both use and generate electricity and may be located behind the meter. • Distribution state estimation will require consistent monitoring of measured distribution grid data to be useful.	Measuring a property over a period of time.	• Architecture support will be needed for increased input of grid sensor data and control messages, including DER. • Improved forecasting algorithms will be needed that use historical prosumer net load or generation as well as near-real time production data. • State Estimation algorithms that produce consistent, accurate results will be needed.
Functional	Performance	Concerns related to whether a CPS can meet required operational targets.	• Geographic and temporal mismatches between supply and demand are growing in some areas. • Energy efficiency and overall energy use of ubiquitous IoT devices, when powered using alternating current (AC) power, may be improved by taking advantage of the capability to run natively on direct current (DC) power to avoid losses due to AC-DC conversion.	Ability to deliver power as required by consumers.	• Architecture support is needed to provide additional balance between supply and demand, for example, supporting installation of DERs with Energy Storage in areas with challenges to support increased DER. • Architecture advances are needed to support new DC networks, such as in homes and commercial buildings, for lighting systems, electric vehicles, and distributed solar PV systems.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	Physical	Concerns about purely physical properties of CPS including seals, locks, safety, and EMI.	• Grid devices and systems have specific physical requirements for operation, protection, and safety. • There are requirements for hardening of devices, e.g., physical enclosure, immunity to EMI, and others.	Ability to ensure proper physical configuration in the operating environment.	• For architectures in which the active operating environment is designed to extend further towards the edge of domains, proper configuration and physical properties of new assets must be assured (e.g., edge devices may need additional physical security to ensure consumer safety).
Functional	Physical Context	Concerns relating to the need to understand a specific observation or a desired action relative to its physical position (and uncertainty). While this information is often implied and not explicit in traditional physical systems, the distributed, mobile nature of CPS makes this a critical concern.	• The physical context, including geographical location of the device in the system as well as its location in the topology, is important for managing functional capabilities including monitoring and control. • The need for local optimization of grid assets increases with physical decentralization of distributed resources towards the edges of systems. Increased congestion (e.g. at the edge) may affect operations of aging infrastructure when load reaches or exceeds the originally designed physical limits of distribution systems.	Concerns relating to the need to understand information on the geographic and topological location of the physical asset.	• Architecture element will need to include physical location as well as network location for the devices. • Architectures should accommodate temporal changes in physical context as new asset deployments and system contingencies impact topology.
Functional	Sensing	Concerns related to the ability of a CPS to develop the situational awareness required to perform its function.	• Internet of Things (IoT)-related grid technology changes include small systems and solutions rather than large centrally controlled solution, flexible solution rather than fixed solutions, and wireless communications increasingly used whenever possible.¹⁸ • Increasing complexity of the grid may impact the ability to sense grid conditions and status.	Ability to detect a property of the electrical grid over time.	• Additional smart devices and distributed sensors are needed to increase the level of information, monitoring, and control at various points of the distribution system. • Sensors and communications for distribution observability are needed to be architected as core infrastructures.⁷³

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Functional	States	Concerns related to the states of a CPS. For example, the functional state of a CPS is frequently used to allow for variation in the CPS response to the same set of inputs. Variation in response based on state is sometimes referred to as functional modes.	• State estimation is one of the most important functions performed by system operators, and its use is extending from the bulk system to distribution systems. Proper state estimation allows control signals to be adjusted to optimize system operations and economics, and is important to maintaining system reliability and resilience by ensuring contingencies are available and activated when grid systems are operated beyond the designed capabilities or fail. • The proliferation of connected devices and systems in the grid will introduce new capabilities and provide new input data for state estimation. This will also require greater situational awareness across the system. • The ability to monitor and control devices is critical in the modernized grid.	Concerns related to the ability to know the operating status and conditions of the grid and connected assets.	• Architectures must clearly identify which smart devices and sensors are important to state estimation, what information is required from those devices, and how that information should be communicated. • As the granularity of state estimation changes over time, architecture elements should define the systems with which smart devices must communicate operational and state information. • Smart devices and sensors with multiple capabilities can affect the ability to measure local system states, and networked devices can impact state estimation across wider areas. With increasing technological diversity, communications about operating status must match the needs and informational capacity of the interfacing systems.
Functional	Uncertainty	Managing the effects of uncertainties is a fundamental challenge in CPS. Sources of uncertainty in CPS can be grouped into statistical (aleatoric), lack of knowledge (epistemic) uncertainty, or systematic uncertainty. In CPS, statistical uncertainty is caused by randomness of accuracy of sensing and actuation, often caused by uncertainty of manufacturing processes. Systematic uncertainty is caused by incomplete knowledge either due to limits of acquired knowledge or due to simplification in modeling. Typical manifestations of epistemic uncertainty are limited validity of models of physical processes or limits of computability of properties of mathematical models.	• Fundamental limitations in the spatial and temporal ability to observe the electrical grid create uncertainty between model forecasts and actual operations. As sensors are deployed that can observe previously unmonitored aspects of the grid, this uncertainty can be minimized. Uncertainty can be reduced but not fully eliminated for a system as large and complex as the electric grid. • High penetration of variable generation renewable technologies and other DERs broadens the drivers of uncertainty that must be accounted for by grid operators. • Improved understanding of uncertainty propagation would benefit grid operators.	Concerns related to the ability to characterize and mitigate uncertainty in the system for improved operations. Sources of uncertainty in the grid can include forecast error; randomness of individual actions affecting supply, load, or infrastructure; sensor limitations; and incomplete knowledge of the system.	• Architecture elements will need to include uncertainty thresholds related to operational schemes.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Business	Cost	Concerns related to the direct and indirect investment or monetary flow or other resources required by the CPS throughout its lifecycle.	• Different amortization schedules exist for grid components, such as for generation, which for solar generation can range from 6 years or less, compared to 20 years or more for other generation assets. • The financial environment for grid investments, including capital expenditures (capex) and operation, maintenance and monitoring (OMM) expenditures, affects utilities’ business practices and decisions broadly, from viability and bankability of individual projects to potential long-term underinvestment in grid operations and maintenance.	Direct and indirect lifecycle costs of electric grid components.	• Consideration of grid asset uniqueness with respect to amortization schedules.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Business	Enterprise	Concerns related to the economic aspects of CPS.	• Grid control algorithms will likely increase in complexity in order to manage market economics, efficient energy usage, and reliability factors based on an increasing variety of resources, such as storage and demand response resources in areas with high penetrations of wind and solar generation. • Investments in energy production (generation) and delivery infrastructure generate a return on investment for utilities and energy producers; grid infrastructure enhancements need to also produce economic value or they will not be built. ¹⁴ • Architecture concerns include network convergence and transition from economies of scale to network economies. ³⁵ • Increasing dynamic grid conditions will require more dynamic markets. • New distribution-level markets and market structures are likely to be created, including the introduction of Distribution System Operators (DSOs) to manage distribution system operations and maintain reliability and increase resilience under much higher levels of uncertainty and complexity.	Long term economic viability of maintaining the grid.	• The Distribution grid of the future may be designed as an open-access network for energy transactions.⁷⁵ • Architecture and enhanced communications are needed to enable new transactive energy approaches to distribution grid coordination and control.⁷⁷ • Economic and societal benefits of architecture changes must be quantifiable to support rigorous regulatory/stakeholder analyses to secure authorized funding. • Network convergence of electric, gas, and water distribution, traffic lights, emergency services, and public safety systems is likely to increase development of common platforms for sensing, communications, and control.⁴⁴ • New Transactive Energy Market architectures are needed. • Architecture support is needed to enable development and implantation of algorithms that incorporate uncertainty (unpredictability) and complexity. • Transparent market/economic business models should be developed to understand business factors that are driving decisions.
Business	Environment	Concerns related to the impacts of the engineering and operation of a CPS on the physical world.	• Outcome-oriented or performance-based regulation, including, for example, Performance Incentives Mechanisms (PIMs), have the potential to align utility motivations with societal goals related to the environment.	Concerns related to the impacts of the engineering and operation of the grid on the physical world.	• Architecture support is needed to enable system-level consideration of additional environmental factors (e.g., carbon use) in addition to economics.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Business	Policy	Concerns related to the impacts of treaties, statutes, and doctrines on a CPS throughout its lifecycle.	Increased use of renewable energy is being required by legislation in many states⁹ including Hawaii, which is requiring 100% renewable usage by 2040, and California (50% by 2030) and Vermont (75% by 2032).¹⁰ In addition, a growing number of large corporations (including Google, Apple, and Amazon) are stating that their goal is 100% renewable energy use.	Concerns related to grid policies such as enterprise goals (e.g. adherence to established standards and protocols) or societal goals (e.g., renewable portfolio standards).	Architecture support is needed to enable new operational system controls for systems with high (up to 100%) renewable energy usage. Currently key operational considerations include use of significant amounts of battery storage, and use of advanced DER generation assets with new functionality.
Business	Quality	Concerns related to the ease and reliability of assessing whether a CPS meets stakeholder (especially customer) expectations.	- Customer expectations are changing as customers become increasingly aware of energy issues and also want ease of interaction with utilities and energy services providers based on their experiences with mobile phones, banking systems, and other modern conveniences. - The emergence of new types of local energy choice and formation of community energy related entities (community choice aggregation/CCAs, community “solar garden” co-ops, etc.) will require operational changes in control systems to maintain customer quality expectations.³⁴	Concerns related to customer satisfaction or perceived quality of grid services.	- Coordination structures and customer outreach are needed to facilitate integration of community energy resources such as multi-user microgrids and solar gardens into overall resilience strategies.⁶⁸ - New hybrid central/distributed control structures are needed for enhanced distribution control to facilitate functional flexibility and grid resilience.⁴⁵ - New concepts in grid architecture (e.g. potential for city distribution grid to support an open-access network for energy transactions⁴⁶) will require significant customer outreach to ensure quality of energy services is maintained.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Business	Regulatory	Concerns related to regulatory requirements and certifications.	- Many state regulatory bodies are developing grid modernization guidance for distribution utilities in their jurisdictions (NY – NY REV, CA – MTS, MN – E21, OH – PowerForward, etc.).⁴³ Such regulatory guidance, and more generally the overall practices and environments of individual state commissions, have significant effects on the asset investment strategies and business models of grid participants. - Utilities with large geographic extent may be under the jurisdiction of several Public Utility Commissions (e.g. in different states) and may face additional difficulties in developing and deploying enterprise-wide solutions while meeting expectations of multiple regulatory bodies. - Renewable energy goals may be articulated at a high level such that the connection to specific grid changes necessary to meet the goals is not well understood.¹² - Utilities and energy service providers working with governmental organizations, such as cities, need to work within local regulatory systems and authorities, and understand local conditions such as a city’s budget management needs and processes for financing new projects.³⁷ - The electric grid directly supports many other infrastructures, such as transportation, waste management, and public safety, that are critical to the creation of safe and efficient urban environments in smart cities.³⁸	Concerns related to the regulatory oversight of the grid.	- Additional standardization of interfaces across US Distribution System Operators (DSO) may be helpful to reduce level of effort needed to implement DSOs nationwide, including under differing regulatory environments. - Significant operational architecture support is needed for design and implementation of 100% renewable systems. - Architecture support needed to design grid systems for which one can calculate costs (e.g. on a year-by-year basis) to support budget analysis needed for regulatory oversight. - Integrated electric grid and smart city architecture is needed to support effective integration of infrastructures. - Market architecture and economic models are needed that support value exploration and communications between regulators and utilities/energy sector participants, including to consider costs and economic benefits of new assets such as DER.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Business	Time to Market	Concerns related to the time period required to bring a CPS from need realization through deployment.	• There is an overall mismatch between speed to market of information technology compared to operational technology in the energy sector. An illustration of this mismatch is found in a comparison of typical 30-year innovation cycles and depreciation schedules in utilities with typical 3-year innovation cycles and depreciation schedules in telecommunications companies. • Technical barriers to DER integration with utility control systems, and high costs of DER interconnections including costs of connection to utility communications network, can lead to delayed time to market.	Concerns related to the time to implement new grid technology from realization to deployment within the constraints of legacy systems.	• Telecommunications and other non-utility communications and interoperability solutions are likely to be implemented on a shorter time scale, followed later by utility solutions. Thus, architectures are likely to be impacted more quickly by non-utility solutions and should accommodate different development time cycles. • To reduce time to market for new innovative products, standardization of utility-DER interfaces and interconnections are needed, including support for automated interconnection applications for consumers.
Business	Utility	Concerns related to the ability of a CPS to provide trusted benefit or satisfaction through its operation. Utility reflects a business concern, especially when considered as the numerator when computing value, which equals utility divided by costs.	• Additional information is needed to understand the comparative value provided by installed infrastructure, T&D, or customer owned assets. • New energy services (volt/VAR, synthetic inertia, demand response, storage, etc.) will provide expanded range of sources of usefulness (value). • Significant changes in energy cost by source have occurred in recent years. For example, the lowest levelized cost of energy from any source (without subsidiaries) is now wind followed by utility-scale solar PV.⁸⁸ • In order to realize all DER benefits, distribution planning should consider use of DERs as an option. • Different business models of vendors, commercial control system developers, generation owners, and utilities (which themselves have multiple business models for IOUs, municipalities, co-ops, government-owned utilities) and different understandings of utility (business value) may impede collaborations. For example, unmetered Behind the Meter (BTM) generation may not be accurately valued.	Ability to reliably supply electric power (as a business value) to consumers.	• Assessment of least cost alternative should include new infrastructure, customer-owned assets, and non-wires alternatives such as Demand Response. • New Distribution feeder structures are needed to facilitate adaptation to stress conditions and sharing of localized energy resources.⁶⁴ • Assessment of least cost alternative should consider multiple revenue streams from DER and other non-wires alternatives, including energy shifting, load shifting, ancillary services and reliability improvements/impacts. • Distribution planning applications should consider DER assets in the set of potential options for new projects • New regulatory tariffs will require BTM and other systems to include the ability to schedule services, e.g. battery's ability to provide energy at specific time periods, based on tariffs⁹¹ e.g., Time of Use (TOU) rates.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Human	Human Factors	Concern about the characteristics of CPS with respect to how they are used by humans.	- Some stakeholders have difficulties in understanding what a kWh is or its economic value, which may prevent consumers from effectively participating in market constructs that deal in kWhs or MWhs. Without needed context and information, consumers “have a hard time estimating the costs and benefits of their actions.”¹³ - Consumer choice including local energy choice²⁹ are among the primary factors driving increased automation with large amounts of DER. - Architecture concerns related to human factors range from system operator ergonomics to interaction/convergence with social networks and social media.³⁶ These concerns, and additional concerns related to human performance, also apply to human operators in grid control center environments	Ability of power system users to understand and respond to grid concepts, functions and operational requirements.	- Value propositions (including regulatory tariffs) are needed in which benefits and costs are clear to consumers and presented at the time that consumer decisions are anticipated to be made. - Additional consumer education is needed to support consumers to select their energy providers (if available), to select an option to request all renewable energy, and to join with others to form Community Choice Aggregation (CCA) districts. - Human factors assessments and inputs in application development process are needed, including for example, evaluation of human factor concerns in control centers to improve the performance of humans-in-the-grid-control-loops. Architectural support is needed for development of interfaces with social media, including to provide easy-to-understand energy price information and outage status to customers.
Human	Usability	Concerns related to the ability of CPS to be used to achieve its functional objectives effectively, efficiently, and to the satisfaction of users (adapted from ISO 9241-210.) The combination of physical and cyber into complex systems creates challenges in meeting usability goals. Complexity is a major issue. The diversity of interfaces creates a significant learning curve for human interaction.	- Improved (simpler/better/intuitive) user interfaces are needed to support human-grid interactions. For example, the inability (and disinterest) of humans to manually control grid-connected equipment requires user-friendly interfaces (and effective automation) to help manage these devices, e.g. potentially millions of DERs, in coordination with grid management systems. - Situational awareness applications are needed to improve system visibility and usability for consumers, market management organizations, market participants, utilities and other stakeholders.	Ability of power system users to understand, interact with, and apply grid technology.	- Improved interfaces including preset or interactive device level controls, as well as aggregation of DER assets, can be used to increase usability and reduce need for direct control of each DER. Such interfaces would help to reduce human-based concerns about difficulties and complexity of managing grid-responsive equipment. - Architecture support is needed for effective delivery of relevant data to stakeholders to include consumers, market management organizations, market participants and utilities.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Trustworthiness	Privacy	Concerns related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components such that individuals or groups cannot seclude themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.	• The availability of high-frequency energy usage data collected for the purpose of energy monitoring may facilitate the unintentional release of private, confidential information. For example, the data has the potential to reveal information about an individual’s behavior, such as when he or she arrives home at night, and what are his or her general day-to-day interactions with CPS systems.³⁹ • Collecting pieces of information from various sources and then using algorithms or machine learning to analyze this information, makes it possible to combine “safe” (privacy-protected) data from many sources to create “unsafe” results that reveal confidential information about individuals (e.g. privacy concerns). • An additional privacy concern is simply one of confidentiality of customer data, including data of commercial and industrial customers.	Concerns related to the ability of the grid to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components such that individuals or groups cannot seclude themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.	• Methods and algorithms can be developed for removing Personally Identifiable Information (PII) and sensitive personal information (SPI) from monitored electric usage data.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Trustworthiness	Reliability	Concerns related to the ability of the CPS to deliver stable and predictable performance in expected conditions.	- Reliability can be understood as the ability of the electric power system to deliver electricity in the quantity and with the quality needed to satisfy demand, typically measured by interruption indices appropriate for normal operation. - Increased onsite generation (including renewables and backup generation), often in the context of a user-controlled microgrid, is a common approach by customers to address their own site-specific concerns about reliability. These assets may also be aggregated and can participate in markets to provide compensated grid reliability resources. - The reliability of intermittent/non-dispatchable DERs (as individual generation assets) can significantly impact the reliability of the connected grid system.	Concerns related to the ability of the grid, or components within a grid, to deliver stable and predictable performance in expected conditions.	- If assets other than those owned by the utility are trusted and compensated to support grid reliability, what happens if reliability norms are violated (e.g. how is the utility or other affected parties informed), and how would organizations be responsible for the localized and regional impacts of the violation? - The ability of grid segments or devices, possibly owned by groups other than the utility, to provide autonomous corrections to system operation (i.e., those corrections not controlled by the central utility) will reduce communications requirements and associated costs for deploying DER, and also increase the speed with which corrective action can be taken throughout the system. An example of this is the automated function of reclosers. - Multi-user microgrids and microgrid networks may require coordination with distribution grids and need for microgrid-to-grid services.⁴⁷ - A lack of verified reliability for individual asset performance could lead grid operators and/or utilities to require direct observability of asset behavior, especially when controllable assets are grouped to provide specific operational characteristics through processes opaque to the utility.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Trustworthiness	Resilience	Concerns related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.	• Different from reliability, in which normal services are provided, resilience includes the ability to prepare for and adapt to changing circumstances, and to withstand and recover rapidly from disruptions. Resilience may include a graceful degradation of performance. The interconnected nature of grids means degradation will likely affect more than just those stakeholders which negotiated (or agreed to) the degraded operating solution. The authority to determine the operating solution had previously resided with utilities and similar load serving entities; the significance of assigning these decisions to others is not yet clear. • The determination (or negotiation) of the degraded state is an unclear process right now, and care must be taken to ensure all stakeholders can participate and have their interests represented accurately in the final solution. • When trustworthy resilience is provided by operating in a degraded state, the necessary communications to external entities must be clarified. • Scientific studies indicate that extreme weather events such as heat waves and large storms are likely to become more frequent and intense⁵³ increasing risk of damage to electric grid infrastructure. • For many industries, a momentary outage of 15 seconds, or an extended outage of 15 hours, results in the same economic loss.⁵	Concerns related to the grid, or components within a grid, to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.	• Coordination, communication, and sensing structures that facilitate use of Distributed Generation (DG) for grid resilience purposes are needed.⁶⁶ • Grid and communication/coordination structures that enable fast use of the results of contingency planning are needed.⁶⁵ • Condition-Based Maintenance (CBM) projects require additional communications bandwidth. • Storage at the distribution level can be used to improve resilience.⁷⁶ • Effective use of smart meters at high-priority sites (such as hospitals and first stations) with enhanced outage detection alerts requires faster higher bandwidth communications networks. • Electric Vehicles charging may be able to provide additional resilience support for grid systems, in addition to meeting customer charging needs.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Trustworthiness	Safety	Concerns related to the ability of the CPS to ensure the absence of catastrophic consequences on the life, health, property, or data of CPS stakeholders and the physical environment.	• Utilities and energy service providers/operators ensure that safety is prioritized within their operations and for the protection of customers. • Potential impacts on safety arise from multiple concerns, many of which are grouped in Trustworthiness. For example, the potential for device (and substation) controllability to be compromised through malicious intent via a cybersecurity attack can have catastrophic life-safety implications. • Safety must be evaluated and maintained or improved throughout all grid system evolution processes. For example, as distributed devices are increasingly deployed to enhance system reliability and resilience, traditional safety practices may no longer be relevant and must be updated.	Concerns related to the ability of the electrical grid to ensure the absence of catastrophic consequences on the life, health, and property due to electrical hazard to consumers, installers, and maintenance workers.	• Dynamic reorganization of system architectures to provide the greatest level of system performance and net economic benefit will create uncertainties in status and safety requirements as workers from multiple organizations work to restore what could be competing architectures of service.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Trustworthiness	Security	Concerns related to the ability of the CPS to ensure that all of its processes, mechanisms, both physical and cyber, and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use.	• Most substation systems were designed as isolated non-connected systems. Thus, connecting IoT-enabled devices and systems within substations requires reevaluation of security concerns, including implementation of device-level cybersecurity in addition to other measures. • Adding cybersecurity later, which is required for most legacy substation and field devices, typically results in less effective security than designing in and implementing cybersecurity at the beginning. • A timing-denial cyber-attack could be conducted either via Global Navigation Satellite System (GNSS) denial or using interference with communications network traffic. Such an attack could lead to a grid or substation failure.²² • A spoofing cyber-attack could be initiated by any device connected to a substation communications bus (including those only temporarily connected), or via an external device that reaches the substation via a poorly protected gateway. Such an attack would provide individual or all subsystems with false time, therefore resulting in an infringement of local or global time synchronization.²³ • Denial of Service (DoS) cyber-attacks over extended time periods could lead to grid or substation failures.²⁴ • Proliferation of additional DER and distributed automation devices requires additional physical security to protect these assets.	Concerns related to physical and cyber processes and mechanisms impacting trustworthiness.	• Architecture for resilience buffering against edge device induced power flow volatilities is needed for defense against IoT-based cyber-attacks.⁸¹ • Cybersecurity architecture is needed to address the inherent risks of connecting devices to a network/the Internet. • Security architecture is needed to address multiple concerns, including for DERs, and to protect against timing-denial and DoS cyber-attacks, and to protect substations against spoofing attacks. In addition, security architecture for securing legacy electric grid systems and securing substations is needed. Security architecture is also needed to support input and monitoring of physical devices, and for transactive energy. • Distribution-level cyber securability approaches are needed for information flow, coordination, and control that are inherently defendable.⁷⁹

