EPRI | ELECTRIC POWER RESEARCH INSTITUTE

U.S. DEPARTMENT OF ENERGY

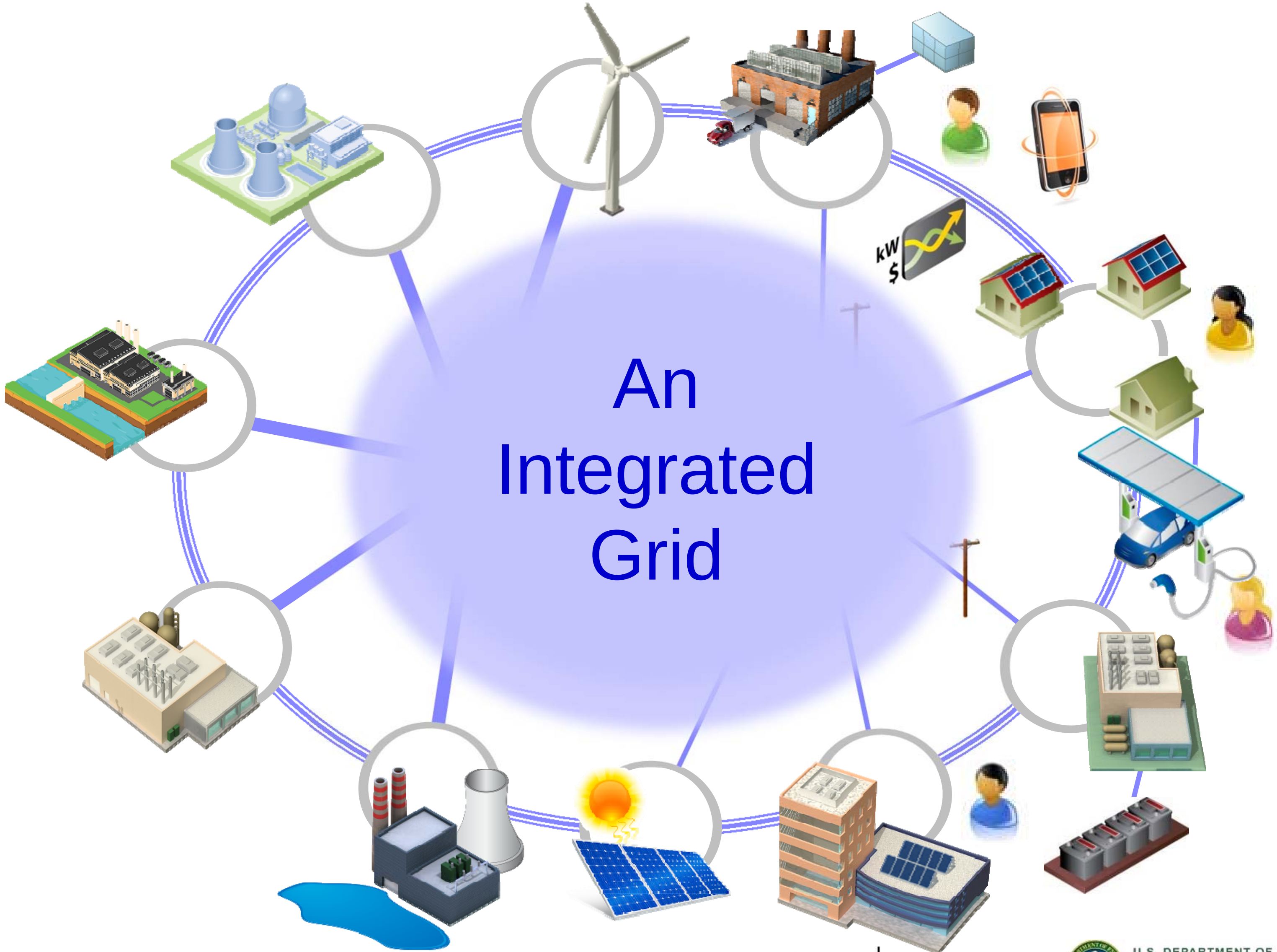
Integrated Communication Networks and the Integrated Grid

Tim Godfrey

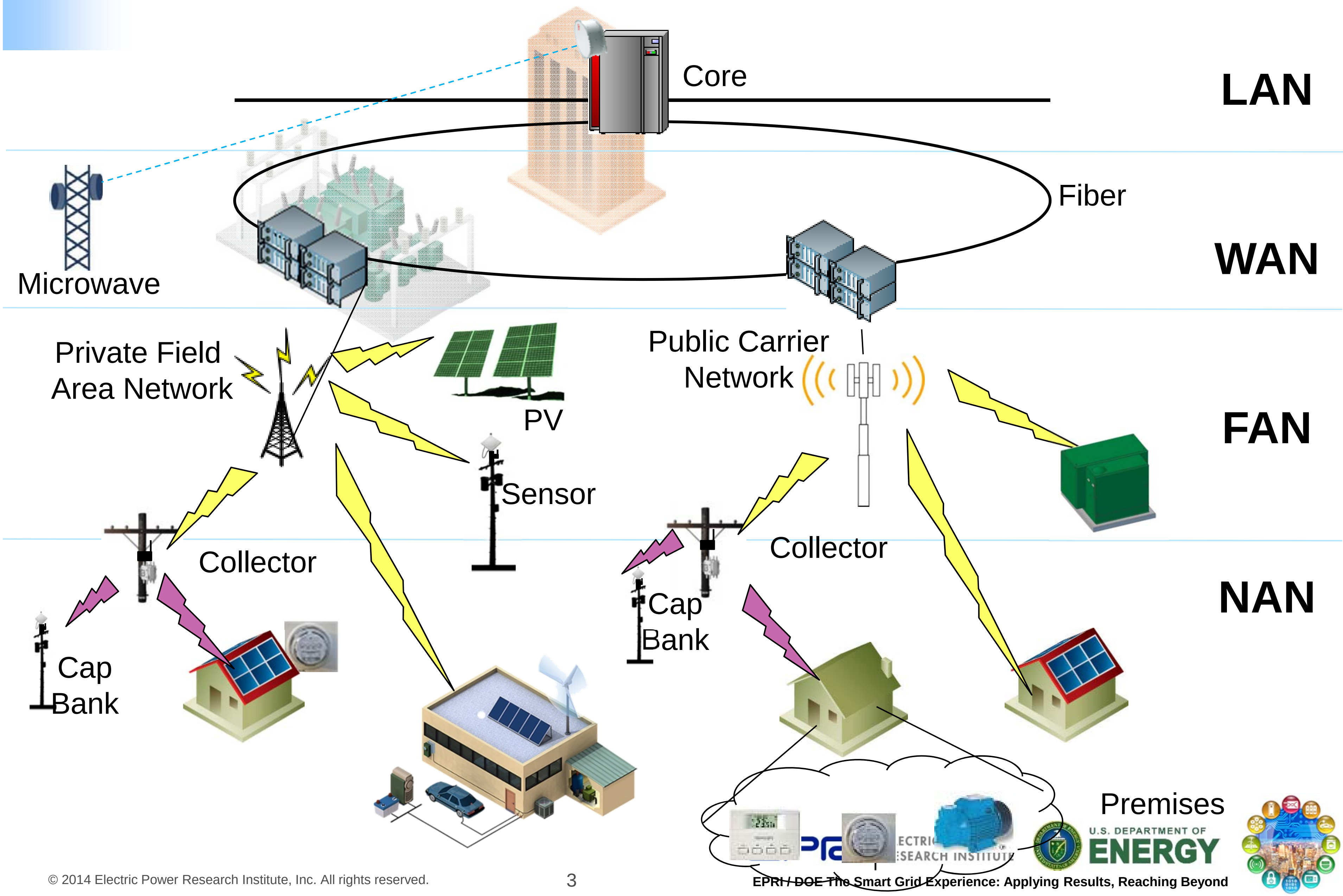
The Smart Grid Experience
Communications & Cyber Security:
The Foundations of the Modern Grid

October 28, 2014

Enabled by communications….



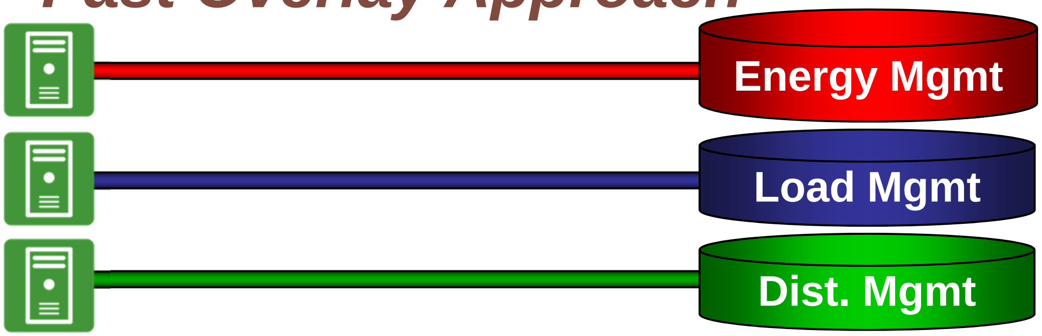
The utility communications hierarchy



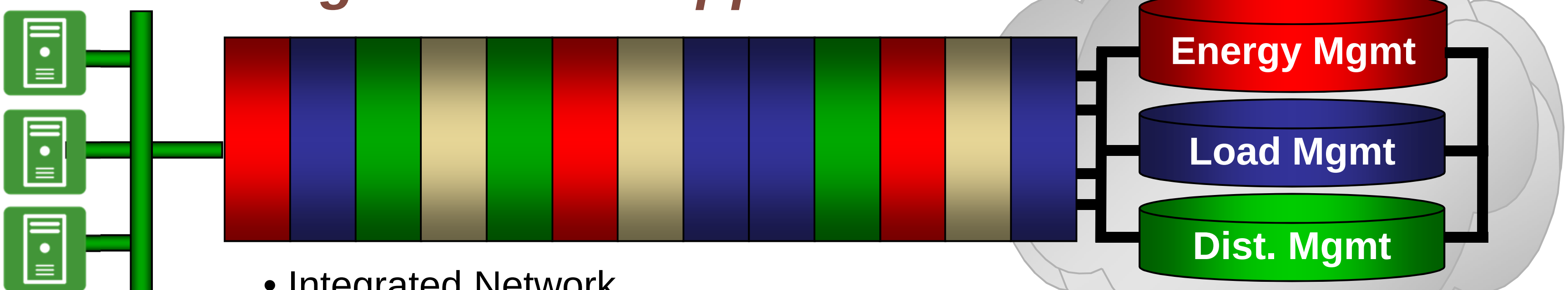
Trends Impacting Utility Communications (1)

- Transition from application-specific (overlay) networks, to integrated and unified networks

Past Overlay Approach



New Integrated Data Approach

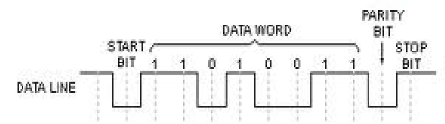


- Integrated Network
- Common Equipment and Interfaces
- Redundant at Critical Sites

Image Credit:
Great River Energy

Trends Impacting Utility Communications (2)

- Legacy: Serial interfaces and protocols based on serial connections



- Now: Packet based networks and interfaces. Protocols based on IP.

