Smart Grid Interoperability and Cybersecurity Workshop

NIST Smart Grid Program

November 13-14, 2018

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

Welcome & Workshop Objectives – Chris Greer

Note: If you want to order lunch for delivery to NCCoE and have not yet done so, please see Konstantina in the registration now.

Tuesday, November 13, 2018

9:30 am	**REGISTRATION**
10:00 am	**WELCOME AND WORKSHOP OBJECTIVES** **Chris Greer**, NIST
10:15 am	**KEYNOTE: GRID MODERNIZATION AND THE CASE FOR INTEROPERABILITY** **John Gibson**, Avista Utilities
11:00 am	**PANEL SESSION: GRID MODERNIZATION AND INTEROPERABILITY** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman**, NIST
12:00 pm	**LUNCH**
1:15 pm	**KEYNOTE: THE ECONOMICS OF INTEROPERABILITY** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**PLENARY: INTRODUCTION TO NIST'S SMART GRID CONCEPTUAL MODELS** **Avi Gopstein**, NIST
2:30 pm	**INTERACTIVE DISCUSSION: MAJOR CONCERNS FOR SMART GRID INTEROPERABILITY** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**BREAK**
3:45 pm	**PLENARY: THREE KEY THEMES FOR CYBERSECURITY AND GRID INTEROPERABILITY** • **Risk Profiles—Jeffrey Marron**, NIST • **Interface Categories—Nelson Hastings**, NIST • **Securing Communications—Michael Bartock**, NIST
4:45 pm	**WRAP UP AND CHARGE FOR NEXT DAY**
5:00 pm	**ADJOURN**

Smart Grid Interoperability and Cybersecurity Workshop

Chris Greer
Director, Smart Grid and Cyber-Physical Systems Office
National Institute of Standards and Technology
U.S. Department of Commerce

November 13-14, 2018

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

Measurements are critical…

to commerce

"Uniformity in the currency, weights, and measures of the United States is an object of great importance, and will, I am persuaded, be duly attended to."

George Washington, State of the Union Address, 1790

to innovation

If you know how to measure something, you can design it, compare it, understand it, and improve it

NIST Illustrated, https://youtu.be/2j9BGVKbzS4

and to international trade

- Up to 92% of U.S. exports affected by standards/technical regulations

NIST measurement science provides the foundation for innovation in every industry and economic sector, from manufacturing to health care to defense

NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

Measurement Science – Creating the experimental and theoretical tools – methods, metrics, instruments, and data – that enable innovation

Standards – Disseminating physical standards, providing technical expertise to documentary standards that enable interoperability and commerce

Technology – Driving innovation through knowledge dissemination and public-private partnerships to bridge gap between discovery /marketplace

NIST Laboratory Programs

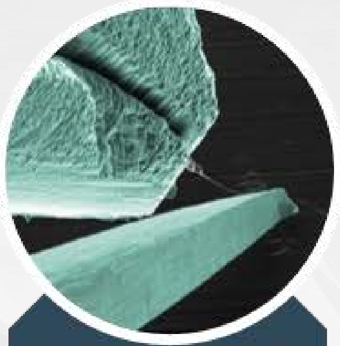
Material Measurement Laboratory

Physical Measurement Laboratory

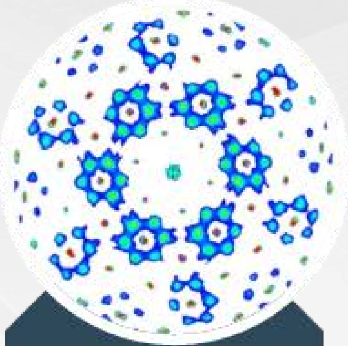
Engineering Laboratory

Information Technology Laboratory

Communication Technology Laboratory



Center for Nanoscale Science and Technology



NIST Center for Neutron Research

Metrology Laboratories

Driving innovation through Measurement Science and Standards

Technology Laboratories

Accelerating the adoption and deployment of advanced technology solutions

National User Facilities

Providing world class, unique, and cutting-edge research facilities

Energy Independence and Security Act

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

Interoperability Frameworks to date

NIST Special Publication 1108

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

Office of the National Coordinator for Smart Grid Interoperability

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

2010

NIST Special Publication 1108R2

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

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

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

2012

This publication is available free of charge from http://dx.doi.org/10.6028/NIST.SP.1108r3

NIST Special Publication 1108r3

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

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

in collaboration with
Quantum Measurement Division,
Semiconductor and Dimensional Metrology Division,
and Electromagnetics Division,
Physical Measurement Laboratory
and
Advanced Network Technologies Division
and Computer Security Division,
Information Technology Laboratory

http://dx.doi.org/10.6028/NIST.SP.1108r3

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

2014

A break for context…

Figure 4.4 Unit costs of key emerging electricity technologies

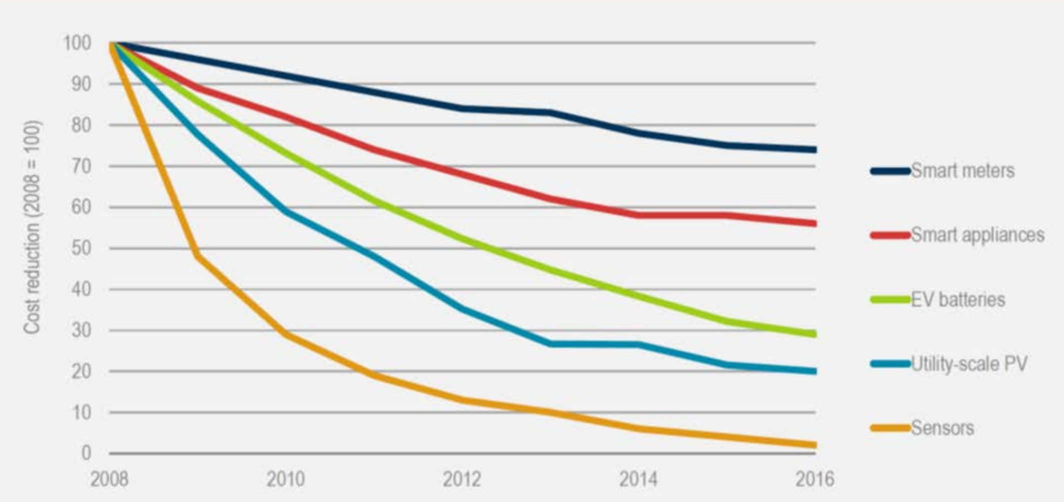


Figure 2.5 Household electricity consumption of appliances and other small plug loads

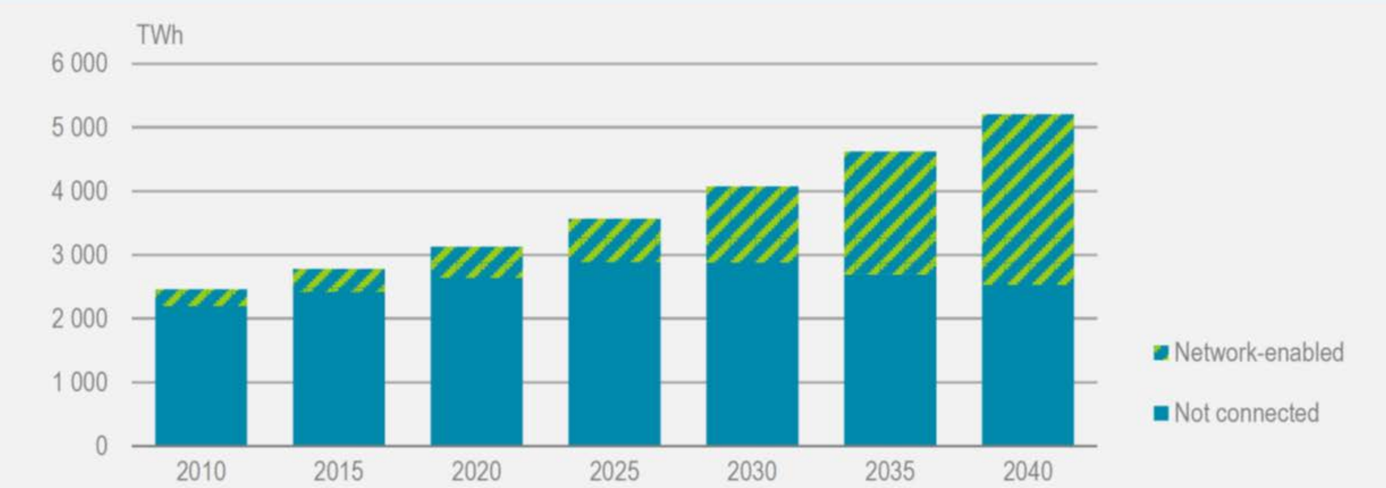


Figure 1.1 Global internet traffic

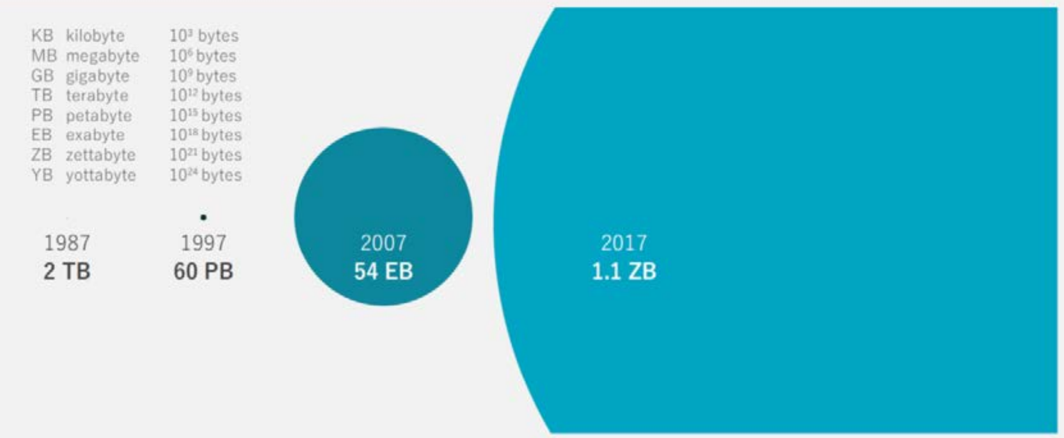
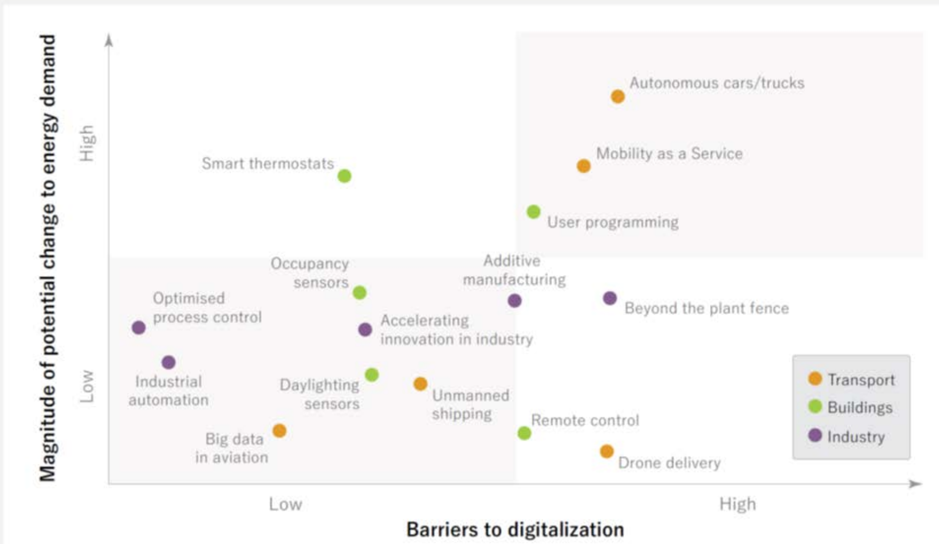


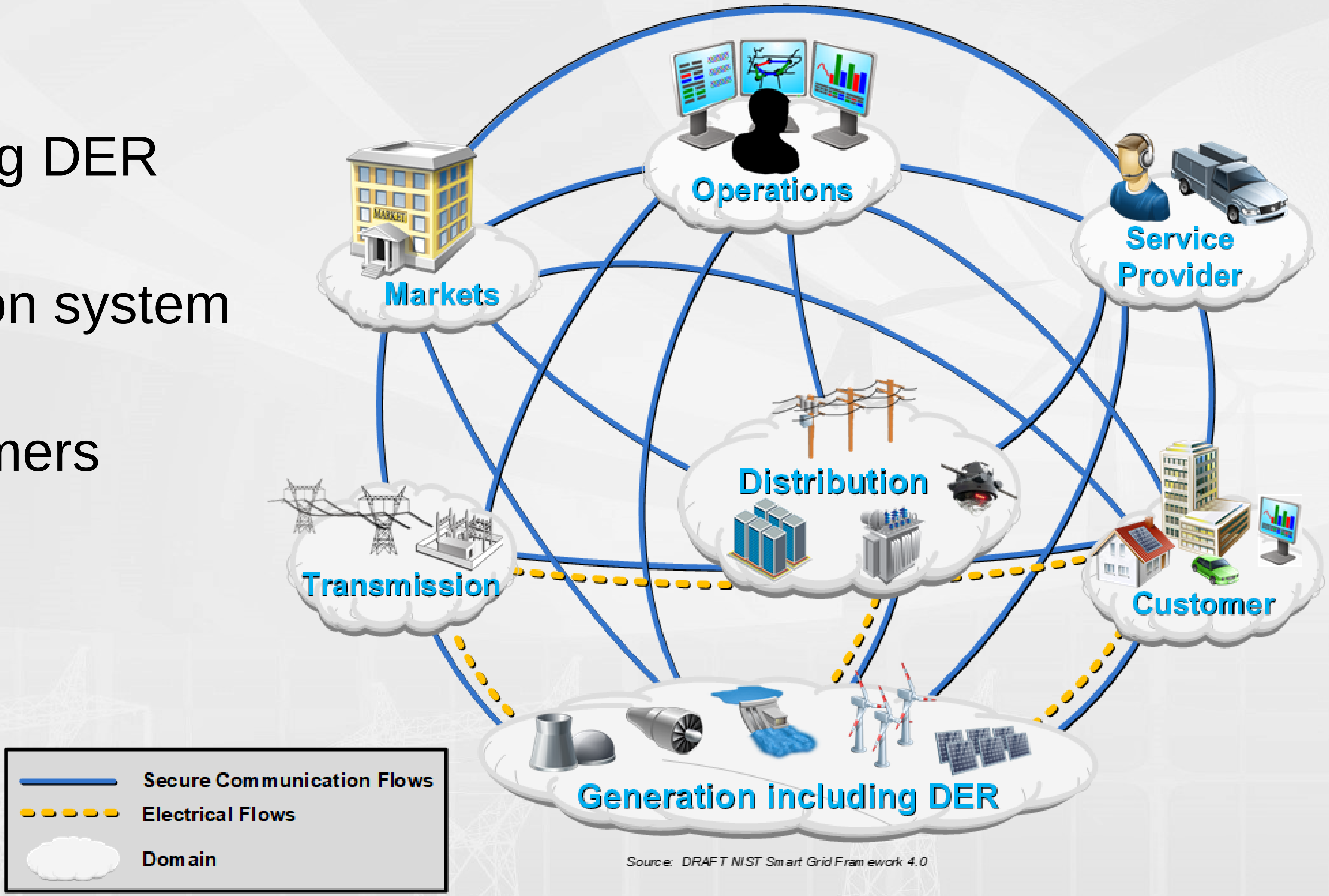
Figure 2.1 Digitalization's potential impact on transport, buildings, and industry



Source (all): IEA 2017, Digitalization & Energy

Smart Grid Conceptual Model (2018, Draft)

- Generation including DER
- Intelligent distribution system
- Empowered consumers
- Emerging Markets



Source: DRAFT NIST Smart Grid Framework 4.0

Workshop Agenda & Purpose

Tuesday, November 13, 2018	
9:30 am	**Registration**
10:00 am	**Welcome and Workshop Objectives** **Chris Greer**, NIST
10:15 am	**Keynote: Grid Modernization and the Case for Interoperability** **John Gibson**, Avista Utilities
11:00 am	**Panel Session: Grid Modernization and Interoperability** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**Lunch**
1:15 pm	**Keynote: The Economics of Interoperability** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**Plenary: Introduction to NIST's Smart Grid Conceptual Models** **Avi Gopstein,** NIST
2:30 pm	**Interactive Discussion: Major Concerns for Smart Grid Interoperability** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**Break**
3:45 pm	**Plenary: Three Key Themes for Cybersecurity and Grid Interoperability** • **Risk Profiles—Jeffrey Marron,** NIST • **Interface Categories—Nelson Hastings,** NIST • **Securing Communications—Michael Bartock,** NIST
4:45 pm	**Wrap Up and Charge for Next Day**
5:00 pm	**Adjourn**

Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Grid Mod. & the Case for Interoperability – John Gibson

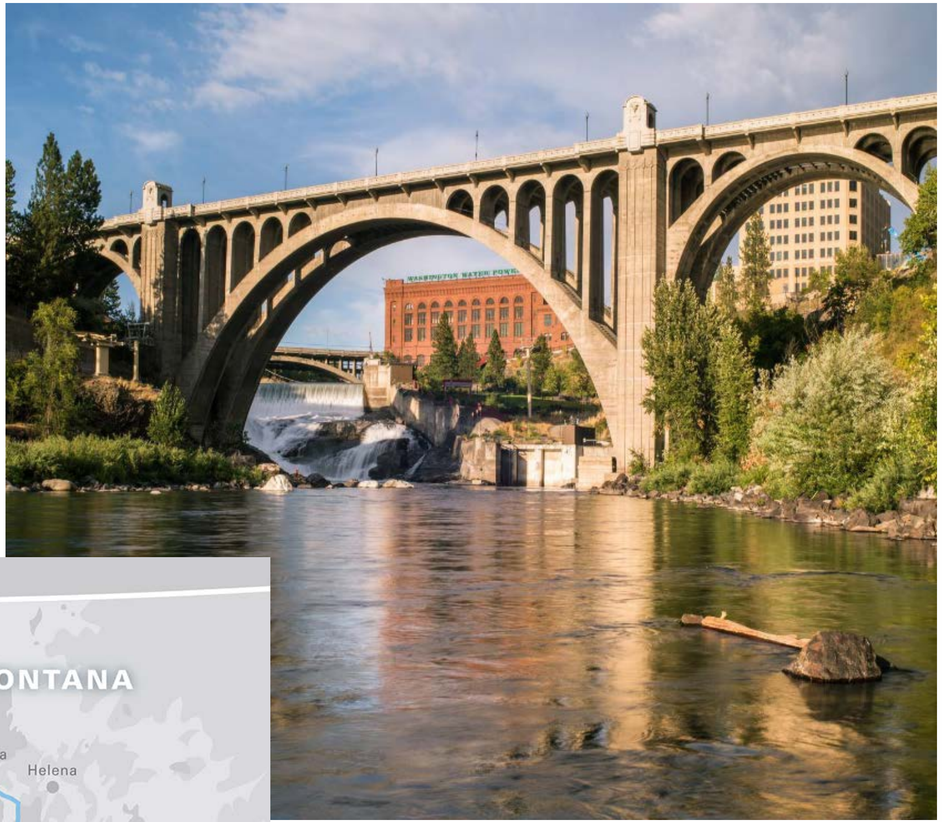
Tuesday, November 13, 2018	
9:30 am	**Registration**
10:00 am	**Welcome and Workshop Objectives** **Chris Greer**, NIST
10:15 am	**Keynote: Grid Modernization and the Case for Interoperability** **John Gibson**, Avista Utilities
11:00 am	**Panel Session: Grid Modernization and Interoperability** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman**, NIST
12:00 pm	**Lunch**
1:15 pm	**Keynote: The Economics of Interoperability** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**Plenary: Introduction to NIST's Smart Grid Conceptual Models** **Avi Gopstein**, NIST
2:30 pm	**Interactive Discussion: Major Concerns for Smart Grid Interoperability** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**Break**
3:45 pm	**Plenary: Three Key Themes for Cybersecurity and Grid Interoperability** • **Risk Profiles—Jeffrey Marron**, NIST • **Interface Categories—Nelson Hastings**, NIST • **Securing Communications—Michael Bartock**, NIST
4:45 pm	**Wrap Up and Charge for Next Day**
5:00 pm	**Adjourn**

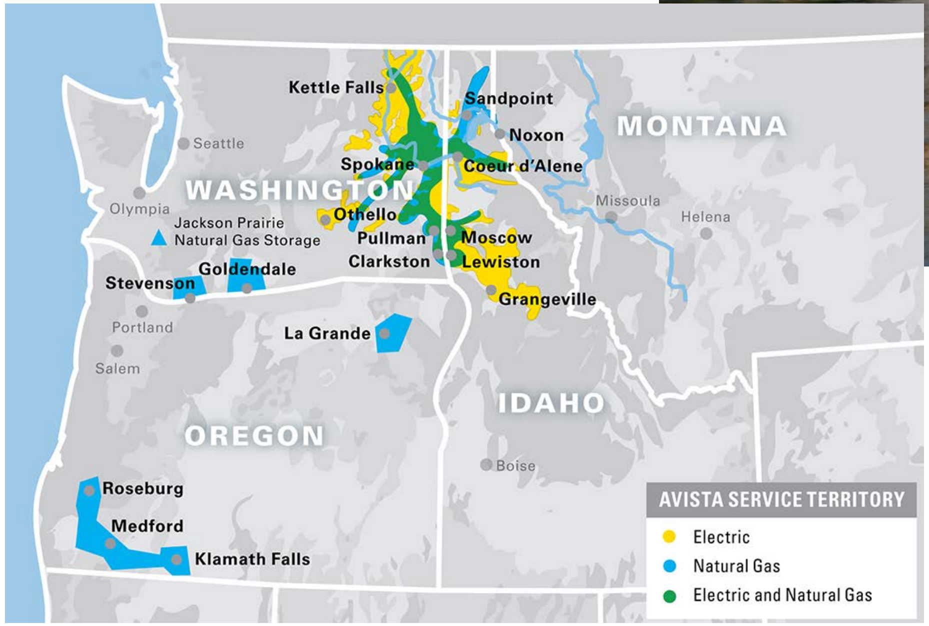
Innovation for Future Utility Business Model

John Z Gibson, P.E.
Avista Utilities Chief R&D Engineer
November 2018

About Avista

- Incorporated in 1889
- Investor-Owned Utility with headquarters in Spokane, Washington
- Over 1,700 employees
- Electric and natural gas service
  - 379,000 electric customers
  - 342,000 natural gas customers

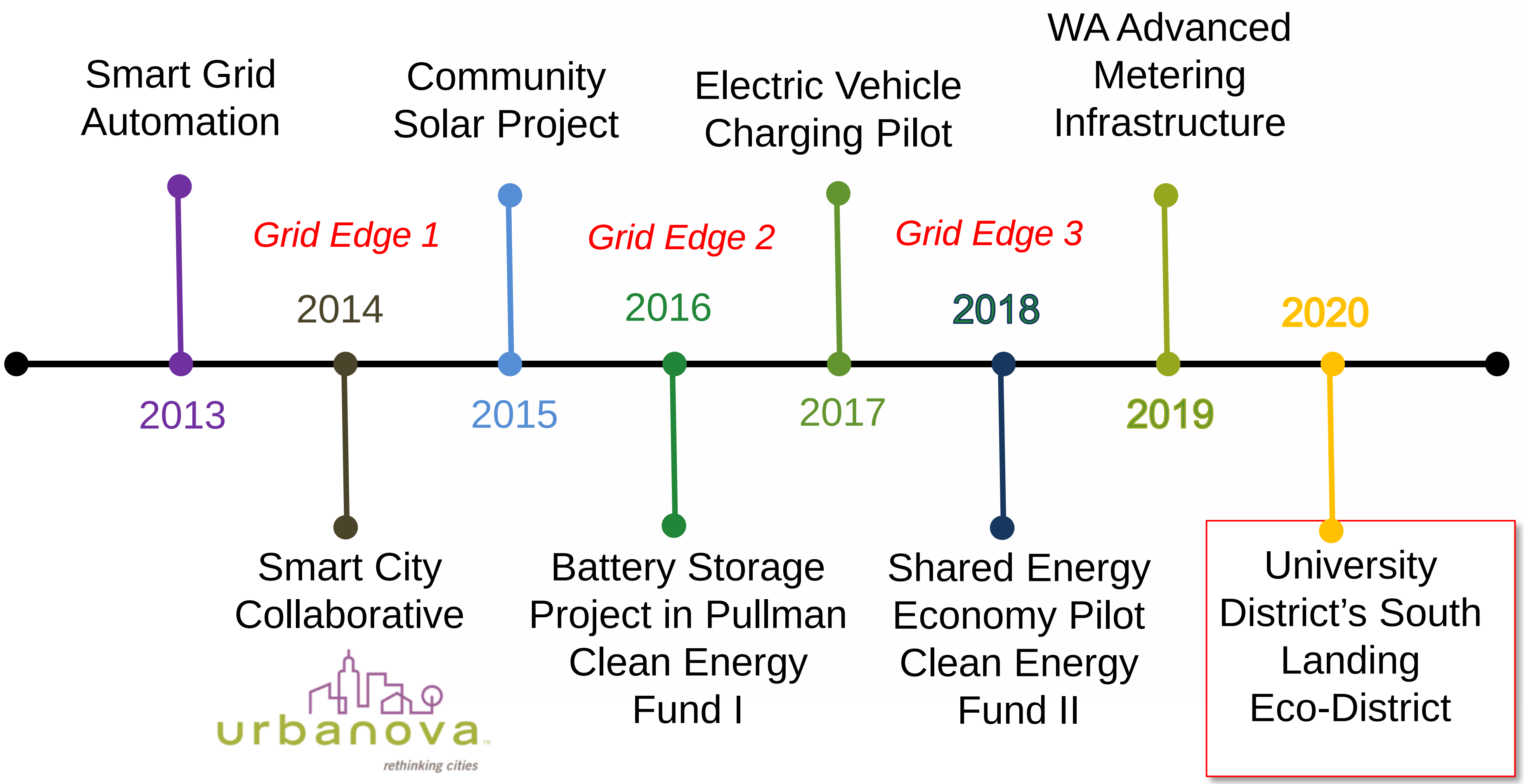




Capture opportunity from the changing electric utility business model

Avista's Business to Invent

Avista's Projects of Grid Edge Journey of Discovery



AVISTA

Introduction: Avista's Use Case Chronology

Movement from inward system improvements to outward customer experience

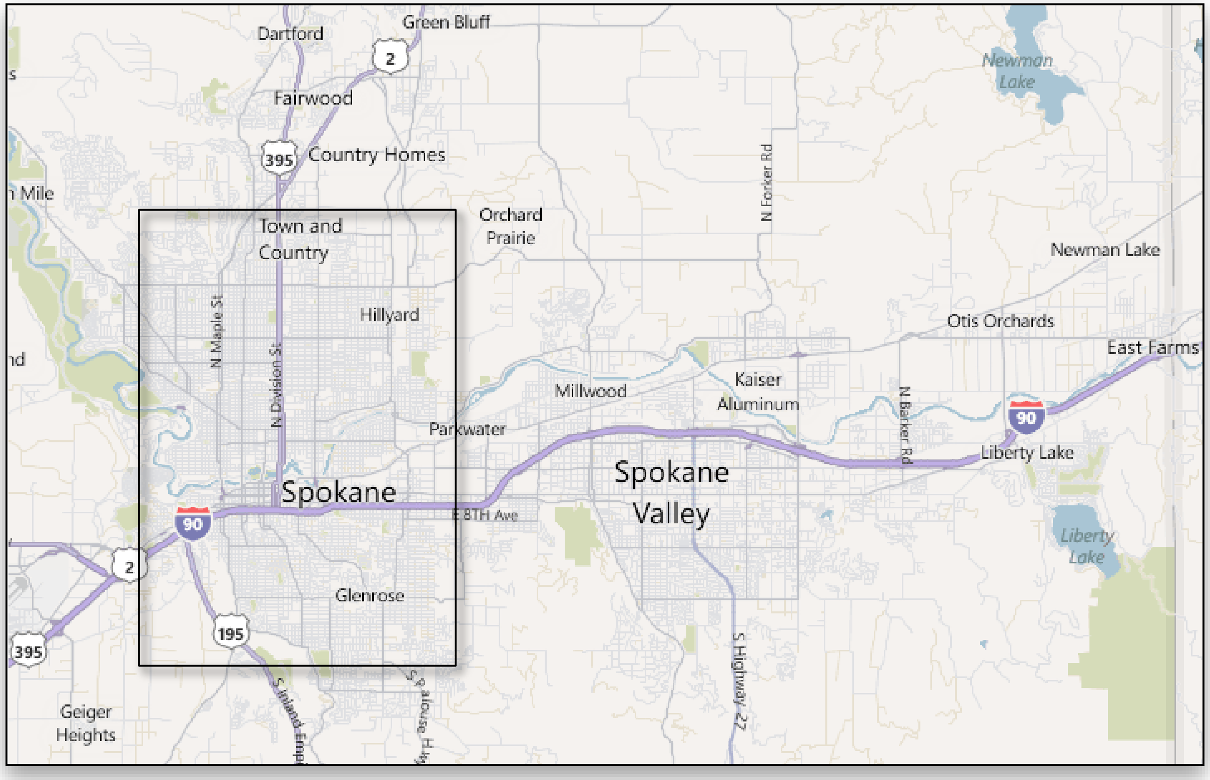
- Smart Grid
- Turner Energy Storage Project
- Shared Energy Economy
- Smart City
- Eco-District

Smart Grid Deployment

American Recovery and Reinvestment Act

Smart Grid Investment Project

- Fifty Nine Distribution Feeders



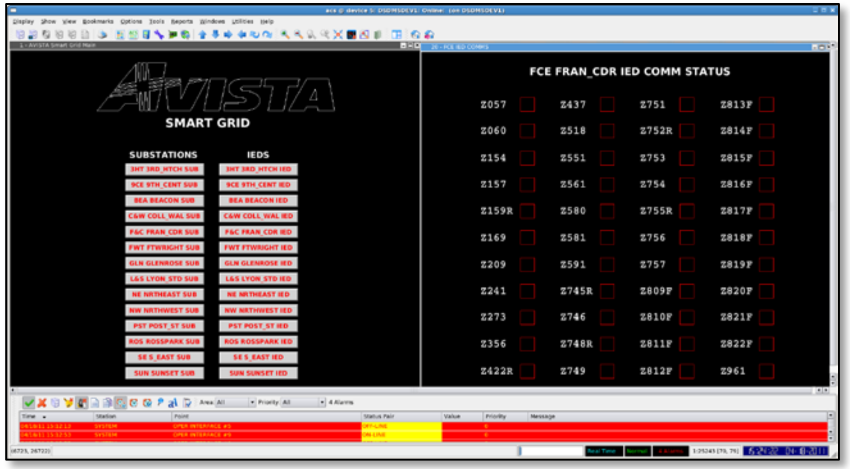
Smart Grid Demonstration Project

- Thirteen Distribution Feeders

Smart Grid Technologies

Communication

- Tropos Radios
- Fiber Backhaul



Control Software

- Distribution Management System (DMS)
- Fault Detection Interruption Restoration (FDIR)
- Integrated Volt Var Compensation (IVVC)

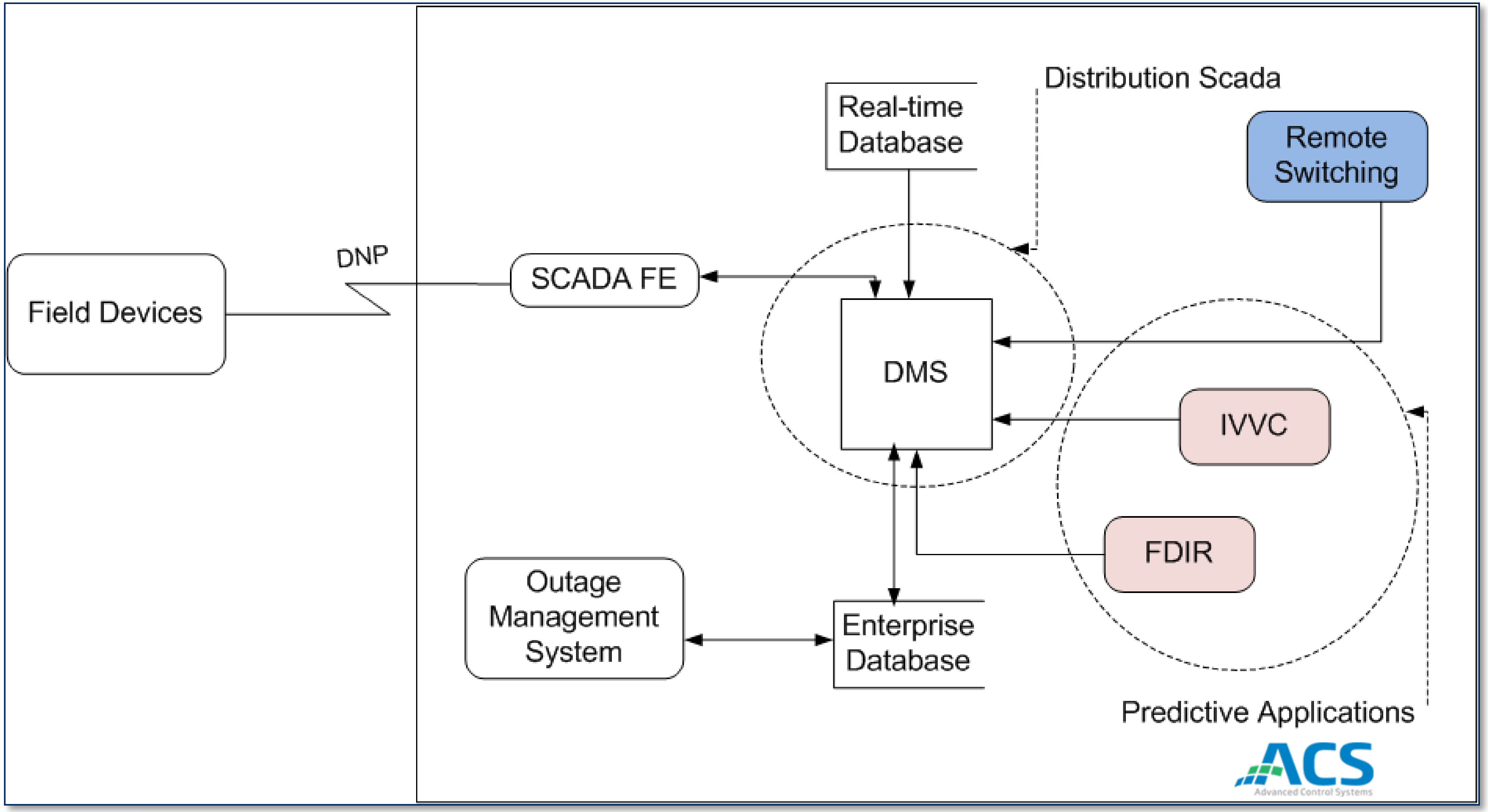
Distribution Equipment

- Switches (S&C) Scada-Mate
- Reclosers (G&W)
- Switch Capacitor Banks (Cooper)
- Individual Phase Regulator (Cooper)

Smart Grid Architecture

Client/Server

- Technology Debt
- Legacy Architecture
- Vendor Eco-System



Turner Energy Storage

Utility versus Customer Value

- 1MW – 3.2 MWh Battery
- Locate on SEL Manufacturing Campus
- UET Vanadium Flow Battery