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Timing	Logical Time	Concerns related to the order in which things happen (causal order relation) or event driven.	• Protection and safety schemes for the grid require sequential operation in time and close coordination across a number of physical events and actuations. • As grid automation increases, especially on distribution systems, these coordinated and sequential operations will become more common within — and important to — daily operations and system optimization. • Hardware in the loop testing and simulation is prevalent among grid operators, especially for modeling distributed energy resources in the system. These efforts depend on logical time steps that enable faster-than-real-time simulation and are conducive to meeting the operational and planning needs of various grid stakeholders.	Concerns related to the ability to specify and coordinate time sequences for operations, simulation and testing.	• Architecture is needed to support logical time sequencing to meet operational, testing, and simulation requirements.
Timing	Synchronization	Concerns for synchronization are that all associated nodes have timing signals traceable to the same time scale with accuracies as required. There are three kinds of synchronization that might be required: time, phase, and frequency synchronization, although frequency synchronization is also called syntonization.	• The increasing importance of coordination across the transmission and distribution systems results in greater need for synchronization on more granular time scales and accurately disseminated over larger physical areas. • Maintaining integrity of time synchronization is can be difficult because reference sources and communication mediums are subject to interruption and failure. For example, loss of GPS timing synchronization for Supervisory Control and Data Acquisition (SCADA) systems and synchrophasors data can compromise grid state estimation and impact the situational awareness and control capabilities of the power system. Redundant time synchronization systems provide benefits of continuity of timing infrastructure during such interruptions and failures. • Awareness and seamless mapping of different time scales and local time are needed to accommodate adjustments (e.g., introduction of leap seconds and daylight savings time)	Concerns that all nodes and devices connected to the grid have timing signals traceable to the same time scale with accuracies as required.	• Synchronized timing allows for localized data analytics and simpler data communications. • Communication infrastructures for timing and alternatives (redundant systems) are needed for timing distribution over distribution grids, in conjunction with or independent of satellite-based methods.⁸⁰ • Architecture is needed to support applications ability to rely on accurate time stamps while recognizing that they can be subject to interruptions and communications failures. • Architecture support is needed to facilitate applications to recognize and account for timing issues including different time zones, local time and daylight savings, as well as technical time synchronization issues such as introduction of leap seconds.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Timing	Time Awareness	Concerns that allow time correctness by design. The presence or absence of time explicitly in the models used to describe, analyze, and design CPS and in the actual operation of the components. This is a life- cycle concern as well as a concern for the ability to build devices without the need for extensive calibration of the timing properties.	• Efficient protection functions require synchronized time, available either locally or globally.²¹ • Timeliness of data availability, computation, and communication is needed in order to meet the system constraints to provide accurate state estimation and precise control automation. • Ability is needed to specify and validate timing constraints. • Grid operations use distributed equipment, which often includes time-aware capabilities based on the availability of timing as an infrastructural resource maintained by utilities.	Concerns related to the ability to design systems and components that are time aware and can acquire and use sufficiently accurate time signals.	• Architecture needs to support time awareness and synchronous time for protection schemes. • Architecture needs to support the ability within applications to apply and validate timing constraints. • Architecture needs to support sufficiently accurate time stamping ideally using designed-in and widely available timing infrastructures.
Timing	Time-Interval and Latency	Specifying requirements for timing generally involves requirements for time-intervals between pairs of events. A time-interval is the duration between two instants read on the same timescale. CPS timing requirements are generally expressed as constraints on the time intervals (TI) between pairs of system significant events. These can be categorized in terms of bounded TIs or latency, deterministic TIs, and accurate TIs.	• As grid applications evolve, time-interval and latency requirements (including bounded latencies, and to prevent system destabilization) are becoming more stringent and complex. • Time-interval specificity is central to many new grid applications, from control systems to cybersecurity protections.	Concerns related to the ability to specify time interval and latency requirements for system events and communications.	• Architecture is needed to support multiple application-driven requirements for time-interval performance and latency.
Data	Data Semantics	Concerns related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.	• Efforts to combine data from multiple sources in the electric grid system face significant data interoperability challenges.⁴⁰ • Data interoperability is a key need for grid modernization. • Data models and many data standards for smart grid devices support many different use cases; as a consequence, data semantics are not always seamless across systems.	Concerns related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.	• Standardization of communication interfaces and data harmonization is needed. • As the ownership of grid devices for communication, sensing and actuation diversifies, additional effort will be needed to maintain data context (i.e., semantic interoperability) across devices and systems.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Data	Data Velocity	Concerns related to the speed with which data operations are executed.	• The operational constraints of the electric grid demand that supply and demand be continuously balanced in real time, which creates significant requirements for data velocity to support real-time operations. • The increasing volumes of data inherent to the smart grid will challenge the ability to perform timely data operations.	Concerns related to the speed with which data operations are executed, and the ability to process data within specified requirements.	• Architecture will need to accommodate different data processing speed requirements as a function of application and device type. • Architecture will need to ensure data processing speed requirements for a given element are consistent with the employed control theory and system/device physical capabilities.
Data	Data Volume	Concerns related to the volume or quantity of data associated with a CPS' operation.	• The proliferation of smart sensors in the grid and other new data sources could overwhelm the data processing and analytics capabilities of the system. • Grid operators may need to selectively manage data streams to prioritize information that is most relevant to their operational goals. • The dramatic growth in data availability from distributed sensing may create an archival data storage problem, in which so much data is stored that useful information may become obscured and access constrained.	Concerns related to the ability to store the growing volume or quantity of data from grid devices and systems.	• Architecture support will be needed to meet growing data requirements for grid systems. • Architecture elements will need to include the ability to address data capacity requirements from different types of devices and applications.
Data	Identity	Concerns related to the ability to accurately recognize entities (people, machines, and data) when interacting with or being leveraged by a CPS.	• Identity management is crucial to grid communications and operations. • As ownership of grid assets diversifies, and as customers increasingly bring their own devices and expect to connect with any and all available communication systems, identity management schemes will have to be developed which allow for effective management of large numbers of diverse devices. • Identity management of physical assets is critical to trustworthiness, cybersecurity, and grid operations.	Concerns related to the ability to uniquely identify devices in the system.	• Grid systems need the ability to identify and incorporate devices subject to diverse constraints and capabilities of distinct organizations, systems, and components. • Highly distributed architectures will need to support device self-identification and registration.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Data	Operations on Data	Concerns related to the ability to create/read/update/delete system data and how the integrity of CPS data and behaviors may be affected.	• The quantity of data available to grid operators is increasing dramatically as sensing and communications capabilities are incorporated into all types of equipment. But the ability to use data is limited by data incompatibility, often driven by conflicts in format and structure. Ensuring appropriate data management, including data compatibility through uniform use of data models or other formatting, is critical to ensuring utilities can process, store, maintain and utilize the data according to their applications.	Concerns related to the ability to define data compatibility and data management requirements, including format, processing, storing and monitoring schemes.	• Architecture will need to support various data operations related to their applications.
Data	Relationship between Data	Concerns related to how and why sets of data must, may, or may not be associated with each other and the value or harm that can be derived from those associations.	• Network convergence, such as referenced in natural gas/electric system harmonization efforts,¹¹ will lead to complex and interconnected data streams, which will need to be managed in coordination to support cooperative operational management of integrated infrastructures. • Utilities and grid operators manage large quantities of sensor data generated by numerous equipment, to inform and improve grid operations efficiency, reliability and other attributes. By itself, or when associated with other data (commercial, residential), this information may add value or cause harm if not managed in an appropriate way. Internally, for example, data on power flows (state estimation) may reveal energy-market-relevant decisions and data that are to be protected. Externally, data about individual customers is typically protected from unauthorized disclosure within a state regulatory construct. • Data from many sources impacts the accuracy of Distribution state estimation and other data analytics applications, and the relationship of disparate data sources will need to be evaluated to identify and enhance the value of such data to meet requirements of many applications.	Concerns related to the relationships of grid data and external data and the value or harm that can be derived from those associations.	• Integrated data management and analysis capabilities are needed effective coordinated operation of grid systems and other interacting systems, e.g. to support operational management of converged natural gas/electric power systems.⁵⁵

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Boundaries	Behavioral	Concerns related to the ability to successfully operate a CPS in multiple application areas.	• Multiple value stacks for responsive grid support systems, e.g. energy storage systems, motivate maximal utilization of equipment and systems to meet multiple application objectives. These potentially overlapping applications are often subject to the requirements and expectations of multiple organizations, including those related to organizational boundaries. • Operational siloes exist within utilities, such as between Informational Technology (IT) and Operational Technology (OT), and often lead to organizational boundaries which may increase the difficulty of managing CPS/IoT devices.⁸⁹	Concerns related to successful operation at boundaries including geographic and system boundaries.	• Architecture must support diverse operational and market uses for grid responsive systems, such as energy storage systems. • Architecture practices need to consider differing IT and OT perspectives.
Boundaries	Networkability	Concerns related to the ease and reliability with which a CPS can be incorporated within a (new or existing) network of other systems.	• Increasing growth of edge-connected devices and systems, e.g. DERs, is requiring development of network capabilities to manage and readily accommodate the incorporation of such devices. Positive attributes, such as ease of connection and reliability of edge devices, are accompanied by the need to reassess existing capabilities and processes, including protection schemes⁶ to prevent negative impacts such as outages that may result from unanticipated two-way power flows.	Ease and reliability of incorporation of newer technology and updated systems models at various grid levels while maintaining the integrity of the grid network.	• With increased networkability and ease of incorporation of new devices and systems into the grid, advanced control systems are needed to manage such systems and protect grid systems from unintended consequences.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Boundaries	Responsibility	Concerns related to the ability to identify the entity or entities authorized to control the operation of a CPS.	• Business model changes for utilities, including those driven by the availability of significant distributed generation, may include creation of new Distribution System Operators with stakeholder expectations that income will result from distribution services instead of the volumetric sale of electricity.¹⁷ These new organizations and structures will result in new organizational responsibilities, which will need to be understood, communicated and agreed with applicable system participants. • Additional coordination will be needed between microgrids and the larger grid and between microgrids and other microgrids.³¹ • Greater understanding and coordinated management of responsibilities between Distribution System Operators (DSO) and RTOs/ISOs will be needed. • Utility resource planning and accommodation of increasing DERs will need to incorporate recognitions of boundary interfaces and associated responsibilities of authorized grid operators. • Customers may have opportunities and responsibilities based on their use of grid-responsive equipment (e.g. demand response) with the ability to vary power consumption to meet multiple objectives.	Identification and determination of the responsibilities of authorized grid organizations and participants, including with respect to ownership and control of diverse grid components.	• Transmission/distribution coordination via Distribution System Operator models is needed.⁷¹ • Circuit structure, protection and control structures are needed for multiple cooperating microgrids.⁸³ • Architectures for multi-scale (e.g. single building versus multiple circuits) coordination of microgrid networks needed.⁸⁴ • Architecture needed for CCAs and aggregated community resources.⁸⁵ • Architecture support is needed for segmentable and coordinated grid sub-systems and for coordination of responsibilities to facilitate agile re-segmentation and cooperation at different microgrid scales (e.g. single building versus multiple circuits).⁸⁶ • Under one proposed framework, the DSO would serve as a system optimizer on the local level, calling on least-cost resources to meet distribution system goals. The least-cost resources could be provided directly by customers or, more likely, by third-party aggregators.⁸⁷ • Standardization of interfaces between utility resource planning tools and DERs would increase effectiveness of DERs. • Consumers would benefit from development of clearly defined guidelines for customer participation, costs, benefits and responsibilities related to the integration of grid-responsive devices and systems.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Composition	Adaptability	Concerns related to the ability of the CPS to achieve an intended purpose in the face of changing external conditions such as the need to upgrade or otherwise reconfigure a CPS to meet new conditions, needs, or objectives.	• Grid components are supplied by various vendors. It can be challenging for components from different vendors to communicate with one another in the power system network, and to be reconfigured as needed to meet new objectives. • Grid control algorithms need to be much more flexible and adaptable in order to consider varying market economics, efficient energy usage, and managing reliability with a diversity of resources, such as storage and demand response, and in areas with high penetrations of wind and solar generation.	Ability to update, adapt or reconfigure grid technology to meet power system needs.	• Interoperability standards for grid components continue to be needed to support composition and integration of components into systems that are adaptable and able to meet system requirements. • Preparedness for future grid technology including attention to its adaptability and reconfigurability to meet new objectives is needed. • Architecture is needed for integration of large-scale energy storage distribution connected resources and grid operations.⁵⁸ • Balancing and stabilization of grids with wide area bulk wind and solar resources is needed.⁵⁹ • Distributed intelligence computations and communication network structures are needed to support distributed analytics, and control.⁶⁹ • Coordination, communication, and sensing structures that facilitate use of Demand Response for grid resilience purposes are needed.⁶⁷ • New hybrid central/distributed control structures are needed for distribution control to facilitate functional flexibility and grid resilience.⁷⁰
Composition	Complexity	Concerns related to our understanding of the behavior of CPS due to the richness and heterogeneity of interactions among its components, such as existence of legacy components and the variety of interfaces.	• Grid complexity is such that it is unlikely any one person or organization can understand and/or plan for the entirety of it.¹⁵	Concerns relating to complexity in grid functionality.	• Movement of control/management/optimization to lower levels will help to manage complexity. • Grid partitioning, coordination and communication are means to adapt to grid complexity and stresses.⁶¹

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Composition	Constructivity	Concerns related to the ability to combine CPS modular components (hardware, software, and data) to satisfy user requirements.	Integrating hardware, software and data components in complex systems is a difficult endeavor, and particularly so in grid systems with their legacy systems and operational requirements. For example, replacing an Outage Management System (OMS) and Distribution Management System (DMS) with an Advanced DMS (ADMS) poses complex deployment issues, including how to replace both the OMS and DMS at the same time, optimize data alignment/transfer, maintain consistency in calculating reliability metrics, and complete operator training.	Integration of power system components of various types and configurations.	Architectures need to be developed with interface design and considerations to support modular composition of components, including the ability to address use of the same data by multiple applications, varying data rates, and standardized data definitions, e.g. CIM.
Composition	Discoverability	Concerns related to the ease and reliability with which a CPS component can be observed and understood (for purposes of leveraging the component's functionality) by an entity (human, machines). Concerns related to the ease and reliability with which a CPS component's functions can be ascertained (for purposes of leveraging that functionality) by an entity (human, machines).	- The grid has increasing needs for system observability and discoverability, including with respect to communication (data flow) and information handling. - System operators want greater visibility into the operation and status of DER assets and other assets that may be owned or controlled by other parties.	Concerns related to the observability of power systems components needed to leverage component data.	- Automated discoverability of edge-connected devices and sensors and their performance characteristics, communications and data models is a need to enable improved visibility, integration, and device management to support grid operations. - Fault tolerant communication structures are needed to enable reliable distributed intelligence.⁶² - Architecture support is needed to enable discoverability and visibility of DERs and to support centralized and decentralized control of DERs.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Lifecycle	Deployability	Concerns related to the ease and reliability with which a CPS can be brought into productive use.	• The mission-critical nature of the grid limits the ability to test new systems, as outages are unacceptable. Thus models, simulations, and testable versions of the grid are needed to test new systems, algorithms, markets capabilities and understand and mitigate factors affecting their deployability on the functioning grid. • Utility-scale wind and solar power often generated in sparsely populated areas with little grid infrastructure. Hence long-distance transmission lines must be built to move wind/solar generation to areas where power is needed, which may lead to additional concerns such as initial deployability of these assets. • Reduction of system inertia, including that associated with inverter-based generation in some cases, may require additional control actions by regulating tap changers and capacitors⁵⁴ and which may affect the perceived deployability of these assets.	Concerns related to the implementation of grid technology to meet power system needs.	• Architectural support is needed for new or updated models and simulation of the electric grid including DERs. • Bulk energy systems require closed loop secondary protection and System Integrity Protection Schemes (SIPS).⁵⁶ - Sensors and communications are needed for transmission state determination and situational awareness.⁵⁷ • Structures are needed for integration of inertia augmentation methods, devices, and systems.⁶⁰
Lifecycle	Disposability	Concerns related to the impacts that may occur when the CPS is taken physically out of service.	• There is an ongoing need to plan for retirement and eventual disposal/deconstruction of large power plants at the end of their lifecycle. • Planning is needed to support identification and disposal of faulty grid equipment, and to enable recycling of out-of-service grid components that may be of use elsewhere.	Concerns related to the disposal of obsolete, aged, or damaged physical grid components.	• Architecture is needed to support environmental-friendly recycling practices. • Improved quality checks are needed to minimize faulty equipment. - Architecture support is needed to enable use of recycled grid components elsewhere in the grid.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Lifecycle	Engineerability	Concerns related to the ease and reliability with which a CPS design concept can successfully be realized via a structured engineering process.	• There are multiple systems engineering approaches and methodologies available to support architecture development and a variety of structured engineering processes. Within systems engineering processes applied at the grid component level, the broader perspective of the grid at-scale is beneficial to identify and address engineerability issues. Included in this approach is research and development needed to better understand and improve the behavior and performance of new innovative products, to ensure that these concepts can be realized and deployed at scale and are likely to function in grid environments. • Microgrid engineering issues have been studied, but architecture coordination issues remain.³² • Time lags may exist in translating new concepts into standards and implementation, which should be identified and mitigated as needed, e.g., through initiating testing and certification development based on earlier working versions of a standard.	Ability to develop theoretical concepts into applicable grid technology.	• Common structured engineering processes should be identified and used broadly across the electric sector to help improve engineerability and integration of new components and systems into the operational power grid. • Microgrid architecture models are needed.
Lifecycle	Maintainability	Concerns related to the ease and reliability with which the CPS can be kept in working order.	• The aging grid means that many assets are reaching or have already surpassed their designed lifetimes, and maintenance of these assets and systems is a growing concern for keeping the system operational. • The introduction of smart devices in the grid are changing maintenance processes and procedures. For example, the different classes of devices require different monitoring schemes (e.g. traditional grid devices may require visual inspection while smart devices could be monitored remotely). • Smart devices and systems may enable predictive maintenance to replace some preventive and reactive maintenance regimes.	Concerns related to the ease and reliability with which the grid and its assets can be kept in working order.	• Architecture needs to support different maintenance intervals for different classes of devices. • Architecture needs to accommodate a variety of emerging maintenance regimes, including predictive maintenance.

Aspect	Concern	Description	Grid Context for CPS Concern	Grid CPS Concern Description	Architecture Significance
Lifecycle	Operability	Concerns related to the operation of the CPS when deployed.	• Electric system components are often designed with long lifetimes that may exceed 30 years⁹⁰ and must maintain operability over this time period. • Like other critical infrastructures, the electric grid is aging, and must be kept operational through upgrade or replacement by new systems. These upgrade or replacement events represent opportunities to introduce additional system advances such as incorporating an IoT-based infrastructure. • The increasing complexity of grid controls requires a more skilled workforce to maintain operability of grid systems. • Firmware upgrades in existing devices provide opportunity to deploy new features such as the ability of advanced inverters to control voltage and frequency.	Concerns related to continuous, effective operation of grid components.	• Architecture needs to accommodate both new and legacy devices. • Architecture needs to support rollout of new Internet connectivity when systems are added or replaced. • Architecture needs to support integrated training/operations simulation. • Architecture needs to support field upgrades of device firmware.
Lifecycle	Procureability	Concerns related to the ease and reliability with which a CPS can be obtained.	• Historically, performance requirements for grid assets or devices have been locally determined, and driven by interfaces with legacy systems or capabilities. This situation often leads to procurement issues as equipment often requires customized configurations to match capabilities with the legacy requirements. Grid operators are moving towards open-source standards-based device requirements, which allows for easier specification in the procurement process. • Common reference procurement language could be useful for purchasers to specify and procure devices that minimize integration overhead.	Concerns related to the ability to specify performance and communication requirements for a device.	• Architecture needs to support standardized device requirements to support procureability. • Common reference language for procurement documentation and examples of standards-based performance requirements should be developed
Lifecycle	Producibility	Concerns related to the ease and reliability with which a CPS design can be successfully manufactured.	• The grid itself is not manufactured, but instead it results as the product of many individual design, procurement, and installation activities. • Absent a comprehensive master design, devices manufactured to meet open standards improves the likelihood that grid components will be manufactured to conform with grid design requirements.	Concerns around the ability to translate grid designs into successful products and installations.	• Architecture needs to support standardized device requirements to support producibility.