Trends Impacting Utility Communications (3)

- Legacy: Utility communications based on private infrastructure

- Now: Hybrid networks including wireless carriers and public broadband services, in addition to utility-owned communications networks

Other Trends Impacting Utility Communications

- Need for higher performance - throughput / latency

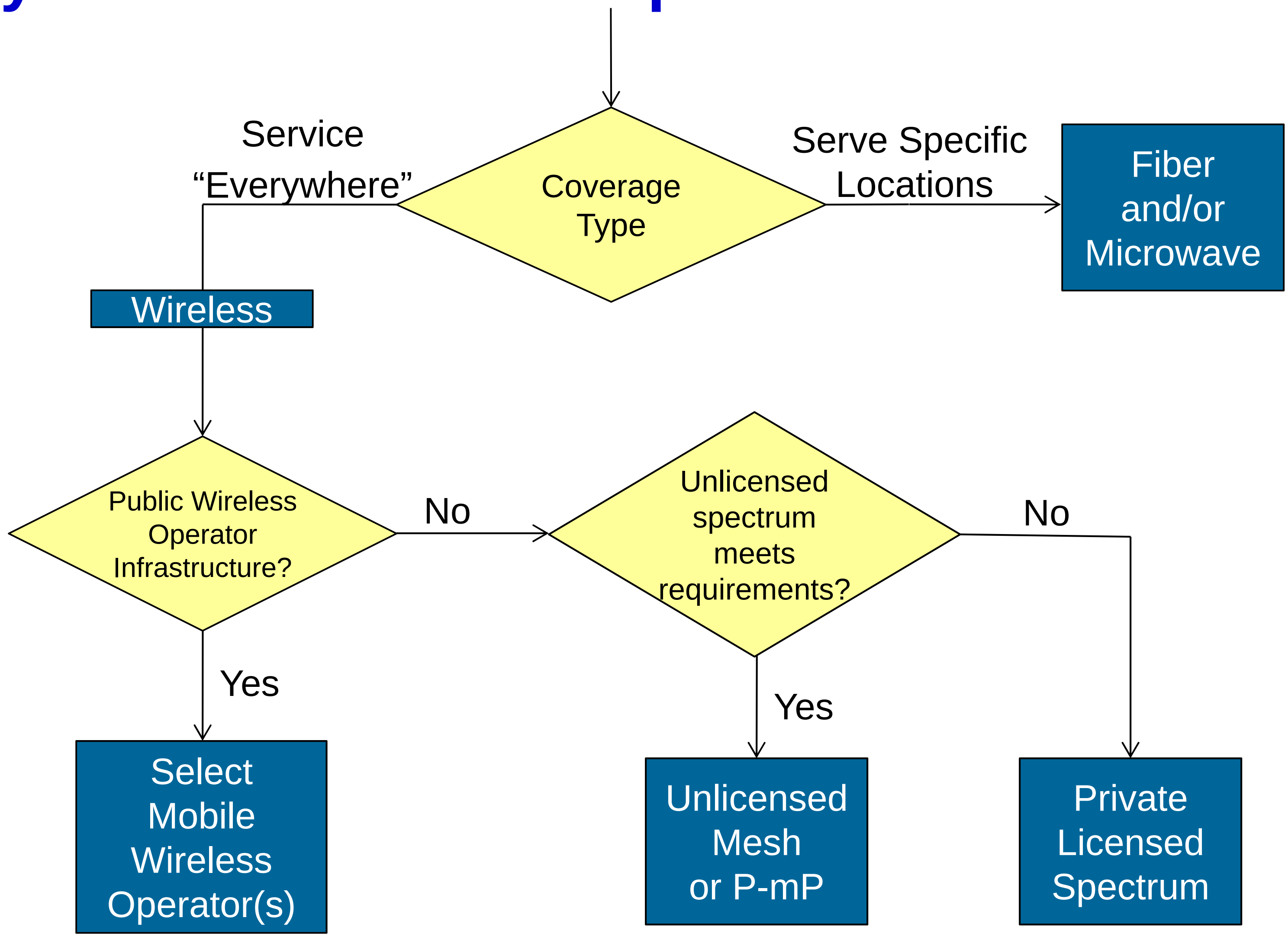
- Increased focus on cyber-security

- More ubiquitous coverage

- Requirements for higher reliability

99.999%

Utility Communications Options



Pros and Cons of Integrated Comm Networks

- Pros
  - Scalable
  - Maintainable (evolution over technology lifecycle)
  - Manageable
  - Improved ROI
- Cons
  - Criticality is magnified: Design for reliability, resilience, and security
  - Challenges of legacy device migration
  - There is no “universal” communications solution
  - Challenges coordinating a strategic development across the organization

FAN Demo Members

SRP

DUKE ENERGY

hydro one

ui The United Illuminating Company

GREAT RIVER ENERGY

Nebraska Public Power District

Hydro Québec

Ameren

Cyber-security in integrated comm networks

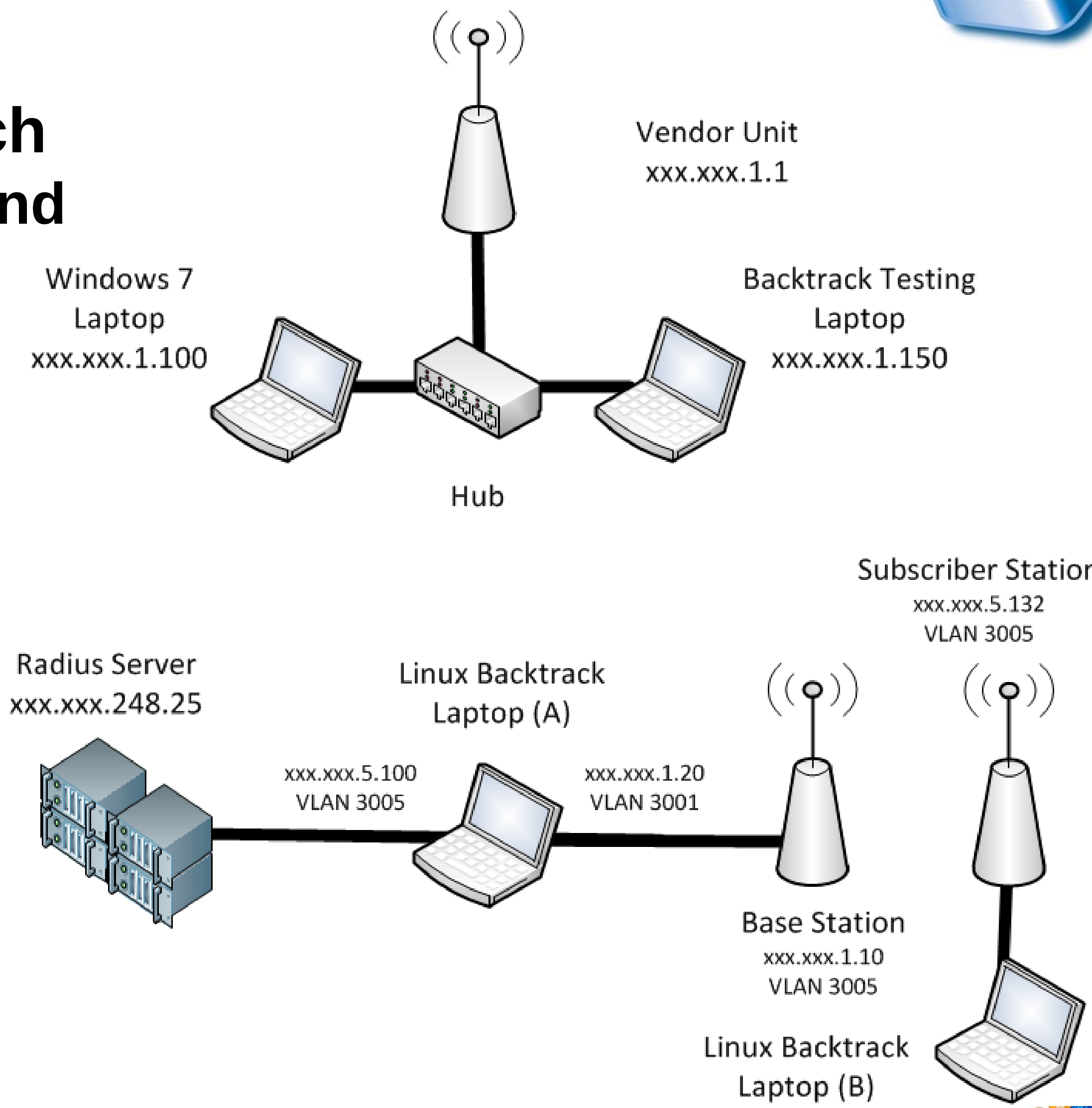
- Multi-functional integrated networks introduce new risks and exposures
  - Best practices for separation of networks is required
    - IT, OT, etc.
    - VLANs, Firewalls, etc.

- Cutting-edge technology can be a mixed bag
  - ☺ Modern “best of breed” security protocols and features are typically supported
  - ☹ Bugs and vulnerabilities may be present and undetected

FAN Penetration Testing

- Collaborative research between FAN Demo and Cyber Security

- Three FAN Demo member utilities have/will perform testing



The challenge of integrated communications

- There is no single solution for utility communications networks – no universal communications technology
- Networks will be hybrids – implementing multiple tiers and multiple technologies
- Ideally the services offered and the management are integrated
  – At least in the upper tiers
- Standards help, but are not a panacea

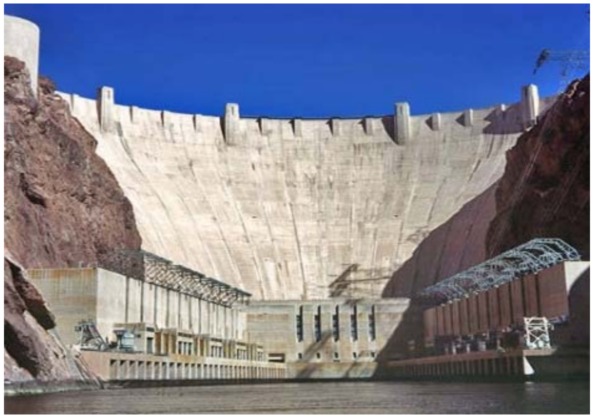
Communicatinos and the Data-Driven Grid

NRECA

A Touchstone Energy® Cooperative

YES, the grid will be smart

- *Smart is the alternative to big.*
- When the grid was first built, it was all about expansion – more power, delivered ubiquitously



- When you reach a limit, you built MORE
- Why we still focus on more, but the first thought now is getting more from what we have.

And Shockley said “let there be transistors”

The rate of the improvement in grid components was slowing in the 1980s. --

Electricity prices were low and stable

Reliability was very high

“Everything had been invented”

Then – solid state electronics entered the power industry

metering

communications

control

power electronics

And it was time to reconsider / reinvent everything

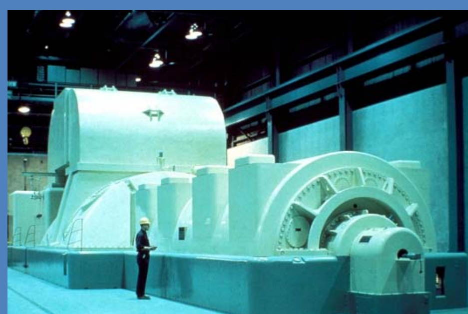
(731 million)