Turner Energy Storage

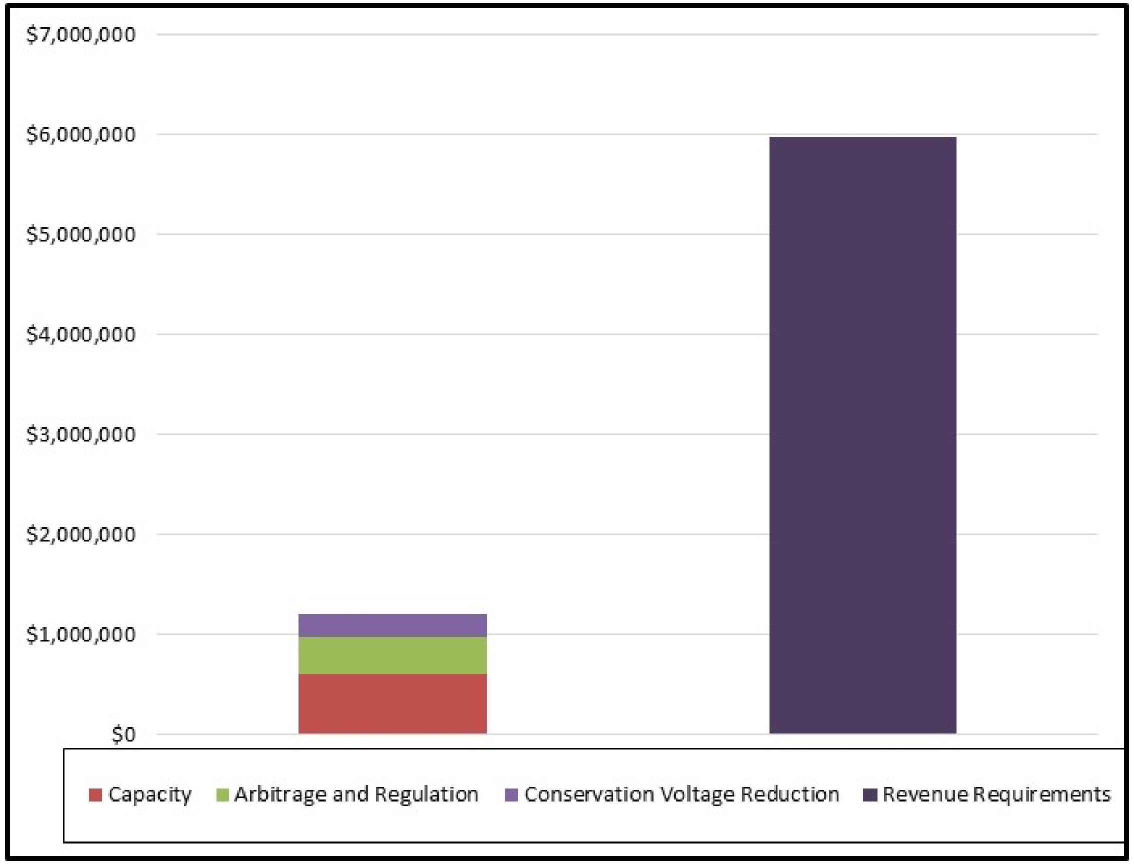
Use Cases

- Ancillary Markets
- Reserve Markets
- Grid Services
- Resiliency Services

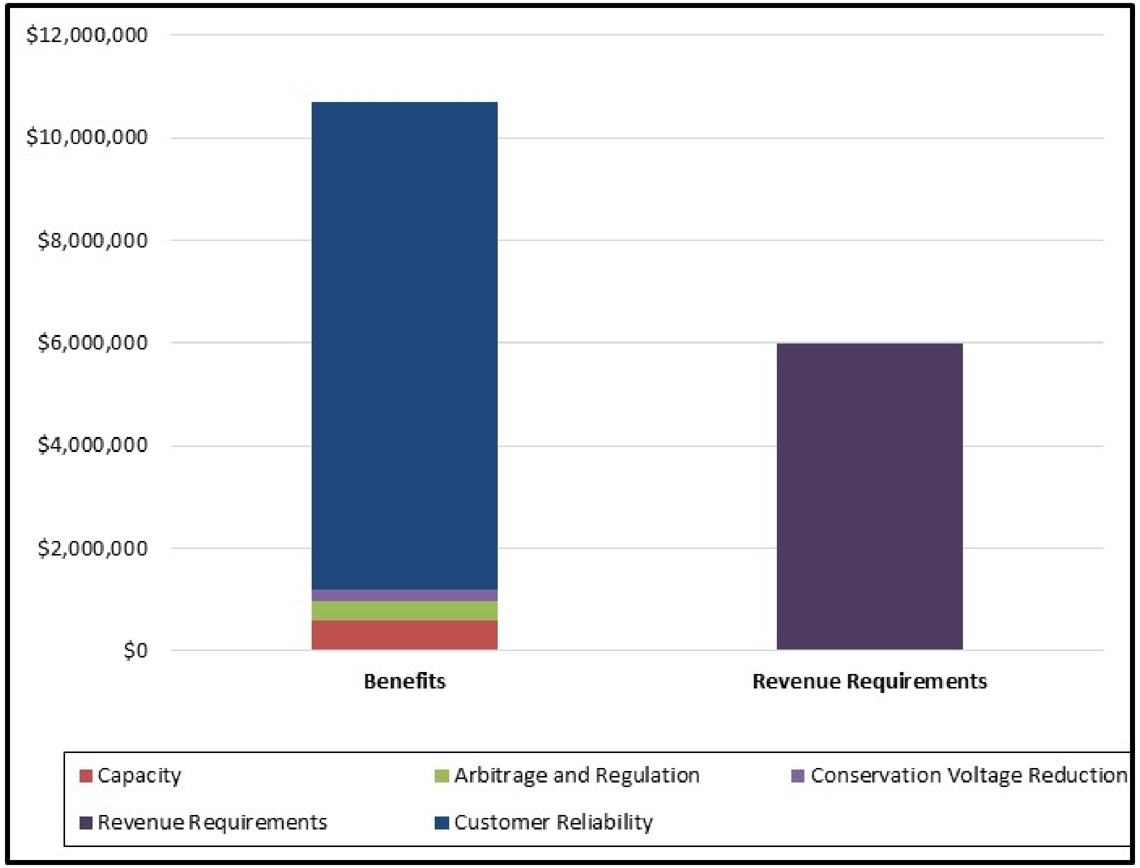
Use Case and application as described in PNNL Catalog	Avista	PSE	Sno – MESA1	Sno – MESA2	Sno - Controls Integration
UC1: Energy Shifting					
Energy shifting from peak to off-peak on a daily basis	Y	Y	Y	Y	
System capacity to meet adequacy requirements	Y	Y	Y	Y	
UC2: Provide Grid Flexibility					
Regulation services	Y	Y		Y*	
Load following services	Y	Y		Y*	
Real-world flexibility operation	Y	Y		Y*	
UC3: Improving Distribution Systems Efficiency					
Volt/Var control with local and/or remote information	Y		Y	Y	
Load-shaping service	Y	Y	Y	Y	
Deferment of distribution system upgrade	Y	Y			
UC4: Outage Management of Critical Loads		Y			
UC5: Enhanced Voltage Control					
Volt/Var control with local and/or remote information and during enhanced CVR events	Y				
UC6: Grid-connected and islanded micro-grid operations					
Black Start operation	Y				
Micro-grid operation while grid-connected	Y				
Micro-grid operation in islanded mode	Y				
UC7: Optimal Utilization of Energy Storage	Y	Y			Y

Turner Energy Storage

Voltage Sag Compensation



Base Case vs. Revenue Requirements – Utility Perspective



Benefits vs. Revenue Requirements – Inclusive of Customer Reliability Benefits

Avista

Develop a roadmap to the future utility business model

Avista's Road Map / Grid Edge 3

Utility Business Model Road Map

Personalized Energy Choice

Local Energy Choice

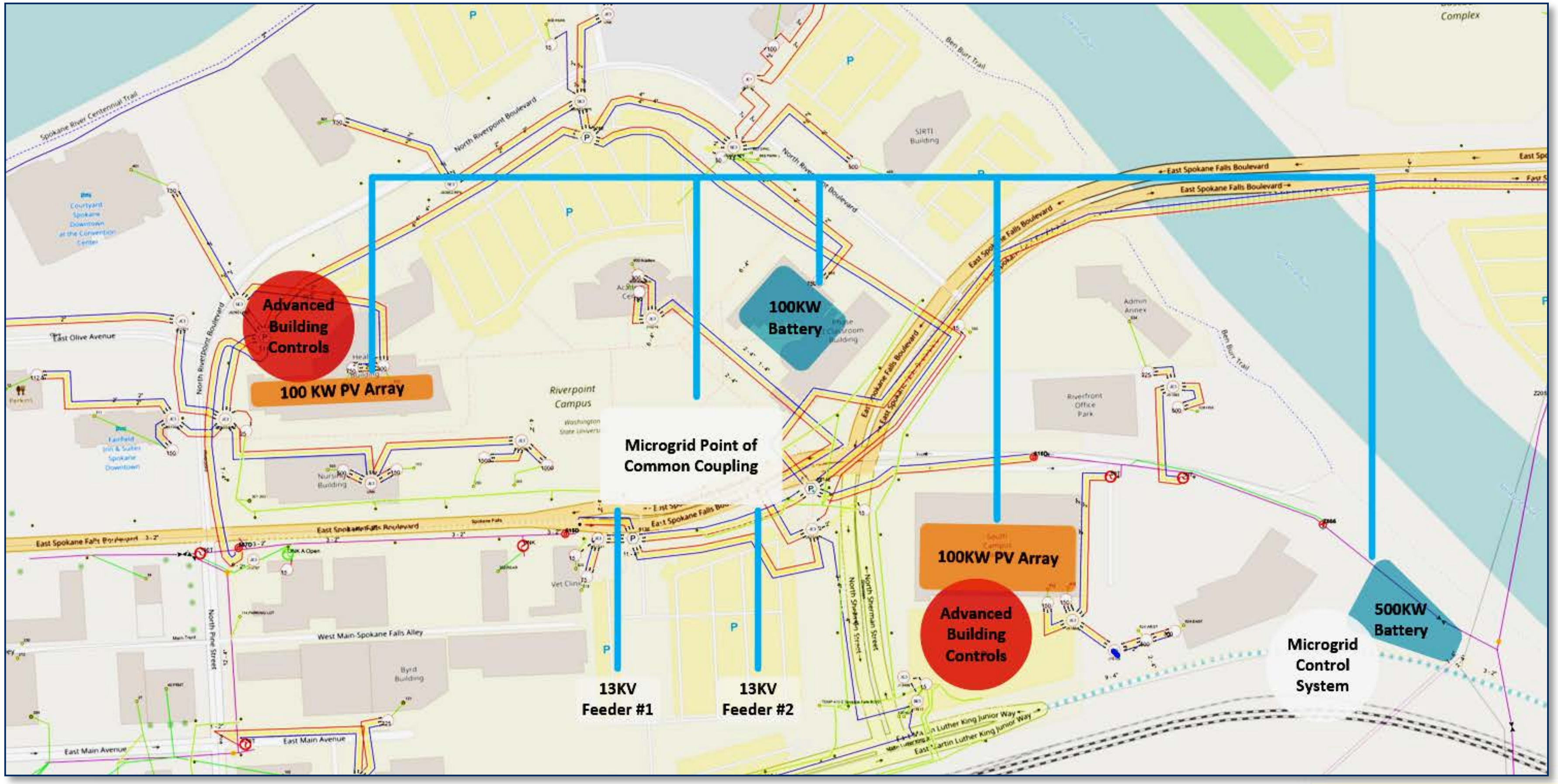
Peer Energy Choice

Shared Energy Economy

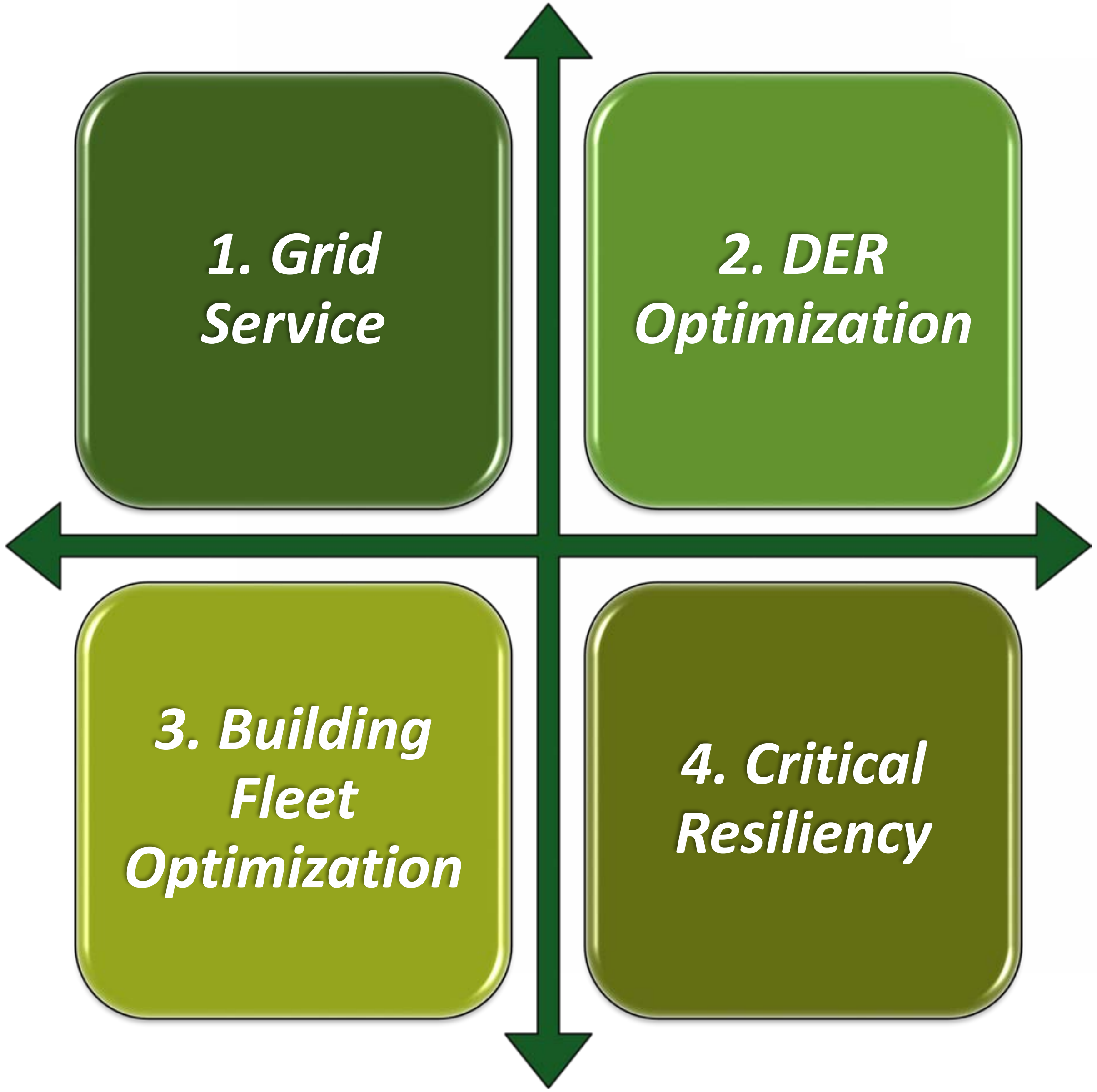
Spokane Udistrict Micro-Transactive

Assets

- Two Roof Top 100 kW Solar Systems
- Two Energy Storage Assets
  - 100 kW and 500 kW
- Two Building Management Systems



Shared Energy Economy/ Valuation



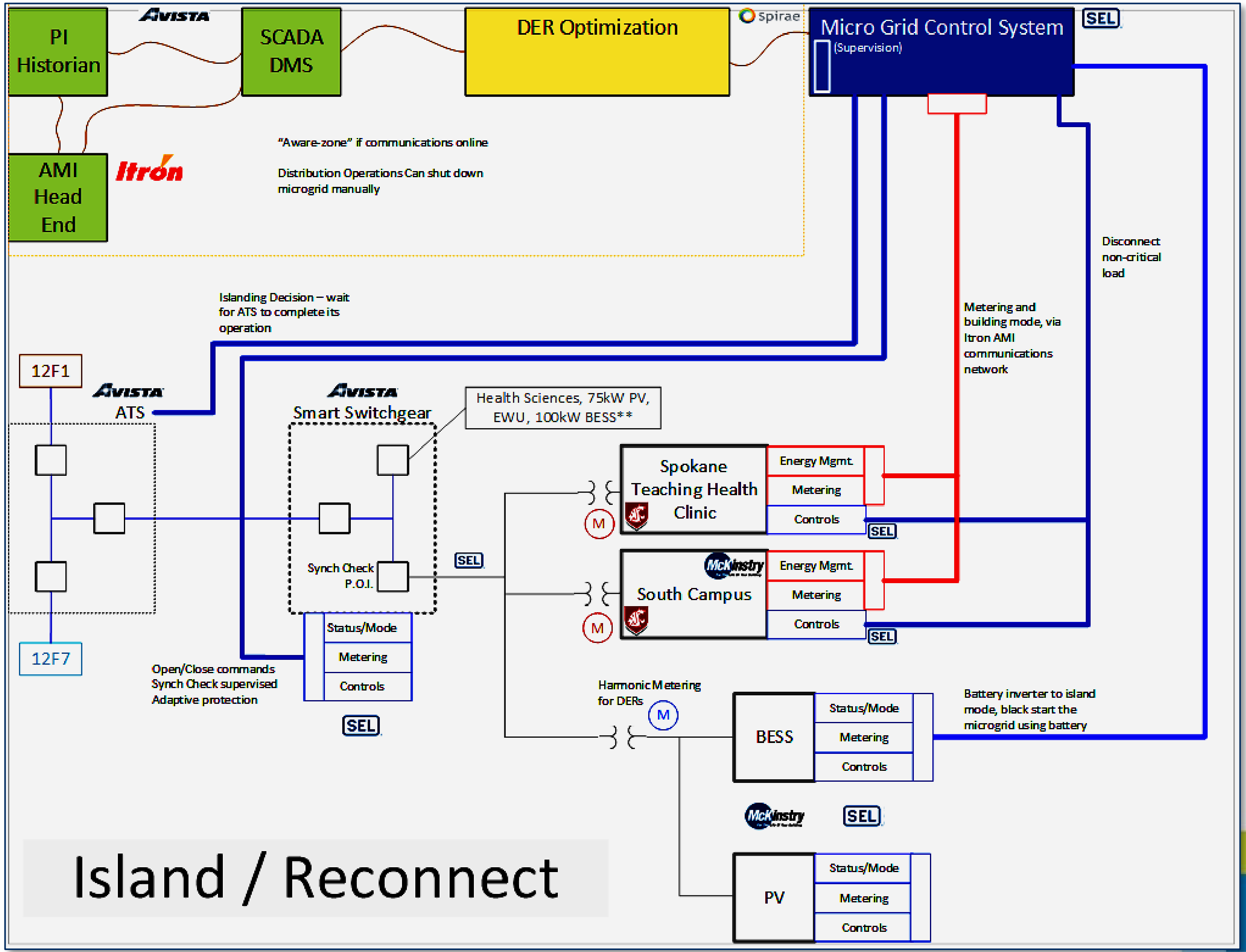
Shared Energy Economy/Interoperability

Multiple Partner Products

- Spirae Business Optimizer
- SEL Microgrid Controller
- McKinstry Building System
- Itron Riva Meter System

Research Partners

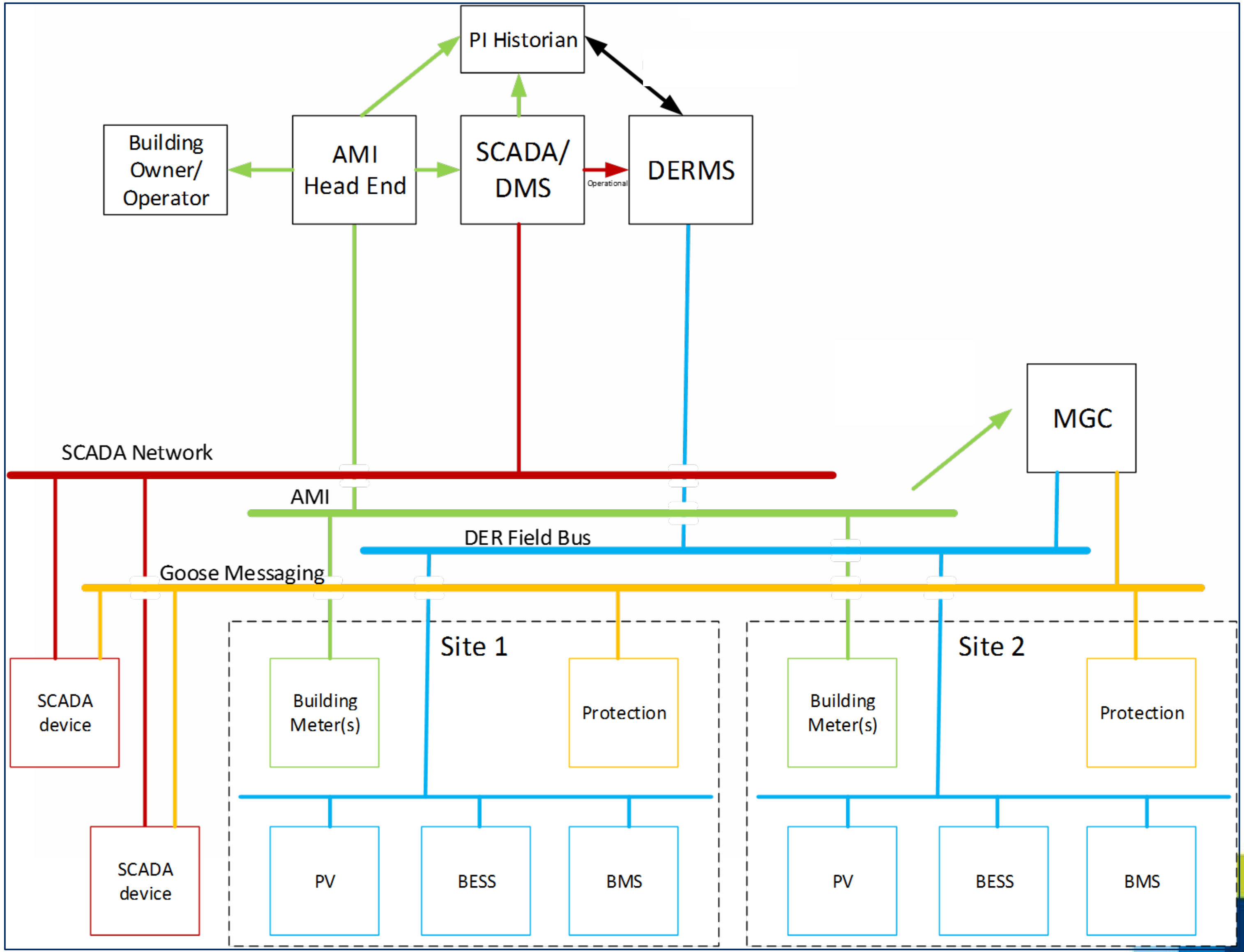
- Washington State University
- Pacific Northwest National Lab



Shared Energy Economy/Communication Latency

Distinct Operational Systems

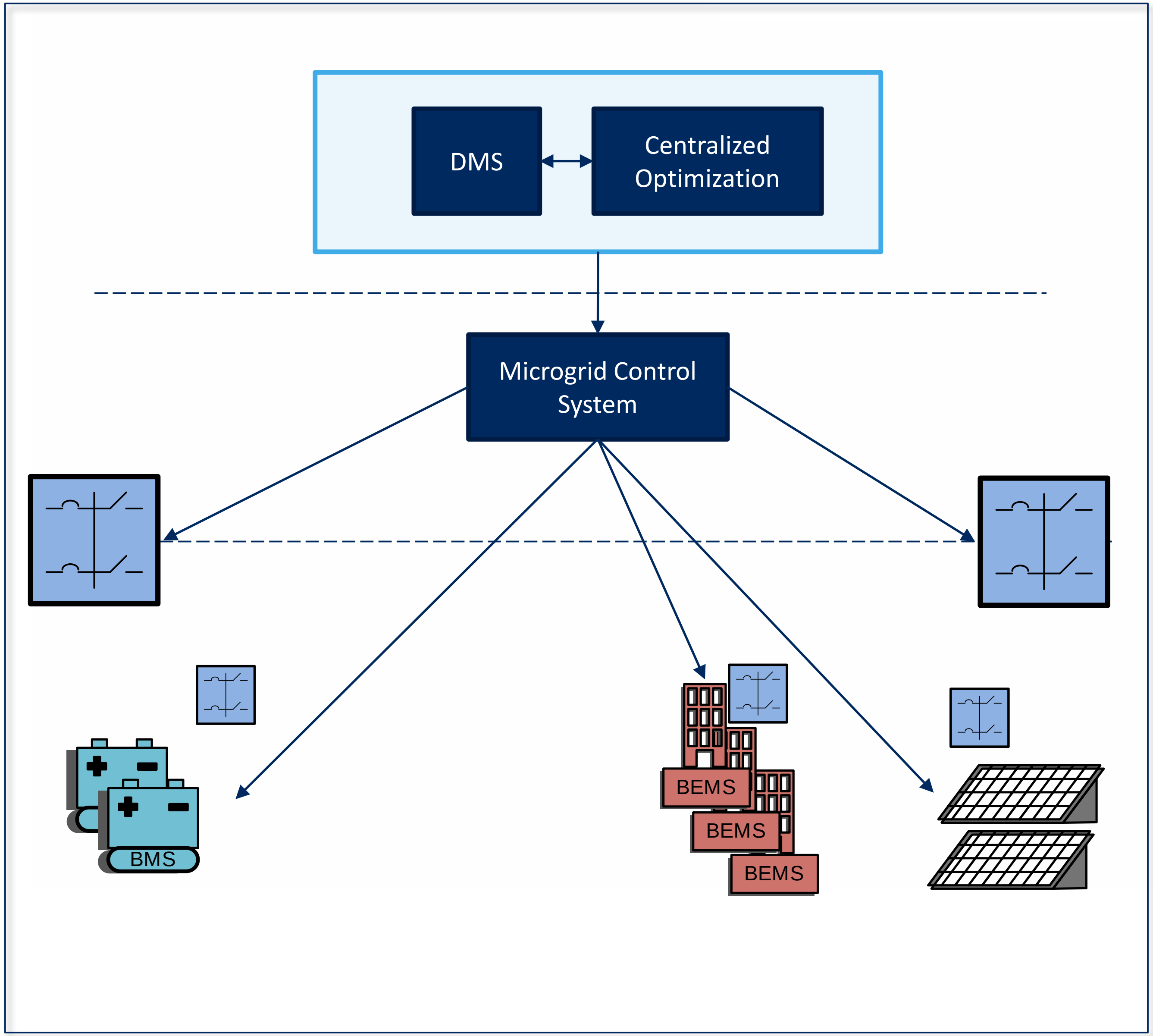
- DER Field Bus - *Minutes*
  - Business Optimizer
- SCADA Network - *Seconds*
  - Distributed Management System
- AMI Network – *Batched 4 hours*
  - Billing/Application Platform
- Goose Messaging - *Milliseconds*
  - Microgrid Controller Platform



Shared Energy Economy/Distributed Applications

Distributed Capability

- Enterprise/Central Control
  - Volt/Var
  - Demand Response
  - Forecasting
  - Market
- Site/Microgrid Control
  - Island Detection
  - Decoupling
  - Re-synchronization
- Local/Autonomous Control
  - Invertor Settings
  - Energy Management System
  - Protection Settings
  - Building Management Operational Parameters



Avista

Blurring the line between utility and municipal infrastructure

Avista Smart City - Urbanova

- Benefiting Cities and Citizens
  - Healthier citizens
  - Safer neighborhoods
  - Smarter infrastructure
  - Sustainable Environment
  - Stronger economy

- Partners
  - City of Spokane
  - Avista Utilities
  - University District
  - Itron
  - Washington State University
  - McKinstry
  - Gallup
  - Version
- Urbanova Projects
  - Smart and Connected Streetlights Pilot
  - Shared Energy Economy Model Pilot
  - Gallup People-centered Research

urbanova.org

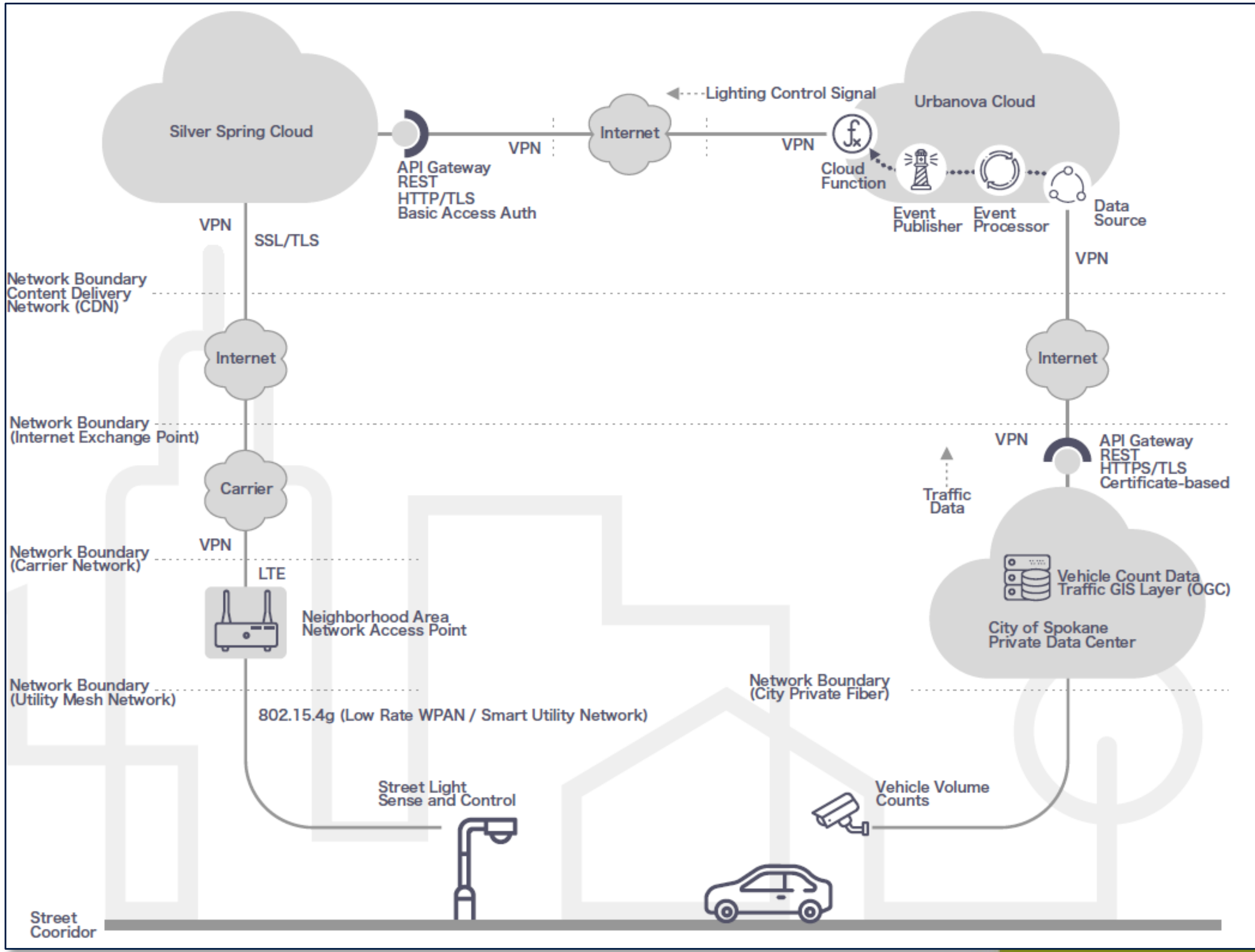
Avista Smart City Street Light Architecture

Use Case

- Adaptive Lighting Based on Traffic Volume
- Leverage Utility Infrastructure for Broader Purpose

Architecture

- Utility AMI Infrastructure
- Urbanova Platform / Amazon Web Services
- City Internal Traffic Management System



Avista

Disrupt the utility business model to ensure fair customer rate reform

Eco-District

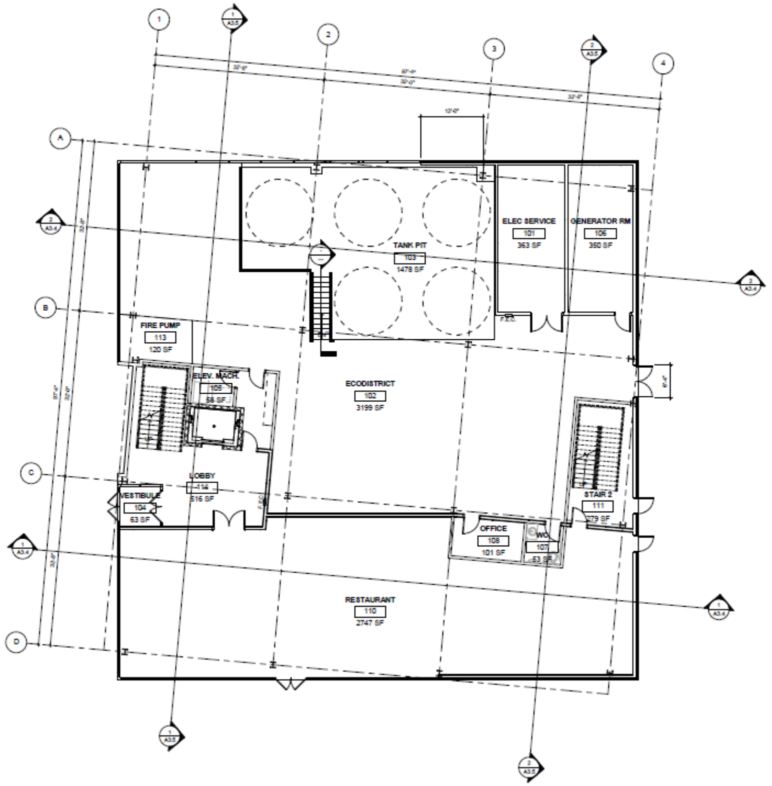
Commercial Development

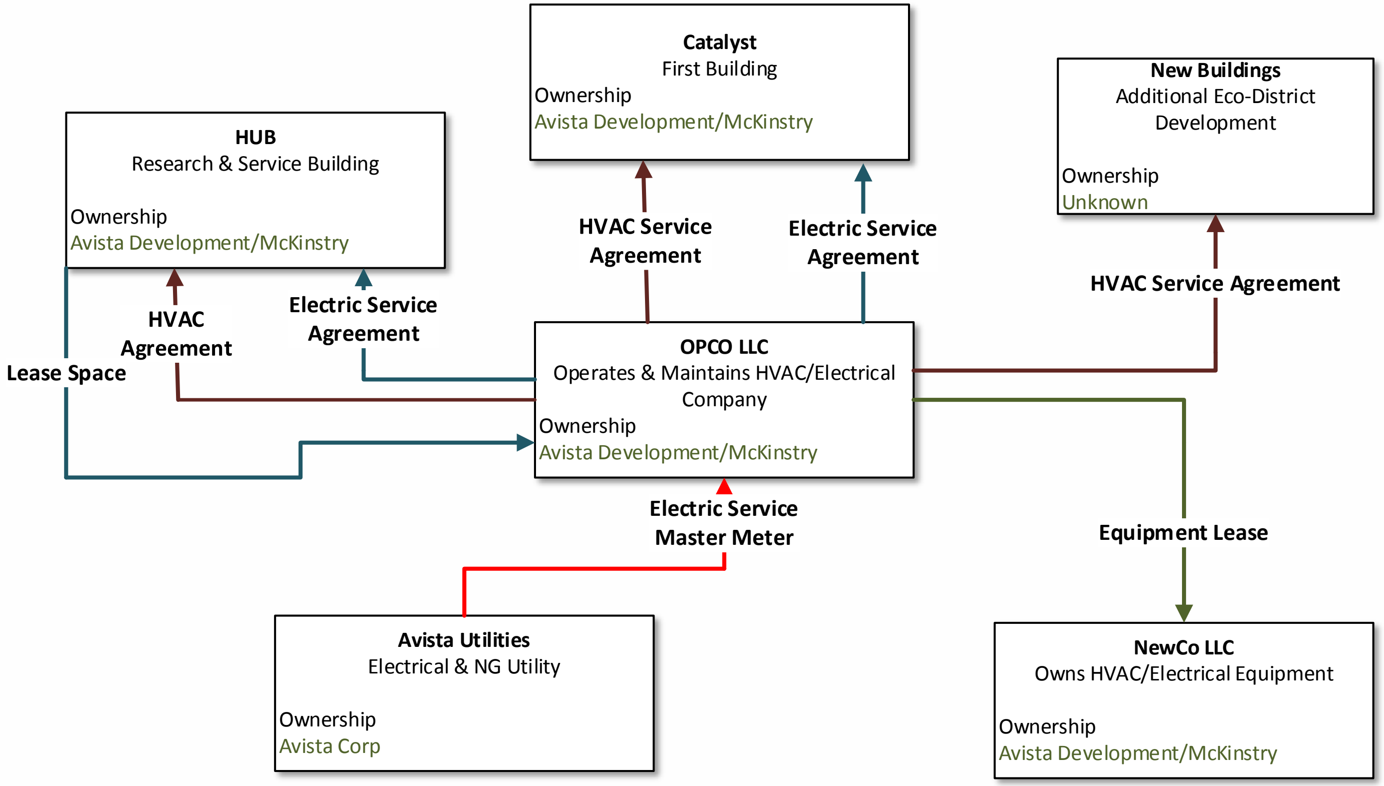
- Eco-District
- Conditioned Environment
- Electric Service
- Self-Generation