Table 14 References

- 1 Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 2 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; pages xi-xii
- 3 Advanced Bulk Energy Systems Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 4 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; pages xxvii-xxviii
- 5 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xv
- 6 Kay Stefferud, Jens Schoene, Vadim Zheglov; EnerNex LLC 2015; Jan Kleissl, UCSD. Utility Scale Solar Forecasting, Analysis, and Modeling Final Report. California Energy Commission. Publication number: CEC-500-2010-060.
- 7 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xvii
- 8 Advanced Bulk Energy Systems Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 9 <https://www.pv-magazine.com/2017/07/19/hawaii-regulators-approve-hecos-100-renewable-energy-plan/>
- 10 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxii
- 11 Advanced Bulk Energy Systems Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 12 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxii
- 13 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxiv
- 14 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxv
- 15 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxvi
- 16 High Resilience Grid Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 17 <http://americaspowerplan.com/2014/09/trending-topics-in-electricity-today-the-distribution-system-operator/>
- 18 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xxx
- 20 Framework for Cyber-Physical Systems: Volume 3, Timing Annex, page 46
- 21-23 Framework for Cyber-Physical Systems: Volume 3, Timing Annex, page 48
- 24-25 Framework for Cyber-Physical Systems: Volume 3, Timing Annex, page 49
- 26 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; page xiii
- 27 Bakke, Gethchen. Introduction in: The Grid: the Fraying Wires between Americans and our Energy Future, New York: Bloomsbury, USA, 2016; pages xiv-xv
- 28-30 High DER High Automation Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 31-32 Microgrid Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.

- 33-38 Architecture Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 39 Framework for Cyber-Physical Systems, Release 1.0, May 2016
- 40 Framework for Cyber-Physical Systems, Release 1.0, May 2016, B.5.2.1.1
- 41 Moving Toward Value in Utility Compensation, Part 2 - Regulatory Alternatives, http://americaspowerplan.com/wp-content/uploads/2016/06/2016_Aas-OBoyle_Reg-Alternatives.pdf
- 42-43 High Resilience Grid Key Influences in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 44-52 Urban Converged Network Architecture Strategy in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 53 Climate Change Indicators: Weather and Climate, United States EPA website, <https://www.epa.gov/climate-indicators/weather-climate>
- 54 Kay Stefferud, Jens Schoene, Vadim Zheglov; EnerNex LLC 2015; Jan Kleissl, UCSD. Utility Scale Solar Forecasting, Analysis, and Modeling Final Report. California Energy Commission. Publication number: CEC-500-2010-060.
- 55-61 Advanced Bulk Energy Systems Architecture Strategy in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 62-69 High Resilient Grid Architecture Strategy in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 70- 81 High DER Grid Architecture Strategy in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 82- 86 Microgrid Architecture Strategy in GMLC 1.2.1 Grid Architecture: Architecture Track Description, DRAFT Version 0.1 25 May 2017.
- 87 America's Power Plan, Trending Topics in Electricity Today, the Distribution System Operator, <http://americaspowerplan.com/2014/09/trending-topics-in-electricity-today-the-distribution-system-operator/>
- 88 Smith, J. Charles, "A Major Player: Renewables are Now Mainstream," IEEE Power & Energy Magazine, 18 October 2017:16. Print. Also Lazard Levelized Cost of Energy Analysis—Version 10.0, pp 4-5
- 89 Derek R. Harp, Bengt Gregory-Brown, IT/OT Convergence: Bridging the Divide, pages 3-5, <https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf>
- 90 UtilityDIVE, <http://www.utilitydive.com/news/making-the-case-for-grid-investment-6-insights-from-the-white-houses-new/160426/>
- 91 Hawaiian Public Utilities Commission, Order Number 34924, page 81, proposed Smart Export schedule, October 20, 2017
- 92 NIST Special Publication 1800-7, Situational Awareness for Electric Utilities, Draft, February, 2017

Appendix C – Inverter and DER Functions

This appendix lists new DER functions which have been identified over the last few years. Some of these are becoming mandatory through California Rule 21 [205] and IEEE 1547-2018 [206]. Others are focused on the market-based services which the DER system could provide.

Table 15 – Inverter and DER functions: mandatory, autonomous, and market-based

#	DER Functions	Description and Key Parameters
<u>Mandatory DER Functions (Regulatory Requirements from IEEE 1547 and California's Rule 21)</u>		
1.	Disconnect/Connect Function Disconnect or connect the DER from the grid at its electrical connection point (ECP)	The disconnect command initiates the galvanic separation (usually via switches or breakers) of the DER at its ECP or at the PCC. There may be a time delay between receiving the command and the actual disconnect The connect command initiates or allows the reconnection of the DER at its ECP or at the PCC. A permission to reconnect may also be issued.
2.	Cease to Energize and Return to Service The DER ceases all active power output Allow active power output at the PCC	“Cease to energize” is a different function from disconnect/connect. IEEE 1547 states the DER shall not export active power during steady-state or transient conditions, and that reactive power exchange (absorb or supply) shall be less than 10% of nameplate DER rating and shall exclusively result from passive devices. There may be a time delay between receiving the command and the actual cease to energize. “Return to service” allows current flow at the PCC. A permission to return to service may also be issued.
3.	High/Low Voltage Ride-Through Mode The DER rides through temporary fluctuations in voltage	The DER follows the utility-specified voltage ride-through parameters to avoid tripping off unnecessarily. The function would block tripping within the fault ride-through zones. Although normally enabled by default, this ride-through mode may be updated, enabled, and disabled.
4.	High/Low Frequency Ride-Through Mode The DER rides through temporary fluctuations in frequency	The DER follows the utility-specified frequency ride-through parameters to avoid tripping off unnecessarily. The function would block tripping within the fault ride-through zones. Although normally enabled by default, this ride-through mode may be update, enabled, and disabled.
5.	Dynamic Reactive Current Support Mode The DER reacts against rapid voltage changes (spikes and sags) to provide dynamic system stabilization dV/dt	The DER provides dynamic reactive current support in response to voltage spikes and sags, similar to acting as inertia against rapid changes. This mode may be focused on emergency situations or may be used during normal operations. When the dynamic reactive current support mode is enabled, the DER monitors the voltage at the referenced ECP and responds based on the parameters.

#	DER Functions	Description and Key Parameters
6.	Frequency-Watt Mode The DER responds to large frequency excursions during abnormal events at a referenced ECP by changing its production or consumption rate	The DER is provided with frequency-watt curves that define the changes in its watt output based on frequencies around the nominal frequency during abnormal events. When the emergency frequency-watt mode is enabled, the DER monitors the frequency and adjusts its production or consumption rate to follow the specified emergency frequency-watt curve parameters.
7.	Volt-Watt Mode The DER responds to changes in the voltage at the referenced ECP by changing its production or consumption rate	The DER is provided with voltage-watt curves that define the changes in its watt output based on voltage deviations from nominal, as a means for countering those voltage deviations. When the volt-watt mode is enabled, the DER receives the voltage measurement from a meter (or other source) at the referenced ECP. The DER adjusts its production or consumption rate to follow the specified volt-watt curve parameters.
8.	Fixed (Constant) Power Factor Mode The DER power factor is set to a fixed value.	The DER power factor is set to the specified power factor. A leading power factor is positive and a lagging power factor is negative, as defined by the IEEE or IEC sign conventions.
9.	Fixed (Constant) Reactive Power Mode The DER is requested to provide a fixed amount of reactive power	The DER is requested to provide a fixed amount of reactive power
10.	Volt-Var Control Mode The DER responds to changes in voltage at the referenced ECP by supplying or absorbing vars in order to maintain the desired voltage level	The DER is provided with curves that define the vars for voltage levels. When the volt-var mode is enabled, the DER receives the voltage measurements from a meter (or other source) at the referenced ECP. The DER responds by supplying or absorbing vars according to the specified volt-var curve in order to maintain the desired voltage level.
11.	Watt-Var Mode The DER responds to changes in power at the referenced ECP by changing its vars	The DER is provided with watt-var curves that define the changes in its vars based changes of power. When the watt-var mode is enabled, the DER modifies its vars setting in response to the power level at the referenced ECP.
12.	Watt-PF Mode The DER responds to changes in power at the referenced ECP by changing its power factor	The DER is provided with watt-PF curves that define the changes in its power factor based changes of power. When the watt-PF mode is enabled, the DER modifies its PF setting in response to the power level at the referenced ECP.
13.	Set Active Power Mode Set the DER to generate or consume energy as a percentage of maximum capability	The DER is set to a percentage of maximum generation or consumption rate. A positive value indicates generation, negative means consumption.

#	DER Functions	Description and Key Parameters
14.	Limit Active Power Production or Consumption Mode Limits the production and/or consumption level of the DER based on the referenced ECP	The production and/or consumption of the DER is limited at the referenced ECP, indicated as absolute watts values. Separate parameters are provided for production or consumption limits to permit these to be different.
15.	Low Frequency-Watt Emergency Mode for demand side management (fast load shedding)	Enable automatic disconnection of a specified proportion of their demand (in stages) under low frequency conditions in a given time frame.
16.	Low Voltage-Watt Emergency Mode for demand side management	Provide capabilities to enable automatic or manual load tap changer blocking and automatic disconnection under low voltage conditions.
17.	Monitoring Function The DER provides nameplate, configuration, status, measurements, and other requested data	The DER provides status, measurements, alarms, logs, and other data as authorized and requested by users. Examples include connect status, updated capacities, real and reactive power output/consumption, state of charge, voltage, and other measurements. Also of interest are forecast statuses and expected measurements.
18.	Scheduling of Power Settings and Modes	The DER follows the schedule which consists of a time offset (specified as a number of seconds) from the start of the schedule and is associated with: • a power system setting • the enabling/disabling of a function • a price signal
<u>Market-Based DER Functions</u>		
19.	Peak Power Limiting Mode The DER limits the load at the referenced ECP after it exceeds a threshold target power level	The active power output of the DER limits the load at the referenced ECP if it starts to exceed a target power level, thus limiting import power. The production output is a percentage of the excess load over the target power level. The target power level is specified in absolute watts.
20.	Load Following Mode The DER counteracts the load by a percentage at the referenced ECP, after it starts to exceed a threshold target power level	The active power output of the DER follows and counteracts the load at the referenced ECP if it starts to exceed a target power level, thus resulting in a flat power profile. The production output is a percentage of the excess load over the target power level. The target power level is specified in absolute watts.
21.	Generation Following Mode The consumption and/or production of the DER counteracts generation power at the referenced ECP.	The consumption and/or production of the DER follows and counteracts the generation measured at the referenced ECP if it starts to exceed a target power level. The consumption and/or production output is a percentage of the excess generation watts over the target power level. The target power level is specified in absolute watts.

#	DER Functions	Description and Key Parameters
22.	Dynamic Active Power Smoothing Mode The DER produces or absorbs active power in order to smooth the changes in the power level at the referenced ECP. Rate of change of power – dW/dt	The DER follows the specified smoothing gradient which is a signed quantity that establishes the ratio of smoothing active power to the real-time delta-watts of the load or generation at the referenced ECP. When the power smoothing mode is enabled, the DER receives the watt measurements from a meter (or other source) at the referenced ECP. New data points are provided multiple times per second.
23.	Frequency-Watt Primary Control mode The DER changes its watt output or input to provide frequency support to maintain frequency within normal limits	The DER changes its watt output or input based on parameters or curves, to provide primary frequency control with the purpose of maintaining frequency within the normal frequency limits
24.	Automatic Generation Control (AGC) Mode The DER responds to raise and lower power level requests to provide frequency regulation support	When AGC mode is enabled, the DER responds to signals to increase or decrease the rate of consumption or production every 4 to 10 seconds, with the purpose of managing frequency.
25.	Operating Reserve (Spinning Reserve) mode The DER provides operating reserve	The DER can provide reserve power available within about 10 minutes
26.	Dynamic Frequency-Watt Mode The DER responds to the rate of change of frequency (ROCOF) by changing its watt output or input to minimize spikes and sags	The DER responds to the rate of change of frequency (ROCOF) by changing its watt output or input to minimize spikes and sags
27.	Coordinated Charge/Discharge Management Mode The DER determines when and how fast to charge or discharge so long as it meets its target state of charge level obligation by the specified time (<i>focus is on Electric Vehicle consumption</i>)	The DER is provided with a target state of charge and a time by which that SOC is to be reached. This allows the DER to determine when to charge or discharge based on price. The DER takes into account not only the duration at maximum consumption / production rate, but also other factors, such as that at high SOC the maximum consumption rate may not be able to be sustained, and vice versa, at low SOC, the maximum discharge rate may not be able to be sustained
28.	Frequency-Watt Smoothing Mode The DER responds to changes in frequency at the referenced ECP by changing its consumption or production rate based on frequency deviations from nominal, as a means for countering those frequency deviations df/dt	The DER is provided with frequency-watt curves that define the changes in its watt output based on frequency deviations from nominal, as a means for countering those frequency deviations and smoothing the frequency. When the frequency-watt mode is enabled, the DER monitors the frequency and adjusts its production or consumption rate to follow the specified frequency-watt curve parameters. New data points are provided multiple times per second.

#	DER Functions	Description and Key Parameters
29.	Power Factor (PF) Limiting (Correcting) Mode The DER supplies or absorbs VARs to hold the power factor at the referenced ECP within the PF limit	When the PF limiting (correcting) mode is enabled, the DER is provided with the target PF. The DER supplies or absorbs VARs in order to maintain the PF at the referenced ECP within the limits of the target PF.
30.	Delta Power Control Function Decrease active power output to ensure there remains spinning reserve amount that was bid into the market	Decrease active power output to ensure there remains spinning reserve amount that was bid into the market
31.	Power Rate Control The power is limited by the maximum ramp rate.	Manage active power ramp time, when the active power should be at the required power level by the end of the ramp time. It may reach the required power level earlier, but not later.
32.	Dynamic Volt-Watt Function Dynamically absorb or produce additional watts in proportion to the instantaneous difference from a moving average of the measured voltage	Dynamically absorb or produce additional watts in proportion to the instantaneous difference from a moving average of the measured voltage. This function utilizes the same basic concepts and settings as the Dynamic Reactive Current function but uses active power as an output rather than reactive current.
<u>Non-Operational Requirements</u>		
33.	Collect and Provide Historical Information Collect and provide detailed measurement and performance data which may be valuable to record in an operational historian	Collect and provide detailed measurement and performance data, which may be used to assess the real-time responses to power system events, control commands, and autonomous functions. This data could also be used to determine actual capabilities, impacts, compliance, and other characteristics of DER systems.
<u>Capabilities Not Yet Defined by Regulations, EPRI, or IEC 61850</u>		
34.	Microgrid Separation Control (Intentional Islanding) Process for normal separation, emergency separation, and reconnection of microgrids	Process for normal separation, emergency separation, and reconnection of microgrids. These microgrids could be individual facilities or could be multiple facilities using electric grid equipment between these facilities.
35.	Provide Black Start Capability Support the reestablishment of power after an outage	Ability to start without grid power, and the ability to add significant load in segmented groups.
36.	Provide Backup Power (Often implemented, but not standardized) Ability to provide power to local loads when not connected to the grid	Ability to provide power to local loads behind a PCC when the facility is not connected to the grid, either during an outage or due to intentional or unintentional islanding.

Appendix D – The Core Set of Electric Industry Roles

The Smart Grid Conceptual Model is useful for describing the core roles across the electricity sector and examining their relationship to system economics.

Generation Including DER. Generators provide value to the industry through the conversion of primary energy to electricity. The source of this conversion most commonly is nuclear fuel, carbon-based fuel (e.g., coal, natural gas, oil), moving or stored water, or renewable (e.g., solar, wind, geothermal). Depending on the state, generators may be owned by the utility or a third party. Nevertheless, generators are typically dispatched either based upon the incremental production costs through bidding into the market. In markets, generators are compensated at the lowest marginal cost of the next available unit of generation.

Generators are compensated, primarily, for the units of energy (MWh) they produce; however, they may also receive compensation for “ancillary services,” which include spinning reserve, frequency control, and other “products” required for stability of the transmission grid. Production costs for generating units consists of fuel cost, non-fuel operations and maintenance costs, and the “carrying cost” of the generation assets.

Currently, some types of DER may be dispatched, such as demand response. In most cases, DER does not currently receive compensation for ancillary services. However, the Federal Energy Regulatory Commission has been lowering barriers to entry for multiple types of DER to participate directly in wholesale markets, and directing RTOs to develop models and tariffs to allow for DER to participate and be compensated for its services[220, 221].

Transmission. Entities within the Transmission domain provide value by delivering bulk generation at high voltages over long distances from its source to either large customers that can utilize these high voltages, or to distribution networks, where voltage levels are lowered and electricity is delivered to end-use customers. With the exception of the ERCOT region of Texas, all transmission providers in the continental United States are regulated by FERC, which regulates the tariffs that serve as the basis for their compensation [222].

Distribution. Distribution companies add value by delivering generated electricity from transmission networks or DERs to end-use customers. Entities within the distribution domain are monopolies -- typically investor-owned utilities, cooperatives, or public power entities whose rates are determined by regulators or other governing bodies. In most jurisdictions, the cost of the energy being delivered is a pass-through cost to the customer, with separate, un-bundled tariffs/fees for the provided delivery services. However, in other jurisdictions, the costs of generation, transmission, and distribution are bundled into a single customer rate.

Markets. Wholesale electricity markets in the US are managed by RTOs or ISOs. They add value through managing bulk power flows, ensuring reliability of the transmission grid, and through transmission planning across its footprint. These FERC-regulated entities are compensated for their market management and settlement services via volume-based tariffs. Broad distribution-level markets do not currently exist within the industry in the United

States; however, recent regulatory activity in California and New York signal the creation of distribution-level market platforms in those states.

Electric Service Providers. Electric Service Providers add value as interfaces between customers and either the distribution or markets domain. A common value-added role that an electric service provider might play is in aggregating the load and/or demand response capability of smaller customers that do not have feasible access to an energy market. In deregulated markets, Electric Service Providers compete to sell electricity to end use customers, with the latitude to structure how energy is priced and what, if any, services are bundled in with the energy. Energy Service Providers also help commercial and industrial customers manage their usage against relevant customer rate designs – typically to manage peak load and related peak demand charges. Non-utility electric vehicle charging networks represent another emerging role for Electric Service Providers.

Customer. Many electricity customers have evolved to be more active in the management of their energy consumption. The majority of US electricity customers now have smart meters installed at their premises. With the customer web portals that utilities often make available with smart meter installations, customers have access to energy usage information and, often, greater insight and awareness into their energy usage and ways to manage it. Residential and commercial customers are increasingly opting to reduce their energy costs through investments in energy efficiency, rooftop solar and energy storage. With rooftop solar achieving cost parity with utility-delivered energy in many states and the declining cost of energy storage, this trend can be expected to continue. Commercial and industrial customers in deregulated energy states have utilized retail electric service providers to lower their cost of energy. Large commercial customers, particularly those with large buildings, are increasingly installing and utilizing building energy management systems to help control their energy costs.

Appendix E – Cost Recovery, Rate Design, and Regulation

Ratemaking is a complex activity that incorporates a number of economic and societal considerations. Because electricity distribution is regulated at the state and local level, executed by utilities with differing ownership structures and business models, and involves balancing of inherently local considerations such as the impact grid design and weather have on the ability to meet customer demand, the electricity rates for each utility will be necessarily unique. Despite this complexity, the elements of cost recovery, rate design, and oversight for natural monopolies are common to the economics of all electrical distribution utilities.

Cost recovery: Utilities recover their costs via customer bills. For utilities that are regulated by a state utility commission, a utility will submit an application for recovery of all costs plus profit for approval by the utility commission. The utility commission will then approve an authorized amount of revenue to be collected (revenue requirement) via customer bills. The approved revenue requirement is then allocated across customer classes based on a determination of which class is responsible for which portion of the costs. The result of this analysis is a determination of billing components, e.g., fixed charges, volumetric charges, and demand charges (where applicable).

In some states, mostly those with retail competition, these charges are unbundled into specific generation, transmission, and distribution costs to allow for more specific billing. For example, a customer who takes electricity service from a competitive supplier will still pay the monopoly for transmission and distribution service, but not generation.

All tariffs, by definition, are set by regulators whose role it is to allocate the utility's capital investments (or rate base) and expenses through the tariff mechanism to ensure that all authorized costs of the utility are recovered and that the utility receives an appropriate return on their investments. However, regulators are increasingly looking for alternatives from this capital investment-based model and toward incentive-based ratemaking of one form or another.

Performance based ratemaking is an example of an alternative form of cost recovery, which puts more of the utility's earnings on performance goals and metrics. In part, through these mechanisms, the distribution utility can become independent on the question of DER ownership, since their compensation is less directly tied to the return on new additions to the rate base.