Living in the Interesting Time

1883→ 1990

2025?→ °°°

Control Through Angular Momentum



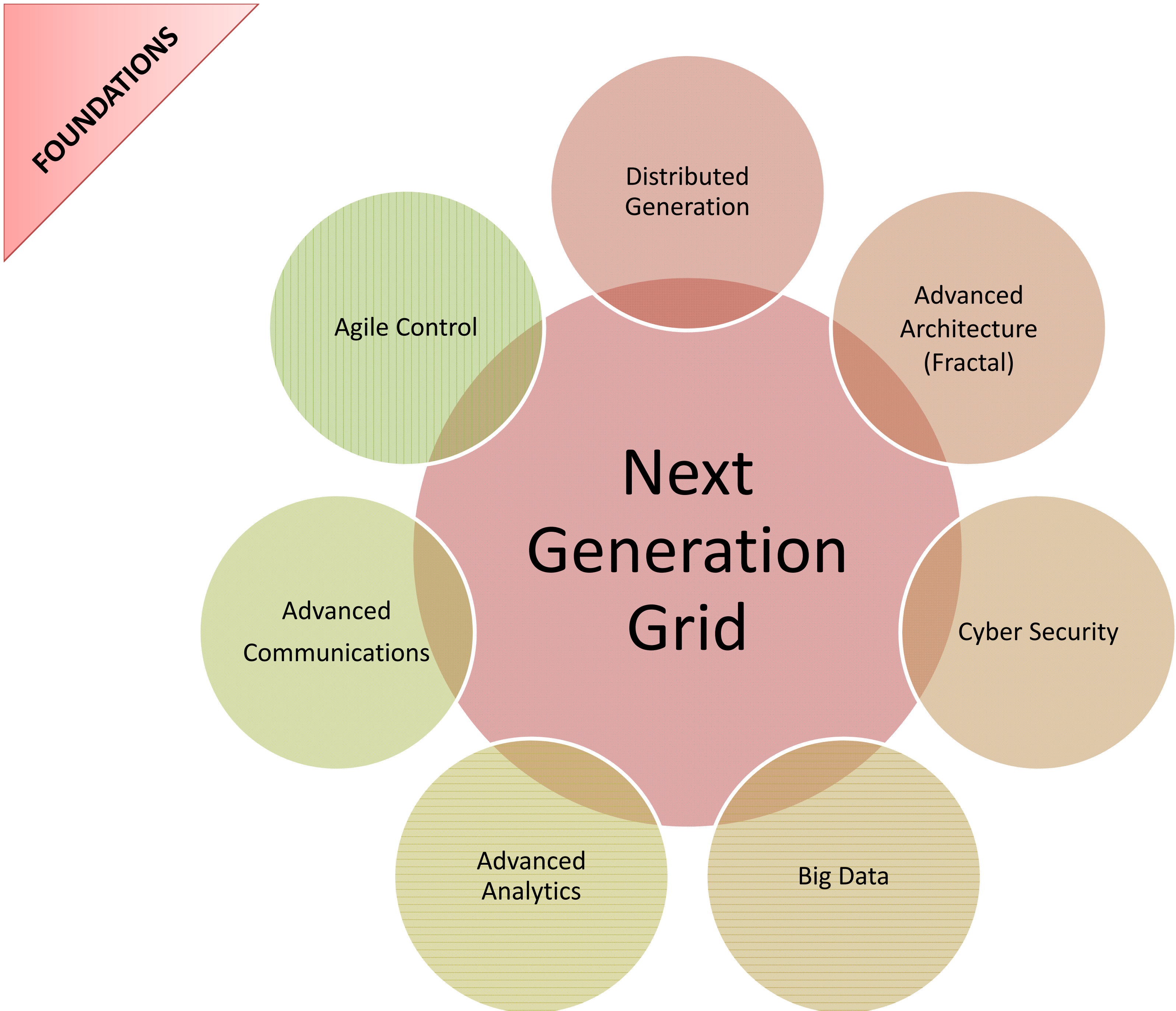
Transition

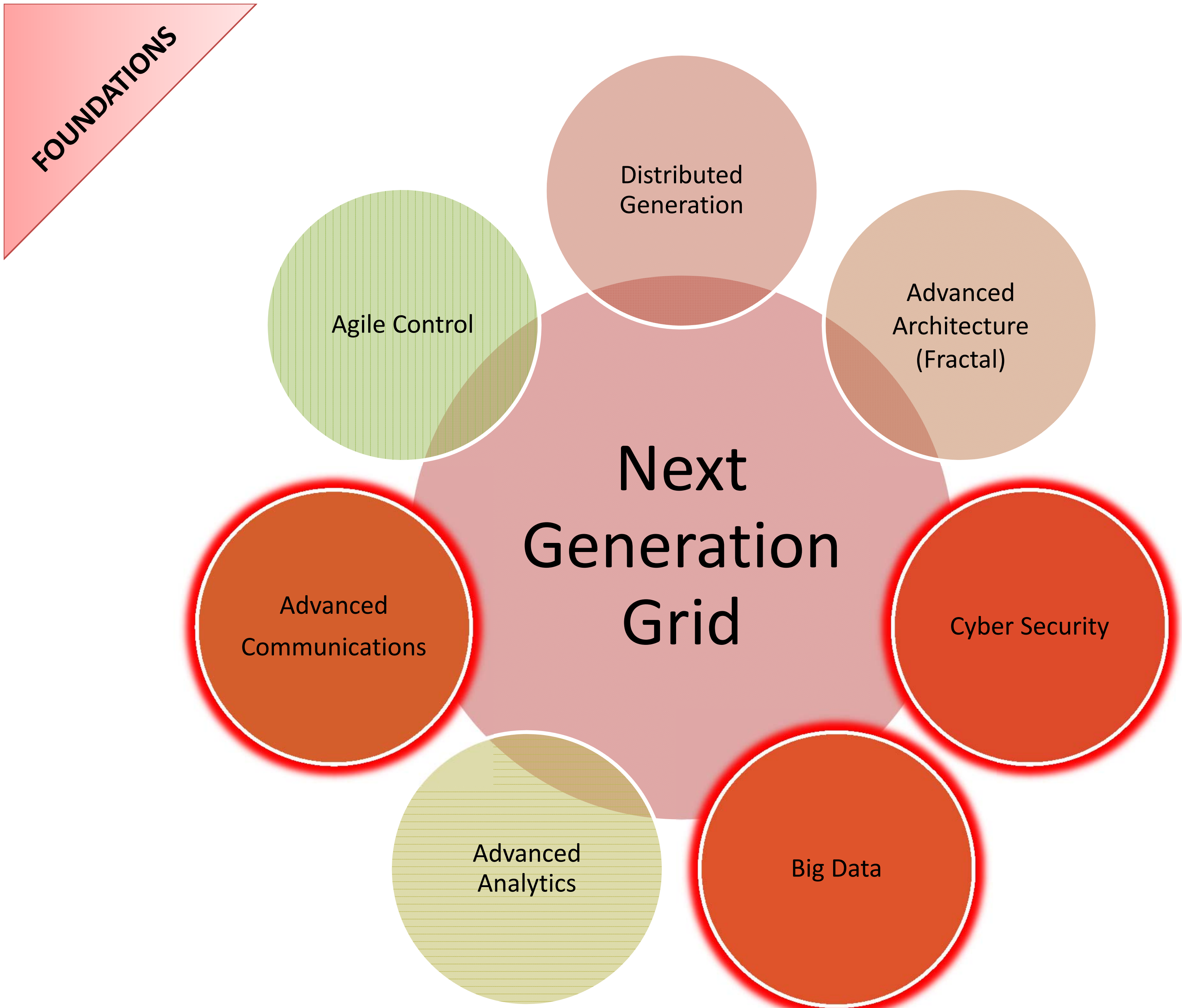
Analytically Driven Control

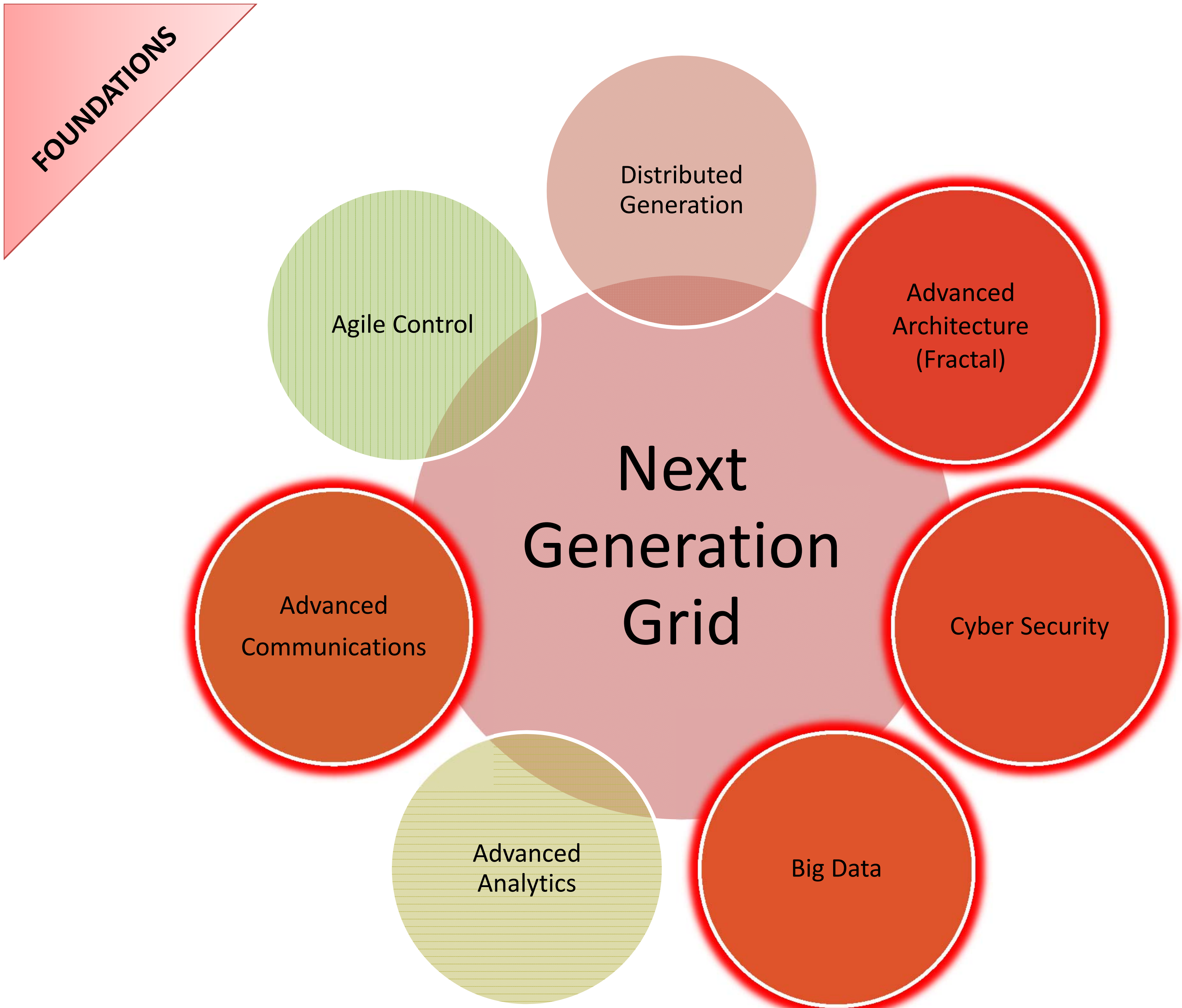
Reliability through overbuilding

Lack of overall model
Changing Technology
Complicated Transition

Knowledge of state
Precise control
High performance analytics


FOUNDATIONS
Distributed Generation
Agile Control
Advanced Architecture (Fractal)
Next Generation Grid
Advanced Communications
Cyber Security
Advanced Analytics
Big Data


FOUNDATIONS
Distributed Generation
Agile Control
Advanced Architecture (Fractal)
Next Generation Grid
Advanced Communications
Cyber Security
Advanced Analytics
Big Data


FOUNDATIONS
Distributed Generation
Agile Control
Advanced Architecture (Fractal)
Next Generation Grid
Advanced Communications
Cyber Security
Advanced Analytics
Big Data

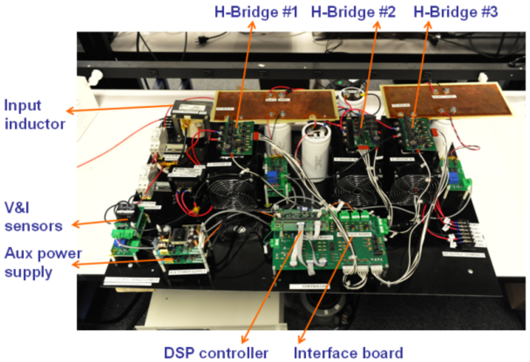
Smart Appliances

Center of Control?

Estimates of 45 Million Smart Appliances by 2020

Navigant Sept 2012


varentec
ENGO-V10


H-Bridge #1
H-Bridge #2
H-Bridge #3
Input
inductor
V&I
sensors
Aux power
supply
DSP controller
Interface board