Eco-District

Distributed Capability

- Enterprise/Central Control





Eco-District

Certification Elements

- Best in Class Building Design
- Energy load offset with on-site and off-site renewables
- Zero energy performance not modeling
- No combustion allowed

Grid Optimal / Grid Opportunities

- Capacity Offsets
- Load Transfer
- Generate Renewable Resource into Load
- Voltage Support
- Phase Balancing

ZERO ENERGY CERTIFICATION

Versus

Grid Optimal

Eco-District – Rate Reform

Goal

- Develop a rate mechanism to incentivize developments to be grid optimal without unfairly burdening other customers with the cost of the utility infrastructure

Observation

- The eco-district proforma is a financial model which provides insight on how future performance base rate making might be accomplished

Challenge

- Existing rate structures do not support the business model for the grid of the future
  - Schedule 21 Energy and demand charges – Infrastructure costs rolled into consumption charges
  - Schedule 51 Line extension allowances calculated buy energy consumption
  - Schedule 90 Electrical energy efficiency programs – Socialized benefits and application
  - Schedule 63 Net metering – kW limit on local generation due to cross subsidy
  - Schedule 65 Interconnection standards
  - Schedule 62 PURPA rates – 5 year schedule

Eco-District – Rate Reform

Opportunity

- To be successful, a special contract would be developed to allow for the developer to obtain economic efficiency, operational flexibility and fair allocation of the utility fixed asset costs

- So, what would this look like?
    - A utility revenue and cost model comparative to the assumptions made in the proforma
    - Unlimited amount of generation behind the meter owned and operated by customer
    - Incentivize the developer to build highly efficient buildings
    - Incentivize the developer to limit utility capacity required to support the development
    - Create a regulatory methodology which can provide a road map for future utility rate reform

Avista

An architecture for our customer OpenDSP

Avista Distribution Management System

Micro-Services Requirements

DISTRIBUTION SCADA	OUTAGE RESTORATION	DISTRIBUTED ENERGY RESOURCES	DISTRIBUTION MANAGEMENT	ECONOMIC OPTIMIZATION
Current System Status	Estimate Restoration Time	Demand Response	Switch Order	Optimal Crew Dispatch
Tagging	Damage Assessment	Distributed Generation	Automatic Generation Control	Optimal DER Dispatch
Alarming	Incident Management	Distributed Strorage	Integrated Volt VAr Control	Optimal Feeder Utilization
Remote Control	Crew Management	Microgrid	Fault Detection Isolation and Restoration	Optimal DER Locational Benefits
	Reliability Reporting	Electric Vehicles	State Estimation	Transactive Markets

Distributed System Platform

Open Architecture

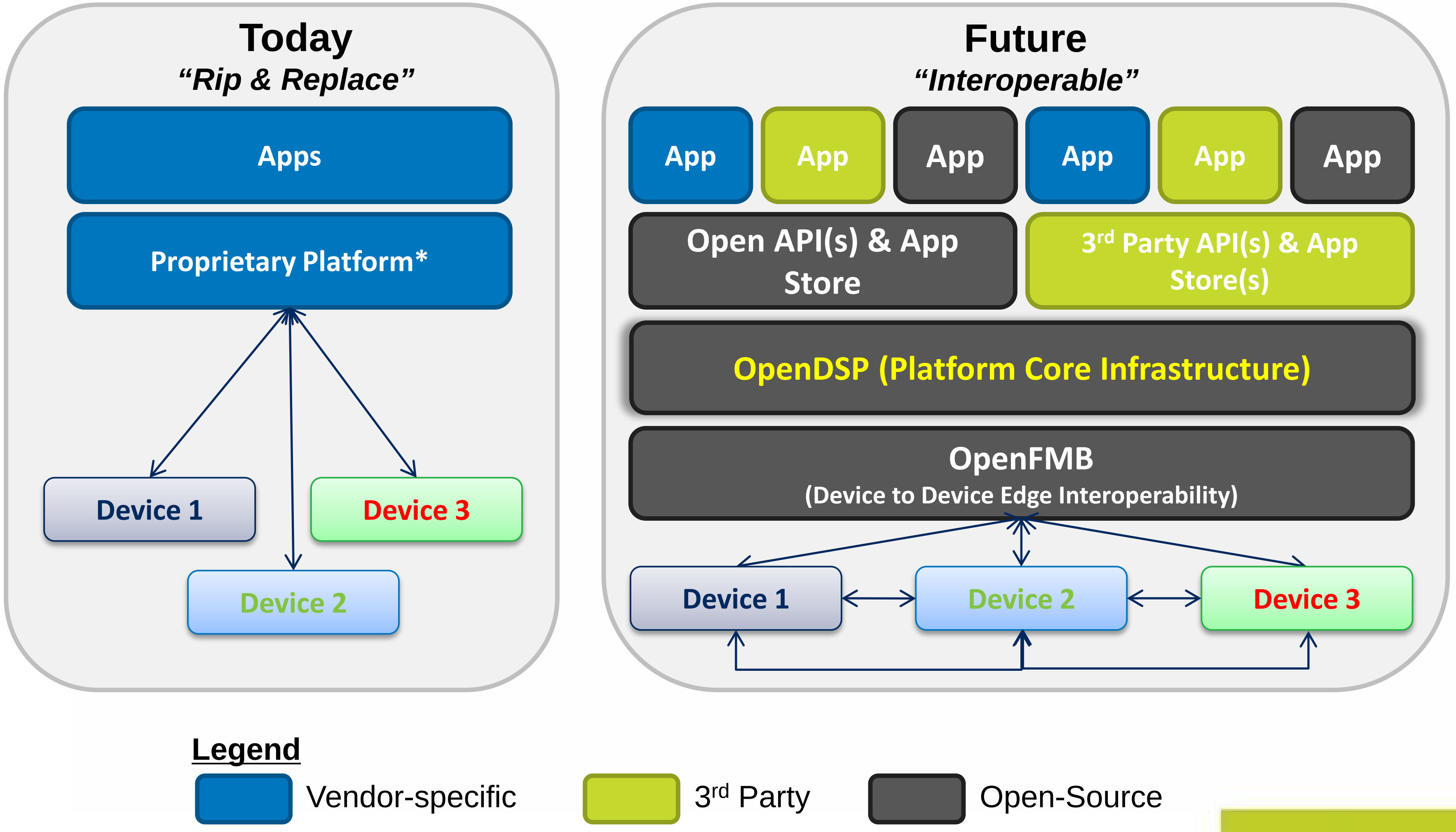
For a Distribution Management System

Today Platform

- Proprietary
- Silo Solutions
- Integration

Future Platform

- Open Platform Services
- Enables Interoperability
- Establishes Application Eco-System
- Scalable Framework for Vendors

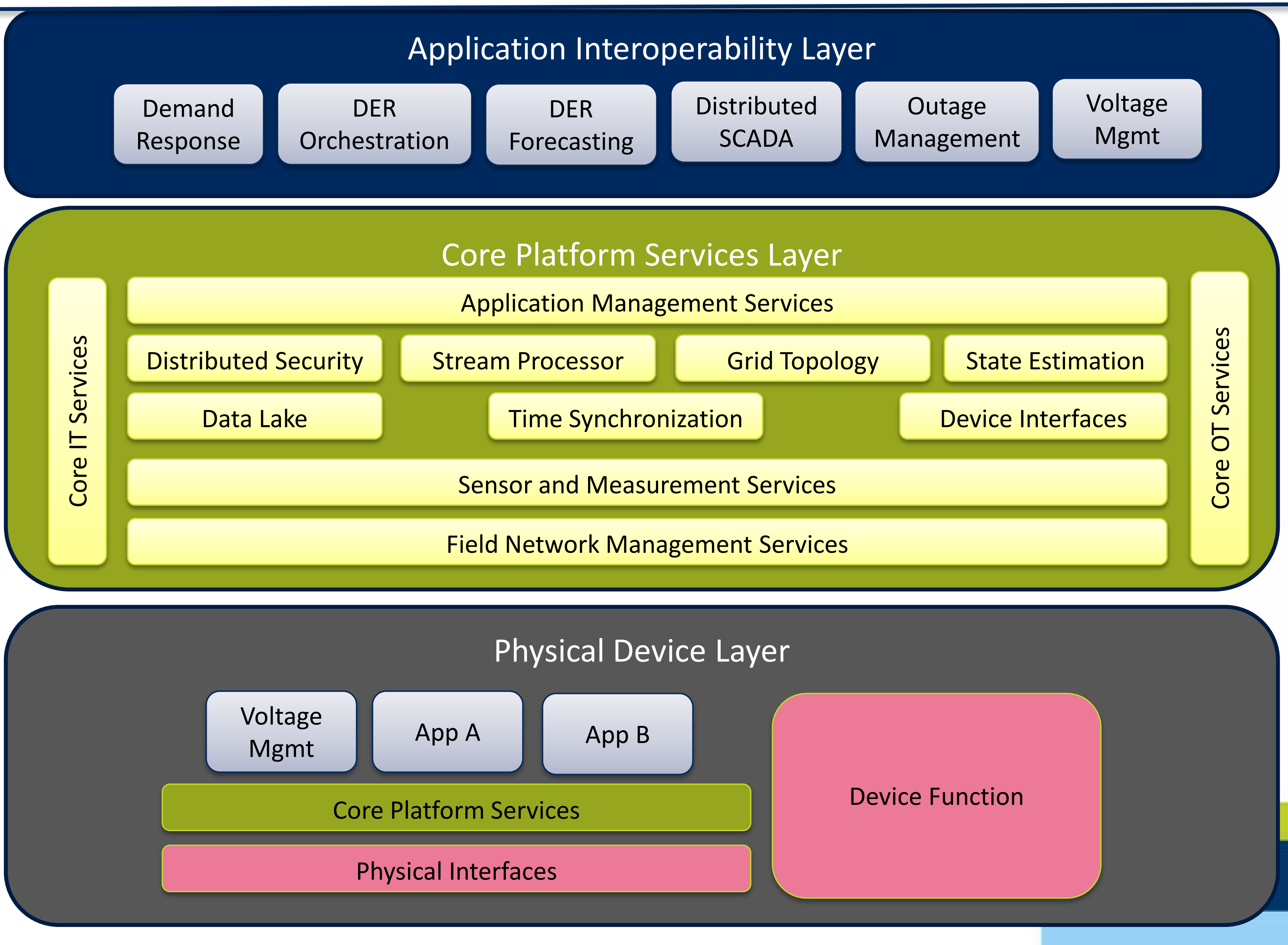


OpenDSP Core Services

Utility Perspective

Core Platform Services Layer

- Application Management Services
  - Distribution and orchestration of distributed Applications
  - Firmware Management
- Sensor and Measurement Services
  - Field Message Bus
  - Device Discovery
- Grid Management Service
  - Topology Awareness
  - State Awareness
  - Content Awareness
  - Simulation Engine
- Core IT Services
  - Stream Processor
  - Big Data
  - Security
  - Time Synchronization

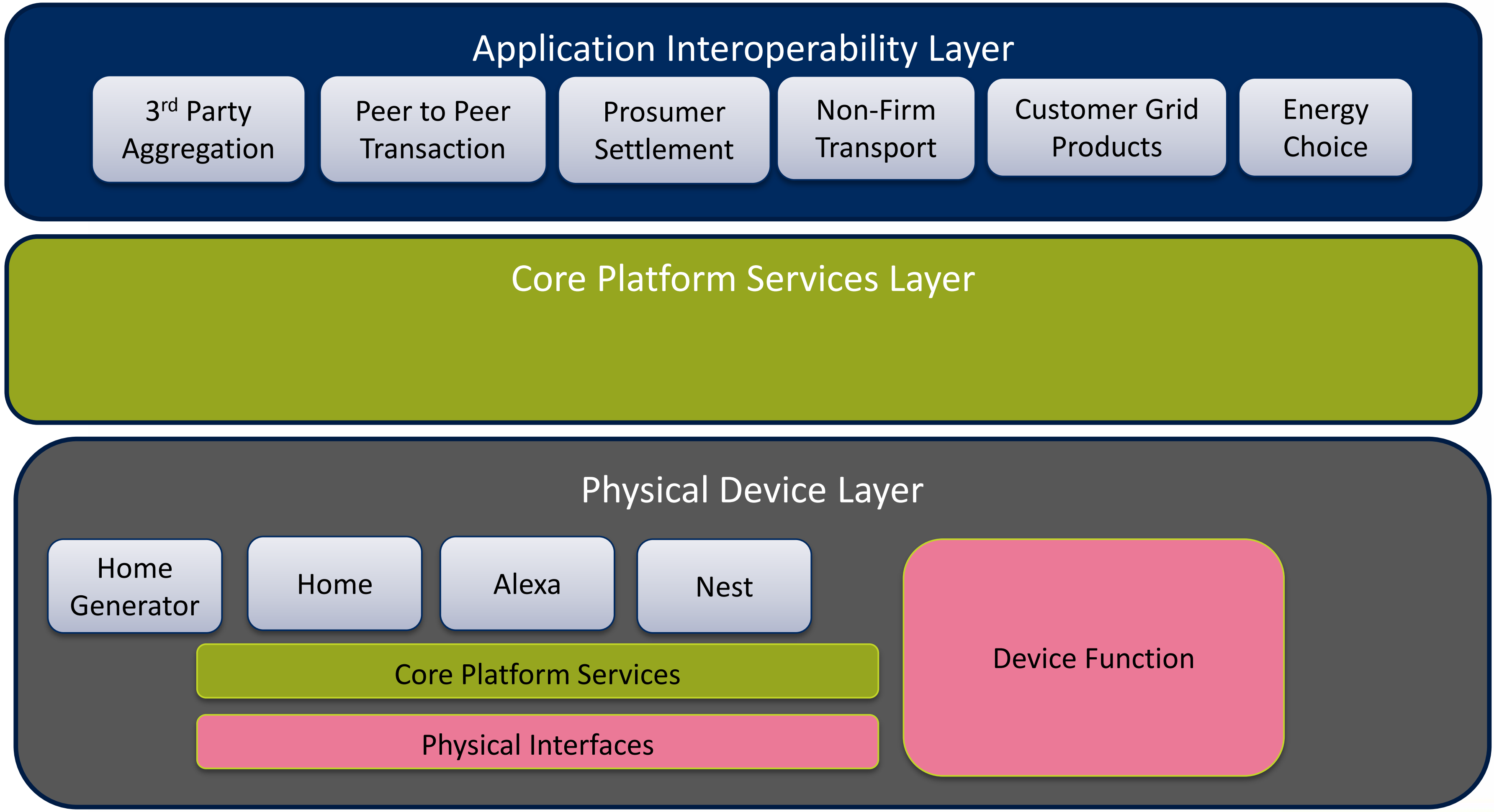


OpenDSP Core Services

Customer Centric

Utility Customers

- Prosumers
- Consumers
- Aggregator
- Eco-Districts
- In Home Service Providers
  - Google
  - Apple
  - Tesla
- Building Management Systems



Questions

Grid Modernization & Interoperability – Panel

Tuesday, November 13, 2018	
9:30 am	**Registration**
10:00 am	**Welcome and Workshop Objectives** **Chris Greer**, NIST
10:15 am	**Keynote: Grid Modernization and the Case for Interoperability** **John Gibson,** Avista Utilities
11:00 am	**Panel Session: Grid Modernization and Interoperability** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**Lunch**
1:15 pm	**Keynote: The Economics of Interoperability** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**Plenary: Introduction to NIST's Smart Grid Conceptual Models** **Avi Gopstein,** NIST
2:30 pm	**Interactive Discussion: Major Concerns for Smart Grid Interoperability** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**Break**
3:45 pm	**Plenary: Three Key Themes for Cybersecurity and Grid Interoperability** • **Risk Profiles—Jeffrey Marron,** NIST • **Interface Categories—Nelson Hastings,** NIST • **Securing Communications—Michael Bartock,** NIST
4:45 pm	**Wrap Up and Charge for Next Day**
5:00 pm	**Adjourn**

Chris Irwin – U.S. Department of Energy

Alvin Razon – NRECA

Unlocking the Value of Data
Optimizing the Distribution System

Alvin.razon@nreca.coop
Senior Director, Distribution Optimization

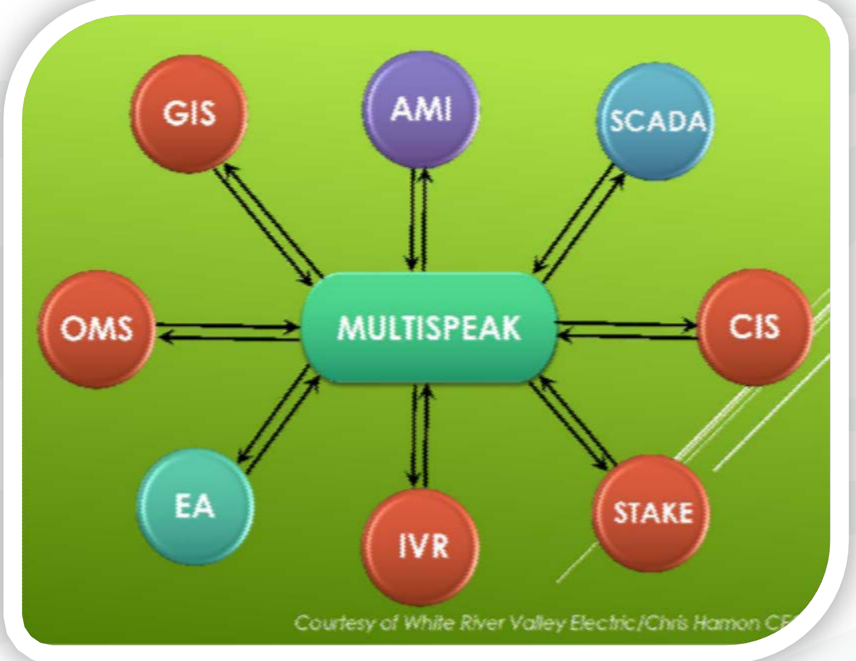
TODAY: NRECA Distribution Optimization (DO) Team

Practical Optimization Solutions
"Enabling Value of DATA"

1. SAFETY
IEEE 1547, NESC, NEC, TDEC, Cybersecurity, Testing & Certification

2. Distribution Reliability
SAIDI Outages, Power Quality, Data Analytics, Reliability Benchmarking,
DER, Dynamic Planning/Operations

3. Cost Effective Integration
MultiSpeak connectivity, De-Risking Technology
Integration, Innovative Apps/Tools

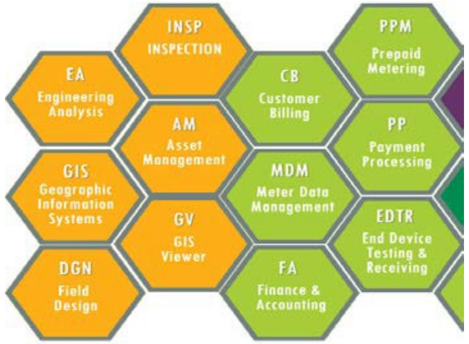


NRECA
America's Electric Cooperatives

MultiSpeak

Ecosystem of Solutions

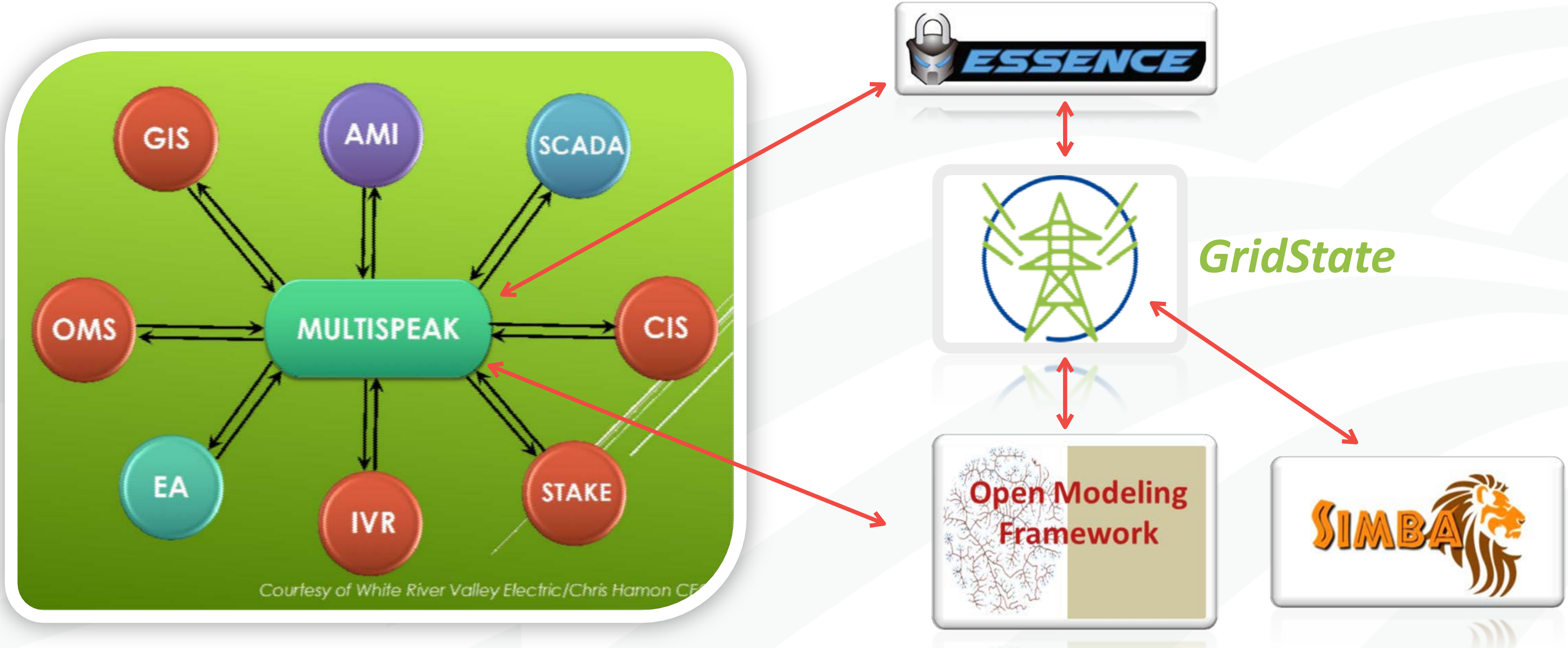
Cyber Security	RFP Templates	Testing & Certification	MultiSpeak Portal
NIST-SGIP	Available Online	V5 Comprehensive Testing	Selection of product solutions
	Step-by-step Help	Function Sets	Use Cases/Best Practices
		Full Profile	Online Testing
		Work Process	Multimedia Training



MultiSpeak Marketplace, MultiSpeak App-Store & More…

FUTURE "Tomorrow" (DO):

Enabling the Electric Utility of the Future

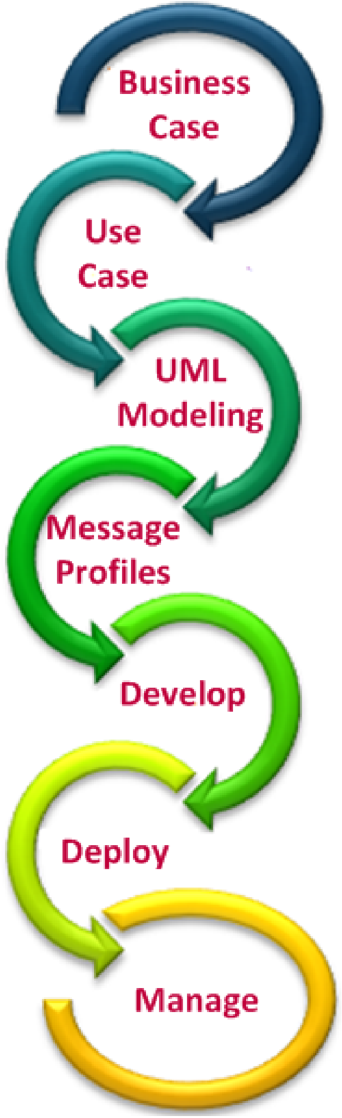


NRECA America's Electric Cooperatives

<u>VALUES & BENEFITS:</u> *Reduction of Losses in Capital Expenses, Outage/Restoration Cost, Custom Integration Cost, Cybersecurity and Resiliency*

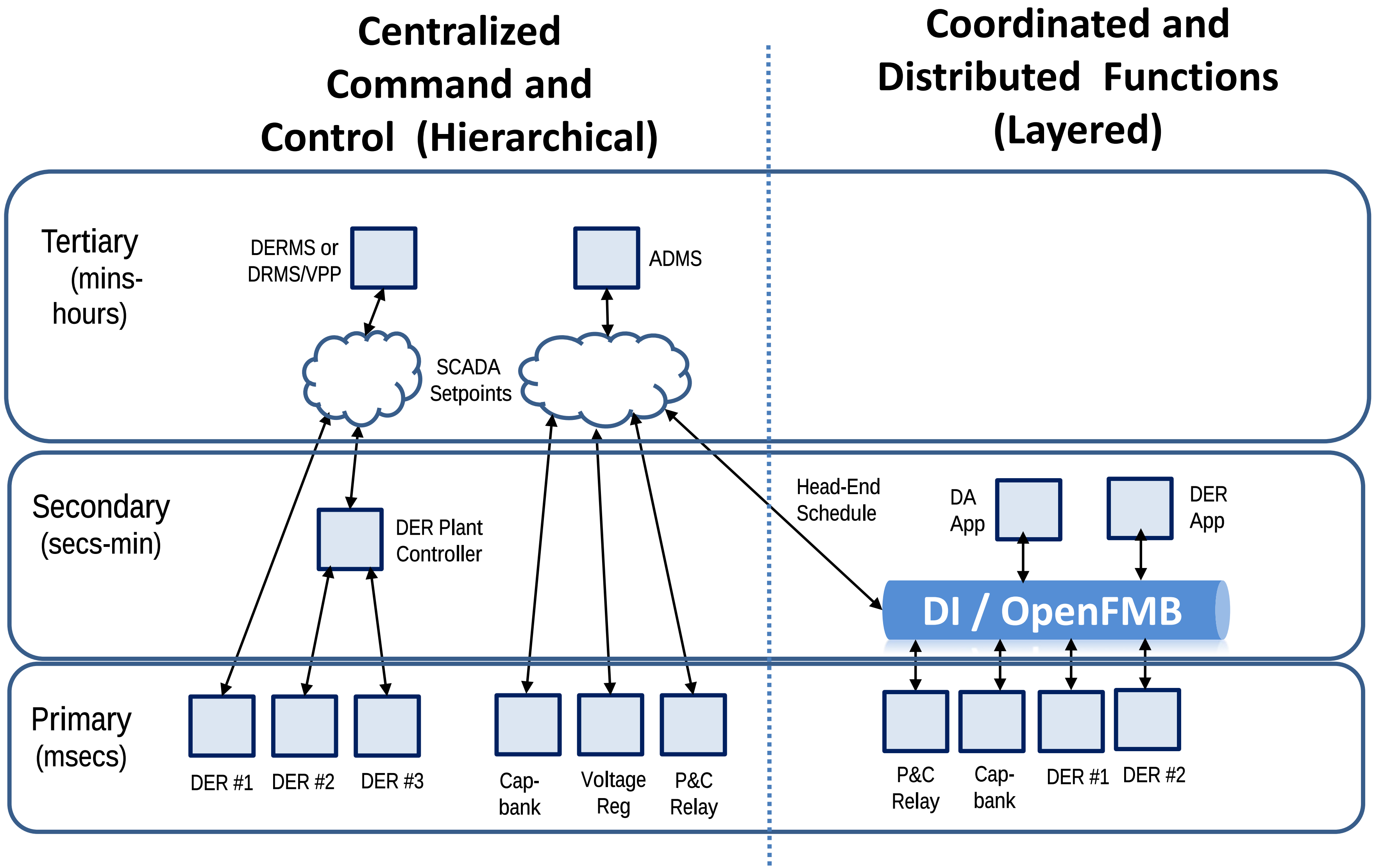
Dwayne Bradley – Duke Energy

OpenFMB Life Cycle Framework

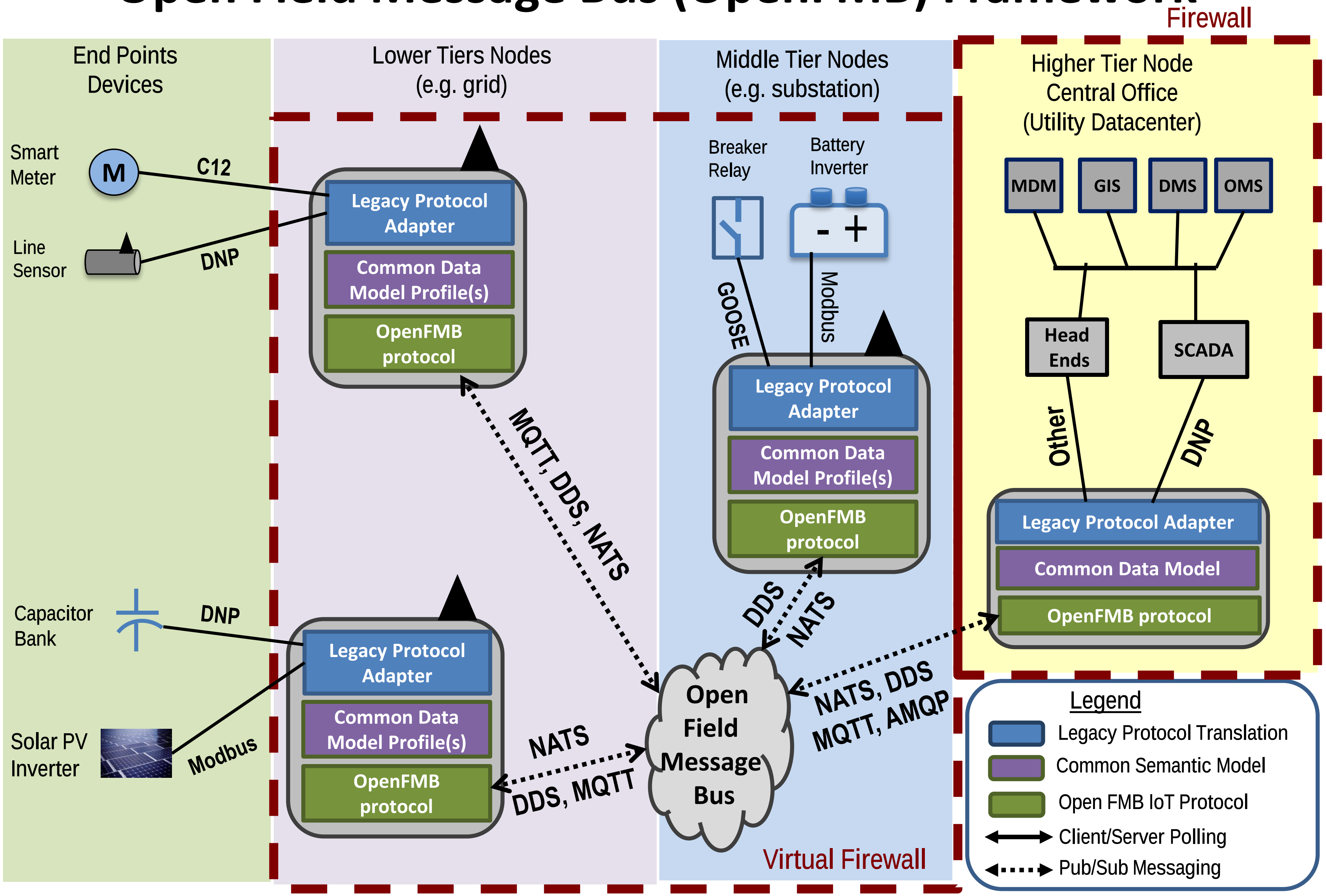


- Business-driven solutions
- Main and extension scenarios
- Platform Independent Model (e.g. IEC CIM and 61850)
- Platform Specific Models (e.g. IDL and Protobuf)
- Application and Adapter Configuration (e.g. DNP3, Modbus, and GOOSE)
- Field Implementation
- Health and lifecycle management

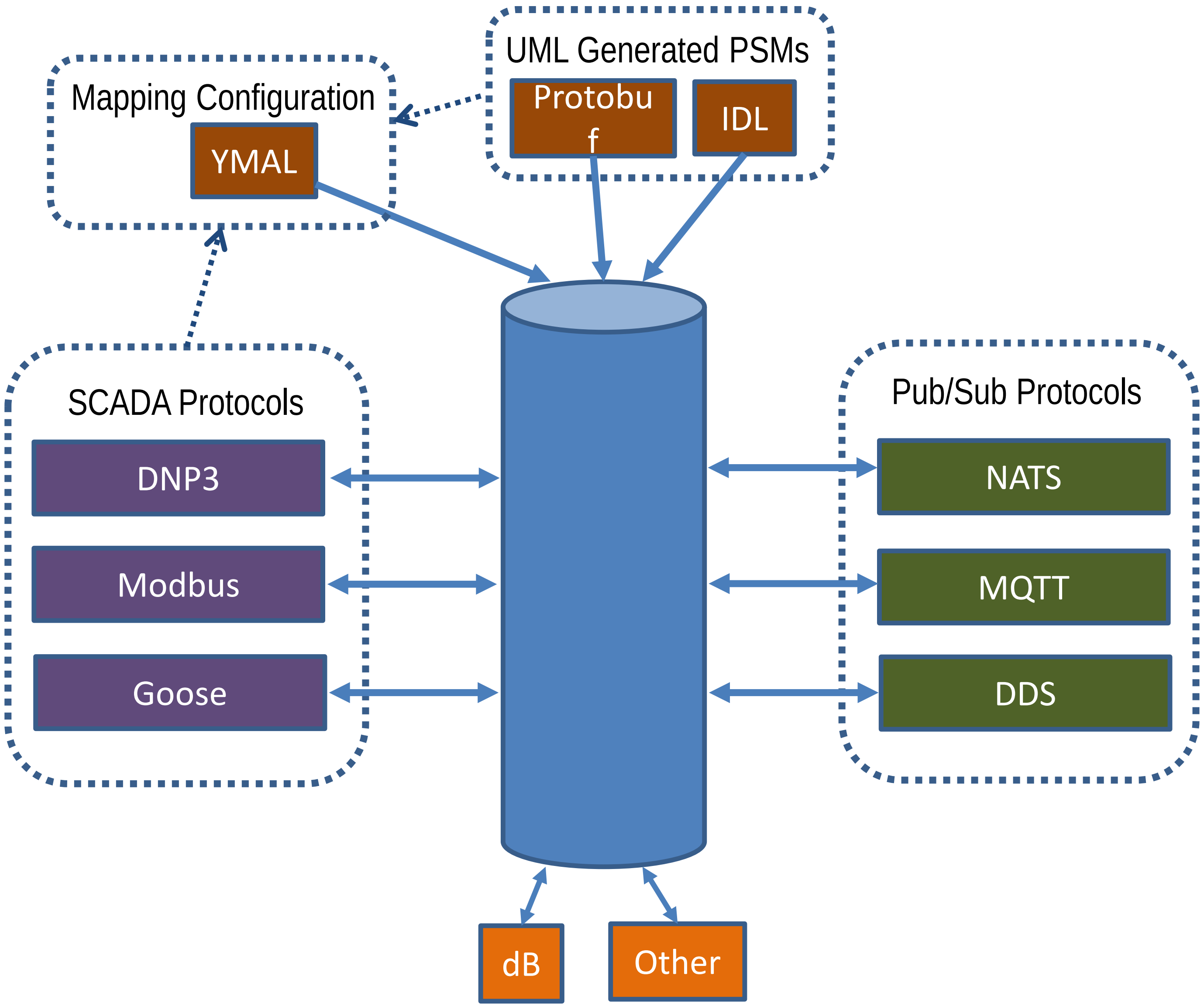
Co-existence of Legacy and Future Architectures



Open Field Message Bus (OpenFMB) Framework



Protocol Translation: OpenFMB Adapters

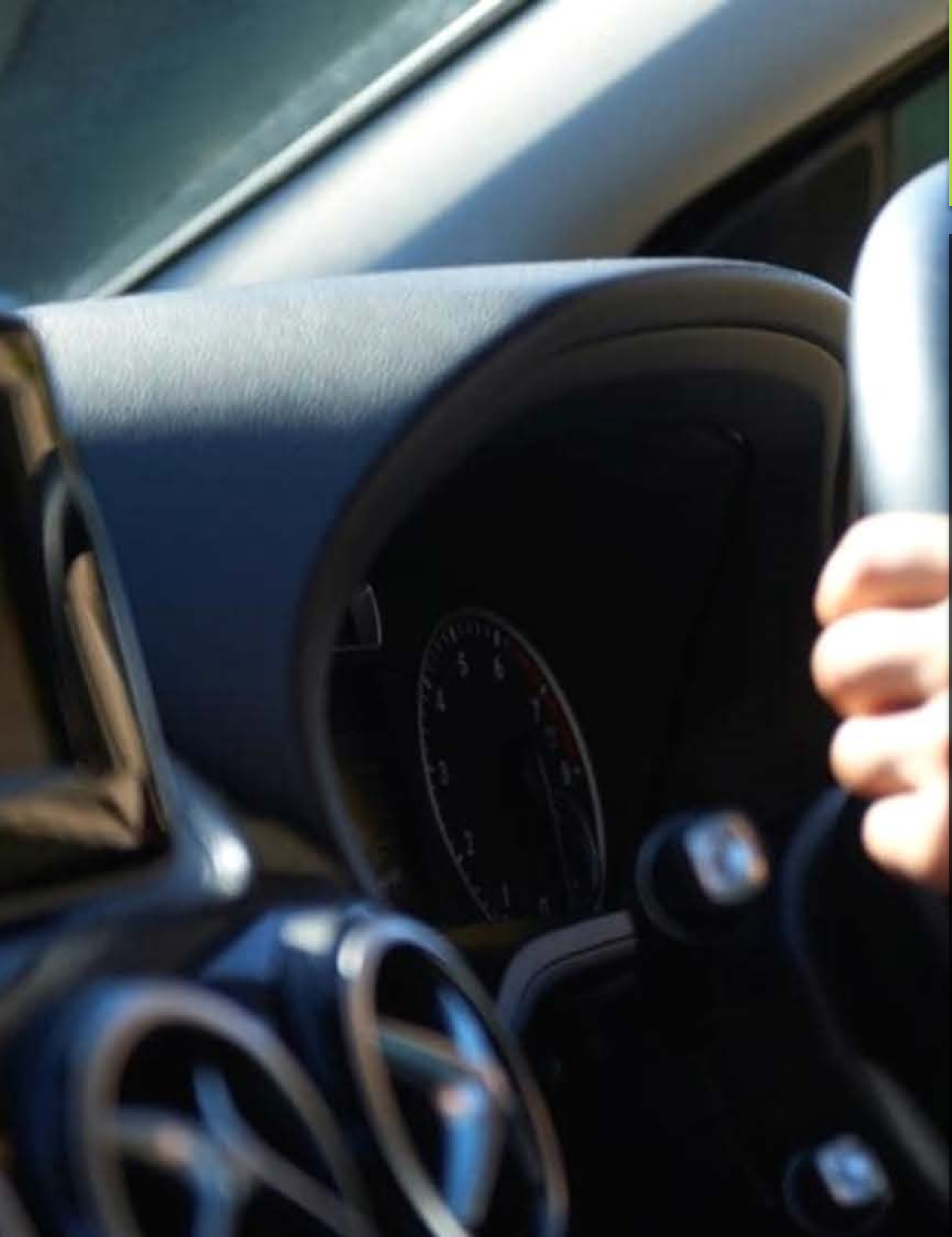


Naza Shelley – D.C. Public Service Commission

Customers & the Future Grid

A State Regulatory Perspective

THE VIEWS AND OPINIONS EXPRESSED IN THIS PRESENTATION ARE THOSE OF THE PRESENTER AND DO NOT NECESSARILY REFLECT THE OFFICIAL POLICY OR POSITION OF THE DISTRICT OF COLUMBIA PUBLIC SERVICE COMMISSION OR THE DISTRICT GOVERNMENT.