Rate design: The collection of authorized utility revenue is accomplished via a rate design. Commercial and Industrial (C&I) customers generally pay for electricity via a tariff that includes two major components: energy and demand. The demand charge is typically based on the peak demand within a billing period, either coincident or non-coincident (individual) with system peak. The construction of the energy component can vary, however, it is typically either an unchanging flat rate, or a "block rate" that changes (increases or decreases) at various levels of consumption in the billing period.

Some states have moved industrial and larger commercial customers into time-varying rate designs, such as time of use or critical peak pricing. In addition to the energy and demand components, C&I customers may pay separate charges based on their load factor and/or power factor. For customers who are able to self-supply, they may also pay a stand-by rate which covers the utility costs to provide electricity to that customer in the event their self-supply is unavailable.

Residential rates are predominantly flat energy-based rates; the same rate is paid for each unit of energy consumed regardless of time or location. Typically, in addition to the base energy rate, customers pay a “fuel adjustment charge” that varies with the actual cost of generation, as well as taxes and other additional charges as approved by the regulator. Some jurisdictions have adopted a block- or tiered-rate construction for residential customers as well. Residential rates almost never include a demand component. However, in addition to the energy rate, residential customers also usually pay some kind of monthly customer charged (fixed fee), regardless of the quantity of energy consumed. Charges for transmission and distribution services may be accounted for separately or bundled into the energy charge.

With rare exceptions, residential rates for electricity purchased in the United States do not vary by time of day (or week), even though electricity generation costs may vary significantly during the day (or week). Dynamic rates, which — to varying degrees — attempt to reflect in electricity pricing the time-variant nature of electricity costs, are typically only offered by utilities as an optional pricing program. Time-of-use rates, which are offered as opt-in programs for residential customers by many U.S. utilities, are structured to reflect in a broad way the varying cost of energy by hour of the day and/or day of the week. Time blocks with generally higher cost energy corresponding to peak demand periods are priced higher than off-peak, lower cost time blocks. In 2019 time-of-use rates became the default rate structure for all residential customers of the California IOUs, a transition planned since 2015 affecting more than 20 million customers [223, 224]. Some other utilities adjust energy pricing seasonally to account for higher energy costs during higher demand seasons. The two IOUs in Illinois, Commonwealth Edison and Ameren, allow customers to opt into a “real-time pricing” program, in which actual energy costs vary each hour according to the actual PJM (for ComEd) or MISO (for Ameren) wholesale market price.

Critical peak pricing and variable peak pricing are mechanisms utilized by a few utilities that allow for higher energy rates during a limited number of designated peak demand or demand response events each year. Each “event” is for a specified block of hours, after which pricing reverts to the normal basis.

With the exception of a few utilities that offer customers the option to prepay for their electricity, energy is paid for after the energy is consumed.

Regulators: The regulator serves as an important check on monopoly market power, and can be described as acting to impute market pressure upon a monopoly with no natural competition. This regulatory market pressure includes consideration of utility costs and revenues, allocating cost recovery across customer classes, and additional requirements often as determined by state legislatures.

Through their oversight capacity, regulators are also responsible for ensuring that the delivery of electricity is done safely and reliably. This can include oversight for construction of new power plants and transmission lines, or establishing requirements that ensure regulated utilities have sufficient electricity resources under contract or otherwise available to provide service at all times.

For municipal or cooperative utilities, regulation is often done at the local level by a city council for a municipal utility or a board comprised of members for a cooperative. Since neither the municipal nor the cooperative utility are for-profit, rates are set to recover the utility's costs.

Appendix F – Distribution Platforms and Markets

There are a number of architectural, resource, and economic structures that can be employed to facilitate the transition to a more flexible and resilient system that better incorporates and values customer contributions to the system. This Framework is agnostic on the specific implementation choices made to achieve those ends, and it is important to note that any economic solution will need to suit the circumstances of each state, utility, and regulatory authority.

When considering the view of planning for, integrating, and investing in the grid to improve operational flexibility and resilience, and accommodate increasing numbers and types of technology, distribution platforms and market structures may be a useful model for how to integrate new technologies at low cost and high efficiency, and to maximize the benefits of interoperability investments. Two of the more commonly referred to options are distribution system platforms and transactive energy markets, which are summarized here.

Distribution System Platforms: As currently envisioned, a future distribution system operator (DSO) would provide a distribution-level market platform that enables a broad range of DER services⁹³ to be incorporated into an open-access distribution level market. The value and pricing of these services would be transparent and include both a local and system-level valuation component.

A distribution-level market platform would connect DER, customers, aggregators, and local markets operated by energy service providers,⁹⁴ allowing for the active exchange of services and resources between a variety of stakeholders and not just via the traditional utility-customer relationship. The value of DER would be dynamically calculated based on the instantaneous location-based value of each resource, and the platform would enable both peer-to-peer and peer-to-grid transactions. The platform would balance supply and demand through the development of a schedule of requirements based on pre-existing commitments, load forecasts, and generation forecasts. The platform would communicate transaction prices to DER and aggregators and then, based on actual operating conditions, readjust pricing as required to ensure supply/demand balance.

The role of the DSO, as outlined in recent regulatory activities in California and New York, is designed to facilitate the growth of DER on the distribution grid in a manner that should lead to a more optimal deployment of these resources. These two are the only states that have yet taken significant steps toward redefining the role of the distribution utility in response to DER proliferation, in which the DSO is viewed as a transformation of the role of the existing utility. More generally, a DSO should facilitate a more optimal development of the grid [225].

In California, the CPUC has defined several new capabilities for distribution utilities. Among the most significant of these, each utility is required to perform hosting capacity analyses, including a locational value analysis of each grid segment, and to publish the

⁹³ For example: voltage and reactive power support, power quality, power flow control, and reliability services.

⁹⁴ For example: demand response aggregation, or electric vehicle charge management.

results of these analyses into a publicly-available geographic interface. By performing these analyses and making this information available, DER providers and developers have an enhanced understanding of the potential value for their investments.

As a more advanced extension of this concept, the DSO would develop scenarios to remediate existing issues on the distribution grid. The DSO, in addition to considering traditional “wires-based” solutions⁹⁵ would consider on an equal basis the potential value of “non-wires” solution alternatives.⁹⁶ The DSO would then conduct a series of modelling and simulation studies to determine which of the alternative solutions would most optimally address the existing grid issues based on forecasted conditions. If a non-wires solution proves to be the preferred approach, the DSO would publish the results of this analysis for public consumption and facilitate the deployment of the preferred solution through economic incentive.

For this approach to work, the DSO has to be indifferent to both the nature and ownership of the solution, and must be neutral in its role of coordinating a distribution-level market. This independence and objectivity can only be realized if the financial incentives that the DSO has are consistent with this impartiality, and so the traditional cost-of-service and rate base structure that drives most distribution utility revenue streams would have to be replaced with other mechanisms.

Transactive Energy Markets: The purpose of transactive energy is to provide least-cost energy using typical market supply and demand principles. Transactive energy has been defined as “a system of economic and control mechanisms that allows the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter.” [226] Transactive energy can be thought of as a robust electricity marketplace in which economic transactions provide the necessary foundation for balancing of supply and demand and maintaining the integrity of the grid.

Through the near-real-time communication of pricing signals, market participants would respond with the necessary resources needed for effective grid operation.⁹⁷ In effect, operation of the grid is accomplished “economically,” with a pure financial engine driving the exchange of required goods and services. Although much work needs to be done to translate the notion of transactive energy into practice, at its core transactive approaches present opportunities to create a platform in which the broadest set of economic resources are always participating in maintaining the grid. The ideal outcome is therefore a more optimal operation of the grid than could otherwise be achieved.

Transactive energy also creates entirely new mechanisms for customers to interact with the grid. Instead of just being passive price takers in an artificially static procurement process, customers become active participants in a dynamic energy market. In doing so, customer roles evolve from purely one of consumption to a supplier of energy and related services. Transactive energy approaches have been extensively demonstrated and analyzed [38].

⁹⁵ Examples of wires-based solutions include re-conductoring the system and equipment upgrades.

⁹⁶ Examples of non-wires alternatives include distributed generation, demand response, and energy storage.

⁹⁷ Examples of the necessary resources include energy, reactive power, or ancillary services.

Appendix G – Smart Grid Cybersecurity Profile Subcategory Prioritization and Considerations Matrices

This appendix includes the excerpted tables that identify which Subcategories directly assist power system owners/operators in achieving the business objectives identified in **Section 5.1.4**, as well as the grid-specific considerations identified for each Subcategory. These prioritizations and considerations form the primary elements of the Smart Grid Cybersecurity Risk Profile, the full version of which is a publicly available NIST publication [176].

G.1 – Identify Function

The Identify Function is critical in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities. This Function guides the owner/operator in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities. The activities in the Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management are the primary security areas that address protections for the four business objectives. The Subcategories below are derived from the [Cybersecurity Framework Core](#), which includes descriptions and informative references for each Subcategory.

Table 16 – Identify function subcategory prioritization and considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories					
Asset Management	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	ID.AM-1	Knowing hardware assets is critical for maintaining safety, reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets ⁹⁸ need to be known and understood. As modernized grids become more distributed, power system owners/operators need to be accountable for all distributed assets that they own.

⁹⁸ Modernized assets/devices refers to power system devices that utilize two-way communication technologies and advanced sensing capabilities to help improve grid operations.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
ID		ID.AM-2	ID.AM-2	ID.AM-2	ID.AM-2	Knowing software assets is critical for maintaining reliability, and resilience, as well as facilitating the transition to the modern grid. Legacy and modernized assets need to be known and understood. This especially applies to modernized assets because the sophisticated logic that they execute is driven by software.
		ID.AM-3	ID.AM-3	ID.AM-3	ID.AM-3	Understanding communication and data flows is important to ensure reliability and resilience. Communications networks are critical for modernized grids, and understanding the different types of data flows (control, monitoring, and management) will provide critical information for managing those flows within modernized infrastructures and between modernized and traditional infrastructure.
		ID.AM-4	ID.AM-4	ID.AM-4	ID.AM-4	The presence of external information systems may have many impacts on the power grid. Grid reliability and resilience may be impacted if power system owners/operators are not aware of all power systems, customer-owned devices, and any other third-party systems connected to the distribution system. With respect to supporting grid modernization, traditional and modernized parts of the grid will exist side by side within a single power system owner/operator and across power system ownership lines. Awareness of external information systems that manage both traditional and modernized components is important to assure security of both Information Technology (IT) and Operational Technology (OT) infrastructures.
		ID.AM-5	ID.AM-5	ID.AM-5	ID.AM-5	Power systems contain many types of resources, including devices, data, personnel, and software. Resources directly involved in the distribution of power should be prioritized ahead of business systems.
		ID.AM-6	ID.AM-6	ID.AM-6	ID.AM-6	Identifying all power system stakeholders and their roles and responsibilities with respect to maintaining and restoring power is critical to all four business requirements.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories					
Business Environment	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	ID.BE-1	"Supply chain" in this Subcategory includes IT and OT products and services business partners, and other relevant third parties that support power delivery. As such it impacts the reliable flow of power and resiliency efforts including the flow of power from modernized parts of the grid.
	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	ID.BE-2	Power system owners/operators should understand their organization's placement in the grid infrastructure in order to manage potential cascading effects on the grid. The magnitude of potential cascading effects should be understood. Because the modernized grid incorporates distributed generation, the points of integration of distributed resources with the larger grid should be well understood. These points of integration may include generation, transmission, distribution, customers, and third-party owners/operators of distributed resources.
	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	ID.BE-3	Power system owners/operators have a variety of state and local regulatory requirements that influence their mission and objectives. See ID.GV-3 .
	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	ID.BE-4	Understanding power system dependencies helps maintain reliability and resilience. It also facilitates grid modernization through providing necessary information to plan and implement grid modernization initiatives. Having a thorough understanding of dependencies within the power system can also improve safety. The power system owner/operator should identify all sources and loads that require power, understand information about the loads, sources, and power delivery network at any given time, and use this information to control the flow of power from source to loads.
	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	ID.BE-5	Power system owners/operators should understand and implement the specific requirements to ensure resilient operation of the power system.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
	Governance	ID.GV-1	ID.GV-1	ID.GV-1	ID.GV-1	Information security policy drives a set of coherent security requirements throughout the organization. In this context, security policy should support safety, reliability, resilience, privacy, and other related concerns. Also within this context, grid components are cyber-physical systems (CPS) themselves, composed into a more complex, networked cyber-physical system of systems. The NIST CPS Public Working Group (PWG) Framework provides a set of relevant concerns. Organizational informational security policy should address OT and IT environments and how they integrate, the complexity of external partnerships, as well as cover both traditional and modernized environments.
		ID.GV-2	ID.GV-2	ID.GV-2	ID.GV-2	Information security roles and responsibilities and their coordination with external partners directly affect all requirements. In the context of the modernized grid, external parties include the owners of distributed resources.
		ID.GV-3	ID.GV-3	ID.GV-3	ID.GV-3	Legal and regulatory requirements regarding cybersecurity are especially applicable in the highly regulated critical infrastructure environment of electric power generation, transmission, and distribution. The modernized grid has additional regulatory requirements that should be considered here.
		ID.GV-4	ID.GV-4	ID.GV-4	ID.GV-4	Because the grid is a large cyber-physical system, governance and risk management processes should address all risks, not just cybersecurity.
	Risk Assessment	ID.RA-1	ID.RA-1	ID.RA-1	ID.RA-1	Identifying and documenting asset vulnerabilities can be performed as part of a risk assessment. Vulnerabilities from traditional and modernized environments should be included, especially cyber-physical devices in the modern grid.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories					
		ID.RA-2	ID.RA-2	ID.RA-2	ID.RA-2	Modernized devices need to be included in information sharing. However, these newer devices that are a part of grid modernization are not yet well-addressed within the information sharing forums of the power system owner/operator community.
		ID.RA-3	ID.RA-3	ID.RA-3	ID.RA-3	Potential threats are greatly increased in the more complex environment of the modernized grid, thereby requiring more extensive analysis. The environment is more complex because 1) the high number of devices exponentially increases the attack surface; 2) these devices may have different and distributed ownership; 3) the devices are likely heterogeneous; and 4) the overall high interconnectivity of the modernized grid.
		ID.RA-4	ID.RA-4	ID.RA-4	ID.RA-4	The modernized grid will have additional and more complex business impacts due to its distributed and multi-owner nature and complex regulatory landscape.
		ID.RA-5	ID.RA-5	ID.RA-5	ID.RA-5	Power systems owners/operators should consider threats, vulnerabilities, and impacts to the converged IT/OT environment, including traditional and modernized components.
		ID.RA-6	ID.RA-6	ID.RA-6	ID.RA-6	The complexity of the stakeholder landscape in the modernized grid can make the risk responses of power system owners/operators more complicated. Power system owners/operators will need to consider how proposed risk responses will impact interconnected stakeholders.
		ID.RM-1	ID.RM-1	ID.RM-1	ID.RM-1	The complexity of the stakeholder landscape in the modernized grid can make risk management processes more complicated.
	Risk Management Strategy	ID.RM-2	ID.RM-2	ID.RM-2	ID.RM-2	Power system owners/operators should consider the development of a comprehensive strategy to manage risk, including integrating the modernized components of the grid into the determination and description of risk tolerance.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category		Subcategories				
		ID.RM-3	ID.RM-3	ID.RM-3	ID.RM-3	When determining organizational risk tolerance, power system owners/operators should consider the potential cascading effects on the immediate geographic area, larger region, and the sector overall.
	Supply Chain Risk Management	ID.SC-1	ID.SC-1	ID.SC-1	ID.SC-1	Power system owners/operators rely on integrators, Industrial Control System (ICS) vendors, and commercial off-the-shelf (COTS) providers to design and implement networks, systems, and applications that run the grid. As power systems owners/operators modernize their grids, their supply chains increasingly include third party service providers and distributed generation owners/operators. Power system owners/operators therefore need to have robust processes for managing cybersecurity risks stemming from these supply chains that include all relevant members of this diverse ecosystem.
		ID.SC-2	ID.SC-2	ID.SC-2	ID.SC-2	Organizational supply chain risk management processes should be continuously improved regardless of whether the environment is traditional or modernized.
		ID.SC-3	ID.SC-3	ID.SC-3	ID.SC-3	When power systems transcend organizational boundaries, it may be beneficial for power system owners/operators to mutually agree on a set of appropriate security requirements in order to manage security risks. In addition to security requirements in supplier agreements, power system owners/operators are encouraged to establish a set of security requirements with their third-party partners. These agreements may be mutual, as in power system owners/operators would also be agreeing to a set of security requirements they would commit to abide by. This is a key risk management consideration for power system owners/operators.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power System Owners/Operators
Category	Subcategories					
		ID.SC-4	ID.SC-4	ID.SC-4	ID.SC-4	Assessments are required to understand whether suppliers and third parties are continuously following agreed-upon cybersecurity requirements. Power system owners/operators should consider that lack of these assurances can have an impact on all critical business/mission goals.
		ID.SC-5	ID.SC-5	ID.SC-5	ID.SC-5	Power system owners/operators should ensure that the modernized (including distributed) power environment is accounted for in response and recovery plans. Testing of these plans helps manage grid modernization efforts. Additionally, suppliers and 3 rd -party providers should be included in testing of these plans. Suppliers and 3 rd -party providers are critical to orderly restoration after incidents; if they are not properly integrated in testing efforts, it may have an impact on all critical business/mission goals.

G.2 – Protect Function

The Protect Function is critical to limit the impact of a potential cybersecurity event. Identity Management and Access Control, Awareness and Training, Information Protection Processes, Maintenance, and Protective Technology are the priority security focus areas. Identity Management and Access Control identifies and regulates personnel ingress and egress. Awareness and Training and the Protection Processes prepare the workforce to achieve cybersecurity. Protective technology implements security decisions. The Subcategories below are derived from the [Cybersecurity Framework Core](#), which includes descriptions and informative references for each Subcategory.