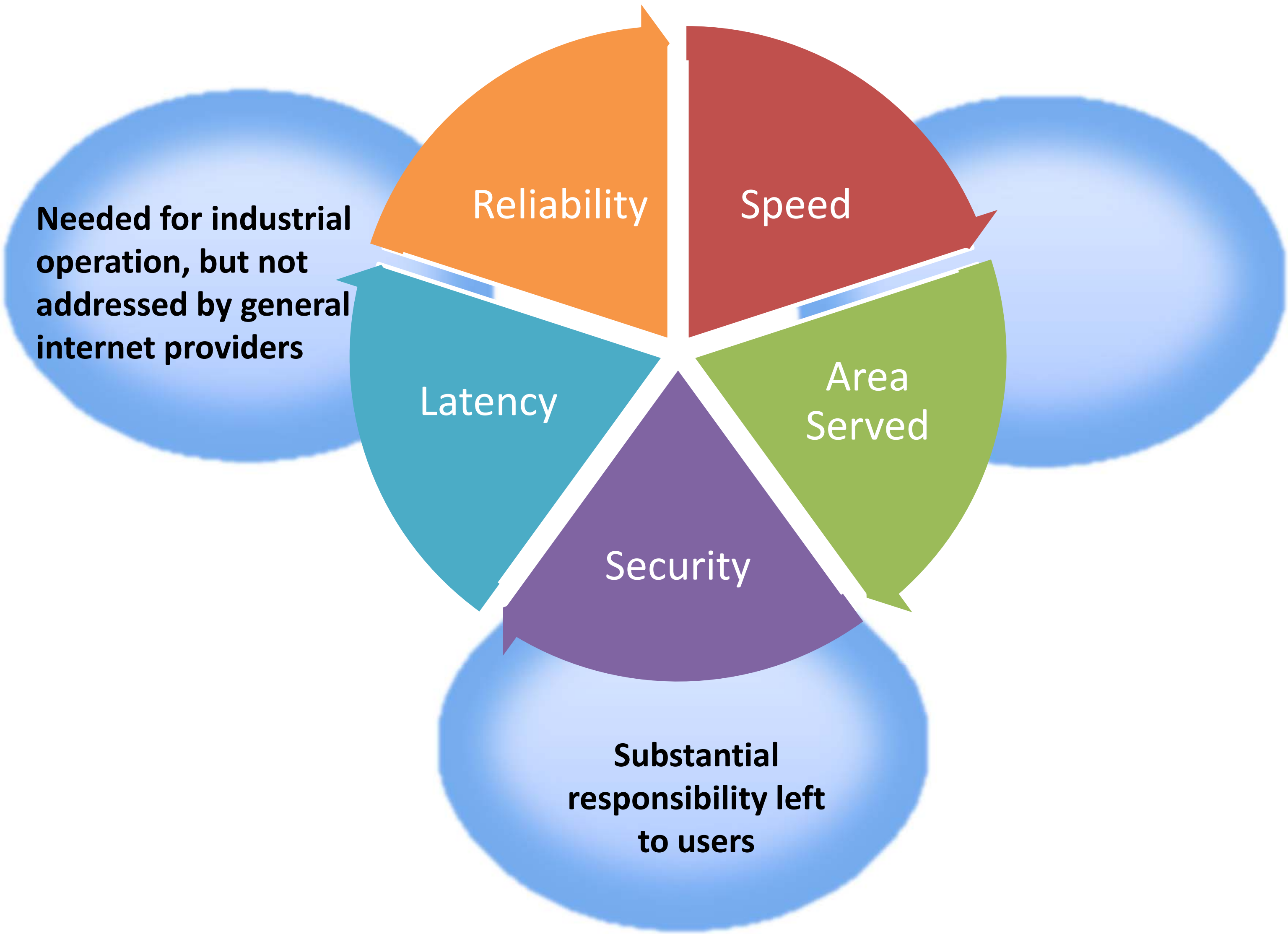
The Fear

- EPRI: 10^4 more data
- IBM: 10^5 more data

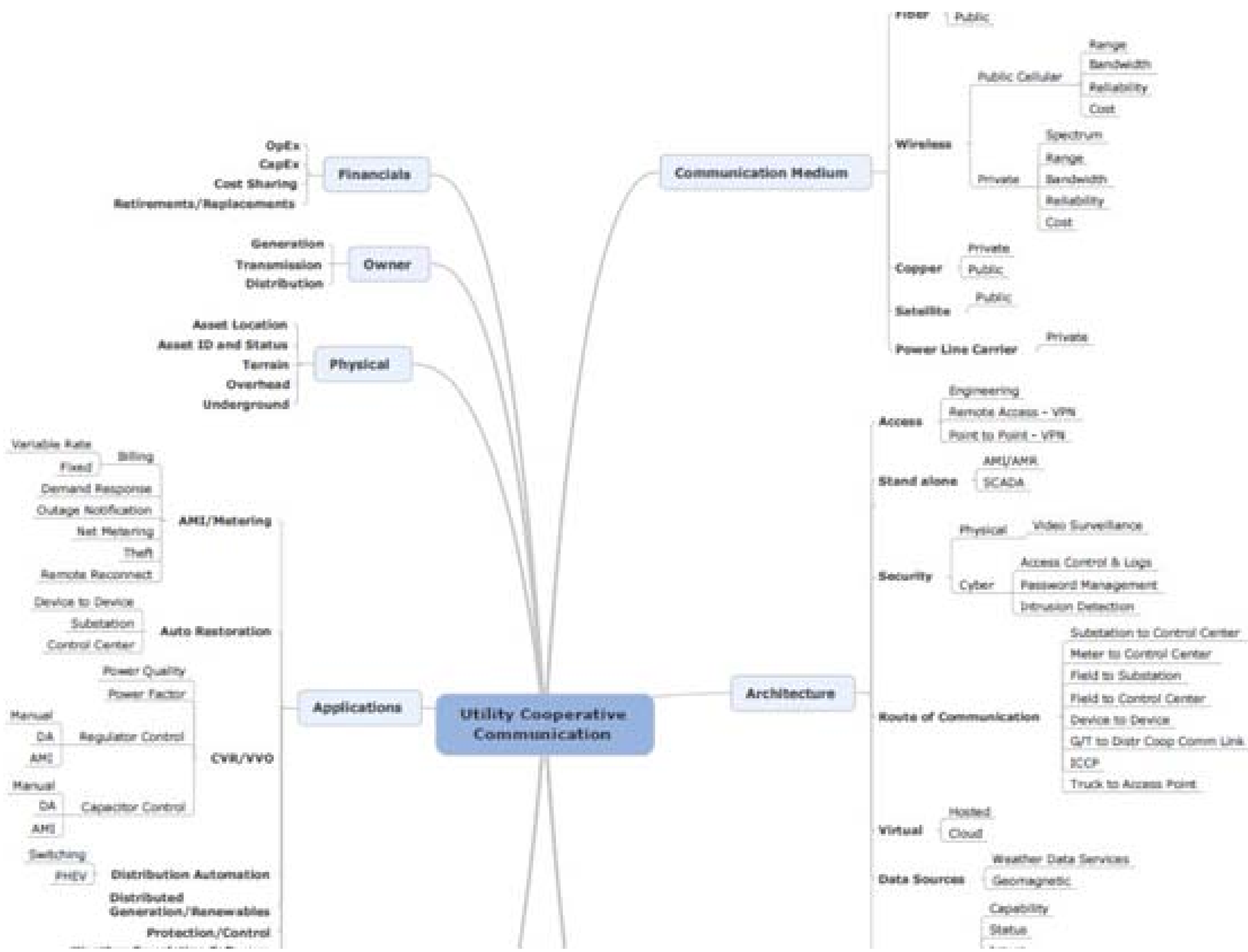
Surprise!! Didn't Happen, but:

Issues

- Transportation bottleneck
- Reporting by exception
- 99.998% redundant information
- Building for the “Interesting Day”


Reliability
Speed
Latency
Area Served
Security
Needed for industrial operation, but not addressed by general internet providers
Substantial responsibility left to users

Taxonomy of Communications



Key Organizations for the Trustworthy Internet

- Internet 2
- Internet of Things
- Industrial Internet

Internet 2


operated by INTERNET
Seattle
Spokane
Missoula
Billings
Dickinson
Fargo
Portland
Eugene
Bozeman
Miles City
Bismarck
Minneapolis
Boise
Madison
Syracuse
Albany
Buffalo
Boston
Detroit
New York (2)
Cleveland
Pittsburgh
Chicago (3)
Philadelphia
acramento
Indianapolis
Washington DC
Salt Lake City
Sunnyvale
Denver
Kansas City
St. Louis
Cincinnati
Louisville
Las Vegas
Raleigh
Los Angeles
Albuquerque
Tulsa
Memphis
Nashville
Charlotte
Atlanta
Dallas
Jackson
El Paso
Jacksonville
U.S. UCAN access point
Pensacola
Houston (2)
Baton Rouge
Draft – Last updated 01/26/11

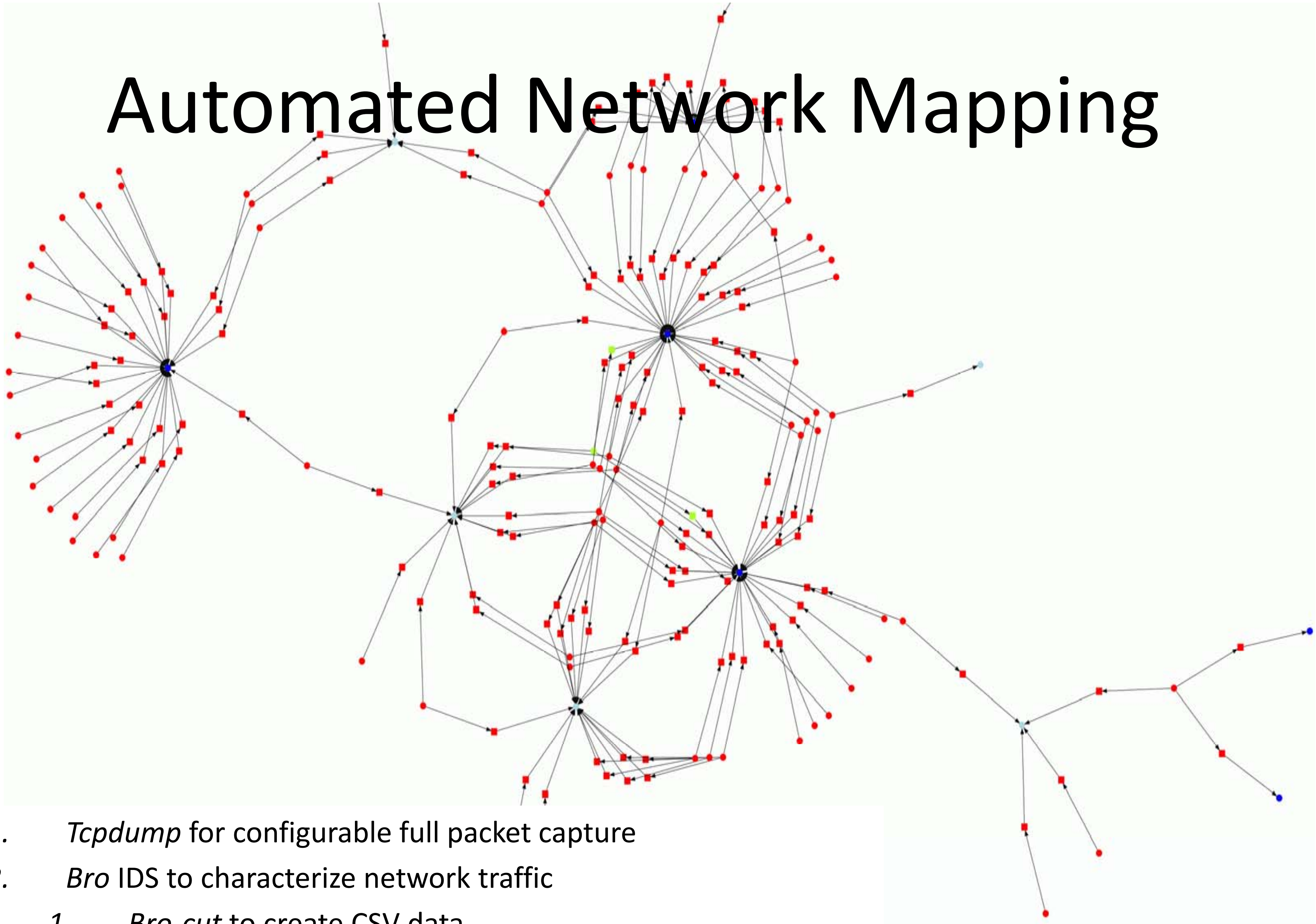
What is non-prescriptive cyber security and why do we need it?