What Customers Want

- Customers are in the driver's seat
- What we are hearing –
  - Clean Energy
  - Competition
  - Data Access & Control
- It's industry's job to figure out what customers want
- What's the regulator's job?

A Regulator's Concerns

- Customer vs. Prosumer
  - Data ownership vs. data protection
- Reliability
- Safety
- Cost

A Regulator’s Responsibility

- Protect and empower customers
- Reduce/remove regulatory barriers
- Establish a clear/flexible regulatory framework
- Tell stakeholders what you need to make a decision
  - Ask the right questions
  - Put the risk on industry to present solutions to problems
  - Put the burden on industry to justify the solution they present if cost sharing is required for implementation
  - Favor the carrot but be willing to use the stick

Questions?

Naza Shelley – Attorney Advisor
D.C. Public Service Commission
1325 G. St. NW, Suite 800,
Washington, D.C. 20011
nshelley@dcpsc.gov

Joe Peichel – Xcel Energy

Who Do You Trust?

- Certified Identity
- Devices, Organizations and People
- Delegations of Authority

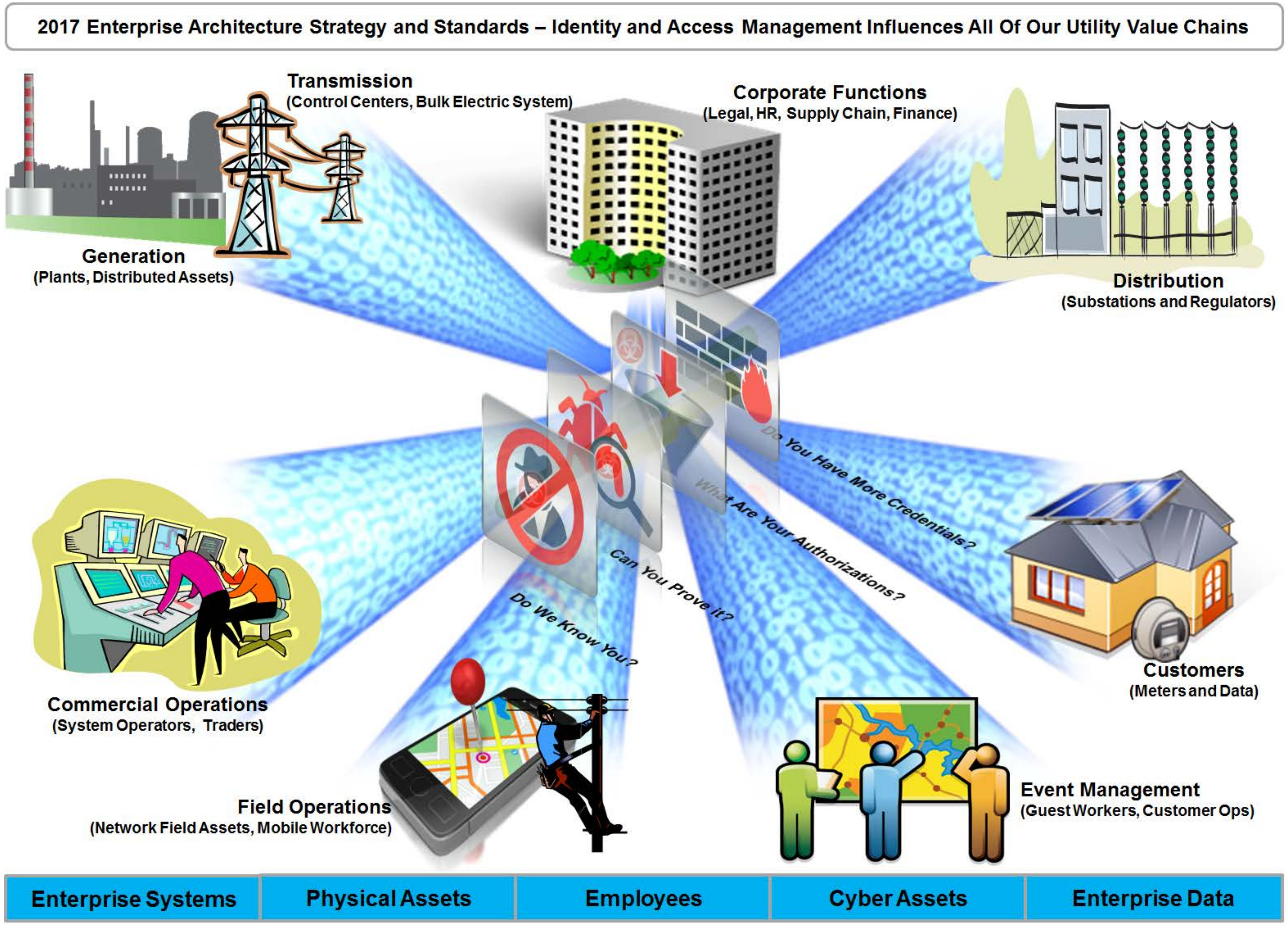


Illustration courtesy of Phil Wilkerson, Xcel Energy

Lunch: 12:00-1:15

Local Restaurants

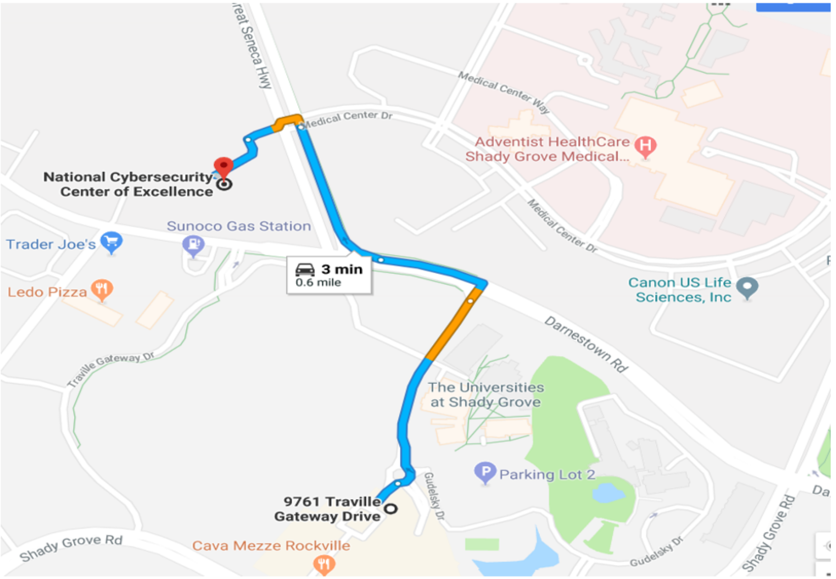
Travilah Village Center (0.6mi)
9761 Traville Gateway Drive
Rockville, MD 20850

Potomac Pizza-301.279.2234
9709 Traville Gateway Drive
Rockville, MD 20850

Sushi Oishii- 301.251.1177
9706 Traville Gateway Drive
Rockville, MD 20850

Bagel Towne Deli-301.279.7035
9749 Traville Gateway Drive
Rockville, MD 20850

Cava Meze-301.309.9090
9713 Traville Gateway Drive
Rockville, MD 20850



Local Restaurants

Most restaurants have vegetarian options

Fallsgrove Village Center (0.9mi)
14955 Shady Grove Road
Rockville, MD 20850

Moby Dick House of Kabob-301.738.0005
14921 Shady Grove Road
Rockville, MD 20850

Panera Bread- 301.545.1874
14929 Shady Grove Road
Rockville, MD 20850

Chipotle Mexican Grill- 301.838.9222
14925 Shady Grove Road
Rockville, MD 20850

Mama Lucia Restaurant-301.762.8805
14921-J Shady Grove Road
Rockville, MD 20850

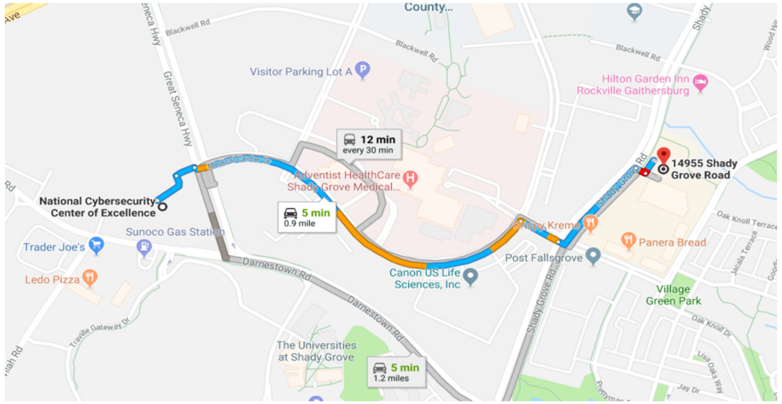
Cheesburger-Cheeseburger- 301.309.9555
14921-G Shady Grove Road
Rockville, MD 20850

Taipei Tokyo-301.738.8813
14921-D Shady Grove Road
Rockville, MD 20850

Wingstop-301.309.9464
14925 Shady Grove Road
Rockville, MD 20850

Starbucks-301.315.0096
14919 Shady Grove Road
Rockville, MD 20850

Krispy Kreme Donuts-240.453.0334
14919 Shady Grove Road
Rockville, MD 20850



Afternoon Keynote begins at 1:15pm

Economics of Interoperability – Wade Malcolm

Tuesday, November 13, 2018

9:30 am	**REGISTRATION**
10:00 am	**WELCOME AND WORKSHOP OBJECTIVES** **Chris Greer**, NIST
10:15 am	**KEYNOTE: GRID MODERNIZATION AND THE CASE FOR INTEROPERABILITY** **John Gibson,** Avista Utilities
11:00 am	**PANEL SESSION: GRID MODERNIZATION AND INTEROPERABILITY** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**LUNCH**
1:15 pm	**KEYNOTE: THE ECONOMICS OF INTEROPERABILITY** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**PLENARY: INTRODUCTION TO NIST'S SMART GRID CONCEPTUAL MODELS** **Avi Gopstein,** NIST
2:30 pm	**INTERACTIVE DISCUSSION: MAJOR CONCERNS FOR SMART GRID INTEROPERABILITY** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**BREAK**
3:45 pm	**PLENARY: THREE KEY THEMES FOR CYBERSECURITY AND GRID INTEROPERABILITY** • **Risk Profiles—Jeffrey Marron,** NIST • **Interface Categories—Nelson Hastings,** NIST • **Securing Communications—Michael Bartock,** NIST
4:45 pm	**WRAP UP AND CHARGE FOR NEXT DAY**
5:00 pm	**ADJOURN**

The Economics of Interoperability
November 13, 2018

Wade P. Malcolm, P.E.
Open Energy Solutions Inc.

Why is Interoperability Important?

- Many solutions are not (easily/cheaply) interoperable and are packaged for a single “silo” or ideal for only a single function
- To achieve lower-cost and better performance, an architecture with intelligence “at the edge” is needed
- Multi-function devices should reduce capital and O&M costs
- Standards-based, modular hardware, communications, software and messaging systems will promote interoperability, lower costs, and improve reliability
- Integration and analysis of multiple data sources creates new value based on its timeliness, location, and availability (e.g. close to where things happen)

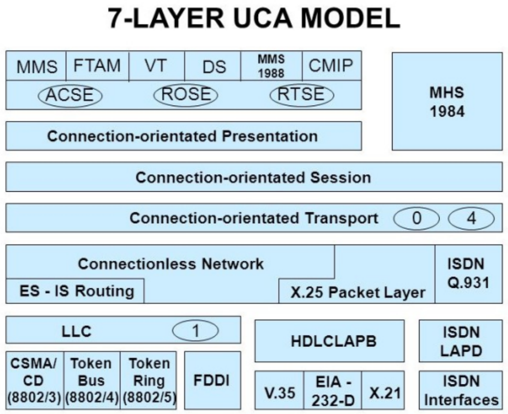
Getting some context:
Four Generations of Interoperability?

1. Energy Management Systems and SCADA

- Integration Protocols
  - Linking large centralized systems
  - WSCC
  - Others
  - SCADA Protocols
- Benefits
  - Interoperability by definition

2. Automated Meter Reading and Distribution Automation

- Profile, Protocols and the OSI Model
  - Utility Communications Architecture
    - IEC61850
    - Common Information Model – CIM (IEC61868/70)
    - ICCP / TASE.2



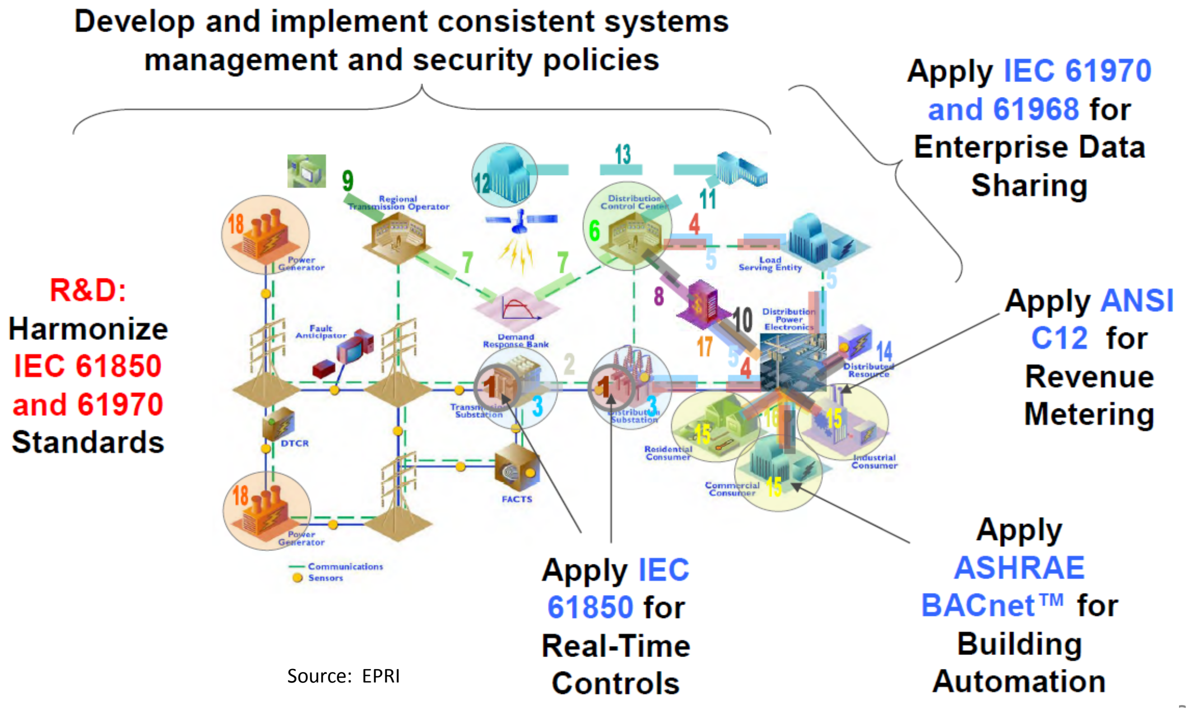
Sources: GE, EPRI

- Additional Benefits
  - Reduced integration costs
  - Reduced training costs
  - Reduced maintenance and upgrade costs
  - Vendor lock-in avoided
  - Reduced stranded assets
  - “Best of breed” deployments

3. Advanced Metering Infrastructure, Smart Grid and Advanced Distribution Automation

- Architectures
  - GridWise
  - IntelliGrid Architecture
- Systems Engineering
- Use Cases

- Additional Benefits
  - Re-use
  - Multi-function H/W, S/W



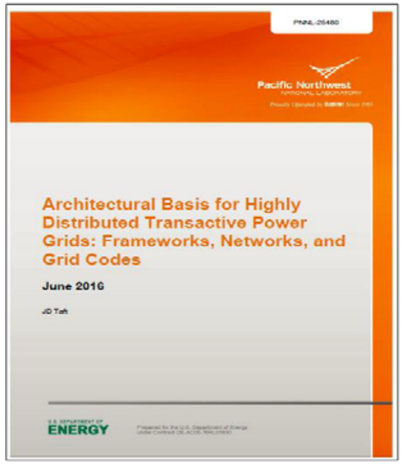
Source: EPRI

4. Distributed Energy Resource Integration, Resiliency and Transactive Energy

- Grid Architecture
  - Laminar Coordination Framework
- Distributed Intelligence
- Grid Edge Interoperability
  - Pub/Sub
- Open Field Message Bus (OpenFMB)
- "Open Distributed Systems Platform"(OpenDSP)
- Conformance and Certification

- Additional Benefits
  - Perhaps a necessity?
  - Managed migration
  - Distributed Intelligence Business Model (DIBM)
    - Stacked Benefits

DOE PNNL's Grid Architecture 2.0:
Laminar Coordination Framework (LCF)



PNNL-25480 (Courtesy of JD Taft)
Available at http://gridarchitecture.pnnl.gov/

SEPA's Open Field Message Bus (OpenFMB):
Internet of Things (IoT) Interoperability Framework

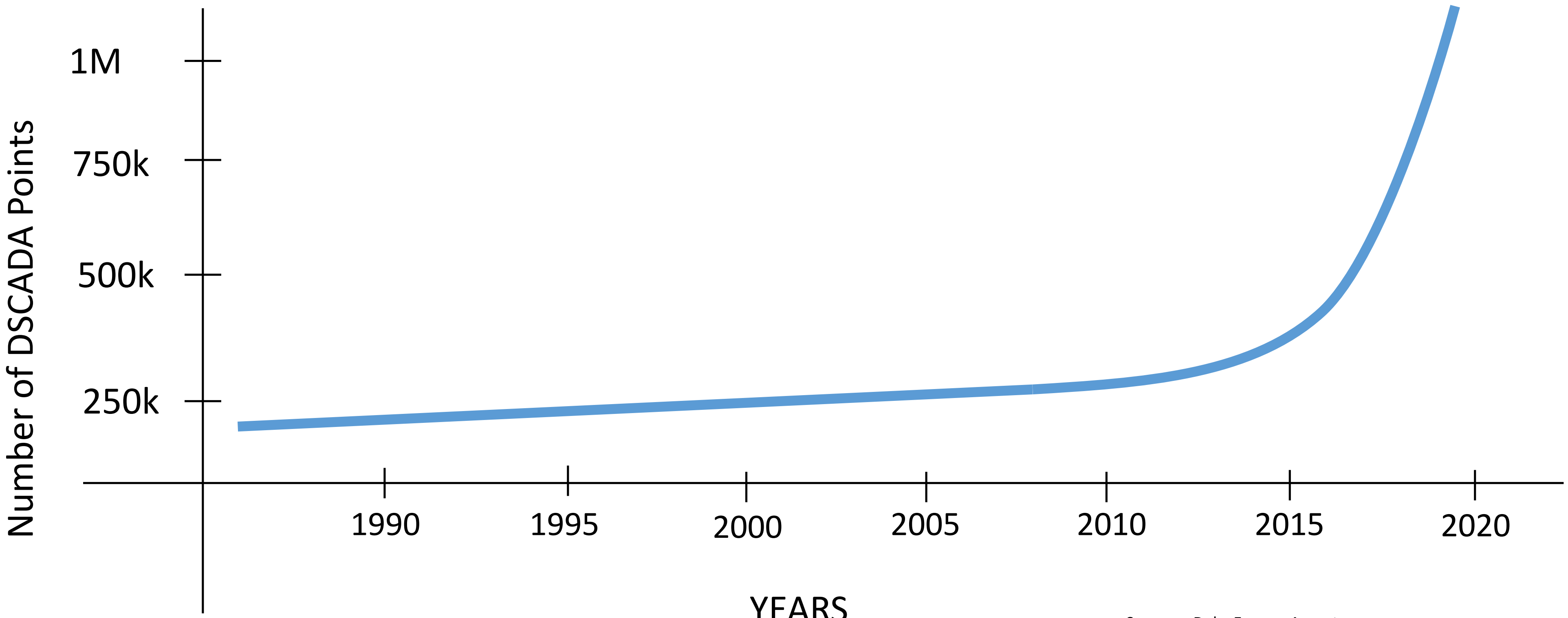
NAESB RMQ.26 Version 3.1
Please contact naesb@naesb.org

Laminar Coordination Framework for …

- Expect additional intelligent devices on the grid
- Today we have gaps of control and uncoordinated control
- No one vendor provides a true end-to-end solution
- “Local Optimization Inside Global Coordination”

Sources: Adam Smith Institute, PNNL-24044 Grid Architecture, OES Analysis

What Happens When We Outgrow our Centralized Control Systems?



Sources: Duke Energy, Accenture

Example – Duke Energy
The power of interoperability and distributed intelligence for the future

Distributed intelligence in the electric grid has the potential to significantly increase benefits realization through additional cost savings by:

- Achieving improved operational performance
- Improving system response times
- More effectively managing the scalability associated with field devices
- Driving greater insight for more efficient decision making

Interoperability is important to Duke Energy because of the benefits it creates for customers by giving them value-added services off the electric grid, and the benefits it creates for the company, making disparate systems work well together at a lower cost

Sources: Duke Energy, Accenture

OpenFMB – The Industry Catalyst for Interoperability

- Open Field Message Bus (OpenFMB^{TM}) is a reference architecture and framework for distributed intelligence
- Leverages existing standards to federate data between field devices and harmonize them with centralized systems
  - IEC Common Information Model (CIM) for semantic data model
  - Internet of Things (IoT) publish/subscribe protocols for peer-to-peer communications
- Allows scaling of operations independently, without a system-wide rollout
  - Flexible integration of renewables and storage with the existing grid
- NAESB's OpenFMB standard was led by utilities and developed by SEPA/SGIP

Source: Duke Energy

What is OpenDSP?

- OpenDSP (Open Distributed Systems Platform) is a collaborative effort led by utilities to develop a real-time operational technology (OT) platform as an extension to the DOE/PNNL DSPx concept
- OpenDSP characteristics
  - Can manage the operation of both **utility and customer assets** allowing for new service and revenue opportunities
  - Leveraging **distributed intelligence (DI) and grid edge interoperability** facilitating interaction with all vendor equipment and software
  - Delivered as an **Open Source core** with a mix of proprietary and open extensions
  - Built upon **other open source applications**
- Creating an "Energy Operating System"
- Broad market support to share cost and risk

OpenDSP: Activity and Roadmap

Where we are

- *Seeing significant OpenDSP industry engagement and interest*

OpenDSP Activity to Date

Pre-Kickoff
Jan 2018
- **DistribuTECH**
- **43 Attendees**
- **17 Utilities**

Kickoff Webinar
Mar 2018
- **87 Attendees**
- **27 Utilities**

In-Person Working Group
April 2018
- **Hosted by Xcel**
- **30 Attendees**
- **12 Utilities**

In Person Special Session
July 2018
- **Hosted by APS**

- *Arizona Public Service, Avista, Consolidated Edison, Duke Energy, Entergy and Xcel Energy have all made contributions to the effort to date*

OpenDSP Future: Initial Strategic Development Plan

Charter and Executive Commitment
Q3 2018

Core Requirements Spec
Q4 2018

Early Adopter Pilots
Q2 2019

Commercial Code Development
Q3 2019

Distributed Intelligence Functions and Use Cases for DER Integration

Function	Use Case
Voltage Management and Optimization	***1. DER Circuit Segment Management***
	2. Volt/VAR Management
	3. Solar Smoothing with PV and Advanced Inverter, and Energy Storage
Planning and Engineering	DER Integration and Interconnection
Capacity Management and Optimization	DER Optimization with Utility-Owned Inverter
	DER Optimization with Customer-Owned Inverter
	Demand Response Optimization
	DER Forecasting
Microgrid Management and Optimization	Point of Common Coupling Management of Utility-Owned Microgrid
	Point of Common Coupling Management of Customer-Owned Microgrid
Protection and Safety	Inadvertent Island Detection / Anti-islanding
	Localized Protection Alarms and Events
	Adaptive Protection
Operational Performance Improvement	Remote Device Configuration
	SCADA Point Aggregation
Resiliency & Reliability Improvement	Self Healing-Network, Radial
Market Interactions	Transactive Energy

Foundational for Distributed Coordination

Why OpenDSP? -Duke Energy

- Increasing DER penetration is forcing a new resiliency approach
- Committed to distributed intelligence and new grid-edge solutions
  - Augmenting existing legacy systems for enhanced functionality and performance
  - Addresses existing scalability and performance limitations
  - Improves cybersecurity of grid devices and telecommunications
- Interoperability emphasis provides additional benefits:
  - Enables greater choice of functionality and suppliers
  - Helps better manage integration efforts
  - Accelerates development and deployment cycles

Distributed Intelligence (DI) As An Emerging Architecture

- **DI is an architecture that supports building layered intelligence on the grid**
  - DI can occur at many locations, including the headend, node, and grid edge
  - It is a method of optimizing the location a decision is made based on primary needs – sensitivity, timeframe, system updates. It dramatically reduces the transportation of data
- **What does DI look like?**

Communications and Controls

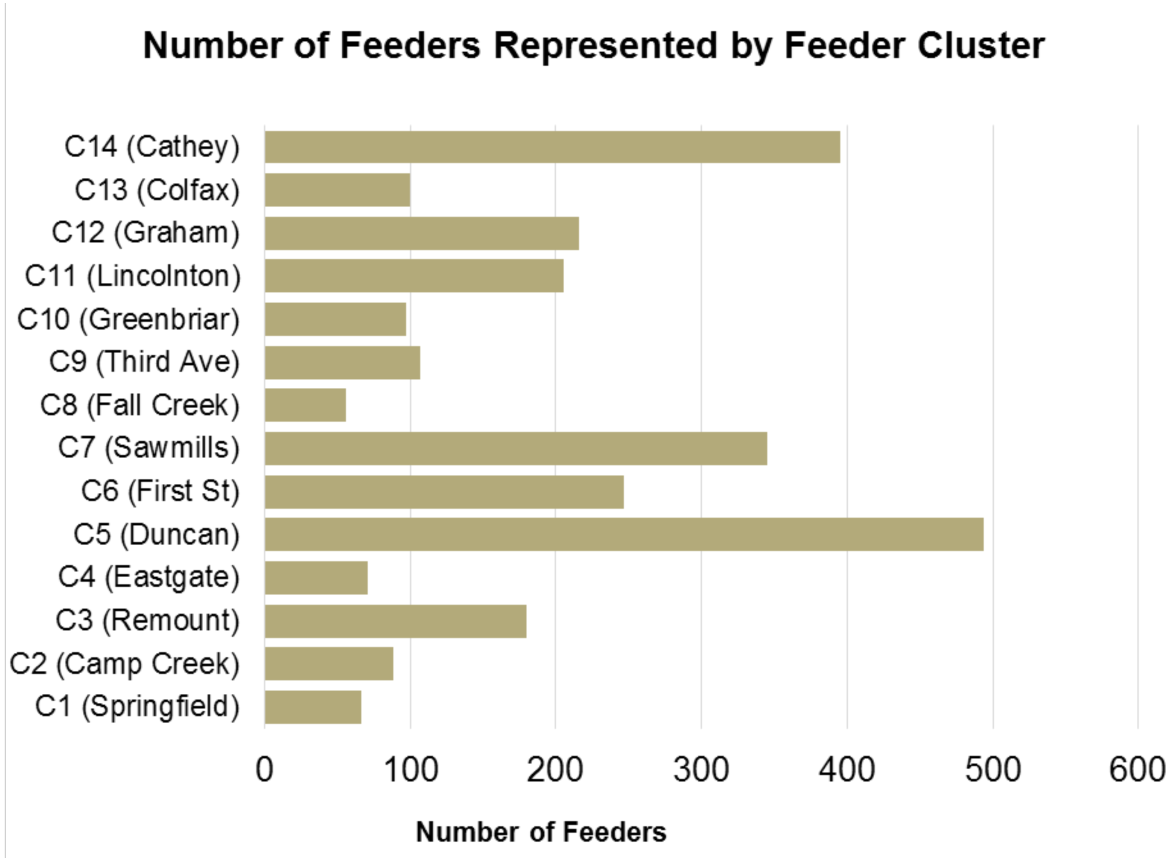
Today **Future**

DI represents an opportunity to proactively and efficiently manage grid operations on distribution circuit segments to account for growing DER and microgrid activities

Sources: Duke Energy, Navigant

Duke Energy Distributed Intelligence Business Model Project: Objectives

- **To quantify the value of DI** in a manner that recognized the value created by DI *above the value* created by individual sensors, controls, and equipment.
- Develop a comprehensive and granular theoretical model that applies 22 DI use cases to **2700 feeders** in North Carolina using 14 representative circuits.