Table 17 – Protect function subcategory prioritization and considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
PR	Access Control	PR.AC-1	PR.AC-1	PR.AC-1	PR.AC-1	Identity management is essential for all users, devices, and processes in both traditional and modernized environments.
		PR.AC-2	PR.AC-2	PR.AC-2	PR.AC-2	Power system owners/operators should control physical access to the power system components as needed, including modernized and distributed grid components. Power system owners/operators should consider the limitations of maintaining physical access to devices on other premises, especially those devices that are owned by a 3 rd party.
		PR.AC-3	PR.AC-3	PR.AC-3	PR.AC-3	Many grid components are maintained remotely and such remote access should be secured. For modernized environments, consider the limitations of managing remote access to devices that are owned by a 3 rd party, such as distributed resources.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		<u>PR.AC-4</u>	<u>PR.AC-4</u>	<u>PR.AC-4</u>	<u>PR.AC-4</u>	Least privilege is important for limiting permissions and authorizations to manage connected devices. This reduces risks of unapproved operations which may create negative impacts to safety, reliability, and resilience. For example, excessive privileges may create an opportunity for compromise during power restoration. Grid modernization efforts should ensure that least privilege principles are designed into and implemented in the modernized grid.
		<u>PR.AC-5</u>	<u>PR.AC-5</u>	<u>PR.AC-5</u>	<u>PR.AC-5</u>	Network segmentation is an important tool for containing potential incidents (safety, reliability), and limiting damage from incidents (resilience). Grid modernization efforts should consider segmenting networks from the design stage into operations (e.g., DER devices could be segmented to limit exposure to the rest of the power system infrastructure).
		<u>PR.AC-6</u>	<u>PR.AC-6</u>	<u>PR.AC-6</u>	<u>PR.AC-6</u>	In the power system, the safe delivery of reliable power is paramount. For this reason, there may be situations (e.g., emergency maintenance or need to restore power) in which the binding and proofing of credentials may interfere with safety, reliability, and resilience. Power system owners/operators will need to consider any risks introduced if identities are not proofed and bound to credentials and if those credentials are not required for certain user actions.
		<u>PR.AC-7</u>	<u>PR.AC-7</u>	<u>PR.AC-7</u>	<u>PR.AC-7</u>	Devices should be authenticated before connecting to the grid network to ensure that only authorized devices are allowed to connect. Proper authentication of users, devices, and assets helps ensure safety and reliability. Special care will need to be taken to ensure that modernized devices are also authenticated to the grid network.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
	Awareness and Training	<u>PR.AT-1</u>	<u>PR.AT-1</u>	<u>PR.AT-1</u>	<u>PR.AT-1</u>	User training needs to include a mention that modernization of a grid affects cybersecurity. For example, the dependence on bi-directional, real-time data flows increases the importance of data integrity. Security awareness training should be provided to all users, including manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, procedures for responding to suspected cybersecurity incidents, and awareness of operational security. Also, it is recommended to incorporate threat recognition and reporting into security awareness training.
		<u>PR.AT-2</u>	<u>PR.AT-2</u>	<u>PR.AT-2</u>	<u>PR.AT-2</u>	Privileged user training needs to include a mention that legacy to non-legacy migration has impact to cybersecurity. For example, the dependence on bi-directional, real-time data flows increases the importance of data integrity.
		<u>PR.AT-3</u>	<u>PR.AT-3</u>	<u>PR.AT-3</u>	<u>PR.AT-3</u>	The stakeholder landscape is complicated in the modernized grid and power system owners/operators will need to include roles and responsibilities of all relevant stakeholders, including third parties.
		<u>PR.AT-4</u>	<u>PR.AT-4</u>	<u>PR.AT-4</u>	<u>PR.AT-4</u>	Executives need to understand the implications of business decisions (e.g., grid modernization) on cybersecurity, which can impact the larger business/mission goals
		<u>PR.AT-5</u>	<u>PR.AT-5</u>	<u>PR.AT-5</u>	<u>PR.AT-5</u>	Training and responsibilities for physical and information security personnel need to be tailored to the unique threats and risks of the grid modernization environment as well as the distributed and multi-owner nature of the environment.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
Data Security		<u>PR.DS-1</u>	<u>PR.DS-1</u>	<u>PR.DS-1</u>	<u>PR.DS-1</u>	In the case of power grid systems, protecting data-at-rest should apply to protecting the integrity of device settings. If tampered with, device settings may cause a safety or reliability issue.
		<u>PR.DS-2</u>	<u>PR.DS-2</u>	<u>PR.DS-2</u>	<u>PR.DS-2</u>	In the case of power grid systems, protecting data in-transit is an important tool to help protect the integrity of control information and device settings. Loss of integrity of control information may cause a safety or reliability issue. Power system owners/operators should consider the potential for resource-intensive cryptographic mechanisms to interfere with the functional performance of control systems and use additional methods to protect data in transit when less resource intensive cryptographic mechanisms are used.
		<u>PR.DS-3</u>	<u>PR.DS-3</u>	<u>PR.DS-3</u>	<u>PR.DS-3</u>	Power system owners/operators need to be aware of all distributed, modernized assets they own and manage them throughout the life cycle. IT components embedded in OT devices within the grid modernization infrastructure (e.g., power control and delivery) may present challenges of ownership/contractual agreements with the manufacturers. During disposal of assets, special care should be taken to not expose device configuration data. The integrity of device configuration data should be protected to not impact future safety and reliability.
		<u>PR.DS-4</u>	<u>PR.DS-4</u>	<u>PR.DS-4</u>	<u>PR.DS-4</u>	Understanding capacity requirements is critical for power system reliability and resilience.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		<u>PR.DS-5</u>	<u>PR.DS-5</u>	<u>PR.DS-5</u>	<u>PR.DS-5</u>	Data can be used to understand system behavior and devise methods to attack the system. Therefore, protection from data leaks is important for safety and reliability.
		<u>PR.DS-6</u>	<u>PR.DS-6</u>	<u>PR.DS-6</u>	<u>PR.DS-6</u>	The integrity of information and of software/firmware running on system components is critical to all business/mission requirements.
		<u>PR.DS-7</u>	<u>PR.DS-7</u>	<u>PR.DS-7</u>	<u>PR.DS-7</u>	The separation of development and testing environments is critical to ensure testing does not accidentally impact operational systems. Insufficient separation could directly impact safety, reliability, and resilience. This applies to both traditional and modernized environments equally; grid modernization is not specifically highlighted. This should be already done for the traditional environment and should also apply to modernized environments. However, it should be noted that applying this to distributed environments may be challenging due to their scope.
		<u>PR.DS-8</u>	<u>PR.DS-8</u>	<u>PR.DS-8</u>	<u>PR.DS-8</u>	The integrity of power system hardware is critical to safety, reliability, resilience, and grid modernization.
	Information Protection Processes and Procedures	<u>PR.IP-1</u>	<u>PR.IP-1</u>	<u>PR.IP-1</u>	<u>PR.IP-1</u>	Baseline configurations are needed for all devices that are owned by a power system owner/operator. However, power system owner/operators should consider that they may have little or no control over the configuration of devices owned by other stakeholders connecting to the grid. Creating and maintaining baseline configurations supports the safety, reliability, and resilience (by providing known state to restore equipment to) of the power grid. Grid modernization efforts are also supported by having a standard configuration for all devices.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		<u>PR.IP-2</u>	<u>PR.IP-2</u>	<u>PR.IP-2</u>	<u>PR.IP-2</u>	Implementing a systems development lifecycle ensures quality and predictable performance of systems and networks. It is critical for safety and reliability. While also important for the maintain resilience and support grid modernization business objectives, the safety and reliability objectives will drive the systems development lifecycle requirements and so only those two goals are selected.
		<u>PR.IP-3</u>	<u>PR.IP-3</u>	<u>PR.IP-3</u>	<u>PR.IP-3</u>	Configuration change control processes support safety, reliability, resilience (known state to restore to), and transition to modernized grid. Power system owners/operators should consider how organizational configuration change control processes will include devices owned by third parties
		<u>PR.IP-4</u>	<u>PR.IP-4</u>	<u>PR.IP-4</u>	<u>PR.IP-4</u>	Backups are essential for retaining device configuration information so that devices can be recovered and restored to proper operational states. Modernized grids are especially susceptible because modern devices have more programmable logic in them. Special consideration should be taken to address backups of devices owned by third parties.
		<u>PR.IP-5</u>	<u>PR.IP-5</u>	<u>PR.IP-5</u>	<u>PR.IP-5</u>	Physical security policies are important for safety and reliability of the power grid. Physical access to sensors can lead to sensors being used as attack vectors. Physical security policies also support the integration of distributed, modernized devices into the grid.
		<u>PR.IP-6</u>	<u>PR.IP-6</u>	<u>PR.IP-6</u>	<u>PR.IP-6</u>	The destruction of data is not directly applicable to these business/mission requirements.
		<u>PR.IP-7</u>	<u>PR.IP-7</u>	<u>PR.IP-7</u>	<u>PR.IP-7</u>	Protection processes should be continuously improved regardless of whether the power system environment is traditional or modernized.
		<u>PR.IP-8</u>	<u>PR.IP-8</u>	<u>PR.IP-8</u>	<u>PR.IP-8</u>	Sharing the effectiveness of protection technologies is not directly applicable to these business/mission requirements.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		<u>PR.IP-9</u>	<u>PR.IP-9</u>	<u>PR.IP-9</u>	<u>PR.IP-9</u>	Power system owners/operators need to be sure to include the modernized environment/devices in the response and recovery plans and their testing to help manage grid modernization efforts. They should also ensure that the plans address the collaboration between IT and OT personnel and the distributed nature of modernized environments.
		<u>PR.IP-10</u>	<u>PR.IP-10</u>	<u>PR.IP-10</u>	<u>PR.IP-10</u>	Power system owners/operators need to be sure to include the modernized environment/devices in cybersecurity response and recovery plans and their testing to help manage grid modernization efforts. The plans need to address the collaboration between IT and OT personnel as well as the distributed nature of modernized environments.
		<u>PR.IP-11</u>	<u>PR.IP-11</u>	<u>PR.IP-11</u>	<u>PR.IP-11</u>	Processes and procedures for including cybersecurity in human resources practices are the same for both traditional and modernized environments. Therefore, no special accommodations are required for the modernized grid.
		<u>PR.IP-12</u>	<u>PR.IP-12</u>	<u>PR.IP-12</u>	<u>PR.IP-12</u>	Modernized distributed energy resources can have vulnerabilities that may allow new and unaccounted threat vectors to the power grid. Power system owners/operators should consider how externally-owned devices and third-party owners/operators will be included in a vulnerability management plan.
	Maintenance	<u>PR.MA-1</u>	<u>PR.MA-1</u>	<u>PR.MA-1</u>	<u>PR.MA-1</u>	Special care needs to be taken when devices are owned by third parties, as may be the case in modernized environments.
		<u>PR.MA-2</u>	<u>PR.MA-2</u>	<u>PR.MA-2</u>	<u>PR.MA-2</u>	Power system owners/operators need to be aware of any remote access capabilities that the device vendor may have to equipment. This is extremely important in energy environments due to the distributed nature, geographical dispersion, and the mission need for remote maintenance of both legacy and modernized devices.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
	Protective Technology	<u>PR.PT-1</u>	<u>PR.PT-1</u>	<u>PR.PT-1</u>	<u>PR.PT-1</u>	Audit logs capture information that will be helpful during an attack to find anomalies and potentially limit the impact or stop the incident from inflicting greater damage (helps safety). Capturing and monitoring audit logs is also important for managing cybersecurity risks to grid modernization. These audit logs may provide visibility into the activities and traffic related to these distributed devices.
		<u>PR.PT-2</u>	<u>PR.PT-2</u>	<u>PR.PT-2</u>	<u>PR.PT-2</u>	Protecting and restricting the use of removable media on modernized devices has the same considerations as on legacy devices.
		<u>PR.PT-3</u>	<u>PR.PT-3</u>	<u>PR.PT-3</u>	<u>PR.PT-3</u>	Power system owners/operators should consider how the principle of least functionality will be applied to third-party assets connected to their grid.
		<u>PR.PT-4</u>	<u>PR.PT-4</u>	<u>PR.PT-4</u>	<u>PR.PT-4</u>	Distributed multi-ownership of some modern grid (e.g., DER) environments may make it challenging to protect communications and control networks.
		<u>PR.PT-5</u>	<u>PR.PT-5</u>	<u>PR.PT-5</u>	<u>PR.PT-5</u>	Power system owners/operators should consider all possible ways to achieve resiliency requirements.

G.3 – Detect Function

The Detect Function enables timely discovery of cybersecurity events. Real time awareness and continuous monitoring of the systems is critical to detect cybersecurity events. The Subcategories below are derived from the [Cybersecurity Framework Core](#), which includes descriptions and informative references for each Subcategory.

Table 18 – Detect function subcategory prioritization and considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
DE	Anomalies and Events	DE.AE-1	DE.AE-1	DE.AE-1	DE.AE-1	A baseline of network operations and expected data flows is extremely important in the OT context because information flows are predictable, and control systems generally have few users. Understanding the control information flows will help monitor and detect unusual network behavior and allow for timely response. This applies to both traditional and modernized grid environments.
		DE.AE-2	DE.AE-2	DE.AE-2	DE.AE-2	Analyzing detected cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.AE-3	DE.AE-3	DE.AE-3	DE.AE-3	When collecting and aggregating data from third-party devices, the devices and the data should be authenticated and validated. Without this authentication and validation, power system owners/operators should carefully consider whether those devices and their data can be trusted.
		DE.AE-4	DE.AE-4	DE.AE-4	DE.AE-4	Determining the impact of detected cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.AE-5	DE.AE-5	DE.AE-5	DE.AE-5	Establishing incident alert thresholds is critical for safety, reliability, and resilience. This practice applies to both traditional and modernized parts of the grid.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
	Security Continuous Monitoring	DE.CM-1	DE.CM-1	DE.CM-1	DE.CM-1	Neglecting to monitor the grid for cybersecurity events may result in missing an event with implications and impact. For grid modernization, monitoring has to be built in for the future. While the selection of safety may be surprising, not monitoring substantially increases the risk of not knowing that there may be safety impacts and being unable to reduce or eliminate them.
		DE.CM-2	DE.CM-2	DE.CM-2	DE.CM-2	Monitoring the physical environment for cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.CM-3	DE.CM-3	DE.CM-3	DE.CM-3	Monitoring personnel activity for cybersecurity events is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.CM-4	DE.CM-4	DE.CM-4	DE.CM-4	Power system owners/operators should consider using malicious code detection methodologies in both traditional and modernized infrastructure. These devices contain complex software which makes them vulnerable to cyber attacks.
		DE.CM-5	DE.CM-5	DE.CM-5	DE.CM-5	Detecting unauthorized mobile code is critical for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		DE.CM-6	DE.CM-6	DE.CM-6	DE.CM-6	Power system owners/operators rely on vendors and external service providers for many capabilities, including industrial control systems and communications networks required to operate the grid. Whether service providers are accessing IT or OT environments, those activities should be monitored to ensure mitigating actions can be taken in case of attack stemming from external connections.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category	Subcategories					
		DE.CM-7	DE.CM-7	DE.CM-7	DE.CM-7	Unauthorized personnel, connections, devices, or software introduce risks into IT and OT, and may impact grid operations. Any connections to IT and OT systems and networks should be authenticated to ensure that only approved and trusted parties gain access to those systems and networks.
		DE.CM-8	DE.CM-8	DE.CM-8	DE.CM-8	Performing vulnerability scans is required to identify vulnerabilities in critical infrastructure. For modernized environments, power system owners/operators may need to consider an agreement to scan 3 rd party-owned devices that are connected to their grid.
	Detection Processes	DE.DP-1	DE.DP-1	DE.DP-1	DE.DP-1	Knowing roles and responsibilities with respect to detection is critical to all four business goals. This includes restoration across power system ownership lines and within a single power system owner/operator with traditional and modernized components and networks. Distributed resources owners/operators may also have a role and responsibilities in detection activities.
		DE.DP-2	DE.DP-2	DE.DP-2	DE.DP-2	Power system owners/operators need to ensure that detection activities comply with jurisdiction-specific safety requirements.
		DE.DP-3	DE.DP-3	DE.DP-3	DE.DP-3	Power system owners/operators should consider any potential negative impact to the power system due to testing of detection processes. The owners/operators of distributed modernized devices may also need to participate in this testing.
		DE.DP-4	DE.DP-4	DE.DP-4	DE.DP-4	Event detection information communication includes communicating detection events across traditional and modernized environments as well as between power system owners/operators in the modernized grid.
		DE.DP-5	DE.DP-5	DE.DP-5	DE.DP-5	Detection processes should be continuously improved.

G.4 – Respond Function

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Rapid and effective response and communication to cybersecurity incidents is critical in protecting personnel and environmental safety. Situational awareness to the event unfolding is needed to properly address it. The Subcategories below are derived from the [Cybersecurity Framework Core](#), which includes descriptions and informative references for each Subcategory.

Table 19 – Respond function subcategory prioritization and considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
RS	Response Planning	RS.RP-1	RS.RP-1	RS.RP-1	RS.RP-1	Response plan execution applies in both traditional and modernized environments.
	Communications	RS.CO-1	RS.CO-1	RS.CO-1	RS.CO-1	Knowing roles and responsibilities with respect to response and grid restoration is critical to all four business goals. This includes restoration across power system ownership lines and within a single power system owner/operator with integration of traditional and modernized components and networks.
		RS.CO-2	RS.CO-2	RS.CO-2	RS.CO-2	Having established criteria for reporting incidents helps support safety objectives to ensure that safety considerations are a part of incident response. Furthermore, resilience benefits from thoughtful criteria.
		RS.CO-3	RS.CO-3	RS.CO-3	RS.CO-3	Assuming that the event response information is shared once an incident has occurred, this Subcategory outcome supports resilience, rather than reliability. Sharing of information is important to ensure safety of restoration crews and has to be executed across traditional and modernized systems and components.
		RS.CO-4	RS.CO-4	RS.CO-4	RS.CO-4	Power system owners/operators should consider that the modernized grid is expected to have an expanded set of stakeholders that includes distributed resources owners/operators.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		<u>RS.CO-5</u>	<u>RS.CO-5</u>	<u>RS.CO-5</u>	<u>RS.CO-5</u>	Sharing information across power system boundaries is important, especially when some of the power systems are modernized and some are not. In this context, external stakeholders are assumed to include neighboring power system owners/operators.
	Analysis	<u>RS.AN-1</u>	<u>RS.AN-1</u>	<u>RS.AN-1</u>	<u>RS.AN-1</u>	Investigating notifications from detection systems is important for safety, reliability, and resilience. There are no special considerations for modernized parts of the infrastructure.
		<u>RS.AN-2</u>	<u>RS.AN-2</u>	<u>RS.AN-2</u>	<u>RS.AN-2</u>	Power system owners/operators should take care to understand any similarities and differences in impacts between the traditional and modernized environments.
		<u>RS.AN-3</u>	<u>RS.AN-3</u>	<u>RS.AN-3</u>	<u>RS.AN-3</u>	Performing forensics of incidents is critical for safety and resilience.
		<u>RS.AN-4</u>	<u>RS.AN-4</u>	<u>RS.AN-4</u>	<u>RS.AN-4</u>	Categorizing incidents is critical for safety and resilience.
		<u>RS.AN-5</u>	<u>RS.AN-5</u>	<u>RS.AN-5</u>	<u>RS.AN-5</u>	Having processes for receiving and analyzing vulnerability information is important for reliability, resilience, and the modernized grid because devices in the modernized grid are smarter than the legacy devices and have their own vulnerabilities. Safety will benefit indirectly from these activities.
	Mitigation	<u>RS.MI-1</u>	<u>RS.MI-1</u>	<u>RS.MI-1</u>	<u>RS.MI-1</u>	Containing incidents is critical for safety and resilience, since once an incident occurs, reliability is at risk and may already have been affected. Containing incidents is important for both traditional and modernized infrastructures.
		<u>RS.MI-2</u>	<u>RS.MI-2</u>	<u>RS.MI-2</u>	<u>RS.MI-2</u>	Mitigating incidents is critical for safety and resilience, since once an incident occurs, reliability is at risk and may already have been affected depending on the nature of the incident. Mitigating incidents is important for both traditional and modernized infrastructures.

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
Category		Subcategories				
		<u>RS.MI-3</u>	<u>RS.MI-3</u>	<u>RS.MI-3</u>	<u>RS.MI-3</u>	Newer devices are likely to be more vulnerable because they are interconnected and more complex than legacy devices. Not patching will hinder the ability of power system owners/operators to be resilient and reliable. Processes should be in place to receive vulnerability information from vendors, as well as to share vulnerability information with device owners/operators across power systems that may have different ownership.
	Improvements	<u>RS.IM-1</u>	<u>RS.IM-1</u>	<u>RS.IM-1</u>	<u>RS.IM-1</u>	Lessons learned will improve future safety, reliability, resilience, and grid modernization.
		<u>RS.IM-2</u>	<u>RS.IM-2</u>	<u>RS.IM-2</u>	<u>RS.IM-2</u>	Updating recovery strategies will improve future safety, reliability, resilience, and grid modernization.

G.5 – Recover Function

The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity event. Defined Recovery objectives are needed when recovering from disruptions. The Subcategories below are derived from the [Cybersecurity Framework Core](#), which includes descriptions and informative references for each Subcategory.

Table 20 – Recover function subcategory prioritization and considerations

		Maintain Safety	Maintain Reliability	Maintain Resilience	Support Grid Modernization	Considerations for Power Systems Owners/Operators
	Category	Subcategories				
RE	Recovery Planning	RC.RP-1	RC.RP-1	RC.RP-1	RC.RP-1	There are implications to the safety of power system owner/operator workers (e.g., linemen) when the cyber security recovery plan is executed. The plan should include both traditional and modernized parts of the grid.
	Improvements	RC.IM-1	RC.IM-1	RC.IM-1	RC.IM-1	Incorporating lessons-learned into plans is absolutely critical for maintaining reliability and resilience. In this case the other two business goals are of secondary importance.
		RC.IM-2	RC.IM-2	RC.IM-2	RC.IM-2	Updating recovery strategies is critical for reliability and resilience and should cover any activities relevant to safety and grid modernization.
	Communications	RC.CO-1	RC.CO-1	RC.CO-1	RC.CO-1	While important, managing public relations is not critical for the four goals.
		RC.CO-2	RC.CO-2	RC.CO-2	RC.CO-2	While important, repairing reputation is not critical for the four goals.
		RC.CO-3	RC.CO-3	RC.CO-3	RC.CO-3	Cyber security event recovery activities have to be coordinated to ensure safety of power system owner operator workers (e.g., linemen) working on power recovery. Recovery efforts also require coordination across power systems, some of which may be modernized and some not.