- Prescriptive cyber security requires the user to identify the characteristics of suspicious communications
- Non-prescriptive is the opposite
- Prescriptive Security requires:
  - Knowing the threat
  - Knowing the system being protected
  - Having updates developed diligently
  - Knowledgeable users
  - Maintaining systems continuously
- There have been failures in all of the above

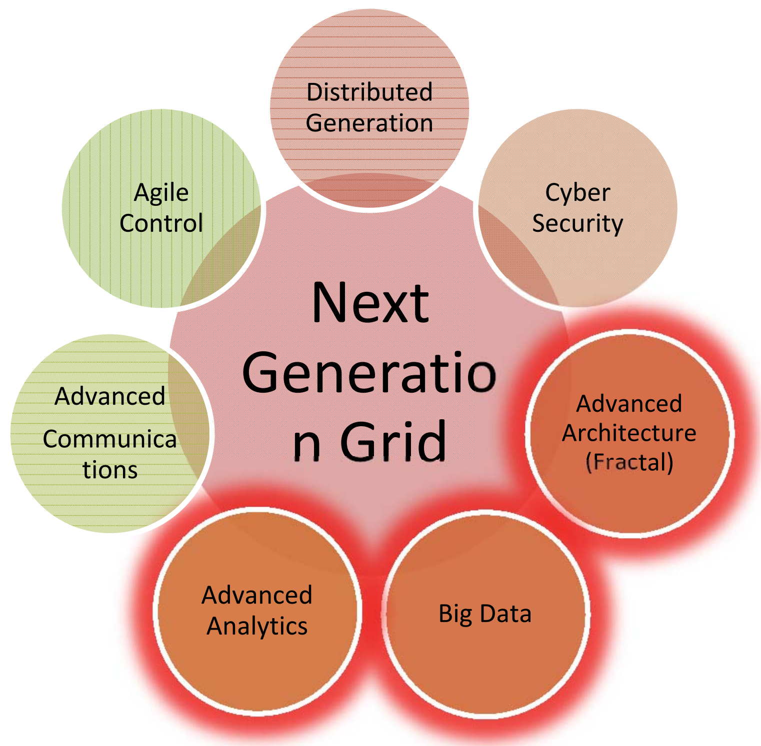
Full Packet Capture

- Data collection to support development
- Completely passive
- *NetOptics* TP-CU3 (copper)
- *Stealth* LPC-100G4
- Can also support fiber
- Open source software

Automated Network Mapping

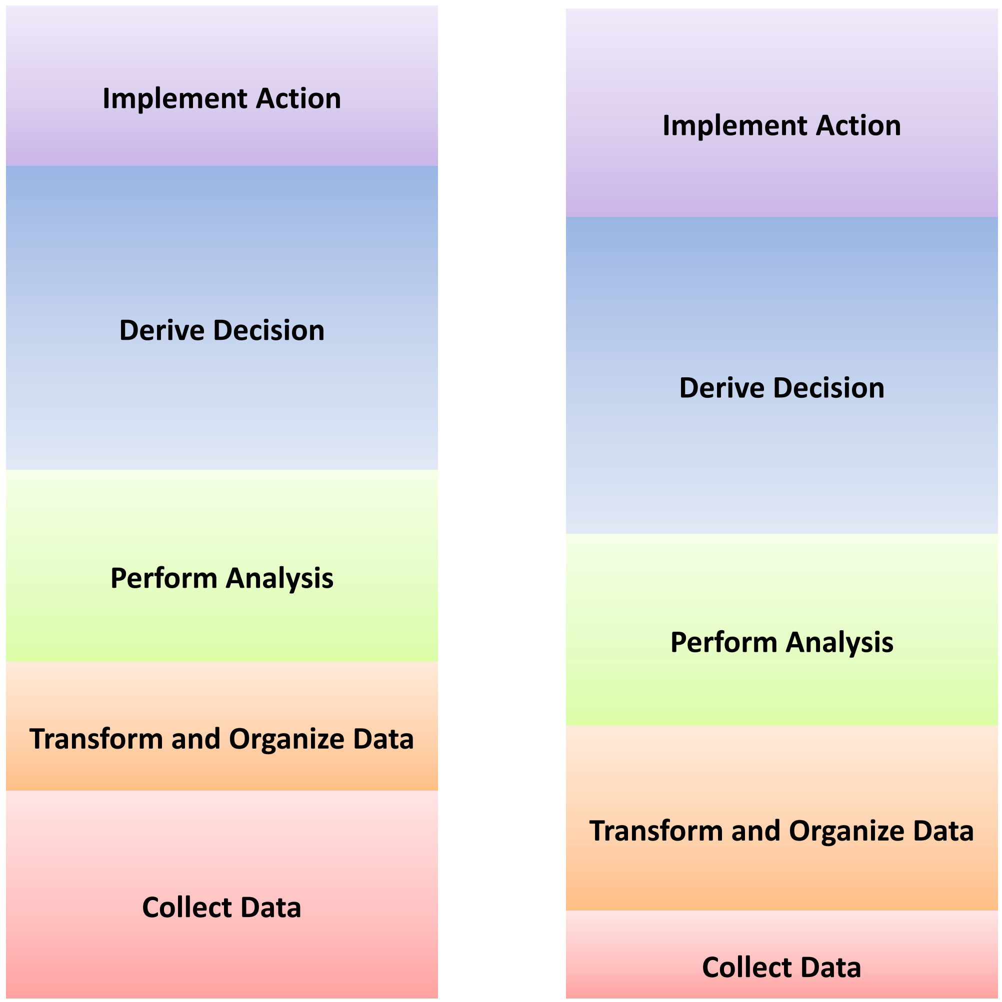


1. *Tcpdump* for configurable full packet capture
2. *Bro* IDS to characterize network traffic
    1. *Bro-cut* to create CSV data
    2. *Afterglow* to create graphviz files from CSV data
    3. *Neato* to draw graphs of observed network