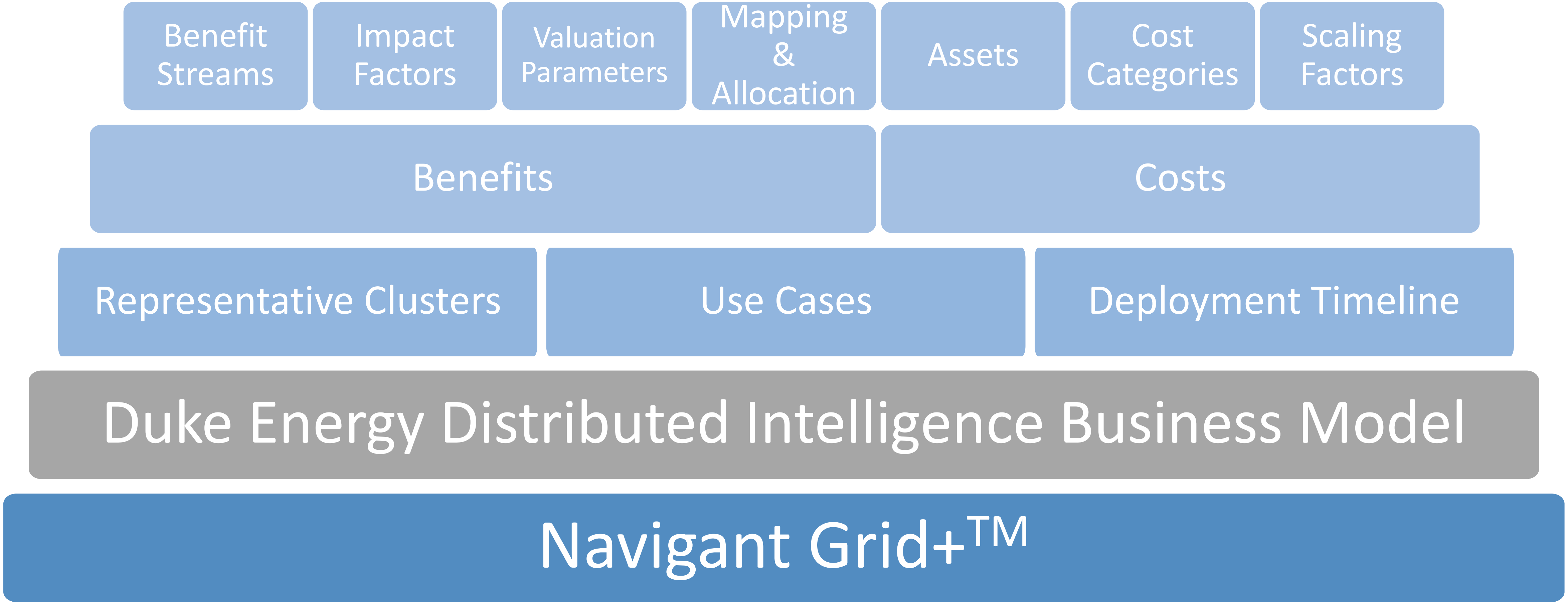


Duke Energy sought to determine whether using DI to optimize distributed grid infrastructure and operations (as new DER assets come online) ultimately drives value for the customer and the utility

Sources: Duke Energy, Navigant

DIBM Project Approach

- Navigant's Grid+™ model was used to support the DIBM development
- DIBM created a comprehensive and highly granular view of DI deployment in North Carolina



Sources: Duke Energy, Navigant

DIBM Use CASE Development

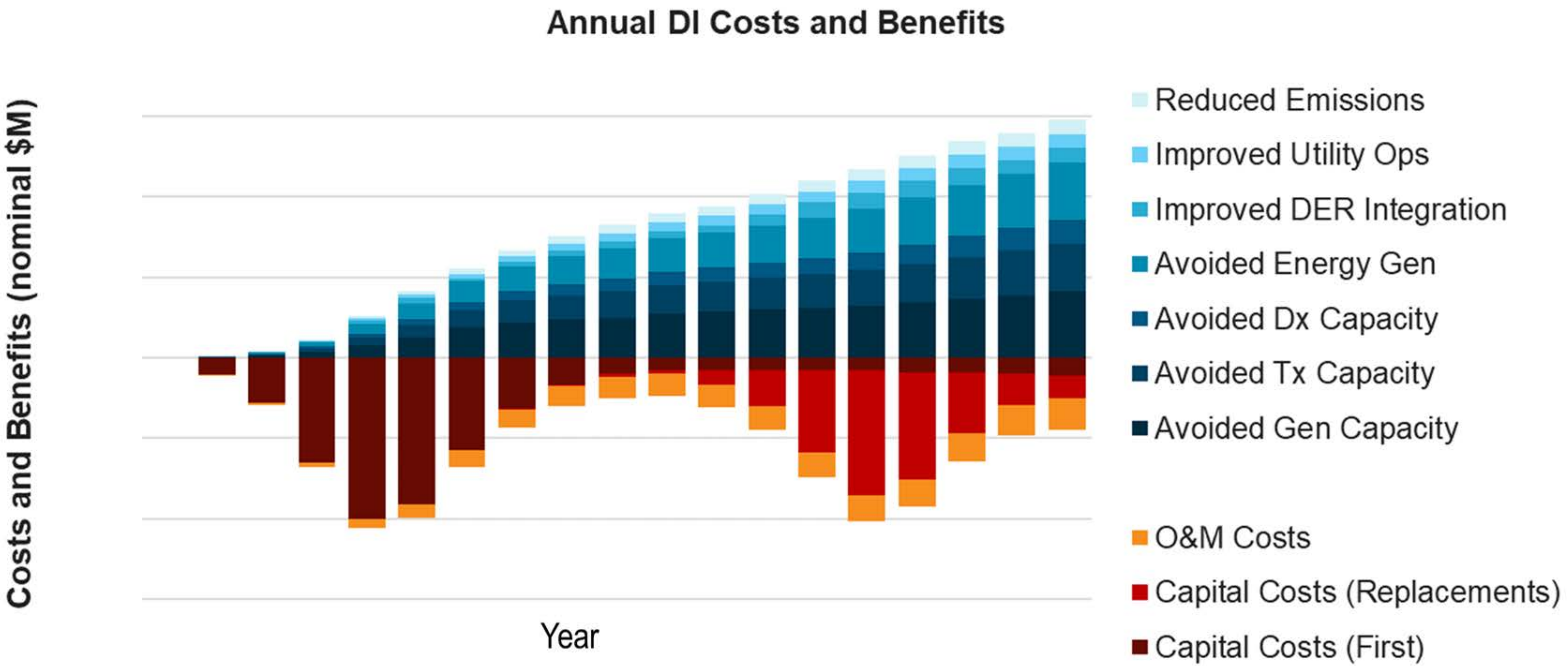
- Use cases were developed and analyzed
- Model provides granular insights for costs, benefits, scalability, and deployment timelines
- Also facilitates stacked benefits analysis to address system challenges

Use Case	Capacity Management	Voltage Management	DER Management	Utility Operations
DER Circuit Segment Management	✓	✓	✓	✓
Baseload Storage Monitoring/Mgmt.	✓		✓	
Peak Power Management	✓		✓	
DER Forecasting w/ Meters	✓		✓	
DER Forecasting w/ Weather Stations	✓		✓	
DER Optimization (Cust. Inverter)	✓		✓	
DER Optimization (DE Inverter)	✓		✓	
Demand Response Optimization	✓			
PCC Monitoring/Mgmt./Opt. (DE µgrid)	✓	✓	✓	
PCC Monitoring/Mgmt. (Cust. µgrid)	✓	✓	✓	
Volt/VAR Management	✓	✓	✓	✓
Grid Connectivity Discovery				✓
Remote Device Configuration			✓	✓
SCADA Point Aggregation			✓	✓
Enhanced COMS Network Ops. Status				✓
Improve Asset Maint. Practices				✓
Localized Protection Alarms & Events			✓	✓
Self Healing Radial Network			✓	✓
Solar Smoothing		✓	✓	
Solar Smoothing (+Battery)		✓	✓	
Inadvertent Island Detection			✓	
DER Integration & Interconnection			✓	

Sources: Duke Energy, Navigant

Benefits And Costs Over Deployment Timeframe

Analysis considers benefits and costs accrued over time through a theoretical deployment



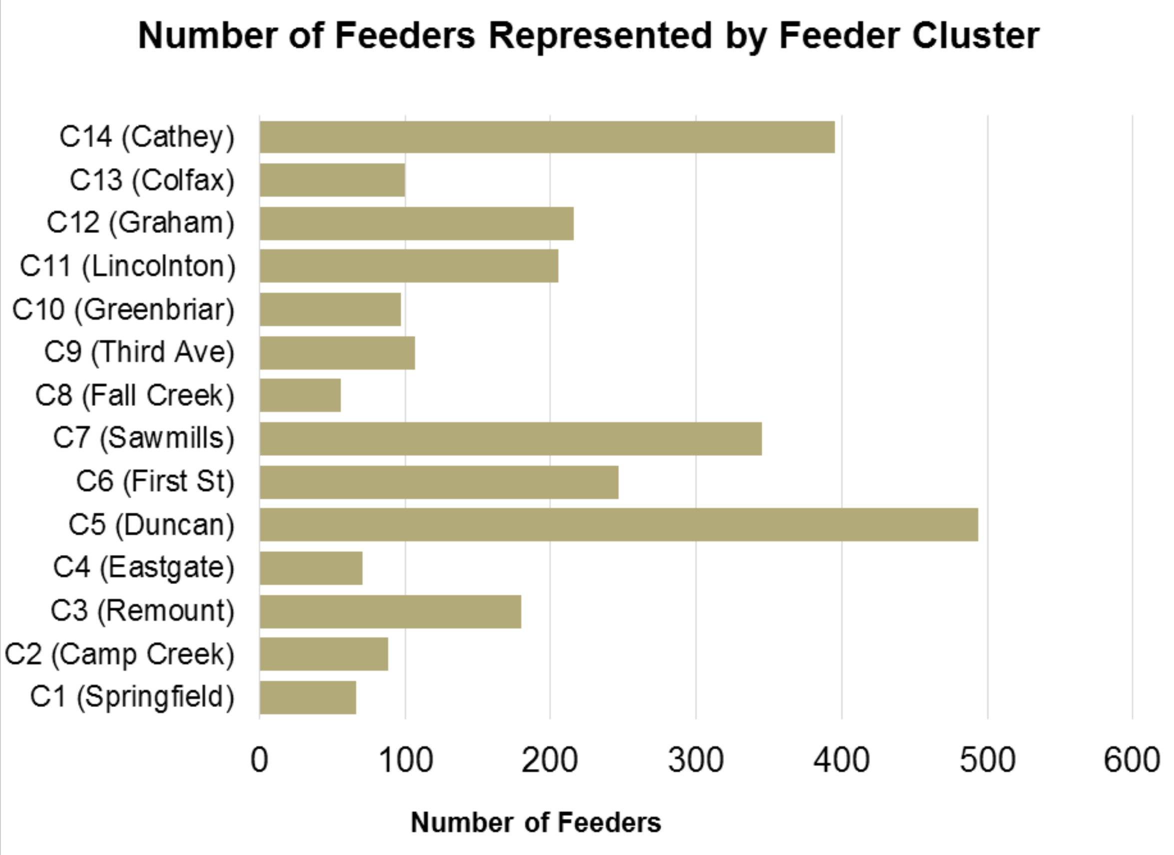
Sources: Duke Energy, Navigant

A Targeted Approach Increases Value

In the early years, an optimal business case should leverage a targeted approach that maximizes system value.

A stronger business case considers:

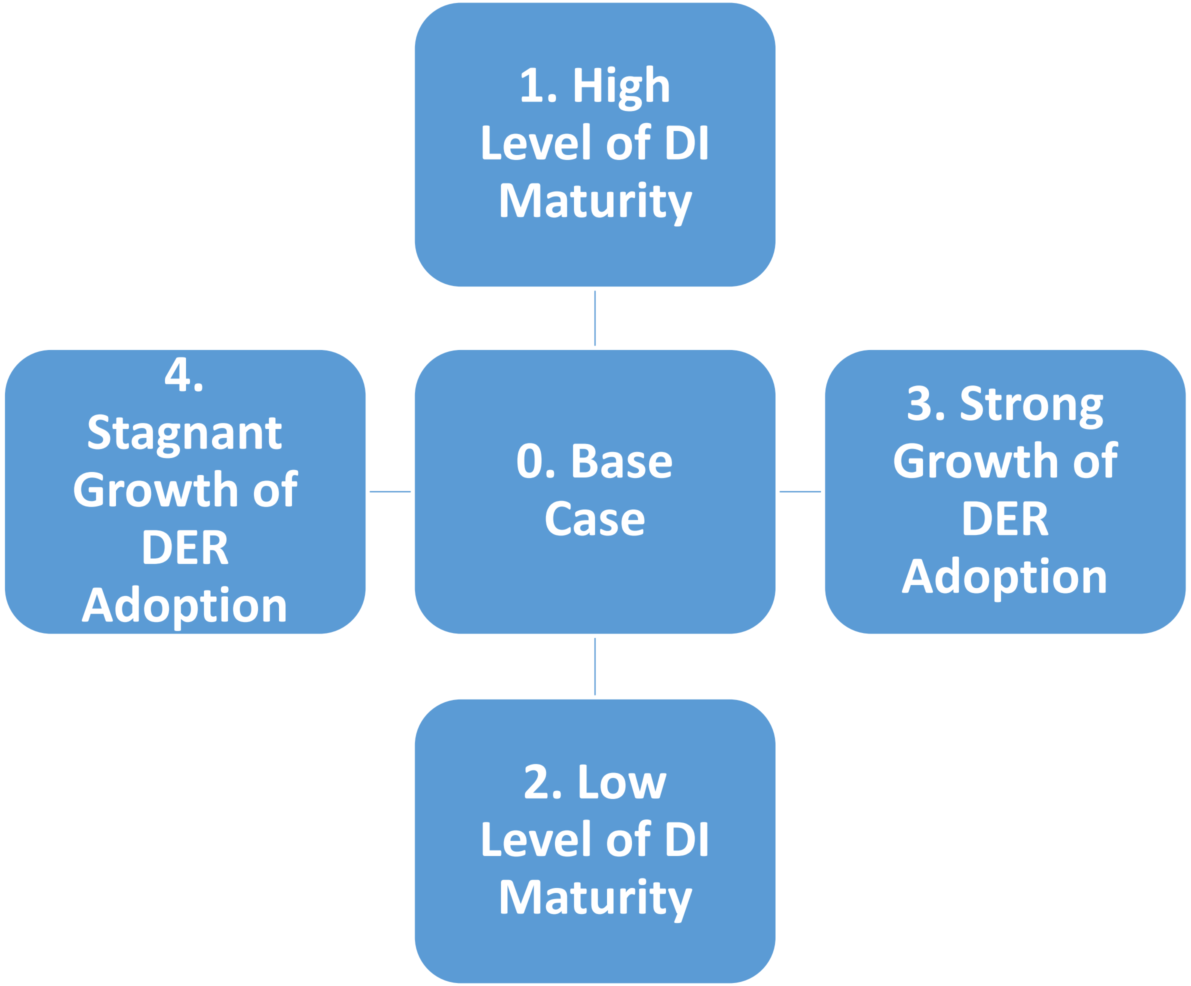
- Feeder characteristics. Ex: DER penetration, sites, and sizes, as well as customer type and count.
- Segmented installations instead of broad-brush system deployments



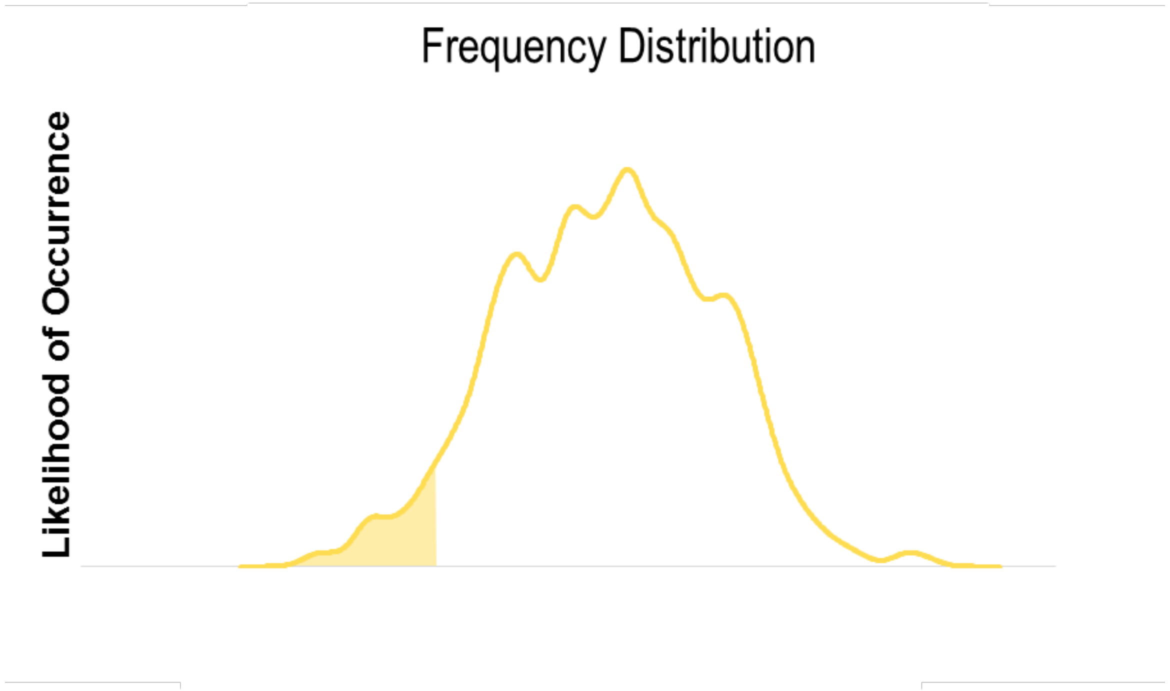
Sources: Duke Energy, Navigant

Scenario And Sensitivity Analysis

Analysis was conducted on four scenarios representing alternate future states



Every benefit and cost input factor could be individually adjusted for ranges of uncertainty



Sources: Duke Energy, Navigant

DIBM Project Insights

- Assuming a theoretical deployment timeline, the DIBM results informed Duke Energy on the incremental value a DI and OpenFMB enabled solution can unlock
- It reinforced the need for utility and vendor community engagement
- A DI enabled product suite will be critical to future success
- DIBM is available to help other utilities investigate Distributed Intelligence approaches
- A positive outcome was determined along with some specific insights
- Duke Energy is working to make more DIBM related work available in 2019

Sources: Duke Energy, Navigant, OES Analysis

Conclusion

- Regulation and legislation will still significantly impact how utilities continue to transform
- At some point, traditional control may no longer be a viable option
- The evolution of interoperability has enabled new coordination and control schemes to be able to address future needs economically

Introduction to NIST’s Smart Grid Models – Avi Gopstein

Tuesday, November 13, 2018	
9:30 am	**REGISTRATION**
10:00 am	**WELCOME AND WORKSHOP OBJECTIVES** **Chris Greer**, NIST
10:15 am	**KEYNOTE: GRID MODERNIZATION AND THE CASE FOR INTEROPERABILITY** **John Gibson,** Avista Utilities
11:00 am	**PANEL SESSION: GRID MODERNIZATION AND INTEROPERABILITY** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**LUNCH**
1:15 pm	**KEYNOTE: THE ECONOMICS OF INTEROPERABILITY** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**PLENARY: INTRODUCTION TO NIST’S SMART GRID CONCEPTUAL MODELS** **Avi Gopstein**, NIST
2:30 pm	**INTERACTIVE DISCUSSION: MAJOR CONCERNS FOR SMART GRID INTEROPERABILITY** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**BREAK**
3:45 pm	**PLENARY: THREE KEY THEMES FOR CYBERSECURITY AND GRID INTEROPERABILITY** • **Risk Profiles—Jeffrey Marron**, NIST • **Interface Categories—Nelson Hastings**, NIST • **Securing Communications—Michael Bartock**, NIST
4:45 pm	**WRAP UP AND CHARGE FOR NEXT DAY**
5:00 pm	**ADJOURN**

Introduction to NIST’s Smart Grid Conceptual Models

Avi Gopstein

Associate Director & Smart Grid Program Manager

National Institute of Standards and Technology

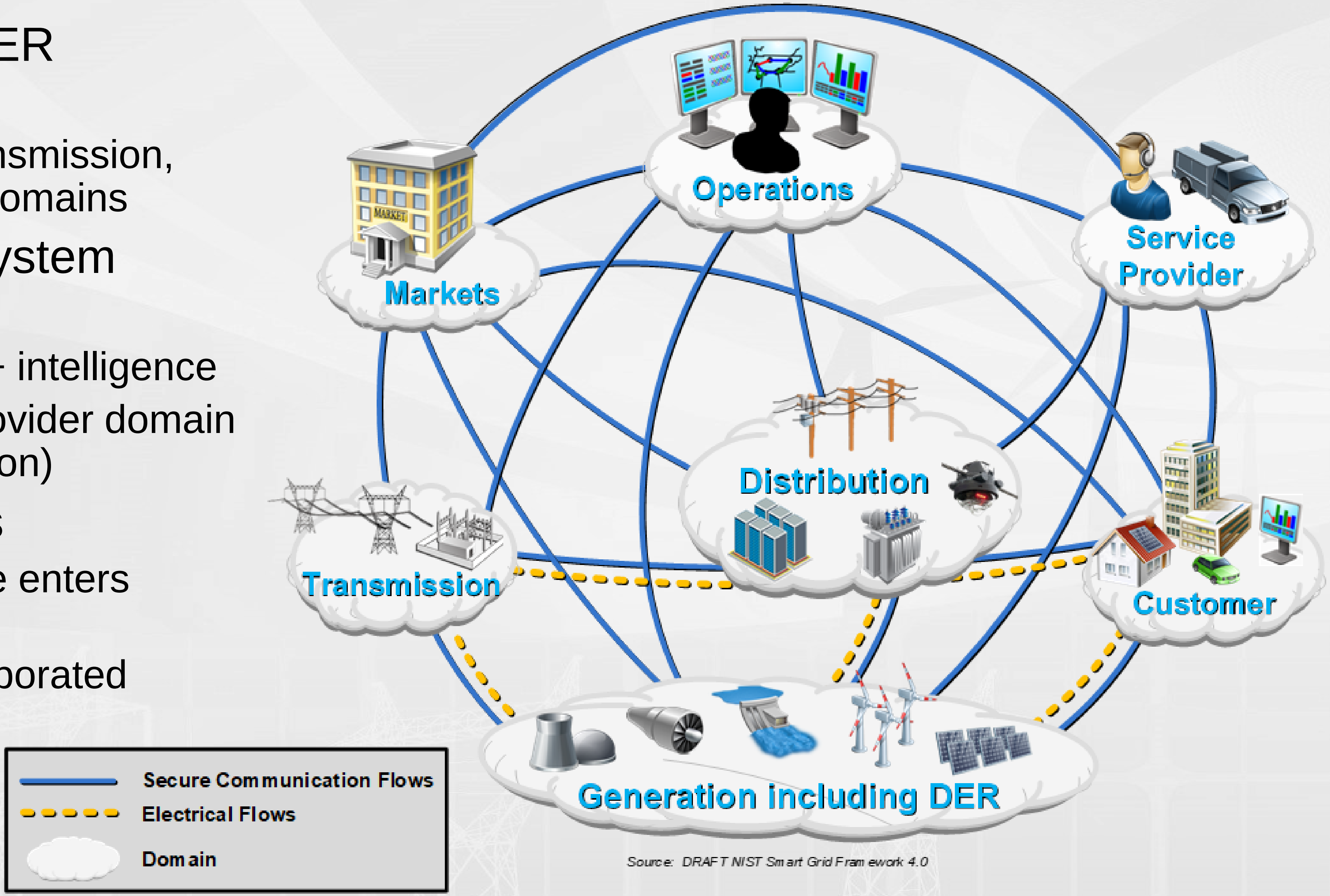
U.S. Department of Commerce

November 13-14, 2018

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

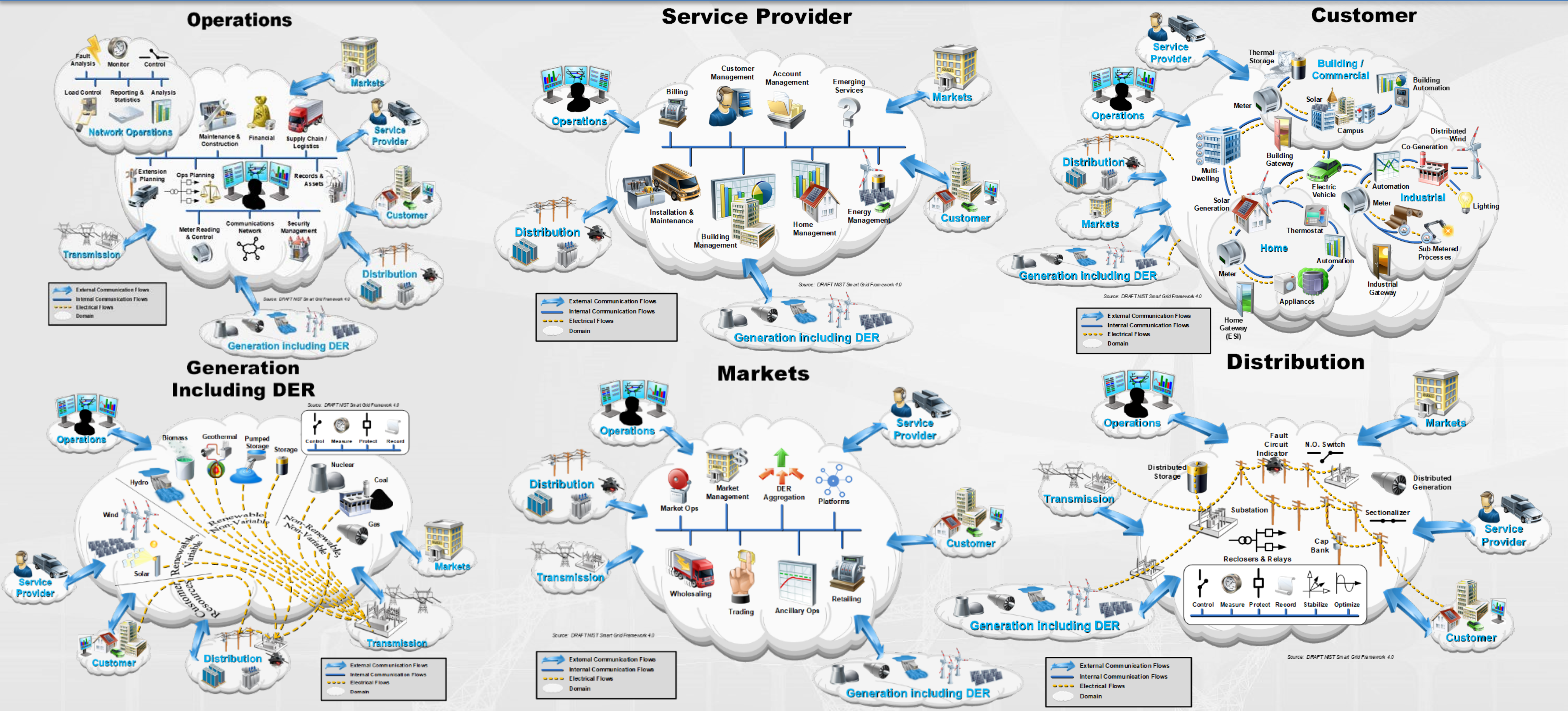
Smart Grid Conceptual Model (2018, Draft)

- Generation including DER
  - Technology diversity
  - Physical proximity to transmission, distribution + customer domains
- Intelligent distribution system
  - Increasing importance
  - Improved controllability + intelligence
  - Connected to service provider domain (e.g., congestion mitigation)
- Empowered consumers
  - Operations & intelligence enters customer domain
  - Customer diversity incorporated
- Emerging Markets
  - Platforms



Source: DRAFT NIST Smart Grid Framework 4.0

Conceptual Model Domains (2018, Draft)