Appendix H – Logical Interface Categories from NISTIR 7628

Table 21 – Logical Interface Categories from NISTIR 7628 [178]

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: - Between transmission SCADA and substation equipment - Between distribution SCADA and high priority substation and pole-top equipment - Between SCADA and distributed control systems (DCS) within a power plant (NOTE: LICs 1-4 are separate due to the architecturally significant differences between the availability and constraints, which impact mitigations such as encryption.)	U67, U79, U81, U82, U85, U102, U117, U137
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: - Between distribution SCADA and lower priority pole-top equipment - Between pole-top IEDs and other pole-top IEDs	U67, U79, U81, U82, U85, U102, U117, U137
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: Between transmission SCADA and substation automation systems	U67, U79, U81, U82, U85, U102, U117, U137
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	U67, U79, U81, U82, U85, U102, U117, U137
5. Interface between control systems within the same organization, for example: Multiple DMS systems belonging to the same utility Between subsystems within DCS and ancillary control systems within a power plant	U7, U9, U11, U13, U27, U65, U67, U83, U87, U115, Ux2
6. Interface between control systems in different organizations, for example: Between an RTO/ISO EMS and a utility energy management system	U10, U56, U66, U70, U74, U80, U83, U87, U89, U90, U115, U116, Ux3
7. Interface between back office systems under common management authority, for example: Between a Customer Information System and a Meter Data Management System	U2, U4, U21, U22, U26, U31, U53, U96, U98, U110, Ux4
8. Interface between back office systems not under common management authority, for example: Between a third-party billing system and a utility meter data management system	U1, U4, U6, U15, U52, U53, Ux4, Ux6

Logical Interface Category	Logical Interfaces
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: Between a Retail aggregator and an Energy Clearinghouse	U4, U9, U17, U20, U51, U52, U53, U55, U57, U58, U72, U90, U93, U97
10. Interface between control systems and non-control/corporate systems, for example: Between a Work Management System and a Geographic Information System	U12, U30, U33, U36, U52, U59, U75, U91, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: Between a temperature sensor on a transformer and its receiver	U111
12. Interface between sensor networks and control systems, for example: Between a sensor receiver and the substation master	U108, U112
13. Interface between systems that use the AMI network, for example: - Between MDMS and meters - Between LMS/DRMS and Customer EMS	U2, U6, U7, U8, U21, U24, U25, U32, U95, U119, U130
14. Interface between systems that use the AMI network with high availability, for example: - Between MDMS and meters - Between LMS/DRMS and Customer EMS - Between DMS Applications and Customer DER - Between DMS Applications and DA Field Equipment	U2, U6, U7, U8, U21, U24, U25, U32, U95, U119, U130
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: - Between Customer EMS and Customer Appliances - Between Customer EMS and Customer DER - Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U120, U124, U126, U127
16. Interface between external systems and the customer site, for example: - Between Third Party and HAN Gateway - Between ESP and DER - Between Customer and CIS Web site	U18, U37, U38, U39, U40, U42, U88, U92, U125
17. Interface between systems and mobile field crew laptops/equipment, for example: - Between field crews and GIS - Between field crews and substation equipment	U14, U29, U34, U35, U99, U101, U104, U105
18. Interface between metering equipment, for example: - Between sub-meter to meter - Between PEV meter and Energy Service Provider	U24, U25, U41, U46, U47, U48, U50, U54, U60, U95, U128, U129, Ux5

Logical Interface Category	Logical Interfaces
19. Interface between operations decision support systems, for example: Between WAMS and ISO/RTO	U77, U78
20. Interface between engineering/maintenance systems and control equipment, for example: - Between engineering and substation relaying equipment for relay settings - Between engineering and pole-top equipment for maintenance - Within power plants	U109, U114, U135, U136, U137
21. Interface between control systems and their vendors for standard maintenance and service, for example: Between SCADA system and its vendor	U5
22. Interface between security/network/system management consoles and all networks and systems, for example: Between a security console and network routers, firewalls, computer systems, and network nodes	U133 (includes interfaces to actors 17-Geographic Information System, 12 – Distribution Data Collector, 38 – Customer Portal, 24 – Customer Service Representative, 23 – Customer Information System, 21 – AMI Headend, 42 – Billing, 44 – Third Party, 43 – Energy Service Provider, 41 – Aggregator / Retail Energy Provider, 19 – Energy Market Clearinghouse, 34 – Metering / Billing / Utility Back Office)

Appendix I – Types of Information Exchange Between Entities in the High-DER Example

Table 22 – Information exchanges in Figure 24 High-DER example

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
<i>Level 1: Autonomous Cyber-Physical Systems</i>							
D09	4a: DER Controller of DER Devices (single or in aggregate)	4b: DER Device or Unit (e.g. PV, Storage, Diesel, Turbine)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DER components and their DER controller typically uses ModBus. Cybersecurity protection of this protocol is not feasible, so physical security, such as locked rooms or cabinets should be used. If necessary, a VPN can be used to secure the transport of ModBus messages.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks may depend on the type and criticality of the DER, but most likely will require aborting communications. The DER may or may not continue to operate.	The controller and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D10	6a: EVSE Charging Stations	6a: EVSE Charging Stations	LIC #4: Interface between control systems and equipment without high availability, without compute nor bandwidth constraints	Most communications between EV Service Elements (charging stations) and EVs use the ISO/IEC 15118 standard, while the actual charging standards vary among different countries and for different levels (Levels 1-3, fast charging) and types of charging (AC vs. DC charging). Cybersecurity for these standards are partially developed.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks would most likely require aborting communications. The EVSE may or may not continue to charge EVs, using local default charging functions.	The EVSE and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D11	4c: Utility-Scale DER System or Plant (e.g. large storage system)	4d: DER Device or Unit (e.g. PV, Storage, Diesel, Turbine)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DER components and their DER controller typically uses ModBus. Cybersecurity of this protocol is not feasible, so physical security, such as locked rooms or cabinets should be used. If necessary, a VPN can be used to secure the transport of ModBus messages.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks	Responses to attacks may depend on the type and criticality of the DER, but most likely will require aborting communications. The DER may or may not continue to operate.	The controller and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
Level 2: Facilities DER Energy Management Systems (FDEMS)							
U45	#5: Facility EMS (DER and Load) or Plant EMS	4a: DER Controller of DER Devices (single or in aggregate)	LIC #3: Interface between control systems and equipment with high availability, without compute nor bandwidth constraints	Communications between DERs and the Energy Management System within their facility could use many different protocols, including IEC 61850, IEEE 2030.5, and Modbus. Cybersecurity would be the responsibility of the facility, and could range from none to very sophisticated, depending upon the facility requirements.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U62	#5: EV Fleet EMS	6a: EVSE Charging Stations	LIC #4: Interface between control systems and equipment without high availability, without compute nor bandwidth constraints	Communications between EVSEs and the EV fleet Energy Management System could use many different protocols including IEC 61850, IEEE 2030.5, and OCPP. Cybersecurity would be the responsibility of the facility, and could range from none to very sophisticated, depending upon the facility requirements.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
Level 3: Third Party, Aggregators							
D92	#5: FDEMS	#41b: Aggregator	LIC#16: Interface between external systems and the customer site	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely be minimal or use traditional IT techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U92	#5: FDEMS	#41a: Retail Energy Provider (REP)	LIC#16: Interface between external systems and the customer site	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely be minimal or use traditional IT techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
Level 4: Utility Operations							
D01	#25: DERMS	#17: GIS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (Common Information Model, CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while role-based access control (RBAC) techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
D02	#27: DMS	#25: DERMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D03	#4c: Utility Scale DER or Plant	#29a: DER SCADA	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D04	#5: FDEMS	#29a: DER SCADA	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D05	#5: FDEMS	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
D07	#31: ISO/RTO Operations	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D08	41b: Aggregator	#25: DERMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D91	#41b: Aggregator	#30: Energy Management System	LIC#10: Interface between control systems and non-control/corporate systems.	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U09	#29a: DER SCADA	#27: DMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
U11	#32: Load Management	#27: DMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.
U27	#27: DMS	#36: OMS	LIC#10: Interface between control systems and non-control/corporate systems	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U52	#41b: Aggregator	#31: ISO/RTO Operations	LIC#10: Interface between control systems and non-control/corporate systems.	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U56	#29a: DER SCADA	#31: ISO/RTO Operations	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U65	#29a: DER SCADA	#25: DERMS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U87	#27: DMS	#30: EMS	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U91	#41a: Retail Energy Provider (REP)	#30: Energy Management System	LIC#10: Interface between control systems and non-control/corporate systems.	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U102	#27: DMS	#17: GIS	LIC#5: Interface between control systems within the same organization	Communications would most likely use proprietary protocols or IEC 61968/70 (CIM) and be protected within an electronic security perimeter. Cybersecurity authentication and authorization would reflect the organization's policies.	Electronic security perimeter techniques would be used to detect intrusions, while RBAC techniques would be used to notify users of unauthorized interactions.	Responses to attacks would most likely require aborting communications, assess the electronic security perimeter, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules, including any electronic security perimeter routers, gateways, etc., would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U106	#5: FDEMS	#32: Load Management System	LIC#6: Interface between control systems in different organizations	Communications would most likely use ISO/RTO protocols such as IEEE 1815 (DNP3), IEC 61850, or IEEE 2030.5 (SEP2). Cybersecurity authentication and authorization would use the security provided by those protocols and/or by establishing gateways to isolate interactions.	External means, such as Intrusion Detection Systems (IDS) and SNMP MIBs (IEC 62351-7) would be used to notify of possible attacks; IEC 62351 security for IEC 61850 could also detect possible attacks.	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
Level 5: Market Operations							
D06	#19: Energy Market Clearinghouse	#25: DERMS	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
D20	#41b: Aggregator	#19: Energy Market Clearinghouse	LIC#9: Interface with business-to-business (B2B) connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U17	#20: Wholesale Market	#19: Energy Market Clearinghouse use	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U20	#41a: Retail Energy Provider (REP)	#19: Energy Market Clearinghouse	LIC#9: Interface with business-to-business (B2B) connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.
U58	#31: ISO/RTO Operations	#19: Energy Market Clearinghouse use	LIC#9: Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary or CIM-based protocols. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Interface	Entity #1	Entity #2	Logical Interface Security	Protection against Attacks	Notification of Possible Attacks	Responding to and Coping with Attacks	Recovery from Attacks
U93	#41a: Retail Energy Provider (REP)	#20: Wholesale Market	LIC#9. Interface with B2B connections between systems usually involving financial or market transactions	Communications would most likely use the Internet with proprietary protocols established by the Retail Energy Provider. Cybersecurity would most likely use traditional IT confidentiality techniques typically used over the Internet.	Internet-based techniques would be used to detect and notify users about malware or other attacks	Responses to attacks would most likely require aborting communications, then attempting to reestablish communications with new keys. If malware was detected, its removal from systems would be required.	The systems and any communication modules would be tested for malware and additional measures for preventing attacks would be added.

Appendix J – List of Reviewed Smart Grid Interoperability Standards

The NIST Review of Smart Grid Standards for Testing and Certification Landscape Analysis [103] evaluated 240 standards drawn from multiple sources⁹⁹ that are relevant to the smart grid. Of those 240 standards, NIST’s functional categorization approach indicated 169 were relevant to interoperability. Each of the 169 standards deemed relevant to interoperability were assessed for the existence — or plan for — a testing and certification (T&C) program.

The 169 interoperability relevant standards are listed in **Table 23**. Included within this table are the functional categories used to identify standards as interoperability-relevant. Also included is the NIST assessment of T&C availability for each standard.

T&C programs in **Table 23** are categorized as follows:

- x – an independent T&C authority (ITCA) exists for this standard
- y – the ITCA program for this standard derives from requirements established in a different standard
- z – 1st or 2nd party T&C programs exist for this standard
- p – a T&C program is planned for this standard

This table is graphically depicted in **Figure 29**. Standards in **Table 23** denoted by the symbol ∇ were submitted to NIST during the public comment period between September 18 and November 2, 2020 [228]. The analysis underlying **Figure 29** was not altered to include these additional standards and remains consistent with the description in the original paper.

The full paper and methodology for this analysis, with detailed descriptions of each of the 240 standards reviewed, can be downloaded via this link:

<https://doi.org/10.6028/NIST.TN.2042>

Table 23 – List of standards reviewed for testing and certification availability

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
ANSI C12.1-2008			x			z
ANSI C12.1-2014			x			z
ANSI C12.18-2006	x	x	x			

⁹⁹ The standards used in this analysis were primarily drawn from the SEPA Catalog of Standards [203], the NIST Framework and Roadmap for Smart Grid Interoperability Standards, R3.0 [24], and the European Distribution System Operator priority standards position paper [227].

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
ANSI C12.19-2008	x					
ANSI C12.19-2012	x					
ANSI C12.20-2015			x			z
ANSI C12.21-2006	x	x				
ANSI C12.22-2012	x	x				
ANSI/ASHRAE 135-2016 (ISO 16484-5:2017)	x	x				y
ANSI/ASHRAE/NEMA 201-2016 (ISO 17800:2017)	x					
ANSI/CEA 709.1-D-2014 (ISO/IEC 14908-1:2012)		x				
ANSI/CEA 709.2-A-2006 (ISO/IEC 14908-2:2012)		x				
ANSI/CEA 709.3-R2004 (ISO/IEC 14908-3:2012)		x				
ANSI/CEA 709.4-2013		x	x			
ANSI/CEA 852-C-2014		x				
ANSI/CEA 852.1-A-2014		x				
CTA 2045		x				
IEC 60255			x			
IEC 60255-1:2009			x			
IEC 60255-24:2013		x				x
IEC 60255-26:2013			x			
IEC 60870-5-101:2003		x				x
IEC 60870-5-102:1996		x				
IEC 60870-5-103:1997		x				
IEC 60870-5-104 Ed. 2.1 b:2016		x				x
IEC 60870-6-503:2014		x				x
IEC 60870-6-702:2014		x				x
IEC 60870-6-802:2014	x					x
IEC 61000-2- 2:2002+AMD1:2017+AMD2:2018			x			
IEC 61000-3-2:2018			x			

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
IEC 61000-4-30:2015			x			
IEC 61334-4-32:1996		x				
IEC 61334-4-41:1996		x				
IEC 61334-4-511:2000		x				
IEC 61334-4-512:2001		x				
IEC 61334-5-1:2001		x				
IEC 61850-5:2013		x	x			
IEC 61850-6:2009+AMD1:2018		x				y
IEC 61850-7-1:2011	x	x				y
IEC 61850-7-2:2010	x	x				y
IEC 61850-7-3:2010	x					y
IEC 61850-7-4:2010(E)	x					y
IEC 61850-7-410:2012+AMD1:2015	x					
IEC 61850-7-420:2009	x					
IEC 61850-7-500:2017	x					
IEC 61850-7-510:2012	x					
IEC 61850-8-1:2011		x		x		y
IEC 61850-8-2:2018		x		x		
IEC 61850-90-1: 2010		x				
IEC 61850-90-10:2017	x					
IEC 61850-90-8:2016					x	
IEC 61850-9-2:2004		x		x		y
IEC 61850-9-2:2004 LE		x		x		y
IEC 61850-9-2:2011		x				y
IEC 61850-9-3:2016		x	x			p
IEC 61850-80-1:2016	x				x	
IEC 61850-80-3:2015		x		x		
IEC 61850-80-4:2016	x				x	
IEC 61850-90-2:2016		x		x		
IEC 61850-90-3:2016		x				

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
IEC 61850-90-5:2012	x	x		x	x	
IEC 61850-90-7:2013	x					
IEC 61850-90-17:2017		x				
IEC 61851-1:2017			x			
IEC 61851-23:2014			x			y
IEC 61851-24:2014	x	x				
IEC 61869-9:2016		x				z
IEC 61968-4:2007		x				z
IEC 61968-5:2020 ^ψ					x	
IEC 61968-8:2015		x				
IEC 61968-9:2013		x				
IEC 61968-11: 2013	x					p
IEC 61968-13:2008		x				p
IEC 61968-100:2013		x				
IEC 61970-301:2016	x					p
IEC 61970-401:2005		x				
IEC 61970-501:2006	x					
IEC 62053-21:2003+AMD1:2016			x			z
IEC 62053-22:2016			x			z
IEC 62053-23			x			z
IEC 62054-21			x			z
IEC 62056-3-1:2013		x				
IEC 62056-4-7:2015		x				x
IEC 62056-5-3:2017		x				x
IEC 62056-6-1:2017	x					x
IEC 62056-6-2:2017	x	x				x
IEC 62056-6-9:2016	x				x	x
IEC 62056-7-3:2017		x				x
IEC 62056-7-5:2016		x				x
IEC 62056-7-6:2013		x				x

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
IEC 62056-8-20:2016		x				x
IEC 62056-8-3:2013		x				x
IEC 62056-8-5:2017		x				x
IEC 62056-8-6:2017		x				x
IEC 62056-9-1:2016		x				x
IEC 62056-9-7:2013		x				
IEC 62056-42:2002		x				
IEC 62056-46:2002		x				
IEC 62282-2:2012			x			
IEC 62325-301:2014	x					
IEC 62325-351:2016	x					
IEC 62325-451:2017	x					
IEC 62325-503:2014		x				
IEC 62357-200:2015	x	x				
IEC 62541-3:2015	x					
IEC 62541-4:2015		x				
IEC 62541-5:2015	x					
IEC 62541-6 :2015					x	
IEC 62541-8:2015	x	x				
IEC 62541-9:2015	x	x				
IEC 62541-10:2015	x					
IEC 62541-13:2015	x					
IEC 62541-100:2015	x	x				
IEC 62689-2:2016			x			
IEC 62689-100:2016	x				x	
IEEE 1377-2012 (ANSI C12.19)	x					
IEEE 1451.0-2007	x	x				
IEEE 1451.1-1999		x				
IEEE 1451.4-2004		x				
IEEE 1451.5-2007		x				

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
IEEE 1547-2018			x			y
IEEE 1547.1-2020 ^ψ			x			p
IEEE 1547.3-2007	x	x				
IEEE 1588-2008		x	x			z
IEEE 1701-2011 (ANSI C12.18)	x	x				
IEEE 1702-2011 (ANSI C12.21)	x	x				
IEEE 1815-2010	x	x				z
IEEE 1815-2012	x	x				z
IEEE 1815.1-2015/Cor1-2016	x	x		x	x	
IEEE 1901-2010		x				
IEEE 1901.2-2013/IEEE Std 1901.2a-2015 (Amendment to IEEE Std 1901.2-2013)		x				
IEEE 2030-2011		x				
IEEE 2030.5-2013	x	x				z
IEEE 2030.7-2017		x	x			
IEEE C37.118.1-2011			x			
IEEE C37.118.1a-2014			x			x
IEEE C37.118.2-2011		x				
IEEE C37.238-2011		x	x			
IEEE C37.238-2017		x	x			p
IEEE C37.239-2010		x				
IETF RFC-6272-2011		x				
ISO 15118-2:2014		x				
ISO 15118-3:2015		x				
ISO 15118-6		x				
ISO 15118-8:2018		x				
ISO/IEC 14908-1:2012		x				
ISO/IEC 14908-2:2012		x				
ISO/IEC 14908-4:2012		x				

Standard No.	Information Model	Communication	Physical Performance	Communication Mapping	Model Mapping	T&C
ISO/IEC 15067.3:2012	x	x				
ITU T-G.9903		x				
ITU T-G.9960-2011		x				
ITU T-G.9972:2010		x				
MultiSpeak Security-V1.0		x		x		x
MultiSpeak V3.0:2015 ^W	x	x				x
MultiSpeak V4.1:2010 ^W	x	x			x	x
MultiSpeak V5.0:2015	x	x			x	x
NAESB REQ.21	x	x				x
NAESB RMQ.18	x					
NAESB RMQ.26	x	x				p
NAESB WEQ.19:2010	x					
NEMA SG-AMI 1-2009 (R2015)			x			z
NISTIR 7761-2011		x				
NISTIR 7862-2012		x				
NISTIR 7943-2013		x		x		
OASIS EMIX V1.0:2012	x					
OASIS EI-2014 V1.0	x	x				
OASIS WS Calendar V1.0	x					
OPC-UA	x	x		x	x	z
OGC-GML	x	x				
OpenADR 2.0 Profile A OpenADR 2.0 Profile B	x	x				x
SAE J1772-2017		x	x			
SAE J2836-Use-Cases-(1-3) SAE J2836/1		x				
SAE J2847/1:2010		x				

References

- [1] Energy Independence and Security Act of 2007 §1301 and §1305, 42 USC §17381 and §17385 (2007).
- [2] USDOE (2015) United States Electricity Industry Primer. (U.S. Department of Energy, Washington, D.C.), DOE/OE-0017.
- [3] Warwick W, Hardy T, Hoffman M, Homer J (2016) Electricity Distribution System Baseline Report. (Pacific Northwest National Laboratory, Richland, WA), PNNL-25178.
- [4] USEIA (2019) Monthly Energy Review April 2019. (U.S. Department of Energy, Washington, D.C.), DOE/EIA-0035(2019/4), April 25, 2019.
- [5] USDOE (2017) Quadrennial Energy Review. Transforming the Nation's Electricity System: The second installment of the QER. (U.S. Department of Energy, Washington, D.C.), DOE/EPSE-0008.
- [6] USDOE (2011) Report on the first Quadrennial Technology Review. (U.S. Department of Energy, Washington, D.C.), DOE/S-0001.
<https://doi.org/10.2172/1186659>
- [7] USEIA (2019) Annual Energy Outlook 2019 with projections to 2050. (U.S. Department of Energy, Washington, D.C.), DOE/EIA-AEO2019, January 24, 2019.
- [8] Perea A, Honeyman C, Mond A, Davis M, Colin S, Shiao M, Jones J, Moskowitz S, Gallagher B, Simon B (2018) US Solar Market Insight Q3 2018. (SEIA and GTM Research, Washington, DC).
- [9] Larsen J , Herndon W (2017) What Is It Worth? The State of the Art in Valuing Distributed Energy Resources. (Rhodium Group, New York, NY).
- [10] Bloom A, Helman U, Holttinen H, Summers K, Bakke J, Brinkman G, Lopez A (2017) It's Indisputable: Five Facts About Planning and Operating Modern Power Systems. *IEEE Power and Energy Magazine* 15(6):22-30.
<https://doi.org/10.1109/MPE.2017.2729079>
- [11] NASEM (2017) Enhancing the resilience of the nation's electricity system. (The National Academies Press, Washington, DC). <https://doi.org/10.17226/24836>
- [12] Barbose G , Darghouth N (2019) Tracking the Sun: Pricing and Design Trends for Distributed Photovoltaic Systems in the United States-2019 Edition. (Lawrence Berkeley National Laboratory, Berkeley, CA).
- [13] Bolinger M, Seel J, Robson D, Warner C (2020) Utility-Scale Solar Data Update: 2020 Edition. (Lawrence Berkeley National Laboratory, Berkeley, CA).
- [14] Wiser R, Bolinger M, Hoen B, Millstein D, Rand J, Barbose G, Darghouth N, Gorman W, Jeong S, Mills A, Paulos B (2020) Wind Energy Technology Data Update: 2020 Edition. (Lawrence Berkeley National Laboratory, Berkeley, CA).
- [15] IEA (2020) Renewables 2020: Analysis and forecast to 2025. (International Energy Agency, Paris, France).
- [16] AEEI, RMI, APP (2019) Case Study: Brooklyn Queens Demand Management Program — Employing Innovative Non-Wire Alternatives. (Advanced Energy Economy Institute, Washington, DC).