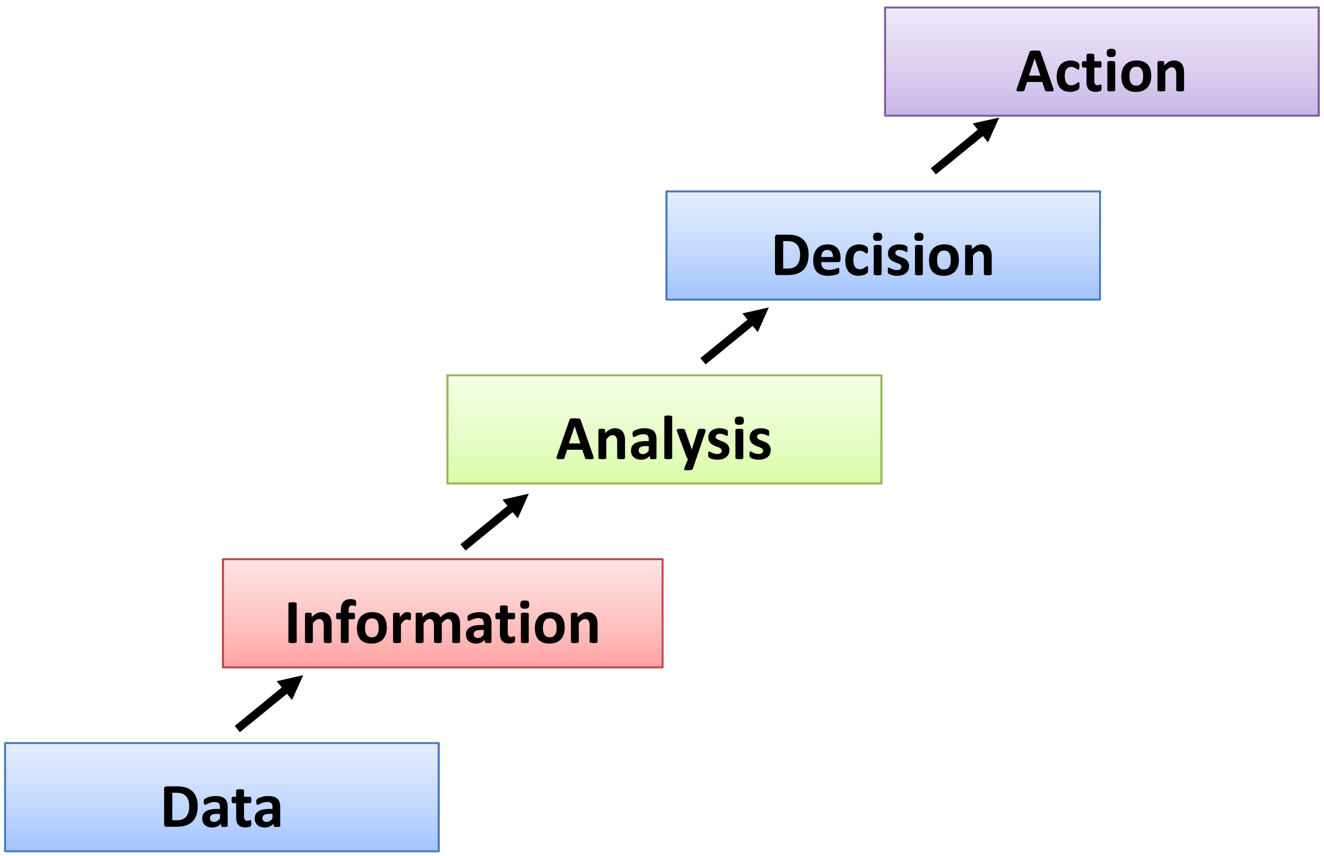


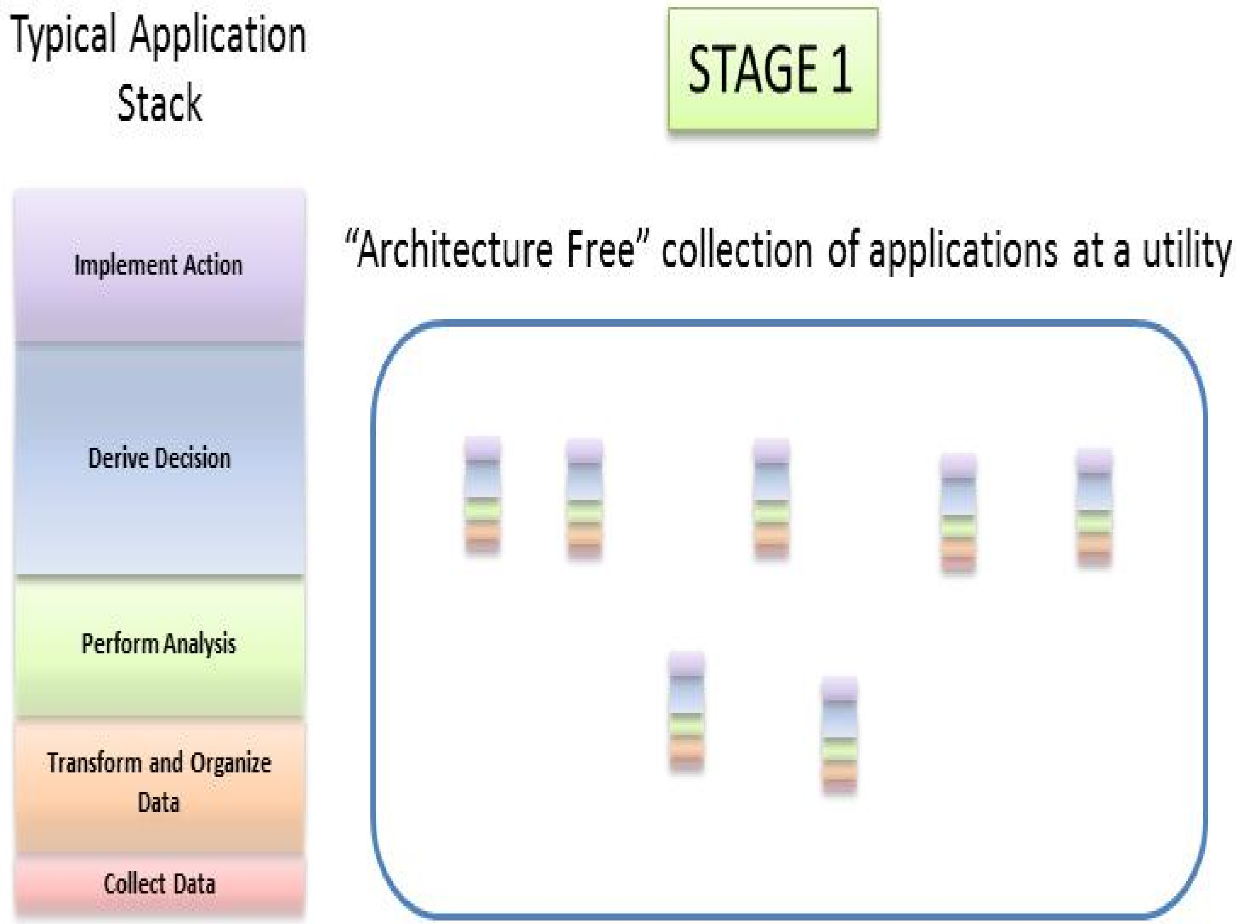
THE SOLUTION TO THE DATA ISSUE MUST BE ROOTED IN ARCHITECTURE

All grid applications have the same basic structure



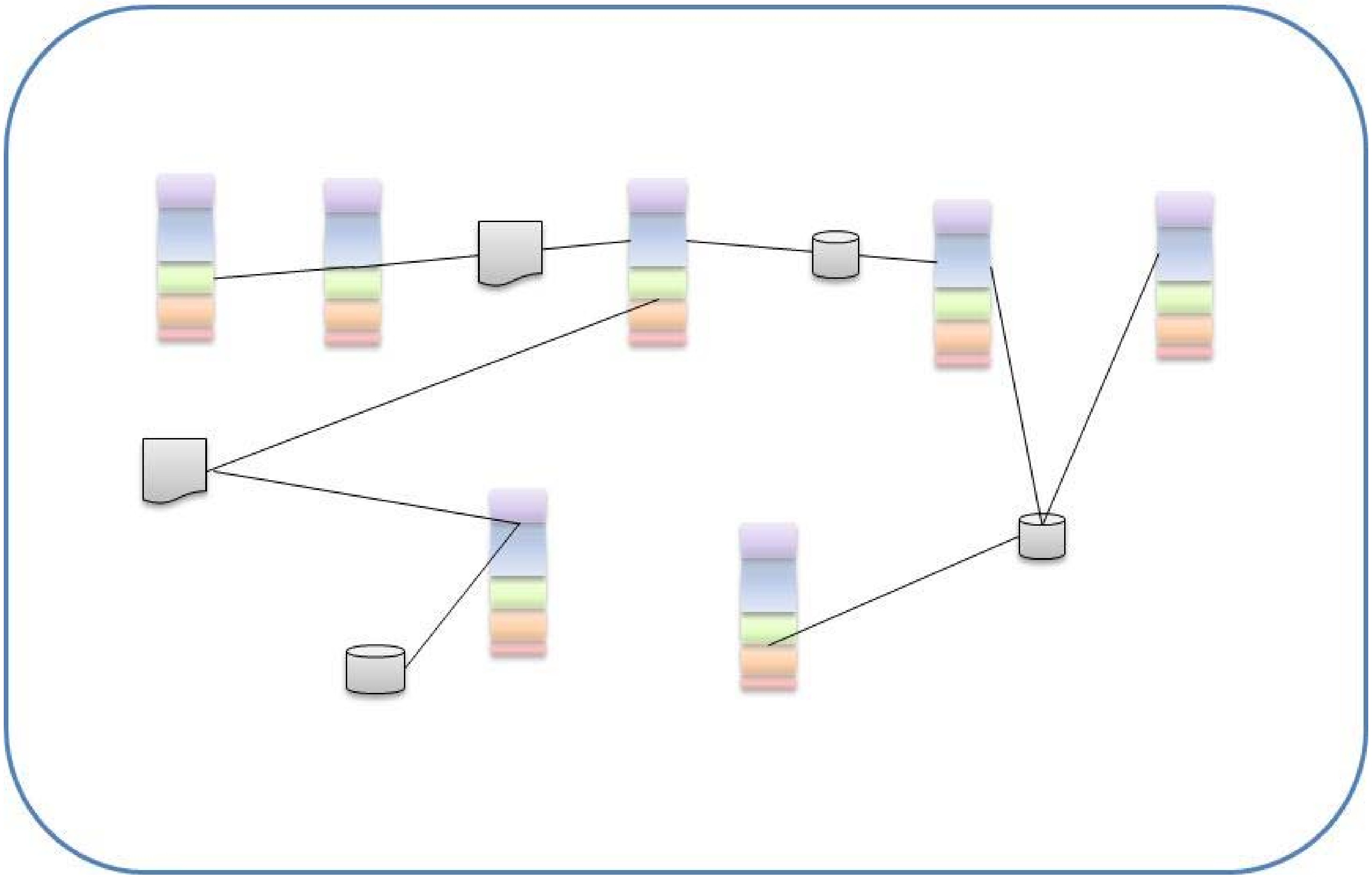
Abstraction Model

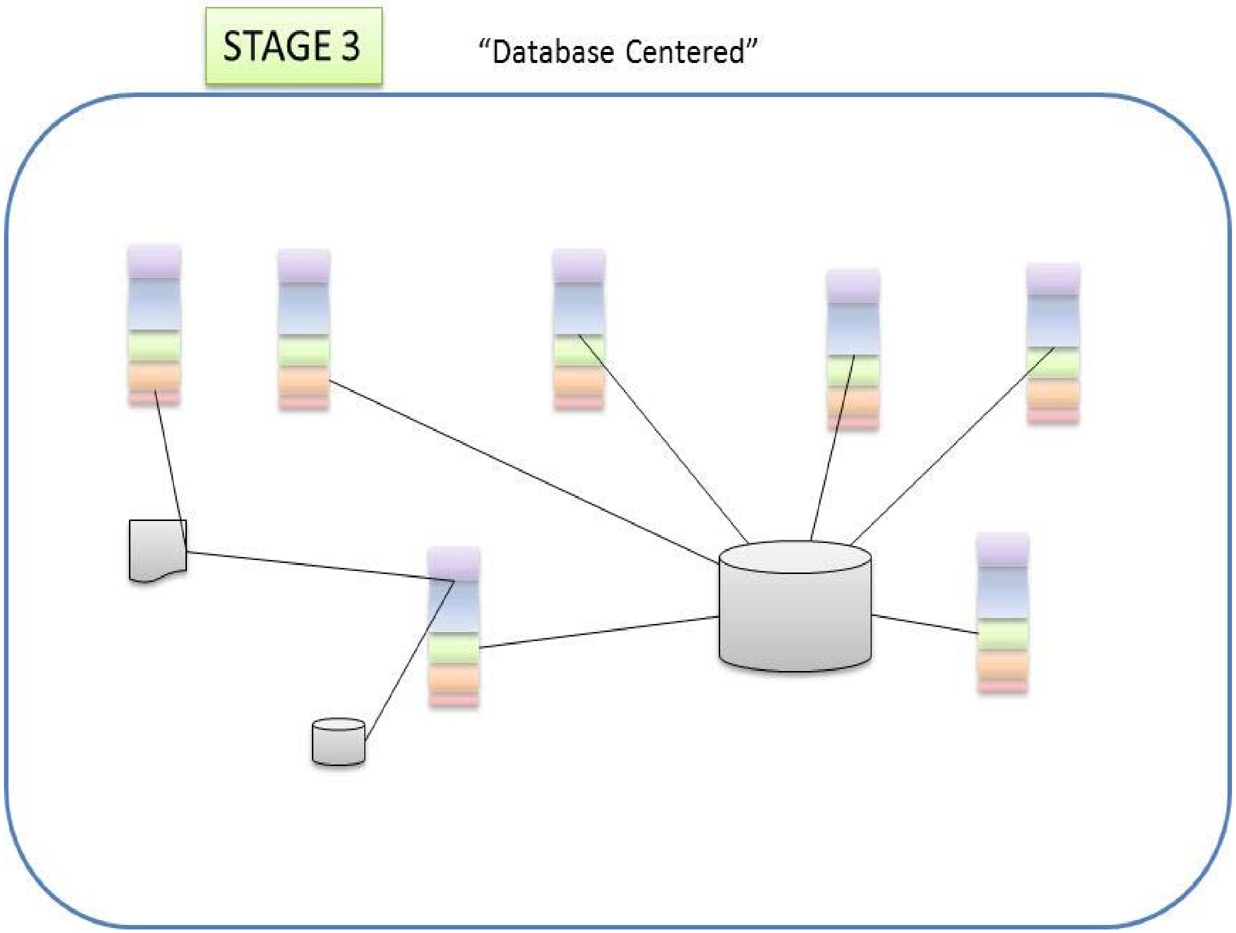



Typical Application Stack
STAGE 1
Implement Action
Derive Decision
Perform Analysis
Transform and Organize Data
Collect Data
"Architecture Free" collection of applications at a utility

STAGE 2

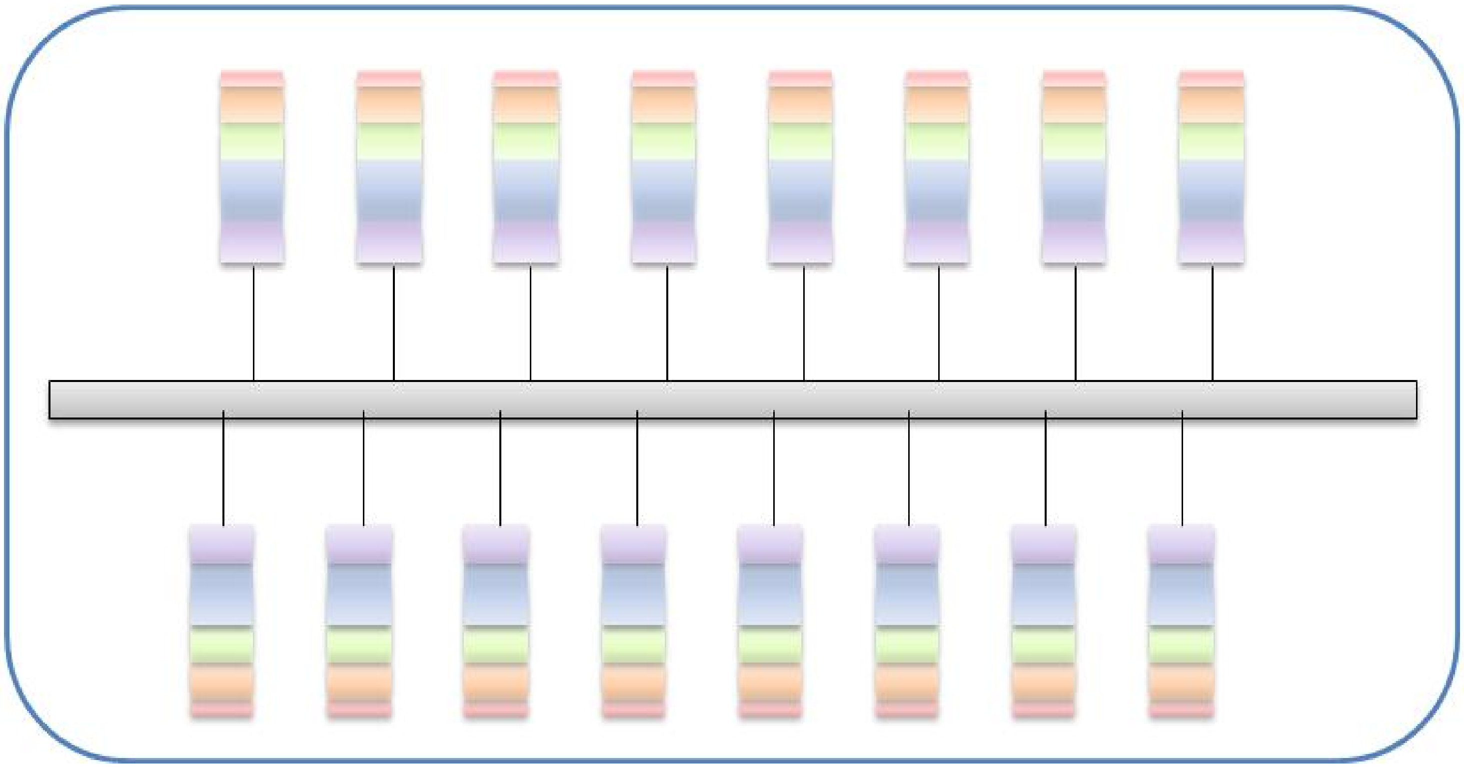
"Point to Point Connectivity"