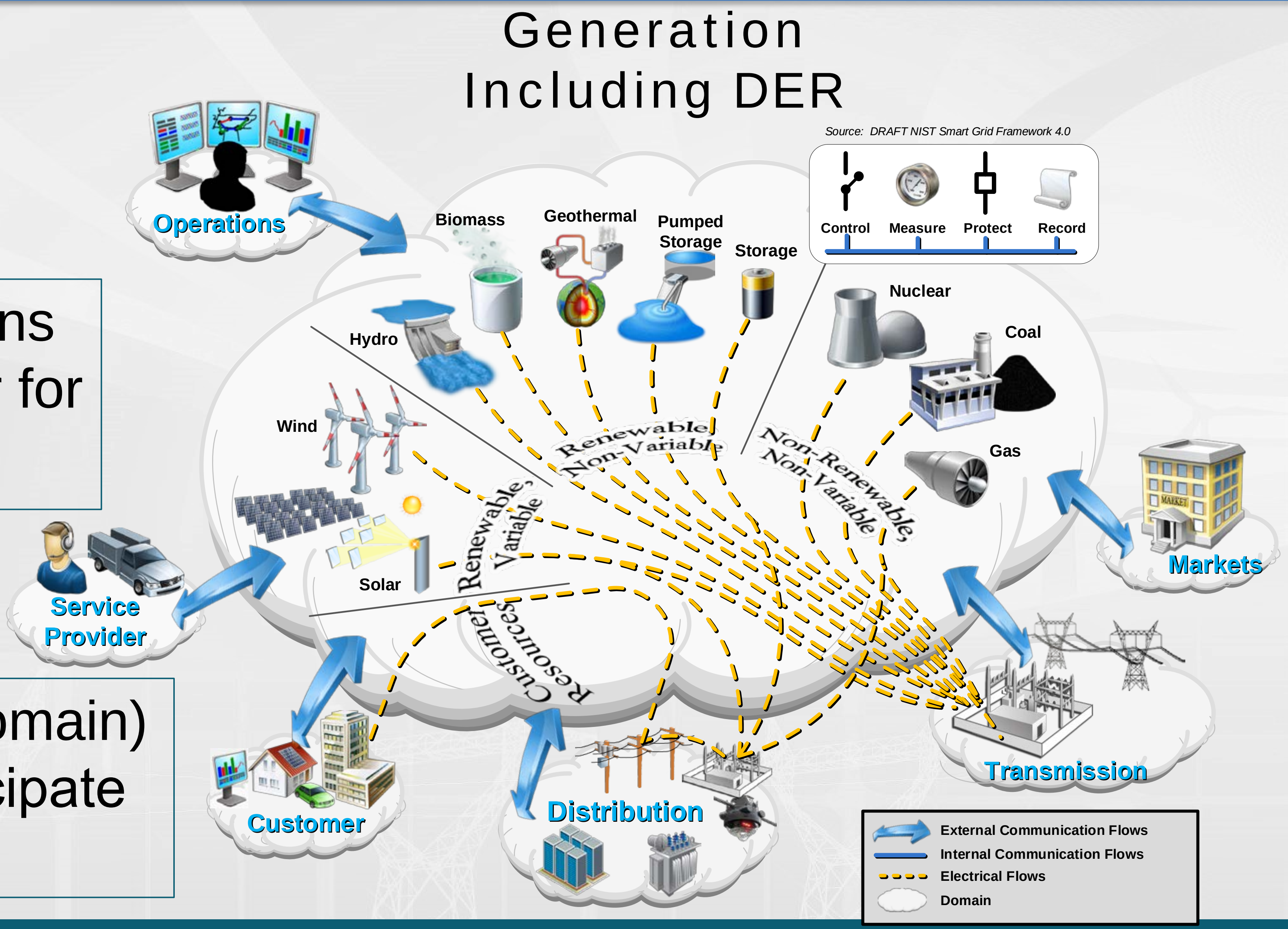


https://www.nist.gov/document/draftsmartgridconceptualmodelupdatev3pdf

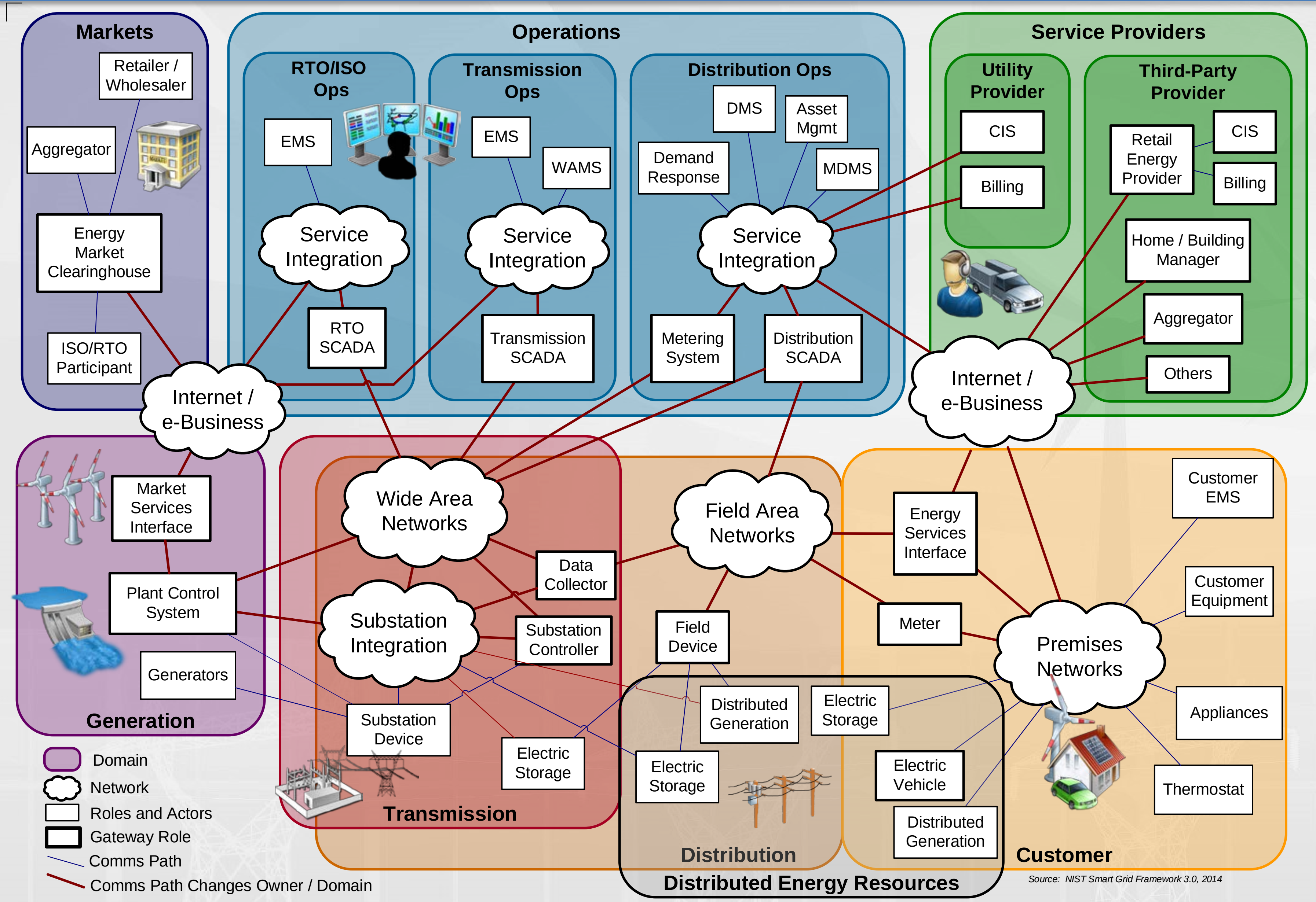
Generation Including DER Domain

Distribution Domain gains role of supply integrator for distributed resources

End-user (Customer Domain) resources (↑ or ↓) participate as supply options

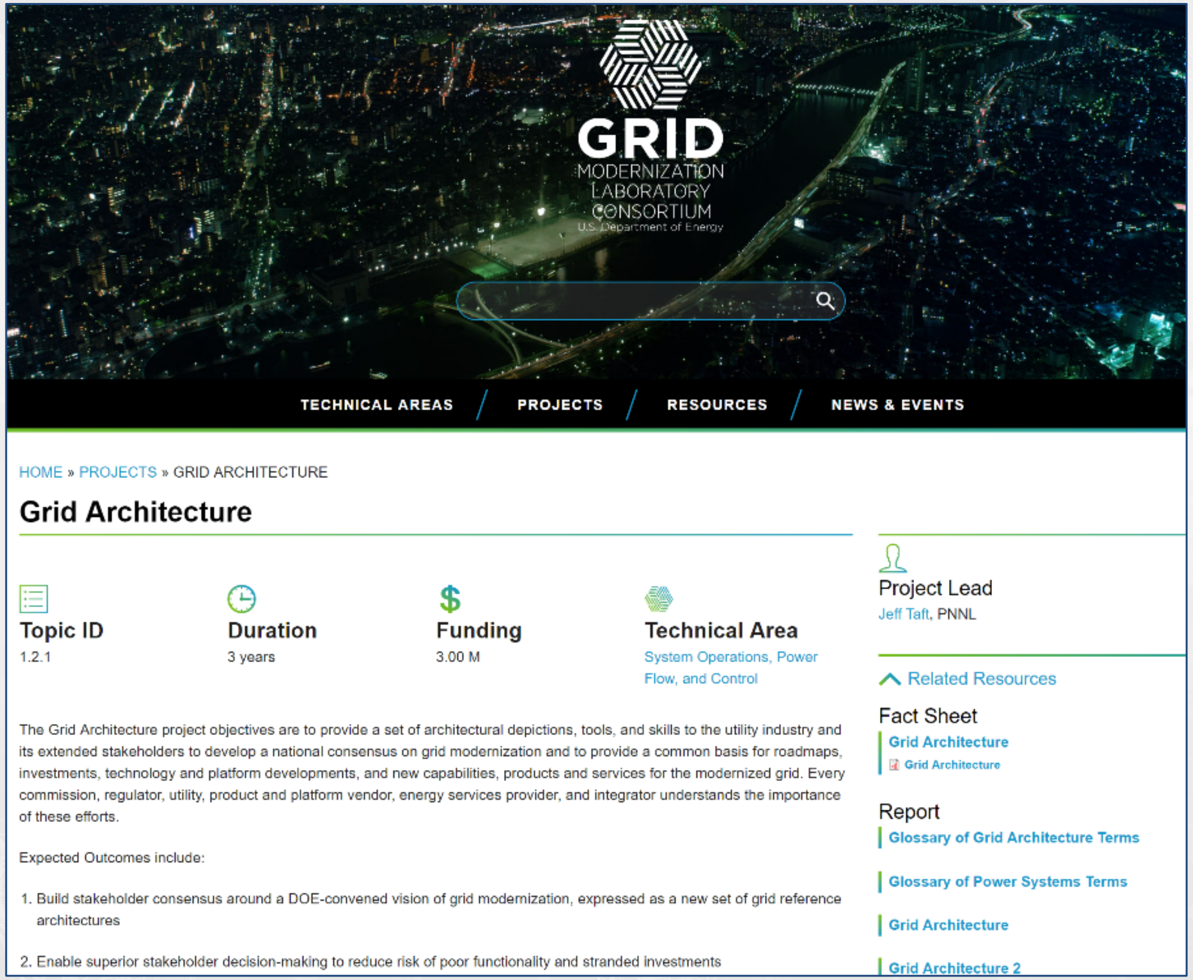


Communication Pathways Diagram—Legacy Utility

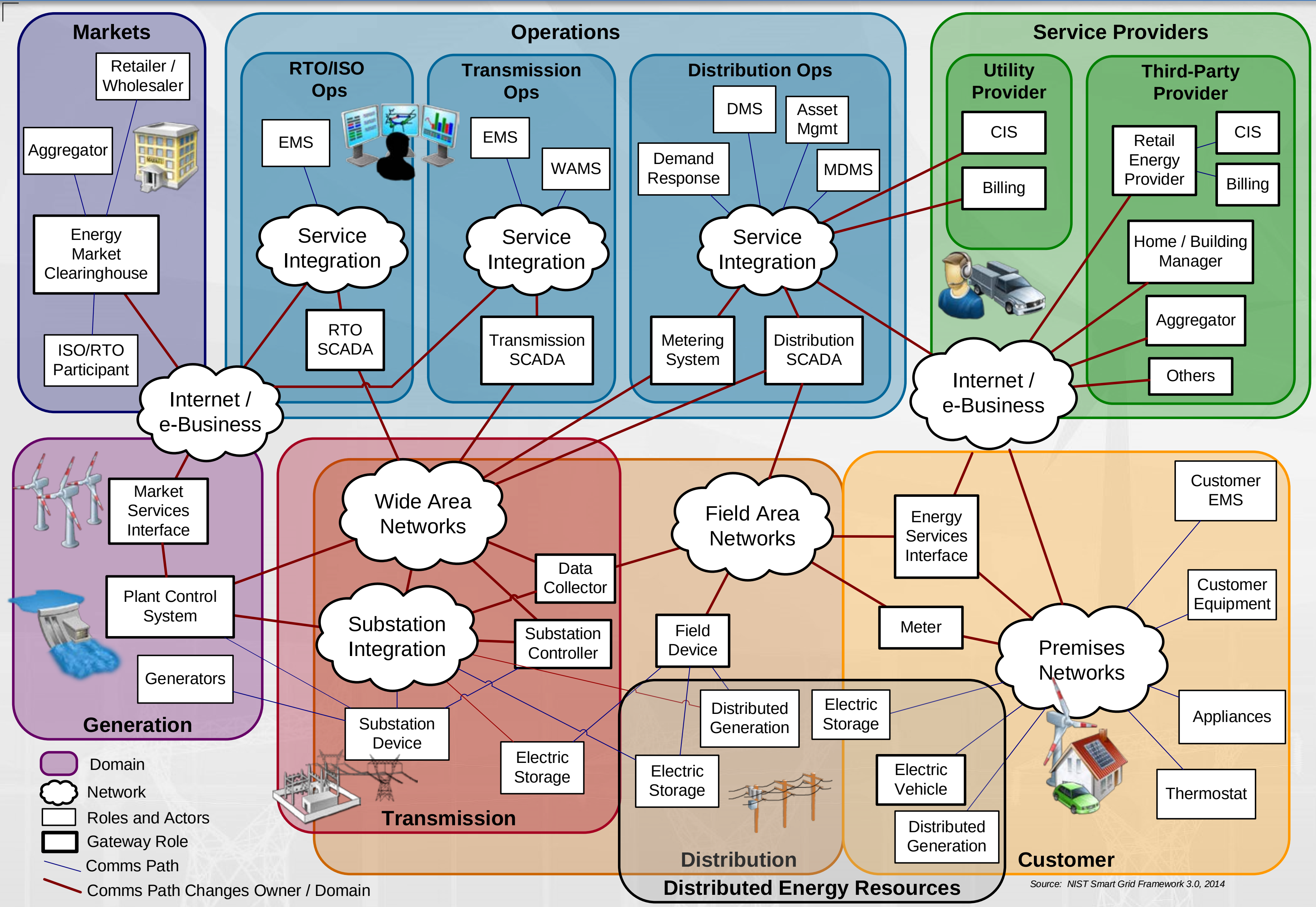


NIST perspective

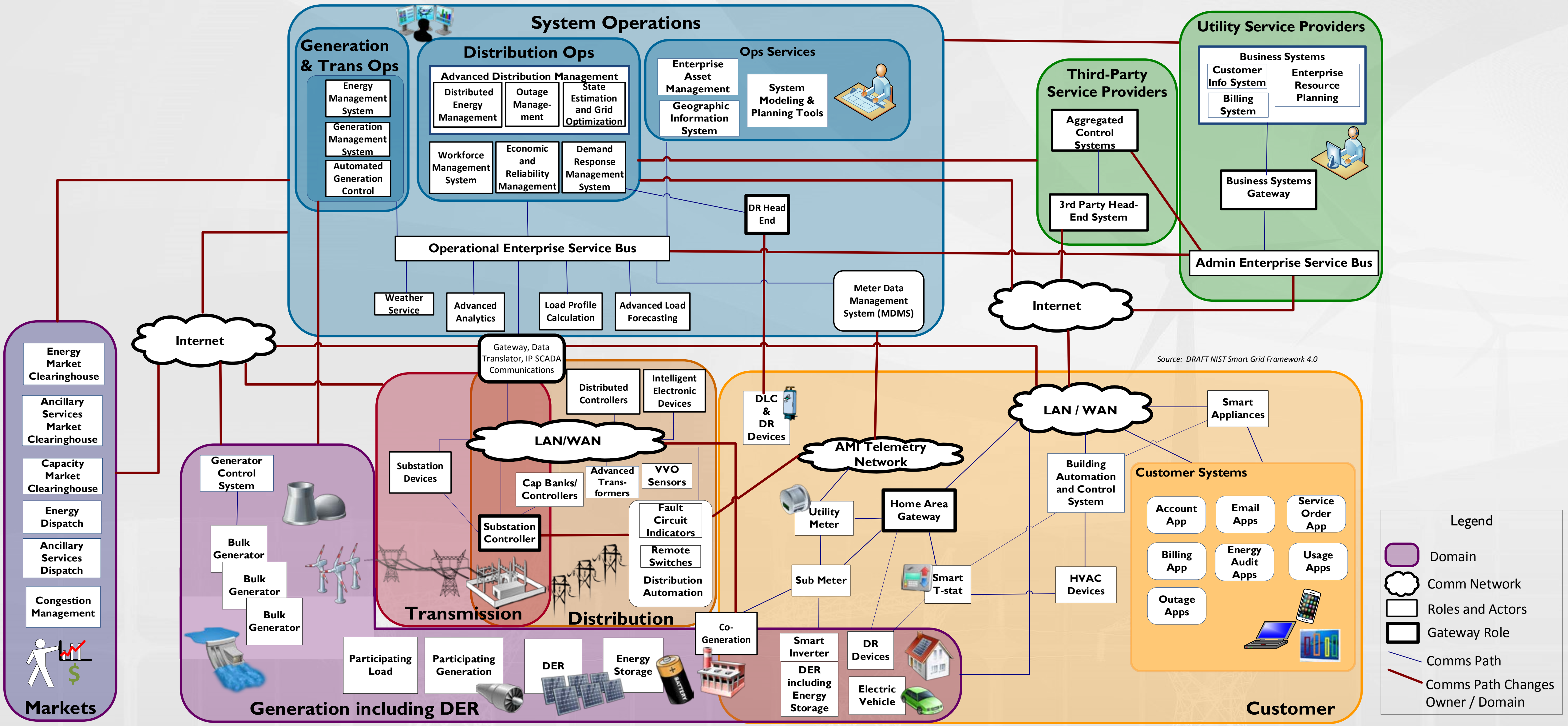
- Grid architectures are changing
  - Driven by technology and policy
- Changes will impact
  - Operations
  - Economics
  - Cybersecurity
  - Testing & Certification
- No single architecture is “correct”
- NIST are not architects



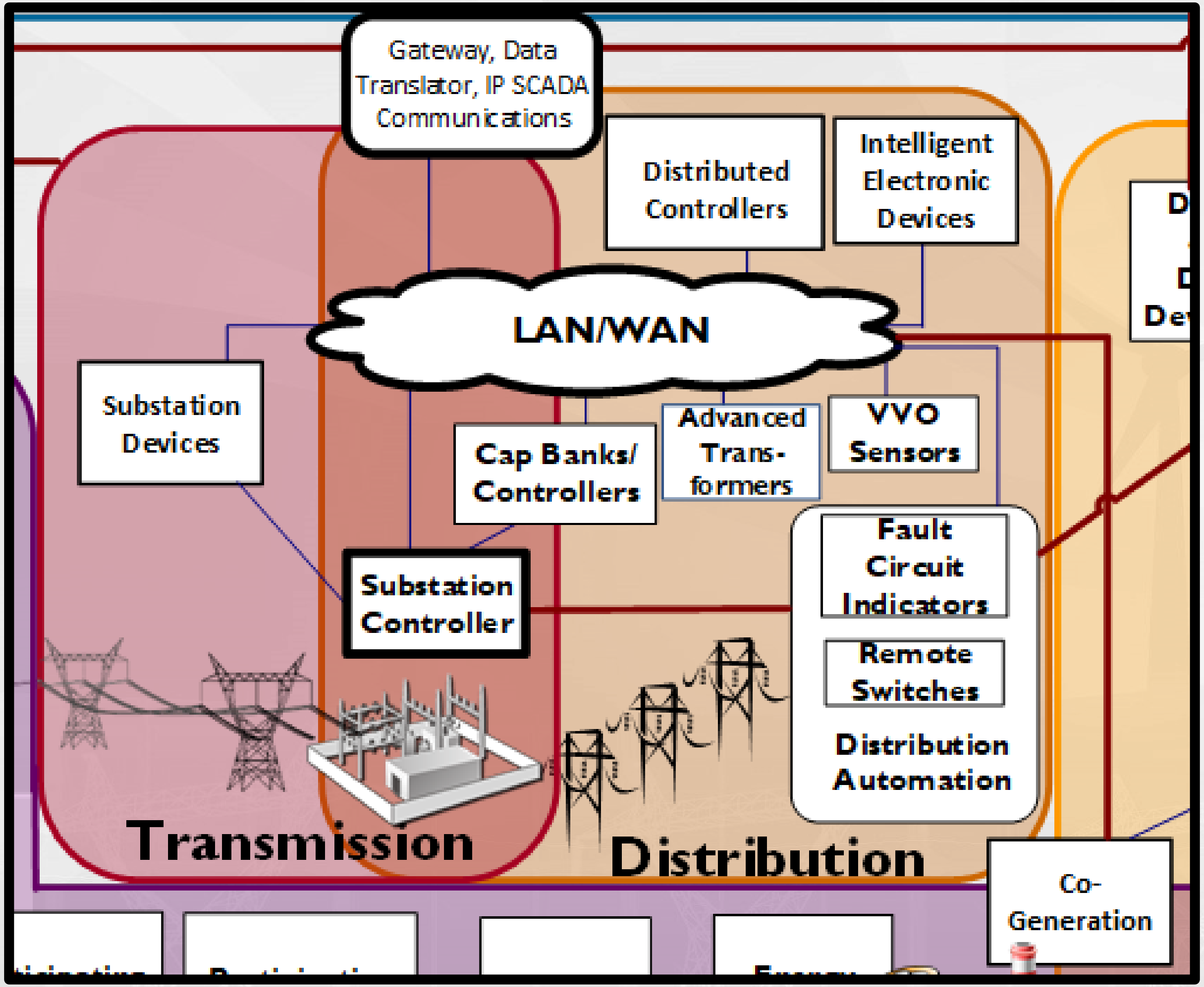
Legacy Communication Pathways Scenario



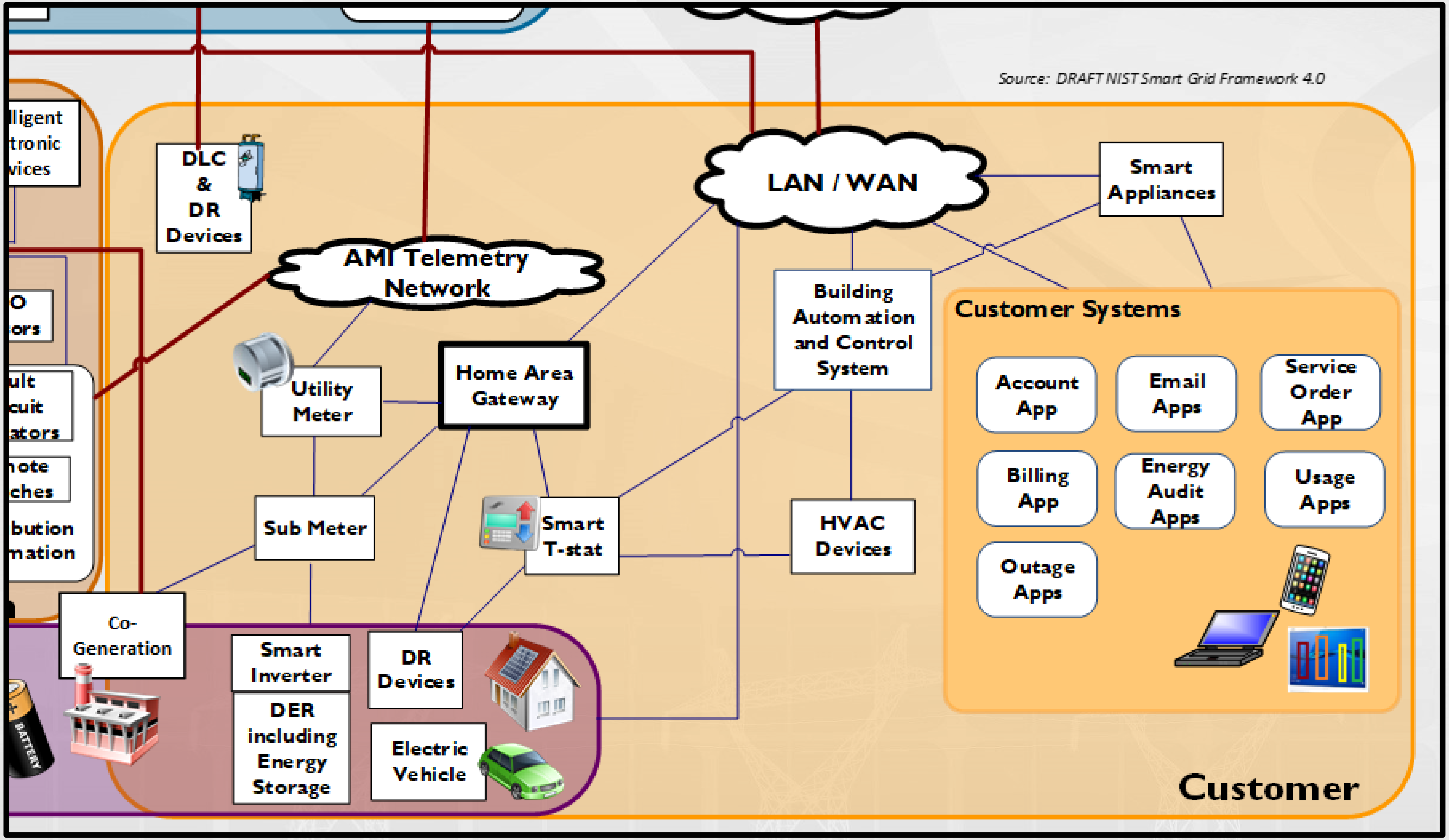
High-DER Communication Pathways Scenario



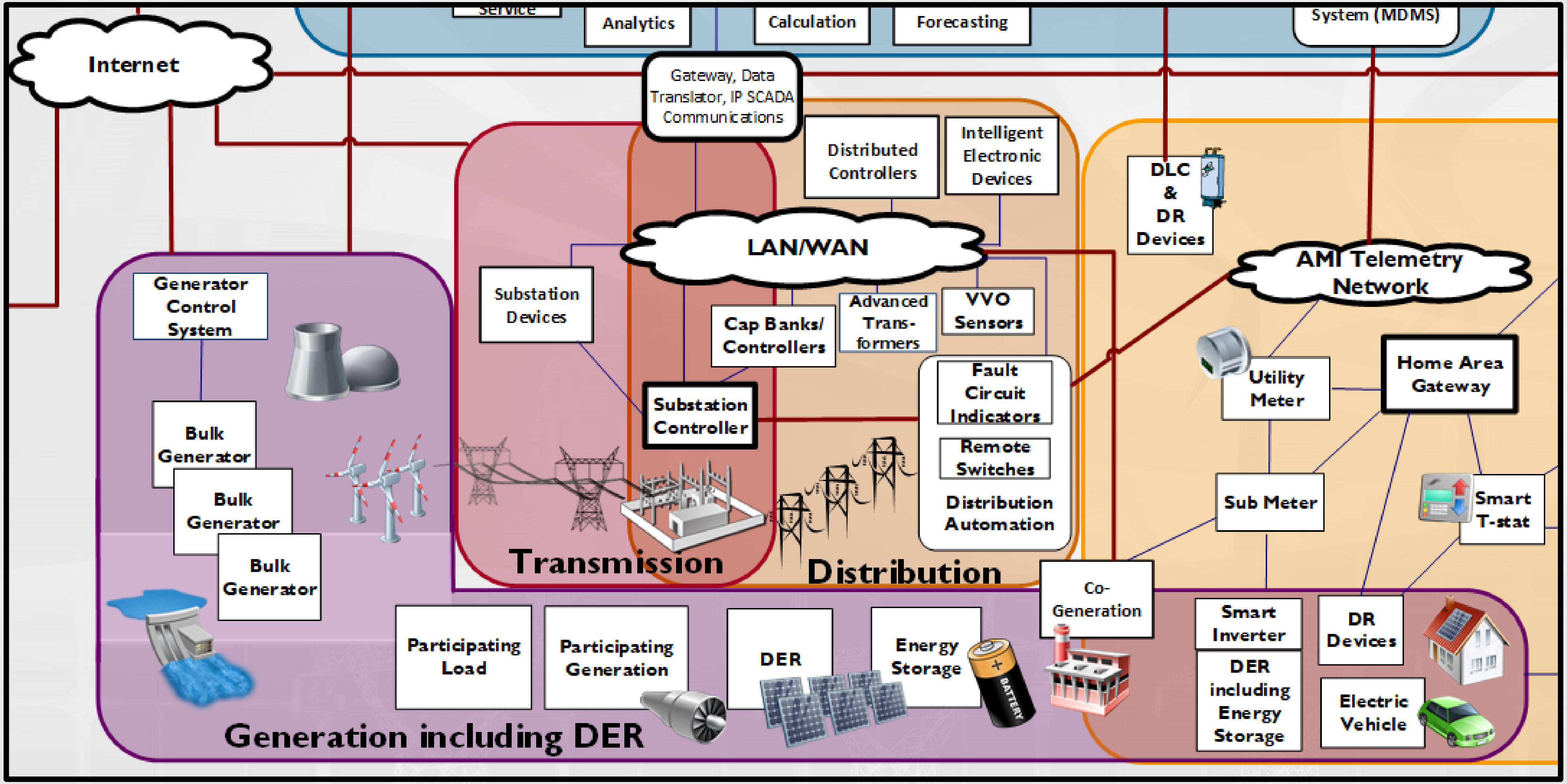
Detail—Transmission/Distribution substation



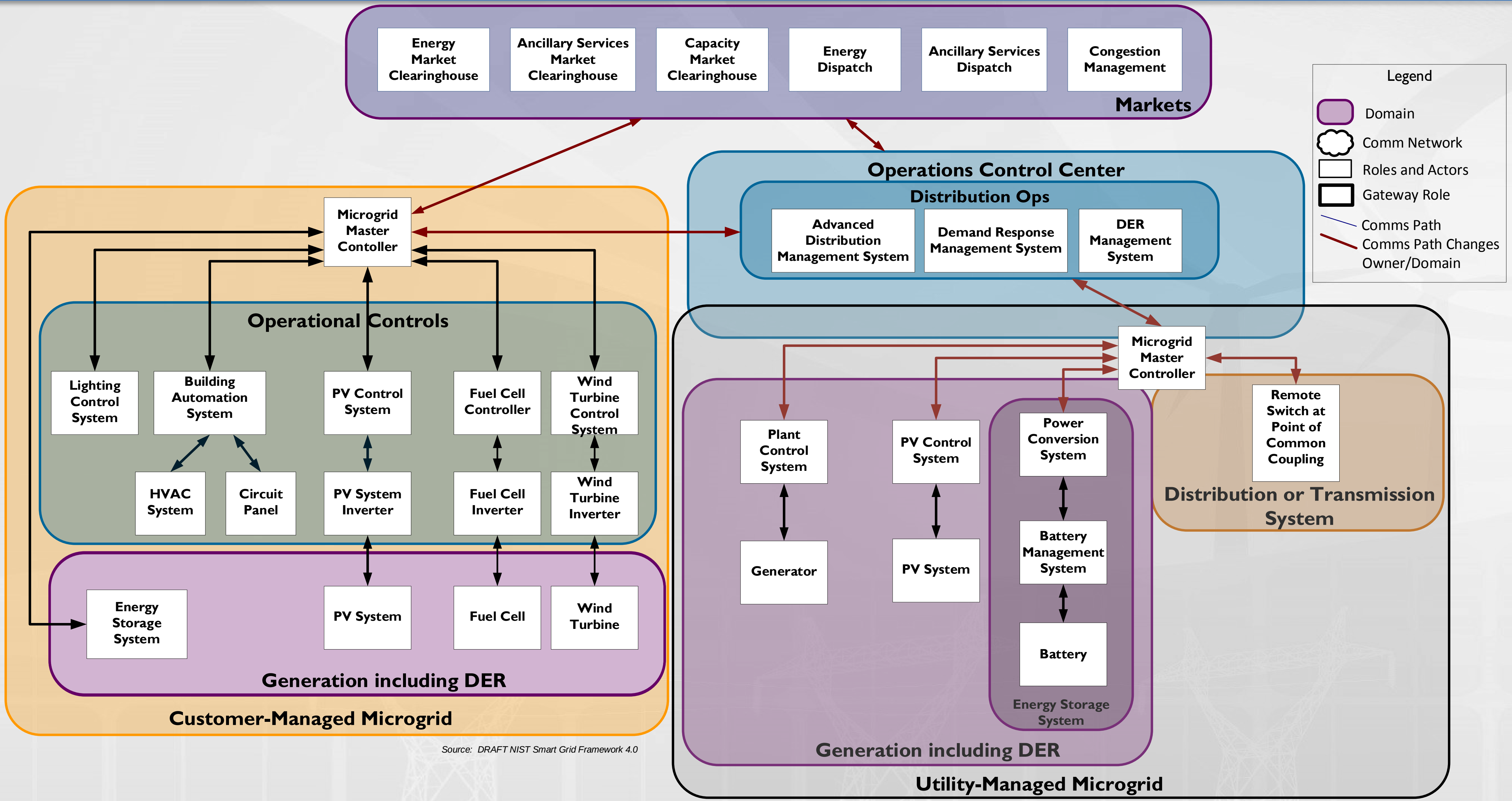
Detail—Customer Domain



Detail—Generation Domain

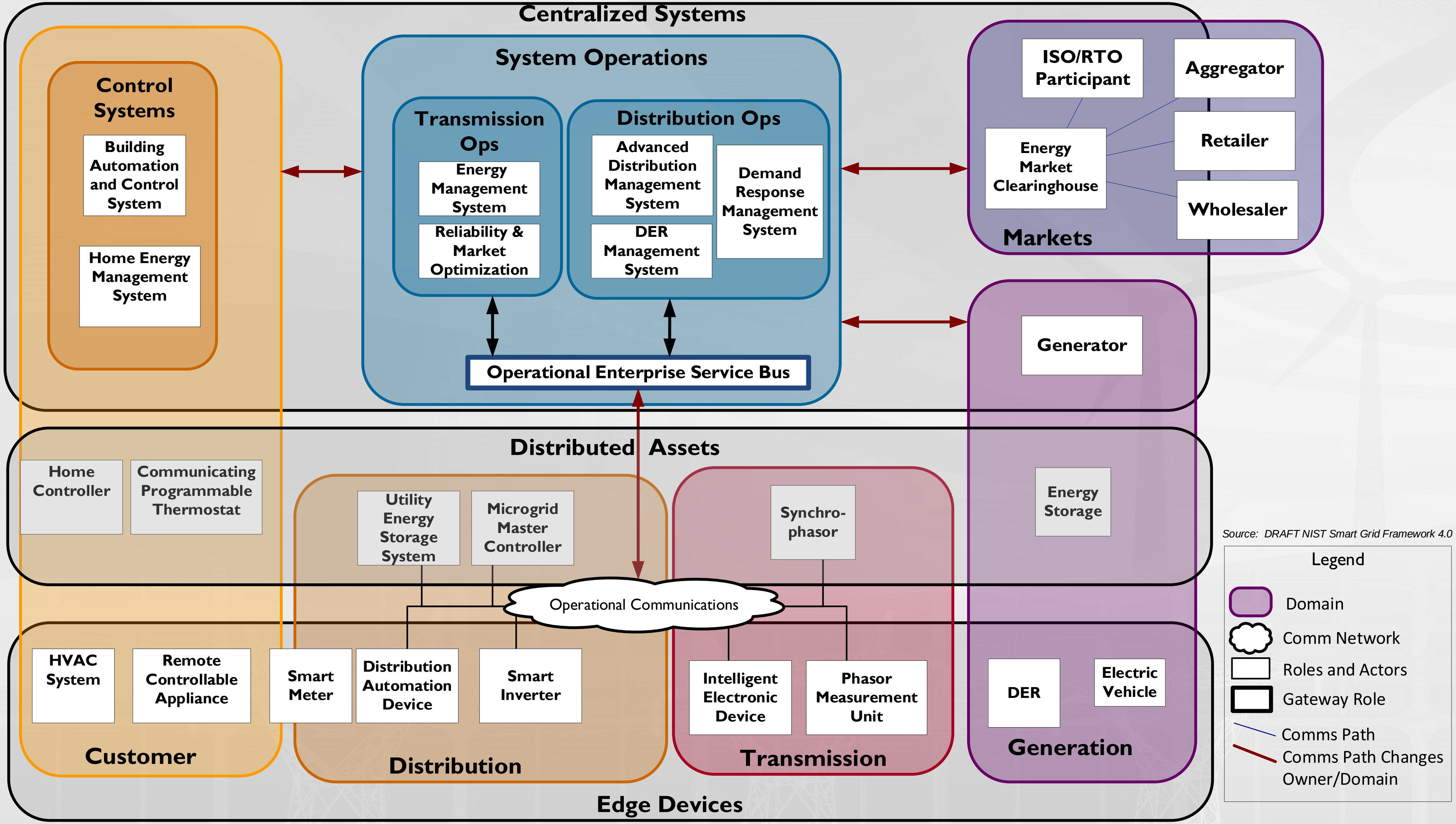


Microgrid Communication Pathways Scenario



Source: *DRAFT NIST Smart Grid Framework 4.0*

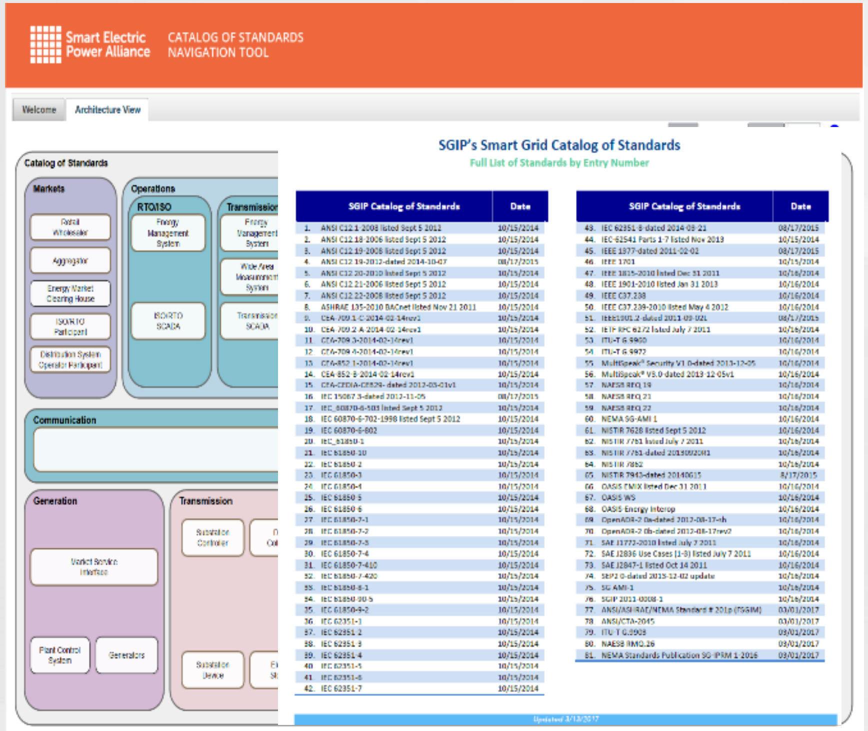
Hybrid Utility Communication Pathways Scenario



What does all of this mean for how we operate a modern grid?

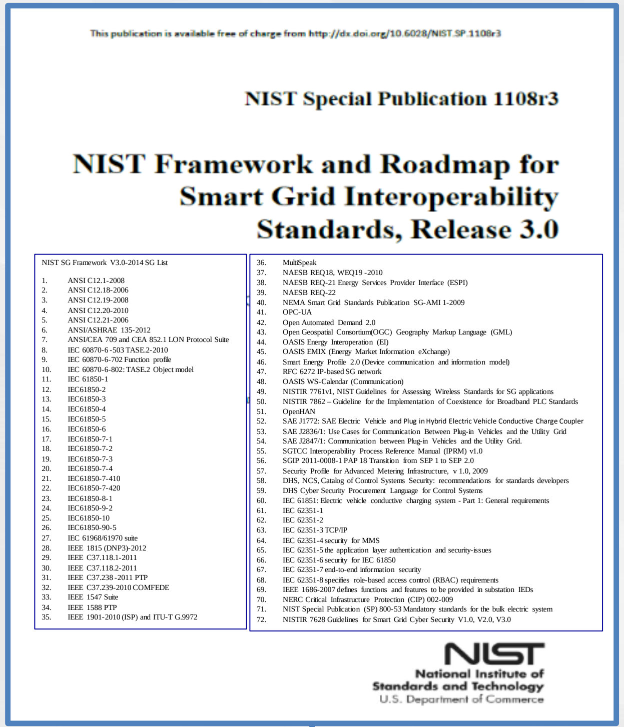
Interoperability standards landscape assessment

SEPA/SGIP SG CoS List



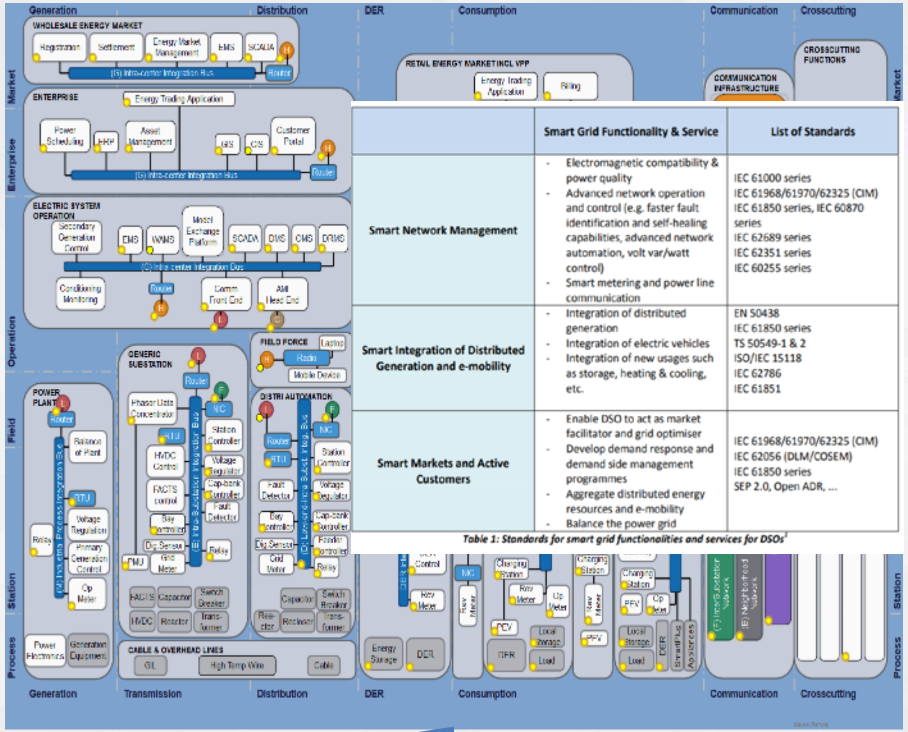
Source: http://www.gridstandardsmap.com/

Identified SG Standard List of NIST Framework R3.0



https://www.nist.gov/news-events/news/2014/10/nist-releases-final-version-smart-grid-framework-update-30

DSO Priority List



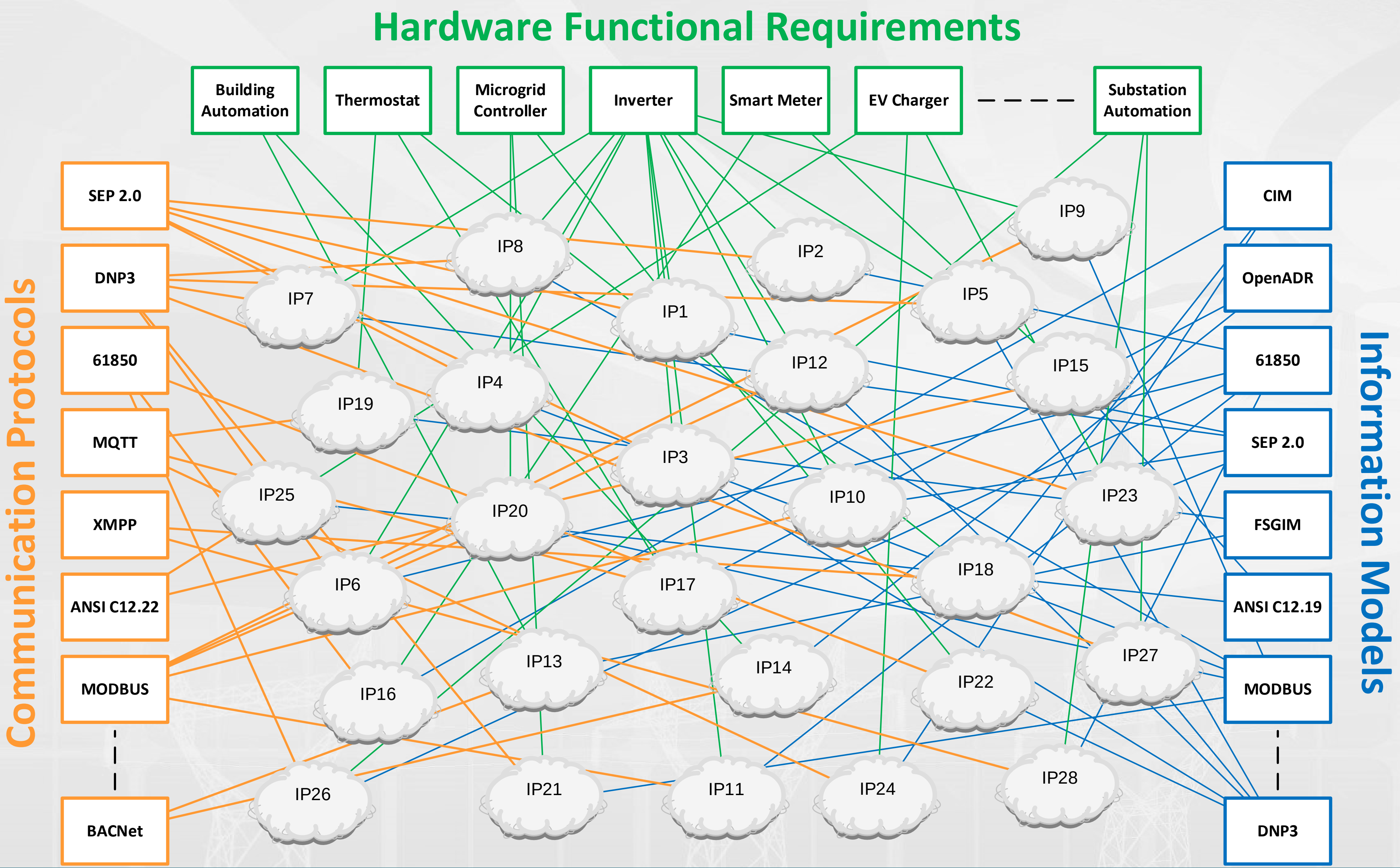
Source: https://www.edsoforsmartgrids.eu/wp-content/uploads/public/DSO-Priorities-Smart-Gird-Standardisation.pdf