- [17] USEPA (2018) Quantifying the Multiple Benefits of Energy Efficiency and Renewable Energy: A Guide for State and Local Governments. (U.S. Environmental Protection Agency, Washington, DC).
- [18] USDOE (2012) Report on the first Quadrennial Technology Review: Technology Assessments. (U.S. Department of Energy, Washington, D.C.), DOE/S-0002.
- [19] Alstone P, Potter J, Piette M, Schwartz P, Berger M, Dunn L, Smith S, Sohn M, Aghajanzadeh A, Stensson S (2017) 2025 California Demand Response Potential Study, Final Report and Appendices on Phase 2 Results: Charting California's Demand Response Future. Lawrence Berkeley National Laboratory. Prepared for California Public Utilities Commission. April, 2017.
- [20] United States Energy Information Administration (2018) Form EIA-860 detailed data. ed Department of Energy (Washington, DC).
- [21] Gopstein AM (2012) Energy Storage & the Grid - From Characteristics to Impact [Point of View]. *Proceedings of the IEEE* 100(2):311-316.
<https://doi.org/10.1109/JPROC.2011.2174890>
- [22] International Energy Agency (2017) Digitalization & Energy. (IEA, Paris, France).
- [23] IEEE Standards Association (2010)– *ISO/IEC/IEEE International Standard - Systems and software engineering -- Vocabulary*, pp 1-418.
<https://doi.org/10.1109/IEEESTD.2010.5733835>
- [24] Greer C, Wollman DA, Prochaska DE, Boynton PA, Mazer JA, Nguyen CT, FitzPatrick GJ, Nelson TL, Koepke GH, Hefner Jr AR (2014) NIST framework and roadmap for smart grid interoperability standards, release 3.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1108r3.
<https://doi.org/10.6028/NIST.SP.1108r3>
- [25] (2018) *Smart Grid System Report, 2018 Report to Congress* (Washington, D.C.), (United States Department of Energy).
- [26] USDOE (2016) The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings. (U.S. Department of Energy), DOE/EE-1341. <https://doi.org/10.2172/1420233>
- [27] Electric Power Research Institute (2017) Point-To-Point Standards Integration Cost Framework. (Electric Power Research Institute, Palo Alto, CA), 3002009981, September 29, 2017.
- [28] Nguyen C , Gopstein AM (2020) Workshop on Smart Grid Interoperability Testing and Certification. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.TN.2085>
- [29] Peck JJ , Smith AD (2017) Quantification and regional comparison of water use for power generation: A California ISO case study. *Energy Reports* 3:22-28.
<https://doi.org/10.1016/j.egy.2016.11.002>
- [30] Elzinga D (2015) Electricity System Development: A Focus on Smart Grids. Overview of Activities and Players in Smart Grids. (United Nations Economic Commission for Europe, Geneva, Switzerland).
- [31] GWAC (2009) Financial Benefits of Interoperability: How Interoperability in the Electric Power Industry Will Benefit Stakeholders Financially. (GridWise Architecture Council), September 2009.

- [32] Schoenwald DA, Munoz K, McLendon WC, Russo TV (2011) The use of electric circuit simulation for power grid dynamics. *Proceedings of the 2011 American Control Conference*, pp 1151-1156. <https://doi.org/10.1109/ACC.2011.5991045>
- [33] USDOE (2015) Quadrennial Technology Review, Chapter 3: Enabling Modernization of the Electric Power System. (U.S. Department of Energy, Washington, D.C.), September 2015.
- [34] Coenen M, Marshall T, Sztur P, Al-Mutawaly N (2014) Impacts of modern residential loads on power grids. *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp 1-6. <https://doi.org/10.1109/CCECE.2014.6901085>
- [35] PJM (2017) Demand Response Strategy. (PJM Interconnection, Valley Forge, PA), June 28, 2017.
- [36] O’Fallon C , Gopstein AM (2021) Quantifying Operational Resilience Benefits of the Smart Grid. (National Institute of Standards and Technology, Gaithersburg, MD), NIST TN 2137. <https://doi.org/10.6028/NIST.TN.2137>
- [37] Bushnell J, Harvey SM, Hobbs BF, Oren SS (2013) Opinion on Initial Implementation of the Energy Imbalance Market and Related Market Design Changes. (California Independent System Operator, Sacramento, CA), October 28, 2013.
- [38] Holmberg DG, Burns MJ, Bushby ST, Gopstein AM (2019) NIST Transactive Energy Modeling and Simulation Challenge Phase II Final Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1900-603. <https://doi.org/10.6028/NIST.SP.1900-603>
- [39] USGCRP (2018) *Impacts, Risks, and Adaptation in the United States: Fourth National Climate Assessment, Volume II*. (U.S. Global Change Research Program, Washington, DC). <https://doi.org/10.7930/NCA4.2018>
- [40] Melosi MV (1987) Energy and Environment in the United States: The Era of Fossil Fuels. *Environmental History Review* 11(3):167-188. <https://doi.org/10.2307/3984086>
- [41] Shea D, Shields L, Hartman K (2020) *2019 Legislative Energy Trends*. (National Conference of State Legislatures, Denver, CO).
- [42] NASEM (2017) Valuing Climate Damages: Updating Estimation of the Social Cost of Carbon Dioxide. (The National Academies Press, Washington, DC). <https://doi.org/10.17226/24651>
- [43] USGCRP (2017) *Climate Science Special Report: Fourth National Climate Assessment, Volume I*. (U.S. Global Change Research Program, Washington, DC). <https://doi.org/10.7930/J0J964J6>
- [44] Lim A, Young LJ, Flatow I (2020) *How Native American Communities Are Addressing Climate Change* (Science Friday Initiative, New York, NY). Available at <https://www.sciencefriday.com/segments/native-american-communities-climate-change/>.
- [45] Stern T (2018) The Paris Agreement And Its Future. (Brookings, Washington, DC).
- [46] Biden JR (2021) *Paris Climate Agreement* (The White House, Washington, DC). Available at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/20/paris-climate-agreement/>.
- [47] WWF , et al. (2020) *We Are Still In: America Is All In* (World Wildlife Fund, Washington, DC). Available at <https://americaisallin.com>.

- [48] USCA (2020) 2020 Annual Report: Leading The Charge. (United States Climate Alliance, Washington, DC).
- [49] IPCC (2014) *Climate Change 2014: Synthesis Report. Contributions of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*. (Intergovernmental Panel on Climate Change, Geneva, Switzerland).
- [50] IRENA, IEA, REN21 (2018) Renewable Energy Policies in a Time of Transition. (IRENA, OECD/IEA and REN21, Abu Dhabi, UAE), ISBN 978-92-9260-061-7.
- [51] NCSL (2021) *State Renewable Portfolio Standards and Goals* (National Conference of State Legislatures, Washington, DC). Available at <https://www.ncsl.org/default.aspx?tabid=27705>.
- [52] Koonin SE , Gopstein AM (2011) Accelerating the Pace of Energy Change. *Issues in Science and Technology* 27(2):45-50.
- [53] IEA (2020) World Energy Outlook 2020. (International Energy Agency, Paris, France), ISBN 978-92-64-44923-7.
- [54] IEA (2020) World Energy Investment 2020. (International Energy Agency, Paris, France).
- [55] IEA (2020) Energy Technology Perspectives 2020. (International Energy Agency, Paris, France).
- [56] NREL (2012) *Renewable Electricity Futures Study*. (National Renewable Energy Laboratory, Golden, CO), NREL/TP-6A20-52409.
- [57] IRENA (2018) *Power System Flexibility for the Energy Transition, Part I: Overview for policy makers*. (International Renewable Energy Agency, Abu Dhabi, UAE), ISBN 978-92-9260-089-1.
- [58] Cheng VKM , Hammond GP (2017) Life-cycle energy densities and land-take requirements of various power generators: A UK perspective. *Journal of the Energy Institute* 90(2):201-213. <https://doi.org/10.1016/j.joei.2016.02.003>
- [59] Cole W, Frew B, Mai T, Sun Y, Bistline J, Blanford G, Young D, Marcy C, Namovicz C, Edelman R, Meroney B, Sims R, Stenhouse J, Donohoo-Vallett P (2017) Variable Renewable Energy in Long-Term Planning Models: A Multi-Modal Perspective. (National Renewable Energy Laboratory, Golden, CO), NREL/TP-6A20-70528.
- [60] Denholm P, Brinkman G, Mai T (2018) How low can you go? The importance of quantifying minimum generation levels for renewable integration. *Energy Policy* 115:249-257. <https://doi.org/10.1016/j.enpol.2018.01.023>
- [61] Hasan KN, Preece R, Milanović JV (2019) Existing approaches and trends in uncertainty modelling and probabilistic stability analysis of power systems with renewable generation. *Renewable and Sustainable Energy Reviews* 101:168-180. <https://doi.org/10.1016/j.rser.2018.10.027>
- [62] Cochran J, Denholm P, Speer B, Miller M (2015) Grid Integration and the Carrying Capacity of the U.S. Grid to Incorporate Variable Renewable Energy. (National Renewable Energy Laboratory, Golden, CO), NREL/TP-6A20-62607.
- [63] McDonald WJ , Hickok HN (1985) Energy Losses in Electrical Power Systems. *IEEE Transactions on Industry Applications* IA-21(3):803-819. <https://doi.org/10.1109/TIA.1985.349501>

- [64] Jackson R, Onar OC, Kirkham H, Fisher E, Burkes K, Starke M, Mohammed O, Weeks G (2015) Opportunities for Energy Efficiency Improvements in the U.S. Electricity Transmission and Distribution System. (Oak Ridge National Laboratory, Oak Ridge, TN), ORNL/TM-2015/5.
- [65] LLNL (2020) *U.S. Energy Flow Chart* (Lawrence Livermore National Laboratory, Albuquerque, NM). Available at https://flowcharts.llnl.gov/content/assets/images/energy/us/Energy_US_2019.png.
- [66] Lazar J , Baldwin X (2011) Valuing the Contribution of Energy Efficiency to Avoid Marginal Line Losses and Reserve Requirements. (Regulatory Assistance Project, Montpelier, VT).
- [67] NRC (2010) *Real Prospects for Energy Efficiency in the United States*. (The National Academies Press, Washington, DC). <https://doi.org/10.17226/12621>
- [68] USEPA (2018) *Centralized Generation of Electricity and its Impacts on the Environment* (U.S. Environmental Protection Agency, Washington, DC). Available at <https://www.epa.gov/energy/centralized-generation-electricity-and-its-impacts-environment>.
- [69] Aniti L (2018) *Major utilities continue to increase spending on U.S. electric distribution systems* (U.S. Energy Information Administration, Washington, DC). Available at <https://www.eia.gov/todayinenergy/detail.php?id=36675>.
- [70] Girouard C (2019) *BQDM program demonstrates benefits of non-traditional utility investments* (Utility Dive, Washington, DC). Available at <https://www.utilitydive.com/news/bqdm-program-demonstrates-benefits-of-non-traditional-utility-investments/550110/>.
- [71] Harrison GP, Maclean EJ, Karamanlis S, Ochoa LF (2010) Life cycle assessment of the transmission network in Great Britain. *Energy Policy* 38(7):3622-3631. <https://doi.org/10.1016/j.enpol.2010.02.039>
- [72] Dyson M , Mandel J (2015) The Economics of Demand Flexibility: How “flexiwatts” create quantifiable value for customers and the grid. (Rocky Mountain Institute, Boulder, CO).
- [73] Hledik R, Faruqui A, Lee T, Higham J (2019) The National Potential for Load Flexibility: Value and Market Potential Through 2030. (The Brattle Group, San Francisco, CA).
- [74] Arnold GW, Wollman DA, FitzPatrick GJ, Prochaska D, Holmberg DG, Su DH, Hefner Jr AR, Golmie NT, Brewer TL, Bello M (2010) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1108. <https://doi.org/10.6028/NIST.sp.1108>
- [75] Arnold GW, FitzPatrick GJ, Wollman DA, Nelson TL, et al. (2012) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1108R2. <https://doi.org/10.6028/NIST.sp.1108r2>
- [76] Taft J (2019) *Grid Architecture* (PNNL, Richland, WA). Available at <https://gridarchitecture.pnnl.gov>.
- [77] Thomas S (2018) Evolution of the Distribution System & the Potential for Distribution-level Markets: A Primer for State Utility Regulators. (NARUC, Washington, D.C.), January 2018.

- [78] Reilly G (2019) Brooklyn Queens Demand Management Program Implementation and Outreach Plan. (Consolidated Edison Company of New York, New York, NY), January 29, 2019.
- [79] PNNL (2019) *Grid Architecture Library* (Richland, WA). Available at <https://gridarchitecture.pnnl.gov/library.aspx>.
- [80] Griffor ER, Greer C, Wollman DA, Burns MJ (2017) Framework for Cyber-Physical Systems: Volume 1, Overview.
- [81] CAISO (2019) *Western Energy Imbalance Market* (California Independent System Operator, Sacramento, CA). Available at <https://www.westerneim.com/pages/default.aspx>.
- [82] FERC (2020) Participation of Distributed Energy Resource Aggregations in Markets Operated by Regional Transmission Organizations and Independent System Operators. (Federal Energy Regulatory Commission, Washington, DC), Docket No. RM18-9-000; Order No. 2222.
- [83] FERC (2020) *Fact Sheet - FERC Order No. 2222: A New Day for Distributed Energy Resources*. (Federal Energy Regulatory Commission, Washington, DC), Docket No. RM18-9-000.
- [84] Taft JD, De Martini P, Kristov L (2015) A reference model for distribution grid control in the 21st century. (Pacific Northwest National Laboratory, Richland, WA), PNNL-24463.
- [85] CPUC (2019) *Consumer FAQ on DR Providers (also known as Aggregators)* (California Public Utilities Commission, San Francisco, CA). Available at <https://www.cpuc.ca.gov/general.aspx?id=6306>.
- [86] Constable G , et al. (2003) *A Century of Innovation: Twenty Engineering Achievements that Transformed our Lives*. (Joseph Henry Press, Washington, DC). <https://doi.org/doi:10.17226/10726>
- [87] Engerati (2018) *Taking intelligence to the grid edge*. Available at <https://www.engerati.com/smart-infrastructure/article/intelligent-electronic-devices/taking-intelligence-grid-edge>.
- [88] Proudlove A, Lips B, Sarkisian D (2019) 50 States of Grid Modernization: Q1 2019 Quarterly Report. (North Carolina Clean Energy Technology Center, Raleigh, NC), May 2019.
- [89] Weiner E , Simpson J (2019) *Ontology* (Oxford University Press, Oxford, UK). Available at <https://en.oxforddictionaries.com/definition/ontology>.
- [90] IEEE SA (2008)– *IEEE 1588-2008: Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems* (IEEE Standards Association, Piscataway, NJ).
- [91] CEA (2013) *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*. (The White House, Washington, DC), August 2013.
- [92] Meier Av (2006) *Electric power systems : a conceptual introduction* (IEEE Press : Wiley-Interscience, Hoboken, N.J.), pp xv, 309 p.
- [93] Schewe PF (2007) *The grid: A journey through the heart of our electrified world*. (Joseph Henry Press, Washington, DC), 030910260X. <https://doi.org/10.17226/11735>
- [94] Public Utility Regulatory Policies Act of 1978, 16 USC § 2601 (1978).

- [95] O'Fallon C , Gopstein A (2019) Economics of Interoperability in the Context of Smart Grid Architectures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1900-604. <https://doi.org/10.6028/NIST.SP.1900-604>
- [96] ICF (2016) Standards and Interoperability in Electric Distribution Systems. (U.S. Department of Energy, Washington, DC).
- [97] Nguyen CT, Gopstein AM, Byrnett DS, Worthington K, Villarreal C (2020) Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report. (National Institute of Standards and Technology, Gaithersburg, MD), NISTIR 8284. <https://doi.org/10.6028/NIST.IR.8284>
- [98] Pendergrass JA (1986) *Letter to Mr. Stephen C. Yohay on electric utility industry concerns* (OSHA, US Department of Labor, Washington, DC). Available at <https://www.osha.gov/laws-regs/standardinterpretations/1986-10-03>.
- [99] USDOE (2016) Smart Grid Investment Grant Program Final Report. (U.S. Department of Energy, Washington, D.C.).
- [100] USDOE (2015) Quadrennial Technology Review Technology Assessments: Transmission and Distribution Components—TA 3.F. (U.S. Department of Energy, Washington, D.C.).
- [101] Tannenbaum M , Sisk E (2009) Plant Support Engineering: Proactive Obsolescence Management. (Electric Power Research Institute, Palo Alto, CA), December 8, 2009.
- [102] Brown RE , Willis HL (2006) The economics of aging infrastructure. *IEEE Power and Energy Magazine* 4(3):36-43. <https://doi.org/10.1109/MPAE.2006.1632452>
- [103] Song EY, Nguyen C, Gopstein A (2019) Review of Smart Grid Standards for Testing and Certification Landscape Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST TN 2042. <https://doi.org/10.6028/NIST.TN.2042>
- [104] Rad MS, Kazerooni M, Ghorbany MJ, Mokhtari H (2012) Analysis of the grid harmonics and their impacts on distribution transformers. *2012 IEEE Power and Energy Conference at Illinois*, pp 1-5. <https://doi.org/10.1109/PECI.2012.6184593>
- [105] NEMA (2019) *ANSI/NEMA MG 1-2016 – Motors and Generators* (National Electrical Manufacturers Association, Rosslyn, VA).
- [106] Doshi M , Zane R (2010) Control of Solid-State Lamps Using a Multiphase Pulsewidth Modulation Technique. *IEEE Transactions on Power Electronics* 25(7):1894-1904. <https://doi.org/10.1109/TPEL.2010.2043447>
- [107] Desai JV, Dadhich PK, Bhatt PK (2016) Investigations on Harmonics in Smart Distribution Grid with Solar PV Integration. *Technology and Economics of Smart Grids and Sustainable Energy* 1(1):11. <https://doi.org/10.1007/s40866-016-0010-5>
- [108] Meyer J, Blanco A, Rönnberg S, Bollen M, Smith J (2017) CIGRE C4/C6.29: survey of utilities experiences on power quality issues related to solar power. *CIGRE - Open Access Proceedings Journal* 2017(1):539-543. <https://doi.org/10.1049/oap-cired.2017.0456>
- [109] Smith J, Rönnberg S, Bollen M, Meyer J, Blanco A, Koo K, Mushamalirwa D (2017) Power quality aspects of solar power – results from CIGRE JWG C4/C6.29. *CIGRE - Open Access Proceedings Journal* 2017(1):809-813. <https://doi.org/10.1049/oap-cired.2017.0351>
- [110] Zou K, Agalgaonkar AP, Muttaqi KM, Perera S (2012) Distribution System Planning With Incorporating DG Reactive Capability and System Uncertainties. *IEEE*

- Transactions on Sustainable Energy* 3(1):112-123.
<https://doi.org/10.1109/TSTE.2011.2166281>
- [111] IEEE Standards Association (2003)– *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, pp 1-28.
<https://doi.org/10.1109/IEEESTD.2003.94285>
 - [112] Kim Y, Aravkin A, Fei H, Zondervan A, Wolf M (2016) Analytics for understanding customer behavior in the energy and utility industry. *IBM Journal of Research and Development* 60(1):11:11-11:13. <https://doi.org/10.1147/JRD.2015.2503988>
 - [113] USEIA (2020) *Monthly Energy Review Table 7.2b Electricity Net Generation: Electric Power Sector* (U.S. Department of Energy,, Washington, D.C.). Available at https://www.eia.gov/totalenergy/data/monthly/pdf/sec7_6.pdf.
 - [114] USEIA (2020) *Monthly Energy Review Table 10.6 Solar Electricity Net Generation* (U.S. Department of Energy,, Washington, D.C.). Available at https://www.eia.gov/totalenergy/data/monthly/pdf/sec10_10.pdf.
 - [115] Steiner R, Farrell M, Edwards S, Ford J, Sarwat S, Nelson T (2019) A NIST Testbed for Examining the Accuracy of Smart Meters under High Harmonic Waveform Loads. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8248. <https://doi.org/10.6028/NIST.IR.8248>
 - [116] Bhattacharyya S , Cobben S (2011) Consequences of Poor Power Quality—An Overview, *Power Quality*, Eberhard A, ed. (IntechOpen, London, UK).
<https://doi.org/10.5772/13787>
 - [117] Vagelis V, Stephen P, Ruby H, Richard EB (2017) DC Appliances and DC Power Distribution: A Bridge to the Future Net Zero Energy Home. *EEDAL '17*, ed Bertoldi P (European Commission Joint Research Center, Luxembourg), pp 316-327.
<https://doi.org/10.2760/264880>
 - [118] Marchionini B , Zheng S (2018) Direct Current in Buildings—A look at current and future trends. (National Electrical Manufacturers Association, Rosslyn, VA).
 - [119] Gohlke D , Zhou Y (2018) Impacts of Electrification of Light-Duty Vehicles in the United States, 2010 - 2017. (Argonne National Lab, Argonne, IL), ANL/ESD-18/1; 141595 <https://doi.org/10.2172/1418278>
 - [120] Rudman K (2018) *EEI Celebrates 1 Million Electric Vehicles on U.S. Roads* (Edison Electric Institute, Washington, D.C.). Available at
<https://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/EEI%20Celebrates%201%20Million%20Electric%20Vehicles%20on%20U-S-%20Roads.aspx>.
 - [121] Xcel Energy (2015) *Electric Vehicle Charging Station — Pilot Evaluation Report*. (Xcel Energy, Colorado), May 2015.
 - [122] Hawaiian Electric (2019) *Power facts* (Hawaii). Available at
https://www.hawaiianelectric.com/documents/about_us/company_facts/power_facts.pdf.
 - [123] HSEO (2019) *Hawaii Energy Facts & Figures* (Hawaii State Energy Office, Hawaii). Available at https://energy.hawaii.gov/wp-content/uploads/2019/07/2019-FF_Final.pdf.
 - [124] Bruckbauer B , Saggau D (2020) *Great River Energy 2019 Annual Report: Powering What's Possible*. (Maple Grove, MN), March 2020.