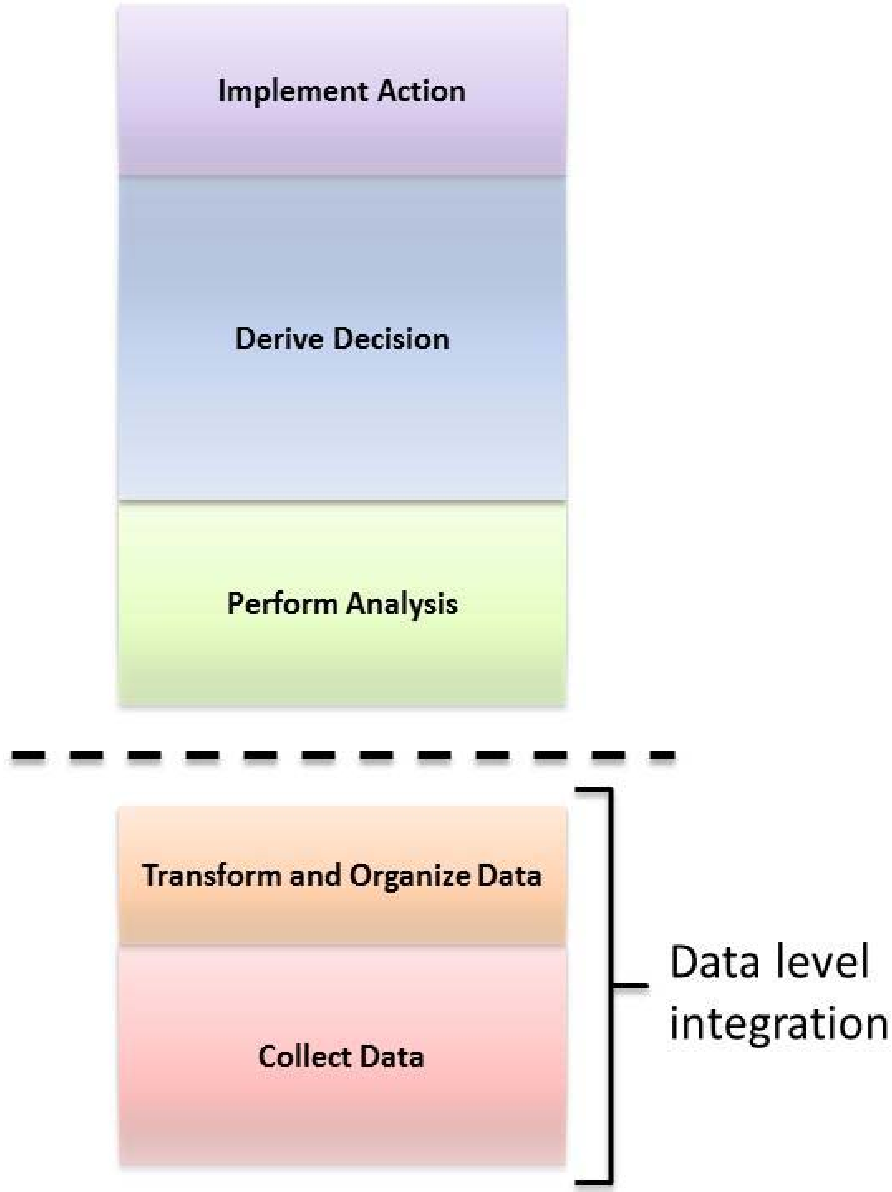


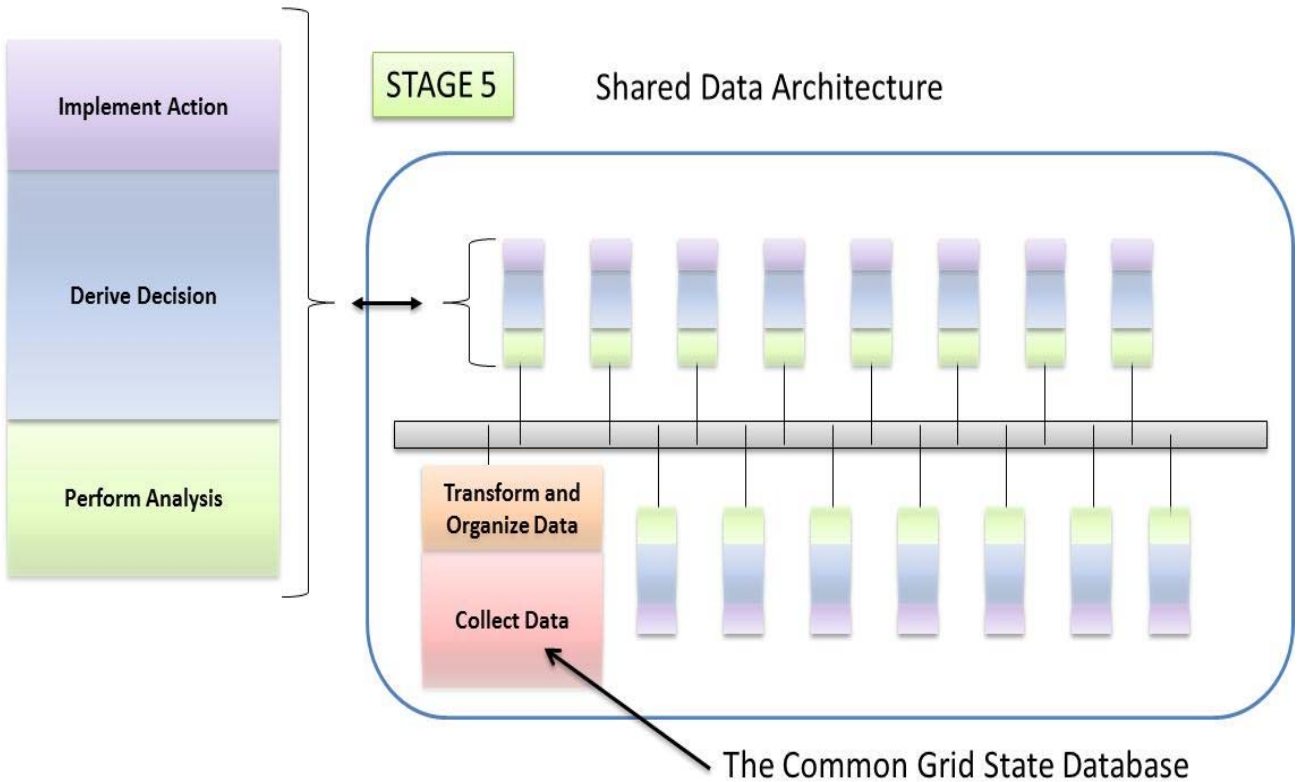

STAGE 3
“Database Centered”

STAGE 4

Enterprise Service Bus Architecture for Integration of Complete (full-stack) Applications




Implement Action
Derive Decision
Perform Analysis
Transform and Organize Data
Collect Data
Data level integration


STAGE 5
Shared Data Architecture
Implement Action
Derive Decision
Perform Analysis
Transform and Organize Data
Collect Data
The Common Grid State Database

ELECTRIC POWER RESEARCH INSTITUTE

U.S. DEPARTMENT OF ENERGY

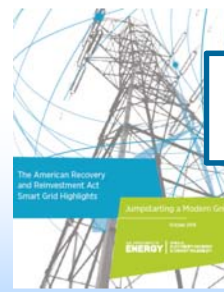
Communications & Cyber Security: Foundations of the Modern Grid

Distributed Intelligence Platform (DIP)

Stuart Laval
Duke Energy

October 28, 2014
Charlotte, NC

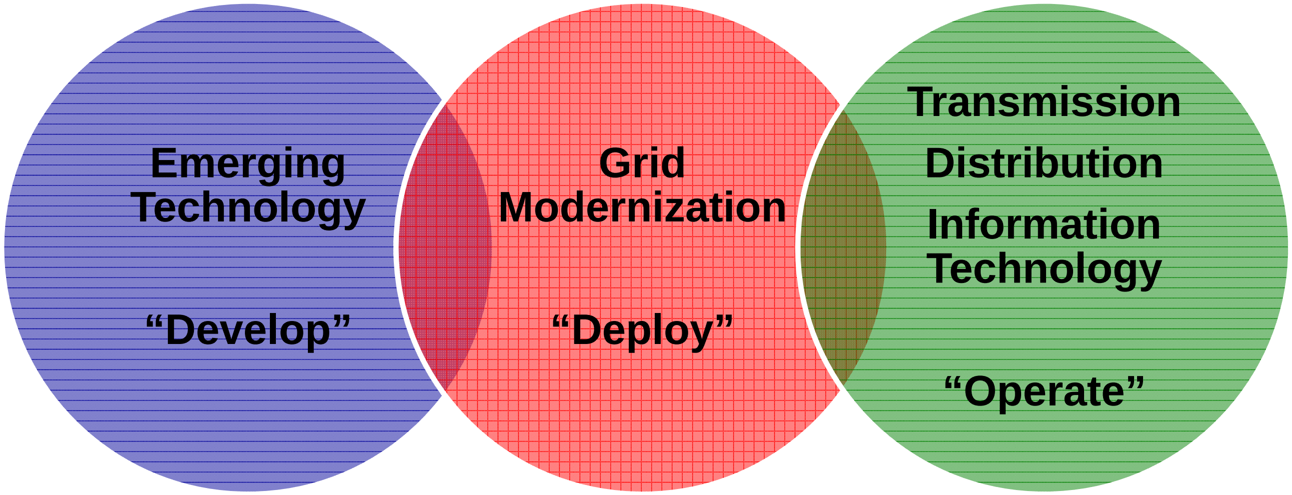
Pages 18-21



Pages 31-32

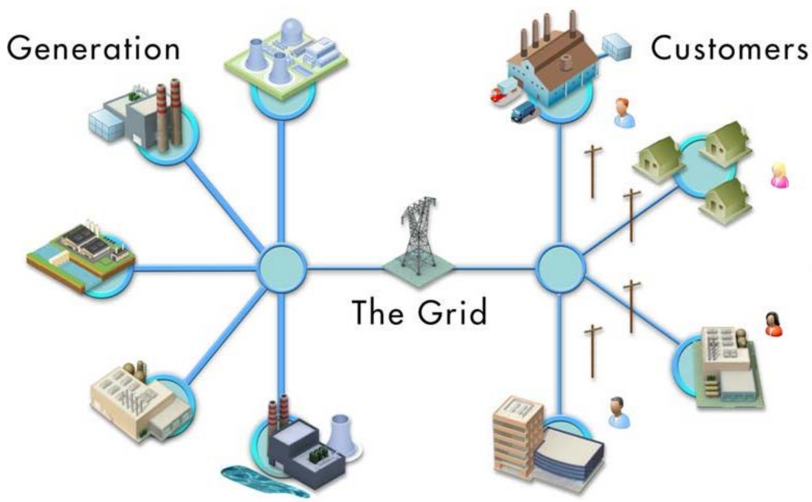
Emerging Technology Roles and Responsibilities

- Duke Energy Emerging Technology is responsible for:
  - Technology development and testing
  - New technology strategy, roadmap, risk and opportunity identification
  - Lab/field testing of new technology
  - Establish business value and initial business case



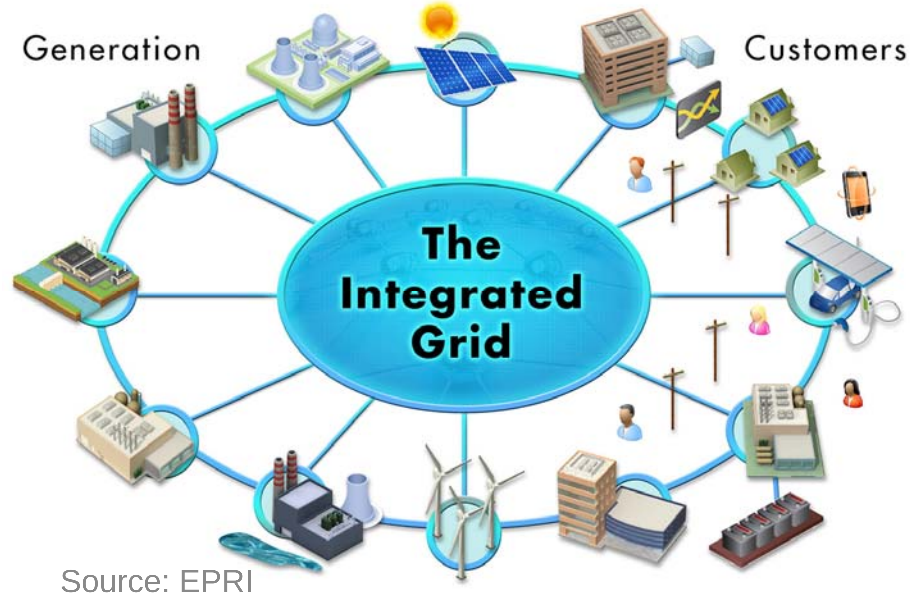
The Electric Grid: Past vs. Present vs. Future

<u>Past</u>



Source: EPRI

Future
<u>Present Path</u>



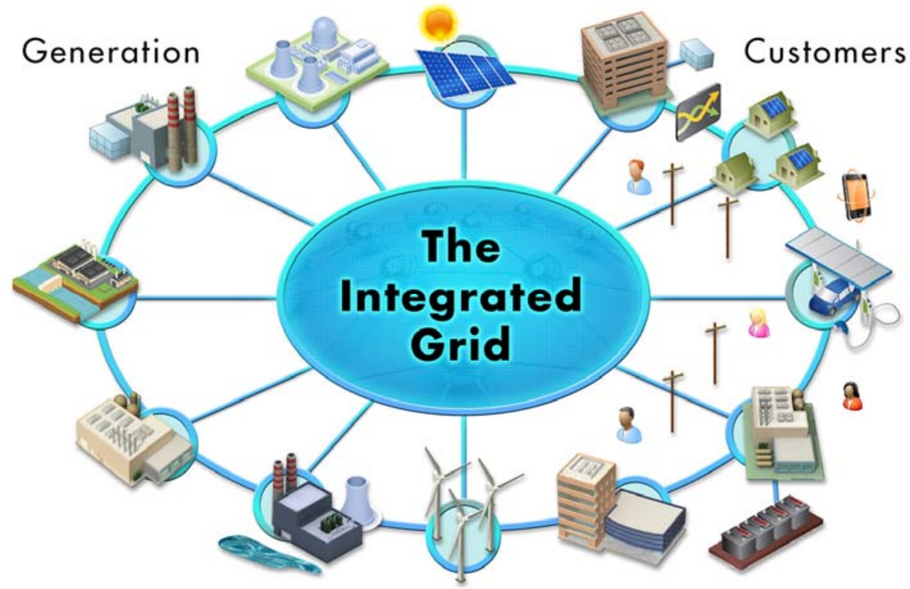
Source: EPRI

Core Mission:
1. Safe
2. Reliable
3. Affordable

Core Mission:
1. Safe
2. Reliable
3. Affordable
4. Environmentally Responsible
5. ~~Connected~~ Integrated