New Standards:

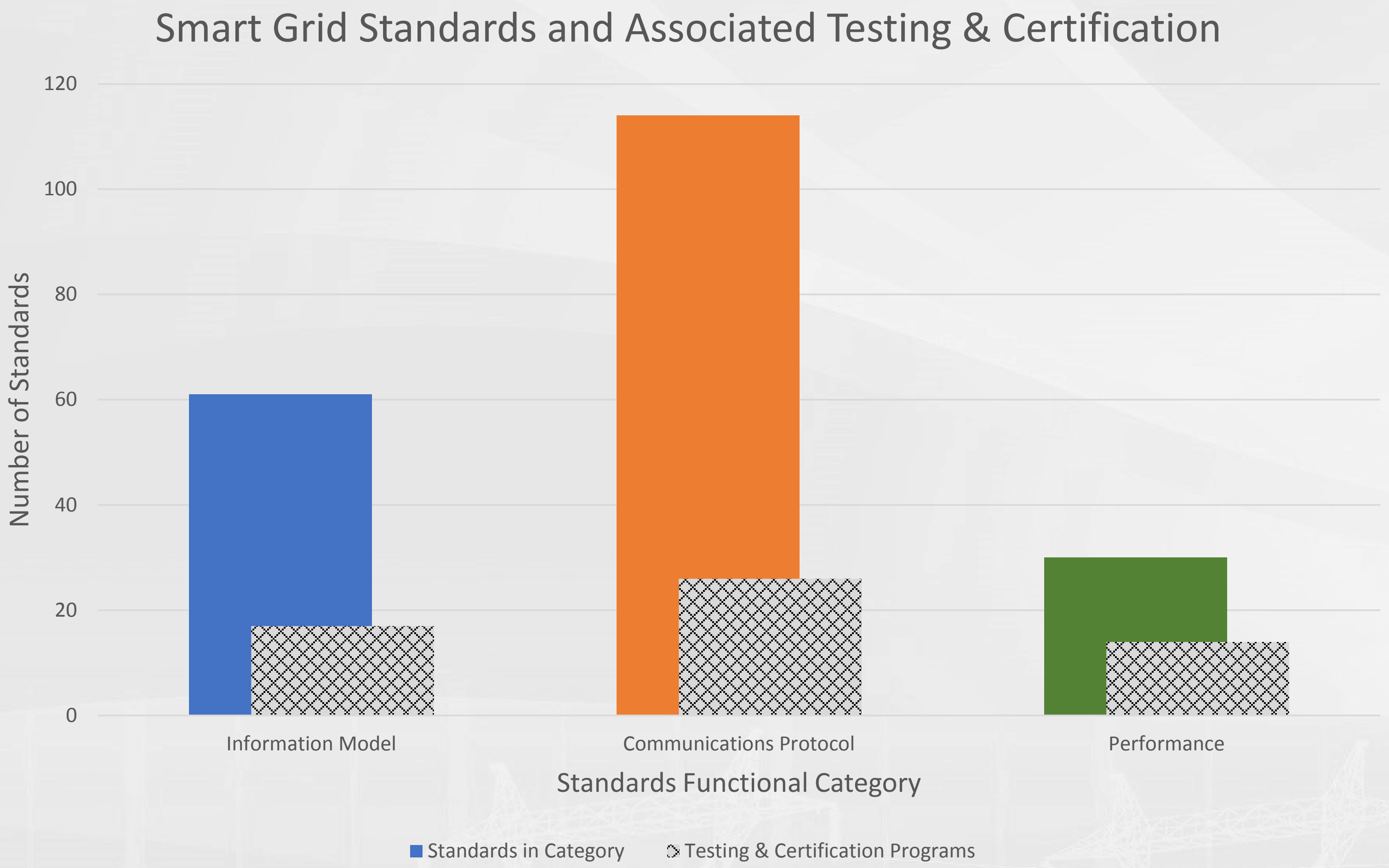
- New Standards
- New versions of old standards

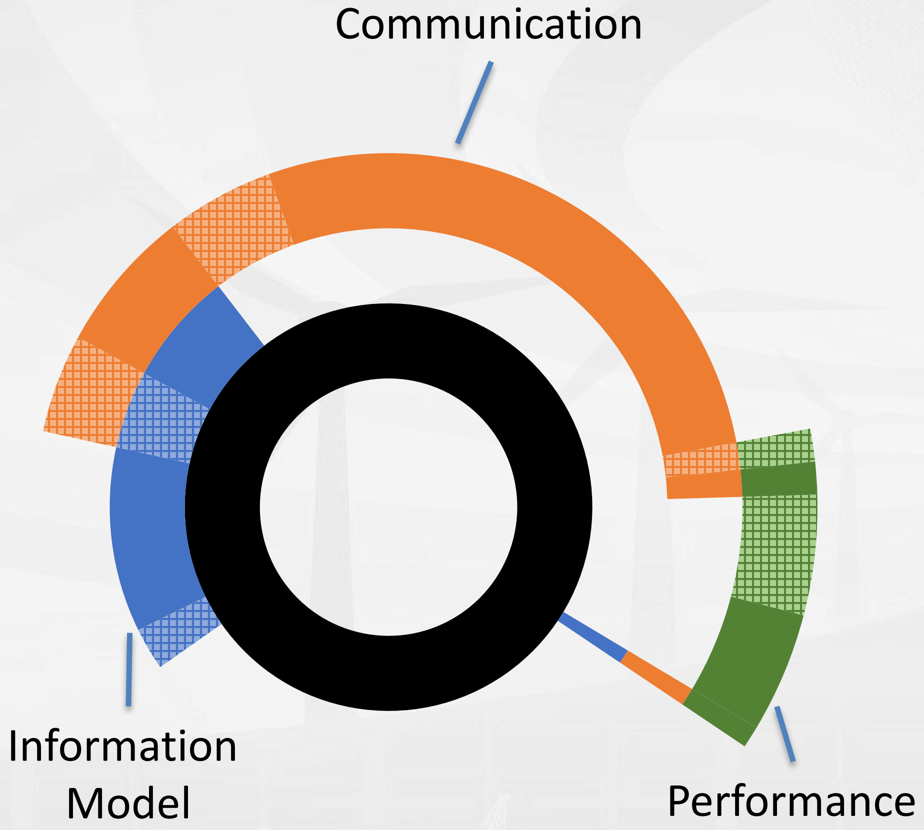
Smart Grid Standards for Evaluation (244 Standards)

Interoperability Profile: Illustrative Landscape



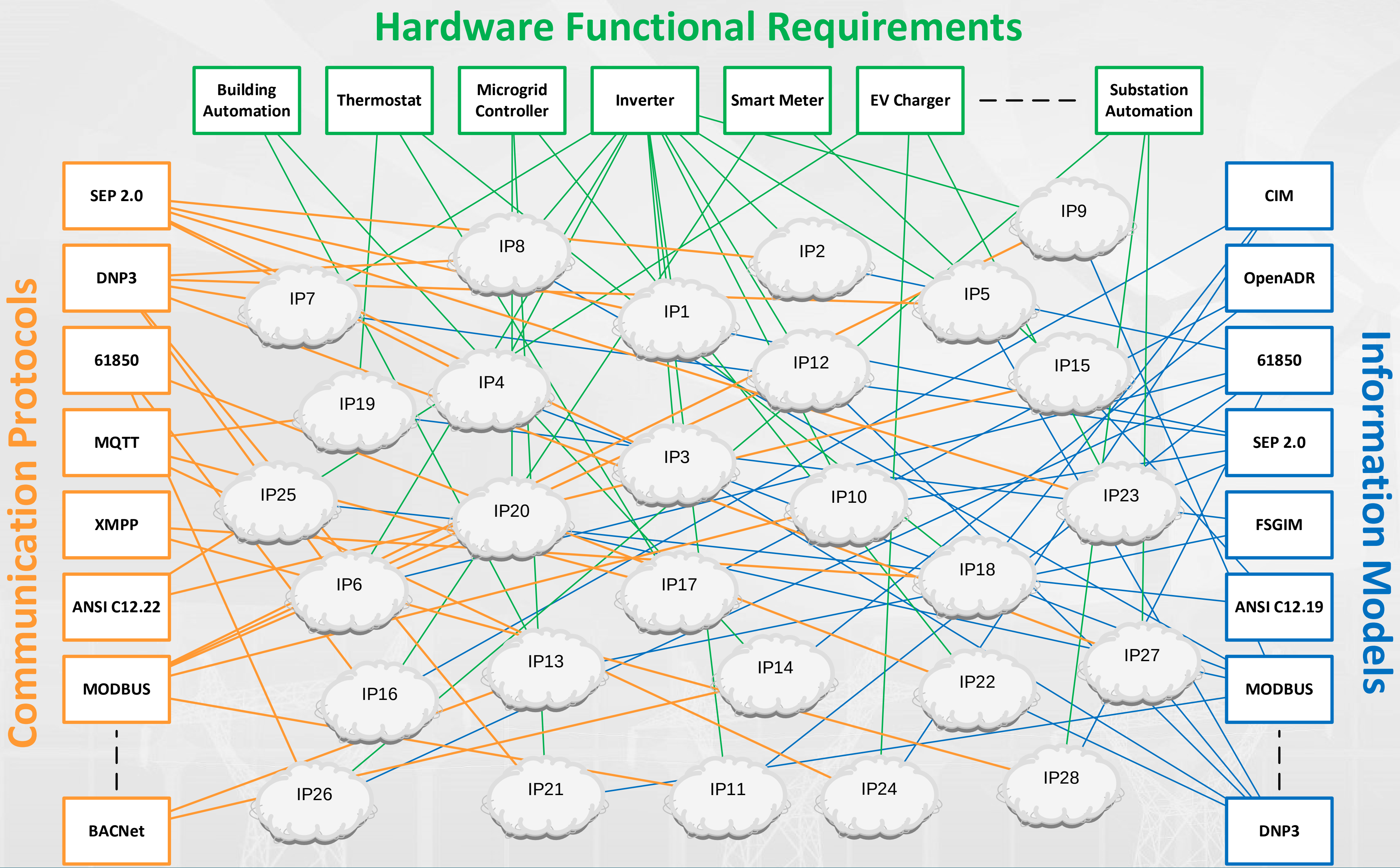
Interoperability landscape assessment



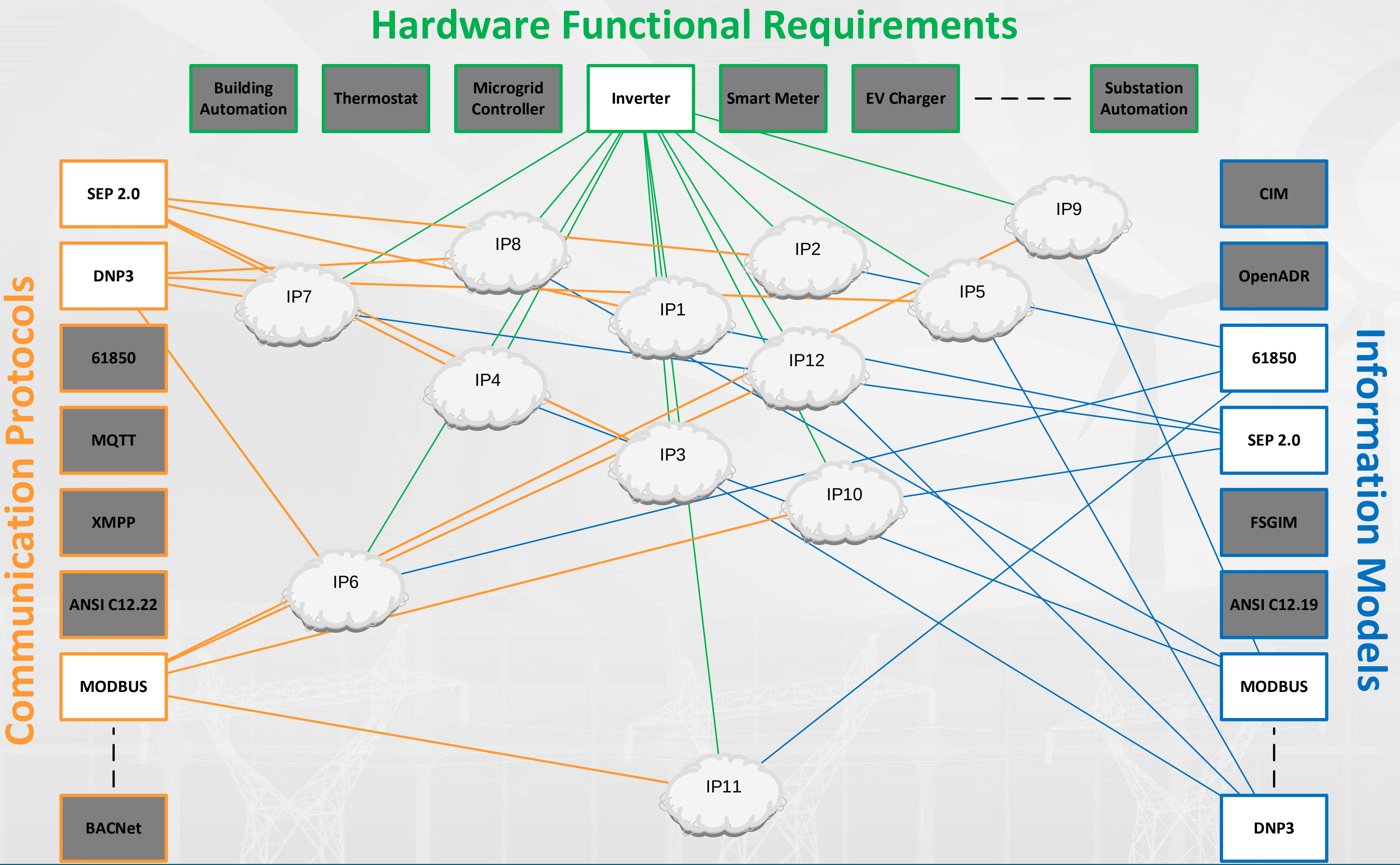


17/61 26/114 14/30

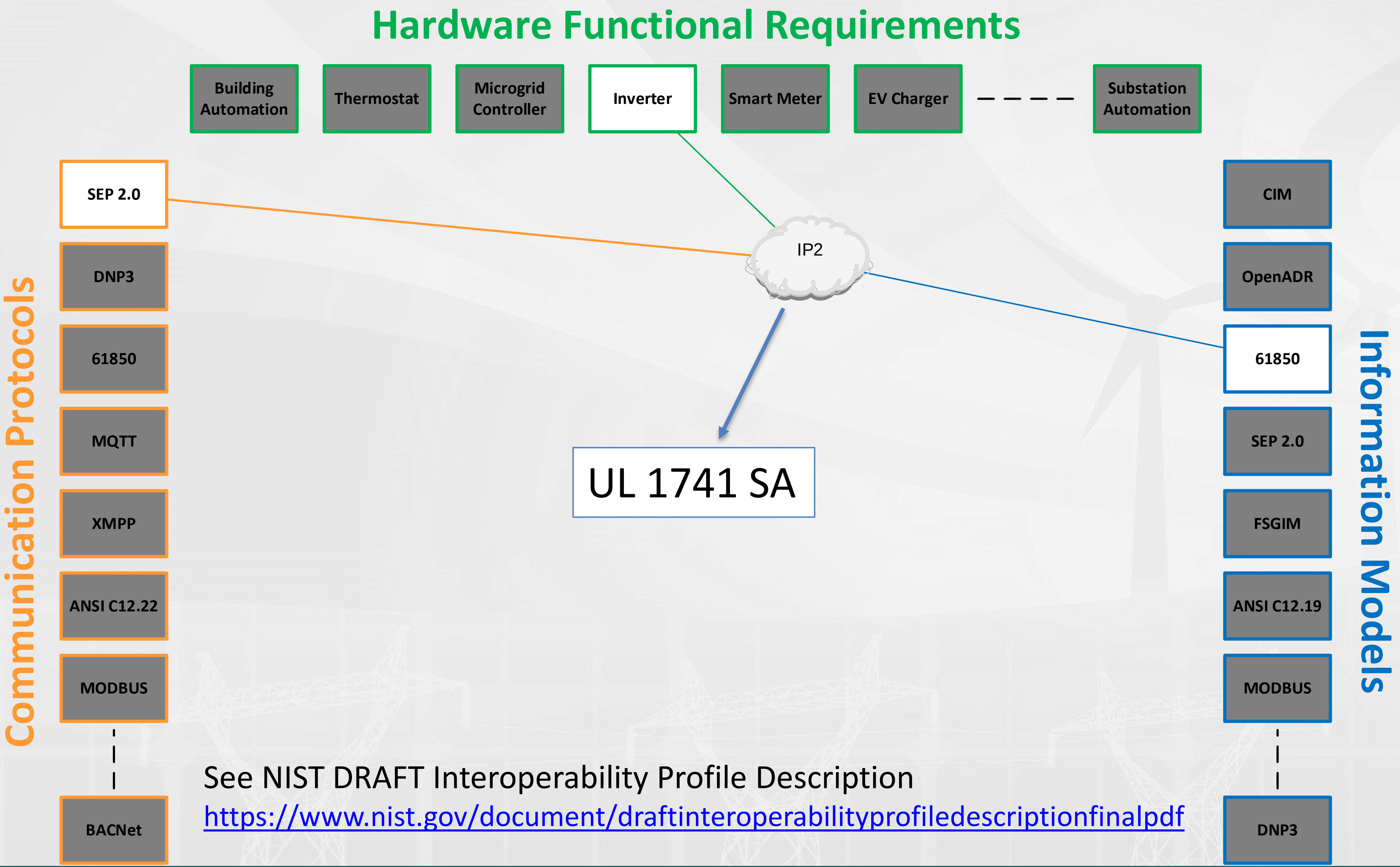
Interoperability Profile: Illustrative Landscape



Interoperability Profile: IEEE 1547 Case Study



Interoperability Profile: California Rule 21 Case Study

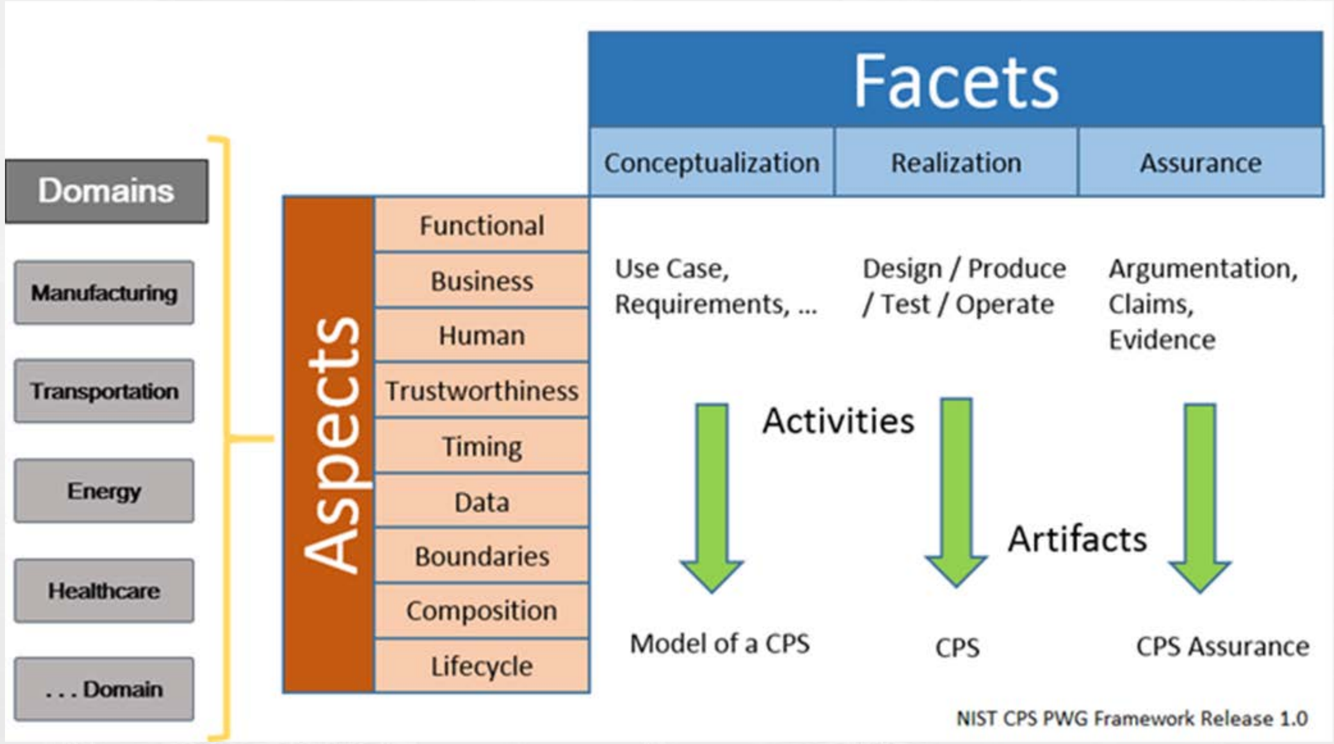


See NIST DRAFT Interoperability Profile Description
https://www.nist.gov/document/draftinteroperabilityprofiledescriptionfinalpdf

The CPS Framework—A Tool to Understand the Smart Grid

Jargon surrounds the electrical grid:

- *Intelligence moving to the edge*
- *Data tsunami*
- *Grid architecture*
- *Cloud / fog computing*
- *Smart grid*
- *Microgrid vs backup power*



The cyber-physical systems (CPS) framework provides a vocabulary of energy sector semantics, or ontology, through evaluation of CPS framework aspects and concerns

CPS Aspects and Concerns

- **Functional**
  - Actuation
  - Communication
  - Controllability
  - Functionality
  - Manageability
  - Measurability
  - Monitorability
  - Performance
  - Physical
  - Physical Context
  - Sensing
  - States
  - Uncertainty
- **Timing**
  - Logical Time
  - Synchronization
  - Time Awareness
  - Time Interval & Latency
- **Business**
  - Cost
  - Enterprise
  - Environment
  - Policy
  - Quality
  - Regulatory
  - Time to Market
  - Utility
- **Human**
  - Human Factors
  - Usability
- **Boundaries**
  - Behavioral
  - Networkability
  - Responsibility
- **Trustworthiness**
  - Privacy
  - Reliability
  - Resilience
  - Safety
  - Security
- **Composition**
  - Adaptability
  - Complexity
  - Constructivity
  - Discoverability
- **Data**
  - Data Semantics
  - Identity
  - Operations on Data
  - Relationship between Data
  - Data Velocity
  - Data Volume
- **Lifecycle**
  - Deployability
  - Disposability
  - Engineerability
  - Maintainability
  - Operability
  - Procureability
  - Producibility

INTELLIGENCE

(Illustrative relationships only)

Description of CPS Concerns for the Smart Grid

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 the condonation of sensing, processing and acting • Multiple inputs are needed to make control decisions • Most grid control systems and hardware were not designed to accommodate large numbers of DERs. • More dynamic monitoring and control to respond to the dynamic network	• Ability to control grid properties (sense, process and change); e.g., intentionally change a phenomenon / property	• Coordination of sensing and processing functions to produce accurate control signals. • Architectures needs to support control applications that input and evaluate multiple optimization factors including carbon usage and market prices • Architecture needs 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)
Functional	**Functionality**	Concerns related to the function that a CPS provides	• The constant evolution of the power system creates new grid functions. • Grid control functionality has expanded to include management of generation assets which require different functionality e.g. diverse generation assets require additional control functionality including distributed assets.	• Ability to provide grid functions e.g. control functions, sensing functions, service-related functions.	• Innovative grid technology needed to facilitate Power Markets, DERs, Microgrids, Electric Vehicles, etc. • Architecture needs to support management of DERs constraints that differ from older types of generation.
Functional	**Manageability**	Concerns related to the management of CPS function.	• Need the ability to manage change across multiple devices at different grid levels.	• Ability to manage change internally and externally to the grid at the cyber-physical boundary e.g. digital equipment and actuators affected by EMC	• Communication topology views and key externally visible properties for multi-tier distribution communications needed for system control, substations, field operations, and Transmission/Distribution integration[74]

Cybersecurity Threats: Increasing and Diversifying

Source: IEA 2017, Digitalization & Energy

Table 6.1 Open source information regarding cyber-attacks affecting energy infrastructure

Incident	Description (from open-source information)
Shamoon 1 and 2 (Saudi Arabia, 2012 and 2016)	"Shamoon 1" virus carried out cyber-sabotage and destroyed over 30 000 computers at Saudi Aramco. There was no direct impact on oil production, but the company was forced to revert to traditional paper and telephone trading for several weeks. Qatari natural gas company, RasGas, was also impacted. The virus was set to execute after working hours in order to minimise detection. "Shamoon 2" virus targeted similar vulnerabilities and was used to overwrite parts of computer hard discs.
Western Ukraine power grid (2015)	The first confirmed cyber-attack specifically against an electricity network. Attackers accessed substations' supervisory control and data acquisition (SCADA) and firmware with a combination of malware, personnel credentials obtained by means of email phishing, and Denial of Service (DoS) to prevent customers from obtaining call centre information about the blackout. Investigators concluded that a large well-co-ordinated team had prepared the attack over several months.
The Mirai Botnet (2016)	"Mirai" malware exploited low security in connected smart devices, such as cameras, to use a botnet (a network of devices under simultaneous command by the attacker to overload the victim by continuously sending data) to deliver the largest DoS attack to date. This attack did not target or impact energy infrastructure, but illustrates the vulnerability of the Internet of Things (IoT).
Industroyer/ Crash Override (Ukraine, December 2016 – reported May 2017)	A second brief but significant attack on the Ukrainian electricity system, thought to have been a test run for malware "Industroyer" (also known as "Crash Override"). This versatile malware enables attackers to view, block, control or destroy grid control equipment such as circuit breakers. Its design suggests expert knowledge of several standardised industrial communication protocols widely used to control infrastructure – not only electricity grids – throughout Europe, Asia and the Middle East. This was an example of a cyber intrusion into the control systems of critical infrastructure.
Nuclear plant spear phishing attack (2017)	This incident occurred in the United States. It used targeted email messages containing fake Microsoft Word résumés for engineering jobs, potentially exposing recipients' credentials for the control engineering network. The hackers also compromised legitimate external websites that they knew their victims frequented (known as a watering hole attack).
WannaCry (2017)	"WannaCry" ransomware hit hundreds of thousands of computers in thousands of organisations in some 150 countries, taking advantage of an access point in Microsoft operating systems for which some users had failed to install the secure update (or "patch"). These attacks did not target energy infrastructure, but several energy companies reported problems. In the People's Republic of China (hereafter, "China"), over 20 000 China National Petroleum Corporation (CNPC) petrol stations went offline.

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
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

NIST Cybersecurity Framework Identifiers

CPS Aspects and Concerns

- **Functional**
  - Actuation
  - Communication
  - Controllability
  - Functionality
  - Manageability
  - Measurability
  - Monitorability
  - Performance
  - Physical
  - Physical Context
  - Sensing
  - States
  - Uncertainty
- **Timing**
  - Logical Time
  - Synchronization
  - Time Awareness
  - Time Interval & Latency
- **Business**
  - Cost
  - Enterprise
  - Environment
  - Policy
  - Quality
  - Regulatory
  - Time to Market
  - Utility
- **Human**
  - Human Factors
  - Usability
- **Boundaries**
  - Behavioral
  - Networkability
  - Responsibility
- **Trustworthiness**
  - Privacy
  - Reliability
  - Resilience
  - Safety
  - Security
- **Composition**
  - Adaptability
  - Complexity
  - Constructivity
  - Discoverability
- **Data**
  - Data Semantics
  - Identity
  - Operations on Data
  - Relationship between Data
  - Data Velocity
  - Data Volume
- **Lifecycle**
  - Deployability
  - Disposability
  - Engineerability
  - Maintainability
  - Operability
  - Procureability
  - Producibility

Which concerns are most important to you?

Break: 3:30-3:45

Tuesday, November 13, 2018	
9:30 am	**REGISTRATION**
10:00 am	**WELCOME AND WORKSHOP OBJECTIVES** **Chris Greer,** NIST
10:15 am	**KEYNOTE: GRID MODERNIZATION AND THE CASE FOR INTEROPERABILITY** **John Gibson,** Avista Utilities
11:00 am	**PANEL SESSION: GRID MODERNIZATION AND INTEROPERABILITY** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**LUNCH**
1:15 pm	**KEYNOTE: THE ECONOMICS OF INTEROPERABILITY** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**PLENARY: INTRODUCTION TO NIST'S SMART GRID CONCEPTUAL MODELS** **Avi Gopstein,** NIST
2:30 pm	**INTERACTIVE DISCUSSION: MAJOR CONCERNS FOR SMART GRID INTEROPERABILITY** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**BREAK**
3:45 pm	**PLENARY: THREE KEY THEMES FOR CYBERSECURITY AND GRID INTEROPERABILITY** • **Risk Profiles—Jeffrey Marron,** NIST • **Interface Categories—Nelson Hastings,** NIST • **Securing Communications—Michael Bartock,** NIST
4:45 pm	**WRAP UP AND CHARGE FOR NEXT DAY**
5:00 pm	**ADJOURN**

Key Themes for Cybersecurity & Grid Interoperability

- Speakers:
  - Jeff Marron
  - Nelson Hastings
  - Mike Bartock
- Limited Q&A:
  - Write down your questions
  - Breakout discussions tomorrow (pick two!)

Tuesday, November 13, 2018	
9:30 am	**REGISTRATION**
10:00 am	**WELCOME AND WORKSHOP OBJECTIVES** **Chris Greer**, NIST
10:15 am	**KEYNOTE: GRID MODERNIZATION AND THE CASE FOR INTEROPERABILITY** **John Gibson**, Avista Utilities
11:00 am	**PANEL SESSION: GRID MODERNIZATION AND INTEROPERABILITY** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman**, NIST
12:00 pm	**LUNCH**
1:15 pm	**KEYNOTE: THE ECONOMICS OF INTEROPERABILITY** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**PLENARY: INTRODUCTION TO NIST'S SMART GRID CONCEPTUAL MODELS** **Avi Gopstein**, NIST
2:30 pm	**INTERACTIVE DISCUSSION: MAJOR CONCERNS FOR SMART GRID INTEROPERABILITY** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**BREAK**
3:45 pm	**PLENARY: THREE KEY THEMES FOR CYBERSECURITY AND GRID INTEROPERABILITY** • **Risk Profiles—Jeffrey Marron**, NIST • **Interface Categories—Nelson Hastings**, NIST • **Securing Communications—Michael Bartock**, NIST
4:45 pm	**WRAP UP AND CHARGE FOR NEXT DAY**
5:00 pm	**ADJOURN**

Cybersecurity Framework Smart Grid Profile

November 2018

The Cybersecurity Framework

The Basics

- Created by industry, academia and government participants in response to U.S. Executive Order, *Improving Critical Infrastructure Cybersecurity*
- Based on workshops, led by NIST, and other outreach to gather input and best practices for improving cybersecurity
- NIST Cybersecurity Framework (CSF) design:
  - Flexible
  - Leverages existing approaches, standards, practices
  - Internationally applicable
  - Focused on risk management vs checklist

The Cybersecurity Framework

Three Primary Components

Implementation Tiers

- A qualitative measure of organizational cybersecurity risk management practices

Core

- Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

- Alignment of an organization’s requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

The Framework Core

Establishes a Common Language

Function
Identify
Protect
Detect
Respond
Recover

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

What processes and assets need protection?

What safeguards are available?

What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management[1.1]
Protect	**Identity Management, Authentication and Access Control**[1.1]
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

An Excerpt from the Framework Core

The Connected Path of Framework Outcomes

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions | 23 Categories | 108 Subcategories | 6 Informative References

Risk-Based Decision Making

Expressed Using Cybersecurity Framework Profiles

Risk-Based Approach - recognizing that each organization's business objectives, cybersecurity requirements, and technical environments create unique cybersecurity priorities.

Profile – an expression of priorities using the outcomes within the Cybersecurity Framework Core

- A customization of the Core for a given sector, subsector, or organization
- A fusion of business/mission logic and cybersecurity outcomes
- An alignment of cybersecurity requirements with operational methodologies
- A basis for assessment and expressing target state
- A decision support tool for cybersecurity risk management

Identify

Protect

Detect

Respond

Recover

Profile Foundational Information

A Profile Can be Created from Three Types of Information

1 **Business Objectives**

Objective 1

Objective 2

Objective 3

2 **Cybersecurity Requirements**

Legislation

Regulation

Internal & External Policy

Subcategory
1
2
…
108

3 **Technical Environment**

Threats

Vulnerabilities

Operating Methodologies

Controls Catalogs

Technical Guidance

Smart Grid Profile – Our Approach

- **Identified high-level business objectives** for a high-DER environment
  - *Business requirements include regulatory requirements and cybersecurity requirements*
  - *Reviewed relevant literature (PNNL smart grid architecture documentation, NIST publications, etc.)*
  - *Interviewed industry experts (i.e., power system owners operators, electric power industry think tanks)*
- **High-level business objectives**:
  - **Maintain safety**
  - **Maintain power system reliability**
  - **Maintain power system resilience**
  - **Support grid modernization**

Smart Grid Profile – Our Approach, continued

- **Prioritized** Subcategory outcomes:
  - *Analyzed Cybersecurity Framework Core Subcategories in relation to identified business objectives*
  - *Does each Subcategory **directly** assist power system owners/operators in achieving the business objectives*
  - *Highlighted relevant Subcategories*
- Provided further **considerations** for implementation:
  - Described the rationale for the selection of each Subcategory
  - Provided implementation considerations for power system owners/operators (e.g., challenges that they may encounter as they seek to achieve cybersecurity outcomes)

An Excerpt from the Smart Grid Profile

NIST CYBER

Table 2 IDENTIFY Smart Grid Profile

		Maintain Safety	Maintain Reliability+E13	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 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.

Smart Grid Profile – Questions

The high-level business objectives defined in the Smart Grid Risk Profile apply generally to all grid architectures. However, cybersecurity and risk considerations for each architecture can differ.