- [125] Great River Energy (2020) *Demand Response* (Great River Energy, Maple Grove, MN). Available at <https://greatriverenergy.com/smart-energy-use/demand-response/>.
- [126] Saggau D (2017) 2018-2032 Integrated Resource Plan. (Great River Energy, Maple Grove, MN), Docket No. ET2/RP-17-286, April 28, 2017.
- [127] DEA (2019) *Circuits for Dakota Electric Members: April 2019* (Dakota Electric Association, Farmington, MN). Available at https://www.dakotaelectric.com/wp-content/uploads/2019/08/Circ0419_FINAL_lores.pdf.
- [128] DEA (2020) *Energy Wise For Your Business: Interruptible Off-Peak Programs* (Dakota Electric Association, Farmington, MN). Available at <https://www.dakotaelectric.com/wp-content/uploads/2017/02/InterruptiblePrograms.pdf>.
- [129] Leferink F, Keyer C, Melentjev A (2016) Static energy meter errors caused by conducted electromagnetic interference. *IEEE Electromagnetic Compatibility Magazine* 5(4):49-55. <https://doi.org/10.1109/MEMC.2016.7866234>
- [130] Claburn T (2017) *Watt the f... Dim smart meters caught simply making up readings: Current-measuring circuits flawed, potentially over-charge homes, study finds* (The Register, London, UK). Available at https://www.theregister.co.uk/2017/03/06/smart_meters_prove_dim/.
- [131] Martindale J (2017) *Smart Meters may be dumber than you think, according to Dutch study* (Digital Trends, New York, NY). Available at <https://www.digitaltrends.com/home/smart-meter-exaggerate/>.
- [132] Patrick A (2017) *Some smart electricity meters 'give readings nearly 600 percent too high'* (Euronews, Lyon, France). Available at <https://www.euronews.com/2017/03/14/some-smart-electricity-meters-give-readings-nearly-600-percent-too-high>.
- [133] Heyes J (2017) *Smart Meters could be overbilling you by a whopping 582%* (Pacific Utility Audit, Inc., Markleeville, CA). Available at <https://pacificutilityaudit.com/smart-meters-overbilling-whopping-582/>.
- [134] Wolpin A (2018) *Meter accuracy is question to answer* (The Leader, Port Townsend, WA). Available at <https://www.ptleader.com/stories/meter-accuracy-is-question-to-answer,5674>.
- [135] ANSI (2017) *ANSI C12.20-2015 – American National Standard for Electricity Meters—0.1, 0.2, and 0.5 Accuracy Classes* (National Electrical Manufacturers Association, Rosslyn, VA).
- [136] Allnutt J, Anand D, Arnold D, Goldstein A, Li-Baboud Y-S, Martin A, Nguyen C, Noseworthy R, Subramaniam R, Weiss M (2017) Timing Challenges in the Smart Grid. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1500-08. <https://doi.org/10.6028/NIST.SP.1500-08>
- [137] Pierre BJ, Wilches-Bernal F, Schoenwald DA, Elliott RT, Neely JC, Byrne RH, Trudnowski DJ (2017) Open-loop testing results for the pacific DC intertie wide area damping controller. *2017 IEEE Manchester PowerTech*, pp 1-6. <https://doi.org/10.1109/PTC.2017.7980834>
- [138] Wilches-Bernal F, Pierre BJ, Elliott RT, Schoenwald DA, Byrne RH, Neely JC, Trudnowski DJ (2017) Time delay definitions and characterization in the pacific DC intertie wide area damping controller. *2017 IEEE Power & Energy Society General Meeting*, pp 1-5. <https://doi.org/10.1109/PESGM.2017.8274082>

- [139] Wilches-Bernal F, Schoenwald DA, Fan R, Elizondo M, Kirkham H (2018) Analysis of the Effect of Communication Latencies on HVDC-Based Damping Control. *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, pp 1-9. <https://doi.org/10.1109/TDC.2018.8440146>
- [140] NIST (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-53R5. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [141] Mansur E , White M (2012) *Market Organization and Market Efficiency in Electricity Markets*. Available at http://www.dartmouth.edu/~mansur/papers/mansur_white_pjmaep.pdf.
- [142] Tainter J, Allen T, Hoekstra TW (2006) Energy transformations and post-normal science. *Energy* 31:44-58. <https://doi.org/10.1016/j.energy.2004.06.002>
- [143] Kwoka J, John E (2002) Governance alternatives and pricing in the US electric power industry. *Journal of Law, Economics, and Organization* 18(1):278-294.
- [144] Saundry PD (2019) Review of the United States energy system in transition. *Energy, Sustainability and Society* 9(1):4. <https://doi.org/10.1186/s13705-018-0178-8>
- [145] Pérez-Arriaga I , Knittle C (2016) *Utility of the future: An MIT energy initiative response to an industry in transition* (Massachusetts Institute of Technology, Boston, MA). Available at <http://energy.mit.edu/research/utility-future-study/>.
- [146] Zummo P, Beauchamp M, Brown A, Faruqi A, Lazar J, Chen G (2019) *Leadership in Rate Design—A Compendium of Rates Essays* (American Public Power Association, Arlington, VA). Available at <https://www.publicpower.org/system/files/documents/Leadership-in-Rate-Design.pdf>.
- [147] Martini PD , Kristov L (2015) Distribution Systems in a High Distributed Energy Resources Future. (Lawrence Berkeley National Laboratory, Berkeley, CA), LBNL-10039797, Vol. FEUR Report No. 2.
- [148] Chew B, Myers EH, Adolf T, Thomas E (2018) *Non-Wires Alternatives: Case Studies From Leading U.S. Projects* (E4 The Future, PLMA, Smart Electric Power Alliance, Washington, DC). Available at https://e4thefuture.org/wp-content/uploads/2018/11/2018-Non-Wires-Alternatives-Report_FINAL.pdf.
- [149] Varian HR (2010) Computer Mediated Transactions. *American Economic Review* 100(2):1-10. <https://doi.org/10.1257/aer.100.2.1>
- [150] Varian HR (2003) *Economics of information technology* (University of California, Berkeley, CA). Available at <https://econ.ucsb.edu/~tedb/Courses/Ec100C/varianinfo.pdf>.
- [151] Andriole SJ (2018) Implement First, Ask Questions Later (or Not at All). *MIT Sloan Management Review* 59(3):1-5.
- [152] Courtney H, Kirkland J, Viguerie P (1997) Strategy under uncertainty. *Harvard business review* 75(6):67-79.
- [153] IEA (2019) World Energy Investment 2019. (IEA, Paris).
- [154] UtilityAPI (2020) *Green Button OAuth* (Oakland, CA). Available at <https://utilityapi.com/docs/greenbutton/oauth>.
- [155] Fort Collins Utilities (2020) *Company Directory* (Fort Collins, CO). Available at <https://data.fcgov.utilityapi.com/directory>.
- [156] Silicon Valley Clean Energy (2020) *Data Hive Directory* (Sunnyvale, CA). Available at <https://data.svcleanenergy.org/directory>.

- [157] PG&E (2020) *2019 Energy Efficiency Annual Report* (California Public Utilities Commission, San Francisco, CA). Available at <https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M337/K862/337862483.PDF>.
- [158] CEDARS (2021) *Details for PGE210010: Pay for Performance Pilot* (California Public Utilities Commission, San Francisco, CA). Available at <https://cedars.sound-data.com/programs/PGE210010/details/2020/>.
- [159] Cragg BT (2019) Complaint of OhmConnect Against Southern California Edison Company for Data Failures. (Docket C1903005, California PUC, San Francisco, CA), pp 4,14.
- [160] Logical Buildings (2020) *What we do* (Livingston, NJ). Available at <https://logicalbuildings.com/what-we-do/#grid>.
- [161] Sustainable Westchester (2020) *GridRewards Pilot Program* (Westchester, NY). Available at https://sustainablewestchester.org/wp-content/uploads/2020/05/GridRewardsFINAL_02_01.pdf.
- [162] Anderson RJ (2008) *Security engineering: A Guide to Building Dependable Distributed Systems* (John Wiley & Sons, Hoboken, NJ).
- [163] Foster B, Burns D, Kathan D, Lee MP, Pierovi S (2018) *2018 Assessment of Demand Response and Advanced Metering: Staff Report* (Federal Energy Regulatory Commission, Washington, D.C.). Available at <https://www.ferc.gov/legal/staff-reports/2018/DR-AM-Report2018.pdf>.
- [164] Anderson R , Fuloria S (2009) Certification and evaluation: A security economics perspective. *2009 IEEE Conference on Emerging Technologies & Factory Automation*, (IEEE), pp 1-7.
- [165] Hill CW (1990) Cooperation, opportunism, and the invisible hand: Implications for transaction cost theory. *Academy of management review* 15(3):500-513.
- [166] Lytton TD (2014) Competitive third-party regulation: How private certification can overcome constraints that frustrate government regulation. *Theoretical Inquiries in Law* 15(2):539-572.
- [167] WEF (2015) *Shared Responsibility: A New Paradigm for Supply Chains* (World Economic Forum, Geneva, Switzerland). Available at http://www3.weforum.org/docs/WEF_GAC_Supply_Chains_%20A_New_Paradigm_2015.pdf.
- [168] Arrow KJ (1969) The organization of economic activity: issues pertinent to the choice of market versus nonmarket allocation. *The analysis and evaluation of public expenditure: the PPB system* 1:59-73.
- [169] ComEd Media Relations (2020) *ComEd Customers Experience Best-Ever Reliability in 2019: Smart grid and system improvements help prevent more than 13 million outages since 2012* (businesswire, New York). Available at <https://www.businesswire.com/news/home/20200128005706/en/>.
- [170] Wolak FA, Nordhaus R, Shapiro C (2000) An Analysis of the June 2000 Price Spikes in the California ISO's Energy and Ancillary Services Markets. (California Independent System Operator, Sacramento, CA), Vol. 2021.
- [171] Muir A , Lopatto J (2004) *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, U.S.-Canada Power System Outage Task Force (U.S. Department of Energy, Washington, DC). Available at

- <https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>.
- [172] Barrett MP (2018) Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>
 - [173] Hayden M, Hébert C, Tierney S (2014) *Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat* (Bipartisan Policy Center, Washington, DC). Available at <https://bipartisanpolicy.org/wp-content/uploads/2019/03/Cybersecurity-Electric-Grid-BPC.pdf>.
 - [174] Knake RK (2017) A Cyberattack on the U.S. Power Grid. (Council on Foreign Relations, New York, NY).
 - [175] NIST (2018) *Cybersecurity Framework V1.1 Core (Excel)* (National Institute of Standards and Technology, Gaithersburg, MD). Available at <https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx>.
 - [176] Marron J, Gopstein A, Bartol N, Feldman V (2019) Cybersecurity Framework Smart Grid Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST TN 2051. <https://doi.org/10.6028/NIST.TN.2051>
 - [177] Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene K, Theofanos MF (2017) Digital Identity Guidelines: Enrollment and Identity Proofing Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-63A. <https://doi.org/10.6028/NIST.SP.800-63a>
 - [178] Pillitteri VY , Brewer TL (2014) Guidelines for Smart Grid Cybersecurity. (National Institute of Standards and Technology, Gaithersburg, MD), NISTIR 7628r1. <https://doi.org/10.6028/NIST.IR.7628r1>
 - [179] FERC (2020) *Cybersecurity Incentives Policy White Paper* (Docket No. AD20-19-000, Federal Energy Regulatory Commission, Washington, DC). Available at <https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf>.
 - [180] Nevius D (2020) *The History of the North American Electric Reliability Corporation* (North American Electric Reliability Corporation, Atlanta, GA). Available at <https://www.nerc.com/AboutNERC/Resource%20Documents/NERCHistoryBook.pdf>
 - [181] NERC (2020) *CIP Standards* (North American Electric Reliability Corporation, Atlanta, GA). Available at <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>.
 - [182] Rusco F , Marinos N (2019) Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid. (United States Government Accountability Office, Washington, DC), GAO-19-332.
 - [183] USDOE (2011) Roadmap to Achieve Energy Delivery Systems Cybersecurity. (U.S. Department of Energy, Washington, DC).
 - [184] Lee A (2015) Electric Sector Failure Scenarios and Impact Analyses - Version 3.0. (Electric Power Research Institute, Palo Alto, CA).
 - [185] NERC (2021) *One-Stop Shop (Compliance Monitoring & Enforcement Program)* (North American Electric Reliability Corporation, Atlanta, GA). Available at <https://www.nerc.com/pa/comp/Pages/CAOneStopShop.aspx>.
 - [186] NEMA (2016) *SG-IPRM 1-2016 – Smart Grid Interoperability Process Reference Manual* (National Electrical Manufacturers Association, Rosslyn, VA).
 - [187] Illinois Statute, 220 ILCS 5/16-108.6

- [188] California Code, PUC § 8360
- [189] Ahmadi M (2011) The Need for Security Testing and Conformance Standards in the Smart Grid. *Grid-Interop Forum*, (GridWise Architecture Council, Phoenix, AZ).
- [190] CPUC Energy Division (2012)– *Resolution E-4527* (California Public Utilities Commission, San Francisco, CA).
- [191] ISO (multiple) *35.100 – Open Systems Interconnection (OSI)* (International Organization for Standardization, Geneva, Switzerland).
- [192] Nguyen C, Heirman D, Bienert R, Tolios K, Masri K, Cain B, Marchionini B (2017) *Interoperability Process Reference Manual—User’s Guide*. (Smart Electric Power Alliance, Washington, DC), November 2017.
- [193] GWAC (2011) *Smart Grid Interoperability Maturity Model Summary* (GridWise Architecture Council, Richland, WA). Available at <https://www.gridwiseac.org/about/imm.aspx>.
- [194] SAE (2017) *SAE J1772-2017 – SAE Electric Vehicle and Plug in Hybrid Electric Vehicle Conductive Charge Coupler* (SAE International, Warrendale, PA).
- [195] IEEE SA (2012) *IEEE 1815-2012 – IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)* (IEEE Standards Association, Piscataway, NJ).
- [196] IEC (2013) *IEC TR 61850-1:2013 – Communication networks and systems for power utility automation - Part 1: Introduction and overview* (IEC, Geneva).
- [197] IEEE Standards Association (2016) *IEEE 1815.1-2015 – IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815 [Distributed Network Protocol (DNP3)]* (IEEE SA, Piscataway, NJ).
- [198] Falk H (2018) 2017 IEC 61850 IOP Final Report. (UCA International Users Group, Shell Knob, MO).
- [199] NIST (2018) *NIST Smart Grid Advisory Committee (SGAC) Minutes of April 24-25, 2018, Meeting* (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/sites/default/files/documents/2018/06/08/nist-sgac-april-2018-meeting_minutes-final.pdf.
- [200] ANSI (2014) *ANSI C12 – Smart Grid Meter Package* (National Electrical Manufacturers Association, Rosslyn, VA).
- [201] Noseworthy B (2019) 1588 Power Profile Conformance Test Suite Specification, Version 1.22. (UNH-IOL, Durham, NH), March 25, 2019.
- [202] Anand D, Brady KG, Song Y, Nguyen CT, Lee KB, FitzPatrick GJ, Goldstein AR, Li-Baboud Y (2019) *NIST Smart Grid Interoperability Test Tools*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1900-801. <https://doi.org/10.6028/NIST.SP.1900-801>
- [203] SEPA (2019) *Catalog of Standards* (Smart Electric Power Alliance, Washington, DC). Available at <https://sepapower.org/knowledge/catalog-of-standards/>.
- [204] Chung D (2020) *Catalog of Test Programs* (Smart Electric Power Alliance, Washington, DC). Available at <https://sepapower.org/knowledge/catalog-of-test-programs/>.
- [205] Newlander J (2019) Working Group Three Final Report, Rulemaking 17-07-007. (California Public Utilities Commission, San Francisco, CA).
- [206] IEEE SA (2018) *IEEE 1547-2018 – IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power*

- Systems Interfaces* (IEEE Standards Association, Piscataway, NJ).
<https://doi.org/10.1109/IEEESTD.2018.8332112>
- [207] UL (2016) *UL Launches Advanced Inverter Testing and Certification Program* (Underwriters Laboratories, Northbrook, IL). Available at <https://www.ul.com/news/ul-launches-advanced-inverter-testing-and-certification-program>.
 - [208] ISO-NE (2018) *Inverter Source Requirement Document of ISO New England* (ISO New England, Holyoke, MA). Available at https://www9.nationalgridus.com/non_html/ISO%20New%20England%20Source%20Requirement%20Document-2018-02-06.pdf.
 - [209] IEC (2015) *IEC 62559-2:2015 – Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list* (IEC, Geneva, Switzerland).
 - [210] USEIA (2013) *Today in Energy: Apartments in buildings with 5 or more units use less energy than other home types* (U.S. Department of Energy, Washington, DC). Available at <https://www.eia.gov/todayinenergy/detail.php?id=11731>.
 - [211] Stigler GJ , Sherwin RA (1985) The Extent of the Market. *The Journal of Law & Economics* 28(3):555-585.
 - [212] Hledik R, Lueken R, McIntyre C, Bishop H (2017) *Stacked Benefits: Comprehensively Valuing Battery Storage in California* (The Brattle Group, San Francisco, CA). Available at http://files.brattle.com/files/7208_stacked_benefits_final_report.pdf.
 - [213] Colvin M, Fellman DI, Rodriguez RL, LaBonte A (2018) California Customer Choice: An Evaluation of Regulatory Framework Options for an Evolving Electricity Market. Draft Green Book. (California Public Utilities Commission, San Francisco, CA).
 - [214] USDOE (2016) *6 Charts that Will Make You Optimistic About America's Clean Energy Future* (U.S. Department of Energy, Washington, DC). Available at <https://www.energy.gov/articles/6-charts-will-make-you-optimistic-about-america-s-clean-energy-future>.
 - [215] PJM (2016) 2019/2020 RPM Base Residual Auction Results. (PJM Interconnection, Valley Forge, PA), PJM #5154776, May 24, 2016.
 - [216] Chew B, Feldman B, Esch N, Lynch M (2017) 2017 Utility Demand Reponse Market Snapshot. (Smart Electric Power Alliance, Washington, DC), October 2017.
 - [217] RGGI (2019) *The Regional Greenhouse Gas Initiative: an initiative of Eastern States in the U.S.* (Regional Greenhouse Gas Initiative, New York, NY). Available at <https://www.rggi.org/program-overview-and-design/elements>.
 - [218] DSIRE (2019) *Database of State Incentives for Renewables & Efficiency* (North Carolina Clean Energy Technology Center, Raleigh, NC). Available at <http://www.dsireusa.org>.
 - [219] CPUC (2015) Order Instituting Rulemaking to consider policy and implementation refinements to the Energy Storage Procurement Framework and Design Program and related Action Plan of the California Energy Storage Roadmap. in *R15-03-011* (California Public Utilities Commission, San Francisco, CA).
 - [220] FERC (2018) Electric Storage Participation in Markets Operated by Regional Transmission Organizations and Independent System Operators: FERC Order No. 841. (Federal Energy Regulatory Commission, Washington, D.C.).

- [221] FERC (2018) Reform of Generator Interconnection Procedures and Agreements: FERC Order No. 845. (Federal Energy Regulatory Commission, Washington, D.C.).
- [222] FERC (2011) Transmission Planning and Cost Allocation by Transmission Owning and Operating Public Utilities: FERC Order No. 1000. (Federal Energy Regulatory Commission, Washington, D.C.).
- [223] Ramdas A, McCabe K, Das P, Sigrin BO (2019) California Time-of-Use (TOU) Transition: Effects on Distributed Wind and Solar Economic Potential. (National Renewable Energy Laboratory, Golden, CO), NREL/TP-6A20-73147.
<https://doi.org/doi.org/10.2172/1508511>
- [224] Trabish HK (2018) *California utilities prep nation's biggest time-of-use rate rollout* (Utility Dive, Washington, D.C.). Available at
<https://www.utilitydive.com/news/california-utilities-prep-nations-biggest-time-of-use-rate-roll-out/543402/>.
- [225] Oosterkamp Pvd, Koutstaal P, Welle Avd, Joode Jd, Lenstra J, Hussen Kv, Haffner R (2014) *The role of DSOs in a Smart Grid environment* (Energy research Center of the Netherlands, Amsterdam, Netherlands). Available at
https://ec.europa.eu/energy/sites/ener/files/documents/20140423_dso_smartgrid.pdf.
- [226] GWAC (2015) *Gridwise Transactive Energy Framework Version 1.0* (GridWise Architecture Council, Richland, WA). Available at
https://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf.
- [227] Lorenz G, Tielemans S, Granstrom P-O, Chapalain F (2013) DSO Priorities for Smart Grid Standardisation. (EURELECTRIC / EDSO Joint Task Force Smart Grid Standardisation, Brussels, Belgium).
- [228] (2020) *Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0* (Federal Register, Washington, D.C.), 85 FR 58338.