- ***What considerations are unique to different grid architectures***?
  - *Or perhaps unique to specific Functions/Categories (e.g., asset management, maintaining inventory for non-grid devices, etc.) from the Cybersecurity Framework*
  - *Or perhaps to varied owner/operator perspectives (e.g., merchant transmission owner, cooperative utility, microgrid joint venture between utility and developer, etc.).*

Smart Grid Profile – Questions, continued

- ***Do you see value in creating additional Risk Profiles to address these considerations, and at what cross-section (e.g., architecture, service level, Functions/Categories, frequency regulation, voltage support within DER, etc.)? If so, Why?***

- ***Is the current risk Profile useful to stakeholders other than power system owners/operators? Should we explore Risk Profiles from the perspective of other smart grid stakeholders, e.g., technology vendors, and why?***

Logical Interface Categories Assessment

Nelson Hastings
Electronics Engineer
Applied Cybersecurity Division
Information Technology Laboratory

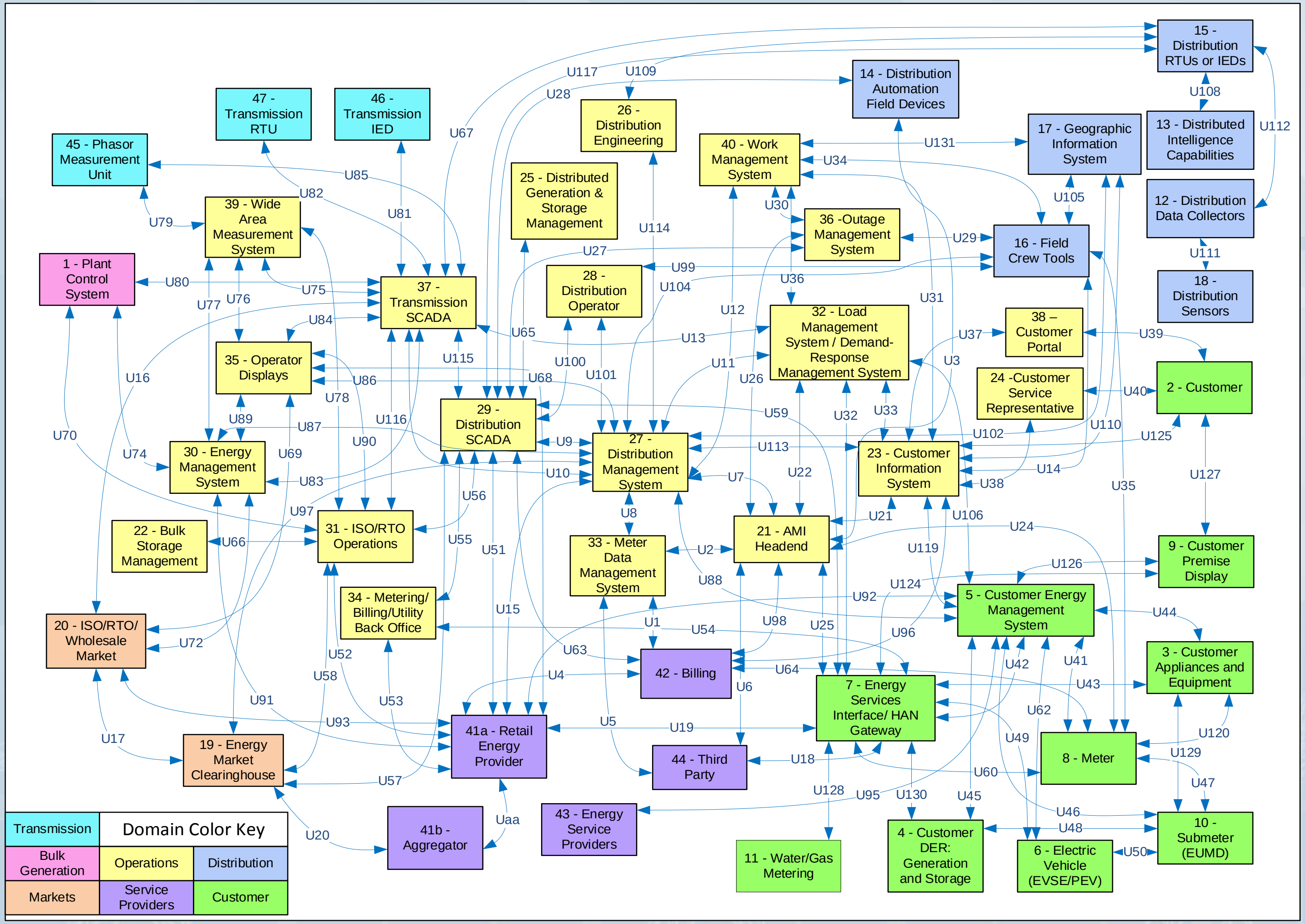
Agenda

- Background
- NISTIR 7628 Logical Interface Reference Model
- High-DER Architecture and New Logical Interfaces
- Potential Security Requirements for New Logical Interfaces
- Q&A

Background

- What are the cybersecurity implications of a High Distributed Energy Rersouce (DER) architecture?
- A High-DER architecture will introduce new logicial interfaces
- What are the cybersecurity implications associated with the newly introducted logicial interfaces?

NIST IR 7628 Logical Interface Reference Model - “Spaghetti Diagram”



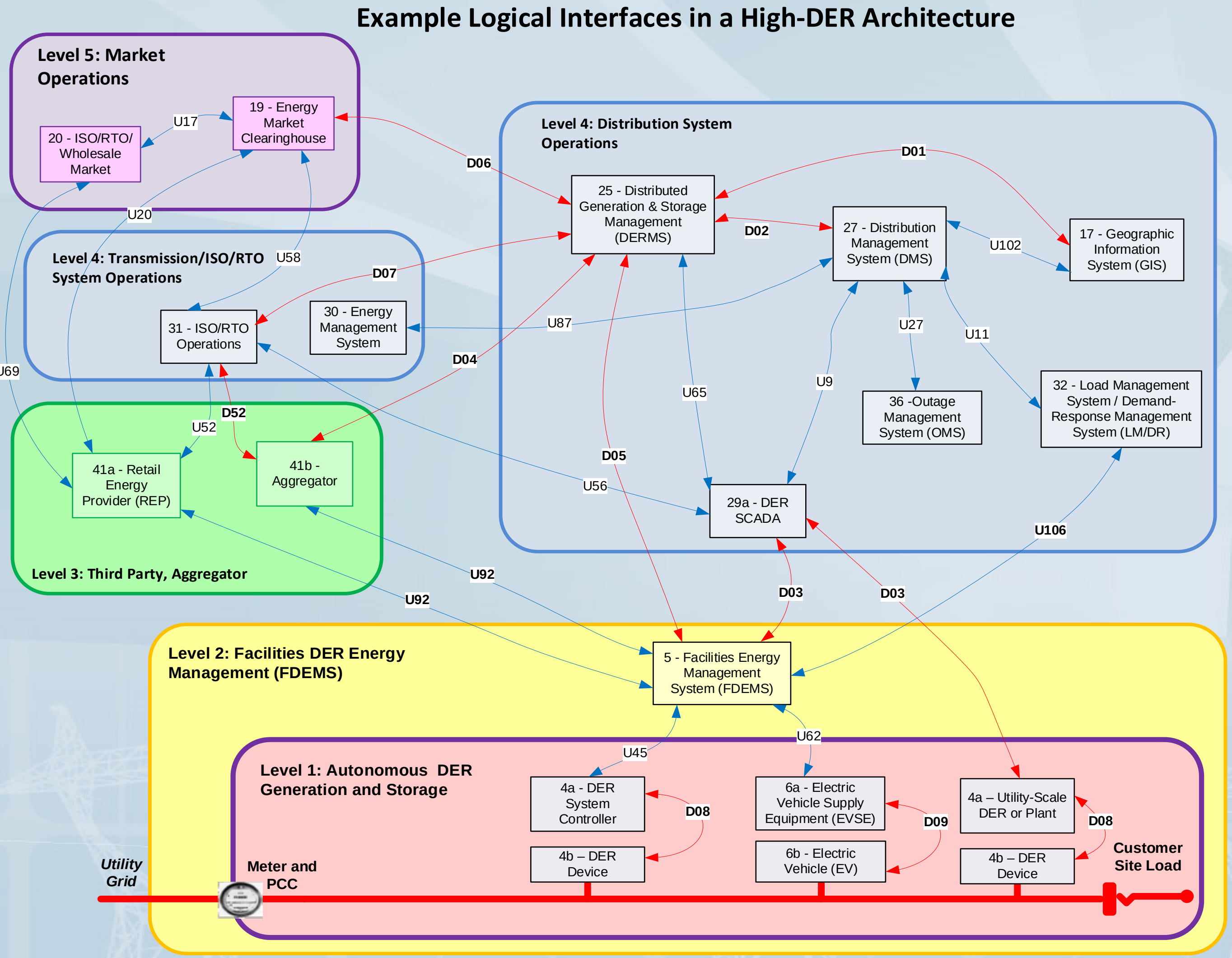
Logical Interface Categories - Sample

- Control System and Equipment
  - High Availability, Compute/bandwidth constraints
  - No High Availability, Compute/bandwidth constraints
  - High Availability, No compute/bandwidth constraints (3)
  - No High Availability, No compute/bandwidth constraints (4)
- Control systems
  - Intra-organizational (5)
  - Inter-organizational (6)
- Back office systems
  - Under common management authority
  - Without common management authority
- B2B connections
  - Financial/Market transactions (9)

High-DER Architecture Description

- Extensive Distributed Energy Resource (DER) penetration on distribution feeder (~1000 DERs)
- DERs involve active management of supply and load
  - Four quadrant inverters
  - Demand-response
  - Electric Vehicle (EV)
  - Battery systems
- Extensive distribution automation beyond current practice
- Reconfigurable system topologies

High DER Architecture – New Logical Interfaces Example



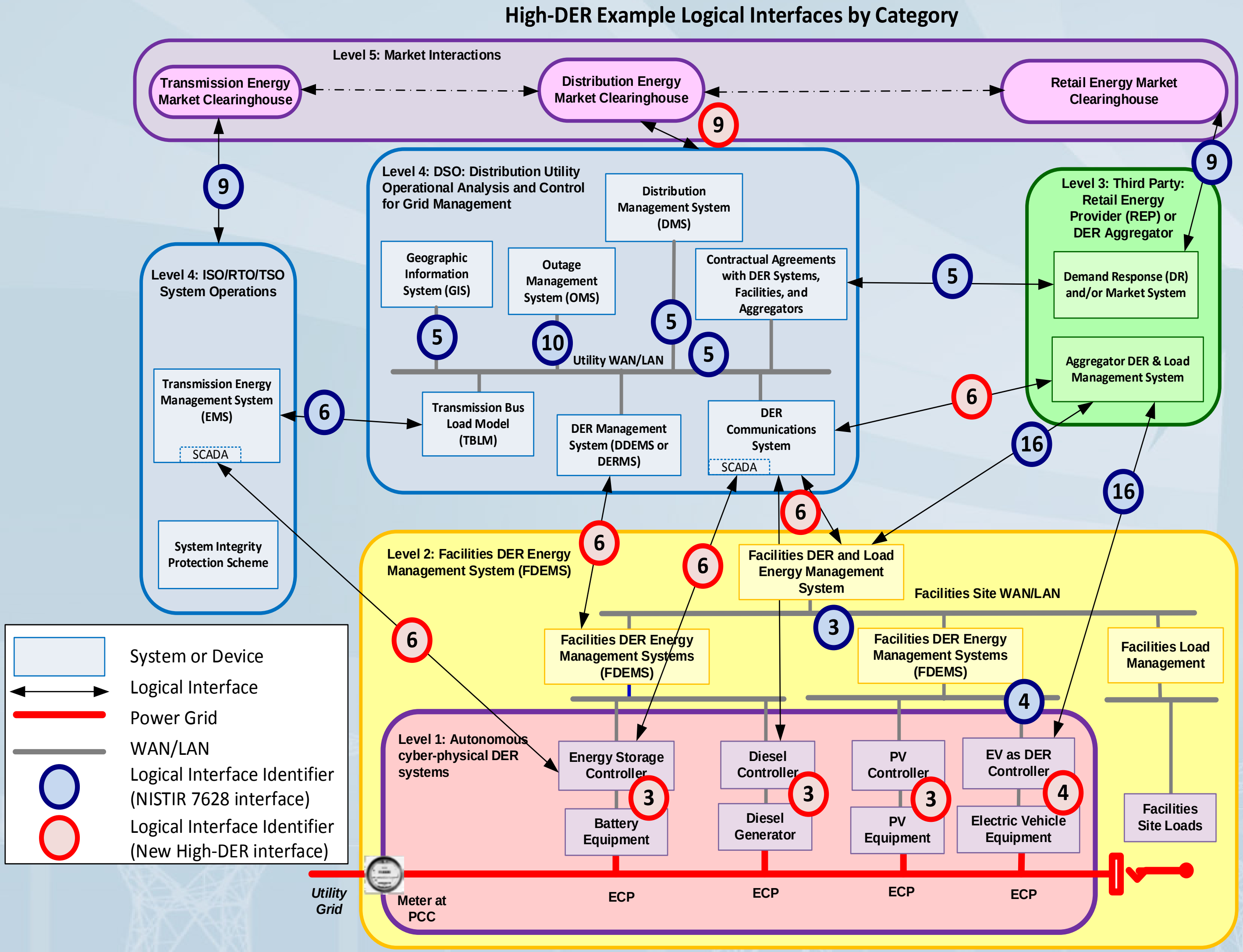
High-DER Architecture – New Logical Interfaces Example

- Distributed Generation and Storage Management → Distributed Energy Resource Management System (DERMS)
  – New interfaces between the DER devices and DER system controllers
  – New external interface to Distribution System Operations
- Customer Energy Management System → Facilities DER Energy Management System (FDEMS)
  – Three new external interfaces with the Distribution System Operations
- Distribution System Operations
  – New external interfaces to Market Operations, Transmission/ISO/RTO System Operations, and Third Party Aggregator
  – Two new internal interfaces from the DERMS to the Geographic Information System (GIS) and Distribution Management System (DMS)

New Logical Interfaces to NISTIR 7628 Logical Interface Categories

NISTIR 7628 Logical Interface Category (LIC)	NISTIR 7628 LIC Descriptions	New interfaces for High-DER Architecture
3	Control System and Equipment, High Availability	D8
4	Control System and Equipment, No High Availability	D9
5	Control Systems, Intra-organizational	D1, D2
6	Control Systems, Inter-organizational	D3, D4, D5, D7, D52
9	B2B Connections, Financial/Market transactions	D6

High-DER Architecture: Logical Interface Categories



Potential Security Requirements for New Logical Interfaces

- New interfaces D3, D4, D5, D7, and D52 map to NISTIR 7628 LIC 6
- Security requirements for NISTIR 7628 LIC 6:
  - SG.AC-14: Permitted Actions without Identification orAuthentication
  - SG.IA-04: User Identification and Authentication
  - SG.SC-05: Denial-of-service protection
  - SG.SC-06: Resource Priority
  - SG.SC-07: Boundry Protection
  - SG.SC-08: Communication Integrity
  - SG.SI-07: Software and Information Integrity

Q & A

Securing Communications

Mike Bartock
IT Specialist
Computer Security Division
Information Technology Laboratory

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

Agenda

- Background
- Publish Subscribe Communications
  - Brokered
  - Brokerless
- Wrap Up
- Q&A

Background

- Participated in the SEPA OpenFMB Cybersecurity Task Force
- Performed a security review of NAESB RMQ.26 and corresponding OpenFMB CTF output
- Publish and Subscribe communications are required by OpenFMB

Motivations

- As recently as 2011, publish and subscribe communications were not being considered within grid architectures[1]
- Publish and subscribe communications provide “improved scalability with regard to the number of communication partners, and ease of application development”[2]

[1]Wayne Weng, Yi Xu, Mohit Khanna. A survey on the communication architectures in smart grid. https://doi.org/10.1016/j.comnet.2011.07.010. July 5, 2011

[2]Michael Hoefling, et. al. Integration of IEEE C37.118 and Publish/Subscribe Communication. https://ieeexplore.ieee.org/document/7248414. June 8, 2015

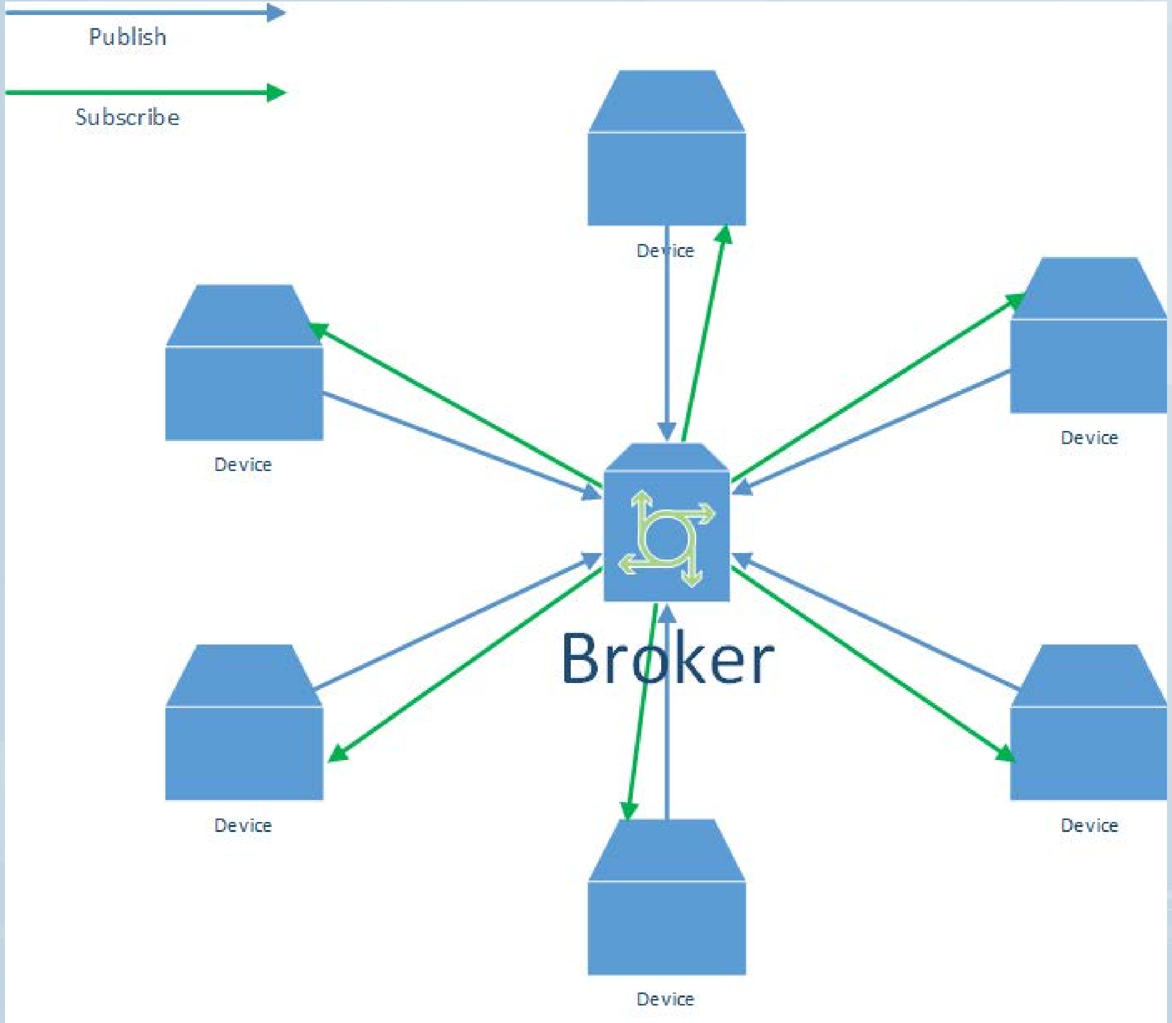
Publish and Subscribe Communications

- Messages are associated with topics
- Topics have hierarchical structure
  - Ex. topic1/topic2/…/topicN
- Published messages must have a topic
  - Ex. topic1/topic2/…/topicX/"Message Text”
- Devices subscribe to specific topics, and receive messages published to that topic

Pub/Sub Example

- Device A subscribes to topic devices/Information
- Device B publishes message “I am Device B” to topic devices/Information
- Device A receives message devices/Information/”I am Device B”

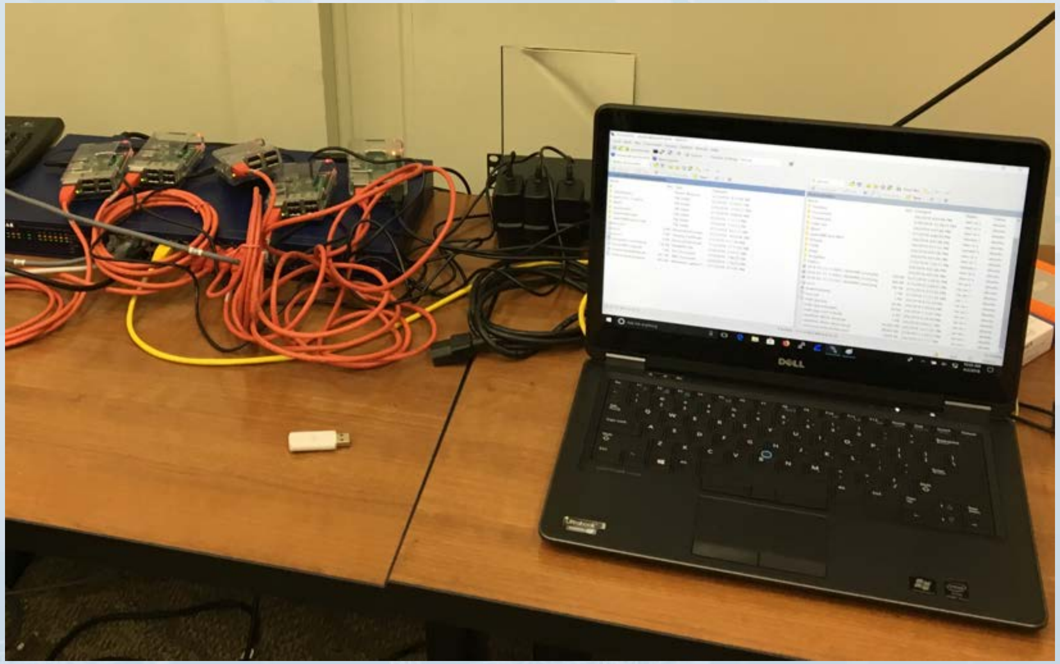
Brokered Pub/Sub Communications



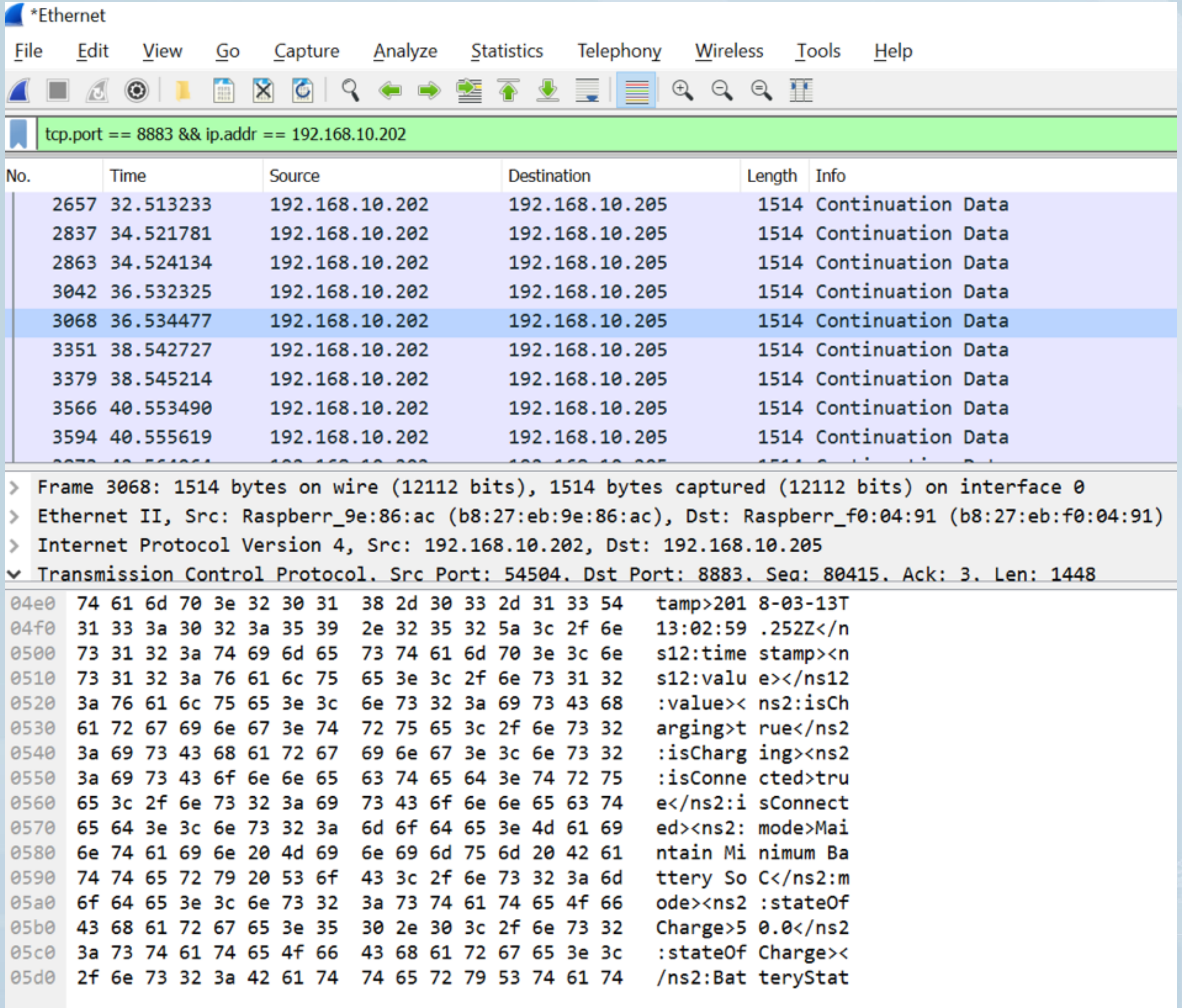
Pros	Cons
Reduces computations on devices	Centralized broker adds extra hops/time for messages to be sent and received
Device management can be standardized	Difficulty in getting new/specialized devices registered
Broker can ensure devices receive all intended messages	Single point of failure if broker goes down
Logging and aggregation of all messages	Device registry with access rules could become very complex

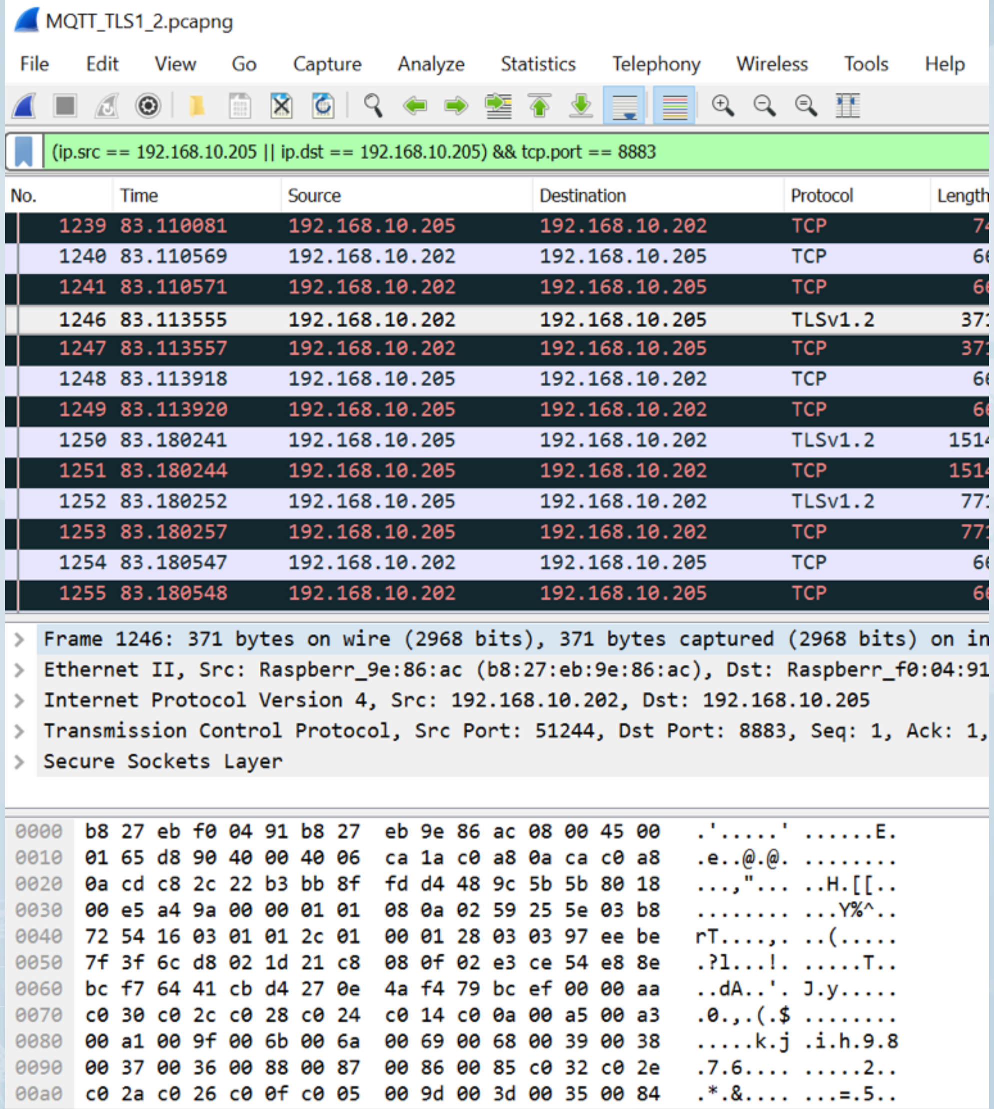
OpenFMB PoC Implementation

- Raspberry Pi 2 – 900MHz quad-core ARM Cortex-A7 CPU
- Ubuntu Linux Operating System
- OpenSSL Crypto Library
- Mosquitto MQTT Broker and Client
- Java Simulation of Grid Devices
- Netgear GS724Tv4 24-Port Gigabit Smart Managed Pro Switch
- Laptops: Windows 10



OpenFMB PoC Implementation Outcomes





OpenFMB PoC Implementation Outcomes

Preliminary Performance Results

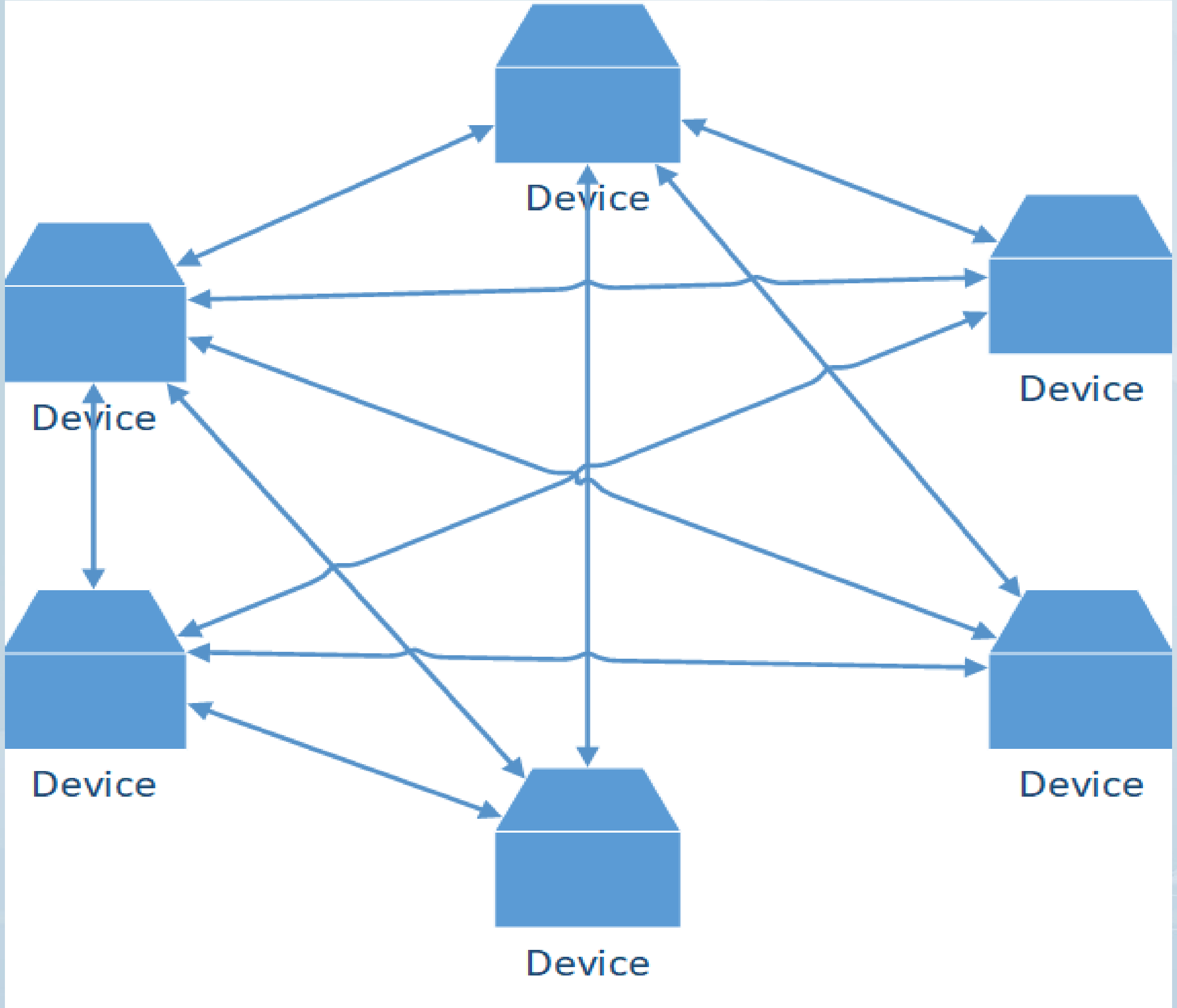
$MQTT_{Init}$ --> $MQTT_{SUBACK}$

Authentication / Encryption	None	TLS 1.2
None	.002855	.108071
Username & Password	.003223	.108458
X509 Certificate	N/A	.201232

$MQTT_{PUB}$ --> $MQTT_{SUB\_RECV}$

Authentication / Encryption	None	TLS 1.2
None	.003242	.109013
Username & Password	.003216	.108034
X509 Certificate	N/A	.186208

Brokerless Pub/Sub Communications



Pros	Cons
Direct device to device communication	Increases computations on devices
Device can be updated dynamically per device	Possibly no standard way to manage devices/message access list
Distributed messaging enables resiliency if any device fails	No guarantee messages are received by all intended devices
Simple message access rules on each device	Difficulty logging and aggregating messages

Communications Security Considerations

- Other communication methods applicable to Smart Grid?
- What to do with legacy equipment?
- How to handle device identity and authentication?
- Acceptable performance overhead due to security implementation?
- What are commonly used pub/sub protocols?
- Are devices supporting pub/sub protocols natively?

Q & A

Day 1: Adjourn

- Tomorrow begins at 8:45am
- Keynote by Ron Ross begins at 9:00am!
- Cybersecurity panel at 9:30
- 3x2 breakout structure
  - Morning breakout sessions repeat in the afternoon
  - Pick your favorite two topics and dive in deep!
- Tomorrow's close will be 4pm

Wednesday, November 14, 2018	
8:30 am	REGISTRATION
8:45 am	WELCOME AND OBJECTIVES
9:00 am	KEYNOTE: CYBERSECURITY OF COMPLEX SYSTEMS **Ron Ross**, NIST
9:30 am	PANEL SESSION: CYBERSECURITY AND GRID MODERNIZATION *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	BREAK
10:45 am	PARALLEL BREAKOUT SESSIONS *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	LUNCH
1:30 pm	PARALLEL BREAKOUT SESSIONS *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	BREAK
3:15 pm	REPORT OUT PANEL
3:45 pm	NEXT STEPS
4:00 pm	ADJOURN