Strategy for the Integrated Grid

Drivers
- Distributed Energy Resources
- Demand Response
- Electric Vehicles
- In-Premise Automation
- Cybersecurity Threats
- Aging Infrastructure
- “Big Data” Complexity
- Stranded Assets



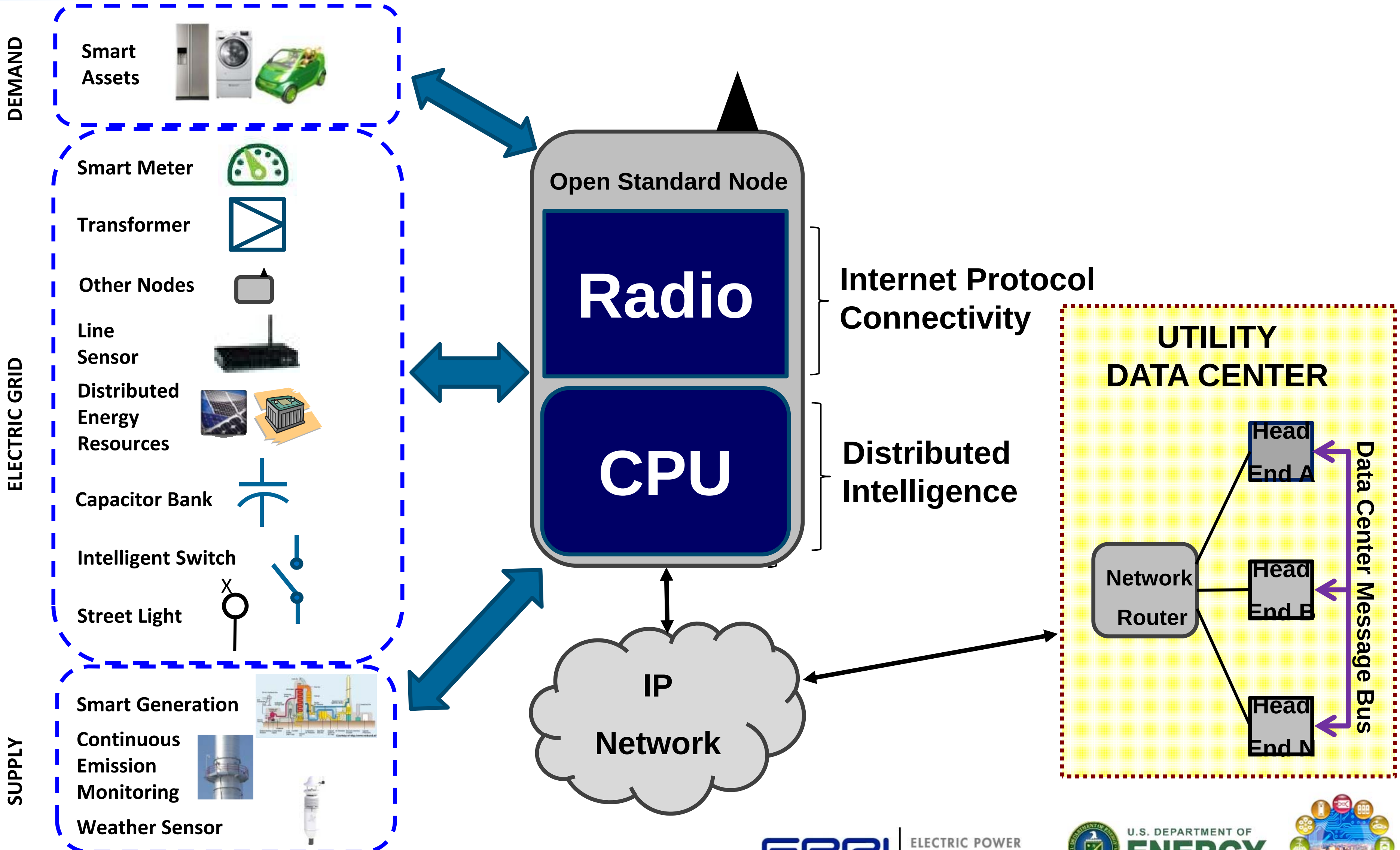
Source: EPRI

New Requirements
- Proactive Operations
- Situational Awareness
- Fast Edge Decisions
- Seamless Interoperability
- Modularity / Scalability
- Hybrid Central/Distributed
- Zero Touch Deployments
- Refined Utility Skillsets

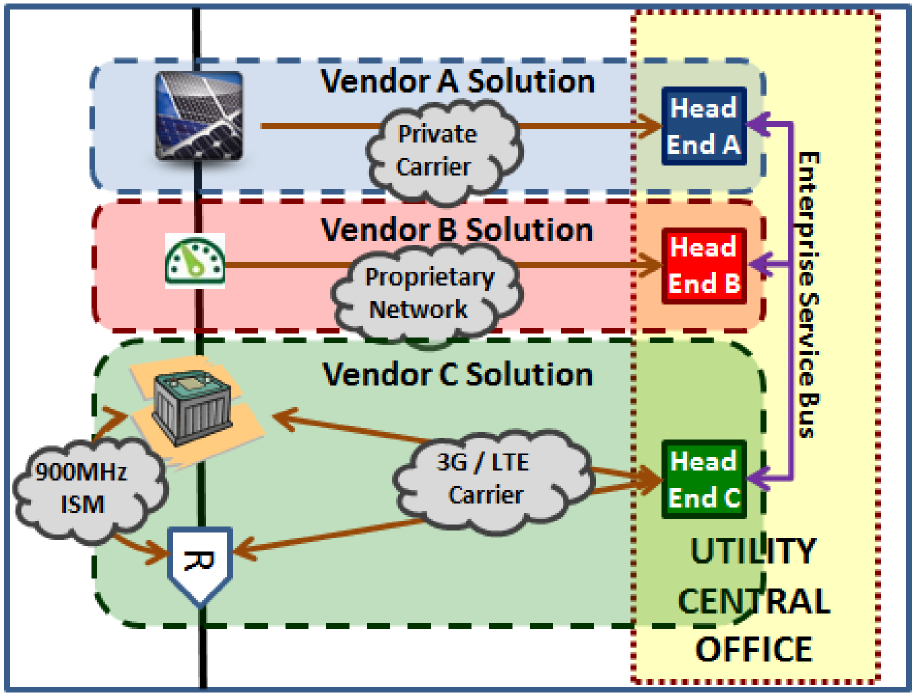
Technology Approach
1. Internet Protocol
2. Translation
3. Common Dictionary
4. Security
5. Analytics

Distributed Intelligence Platform (DIP)

DIP: "Internet of Things" Platform for the Utility



Field Message Bus: The Distributed "Internet of Things" Enabler

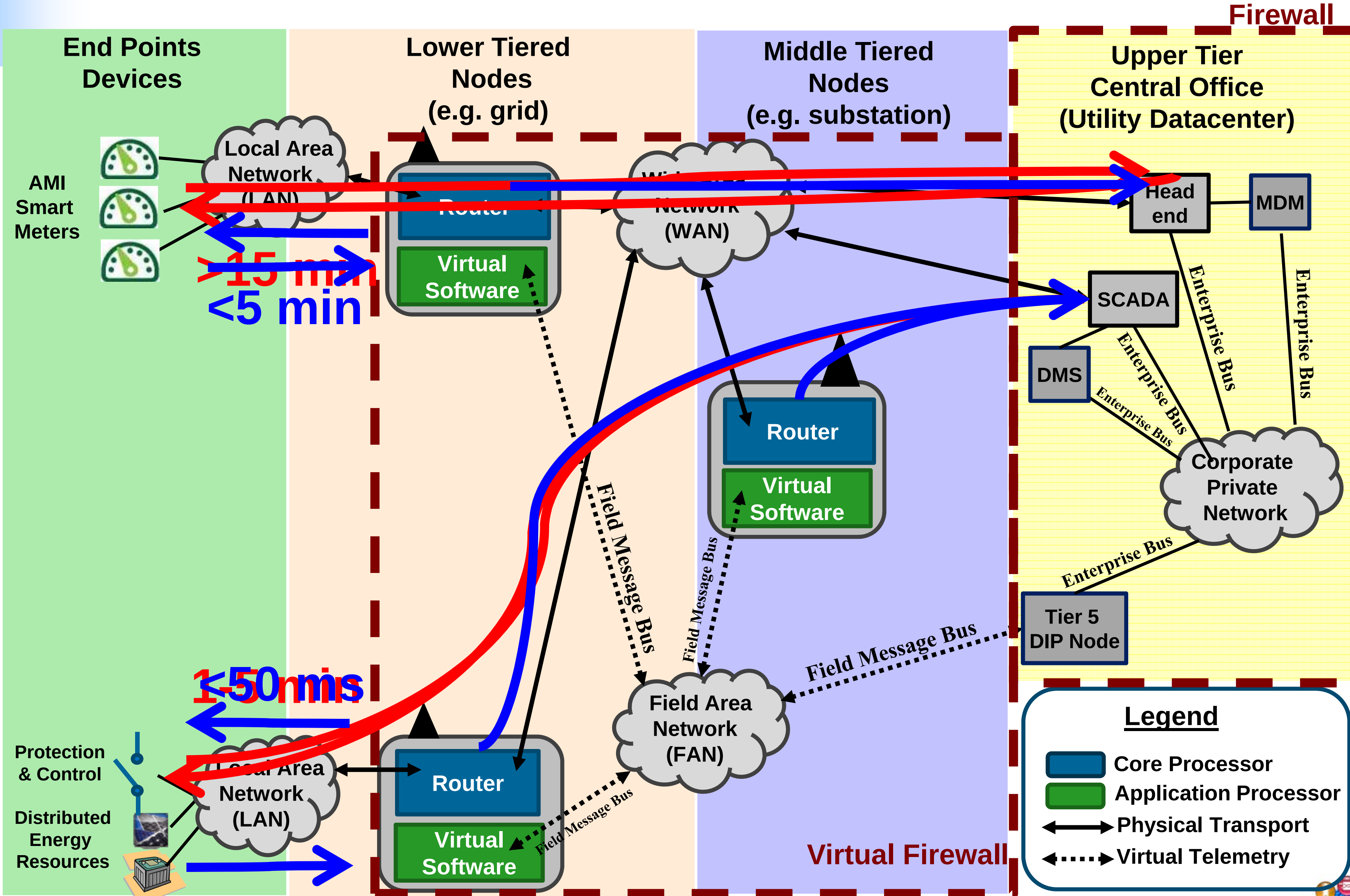


Current State – Message Bus at Data Center

- Interoperability between OT, IT, & Telecom
- Modular & Scalable Hardware and Software
- End-to-End Situational Awareness

Distributed Intelligence Platform

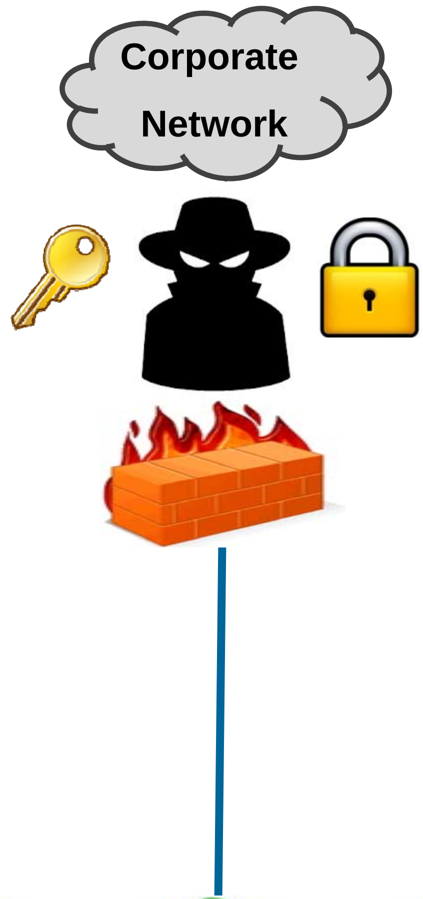
Multi-level Hierarchy: Seamless, Modular, Scalable



How Should We Evolve Our Cyber Security Capabilities?

A traditional firewall and encryption schema on a centrally-managed platform is not enough to survive against modern threats.

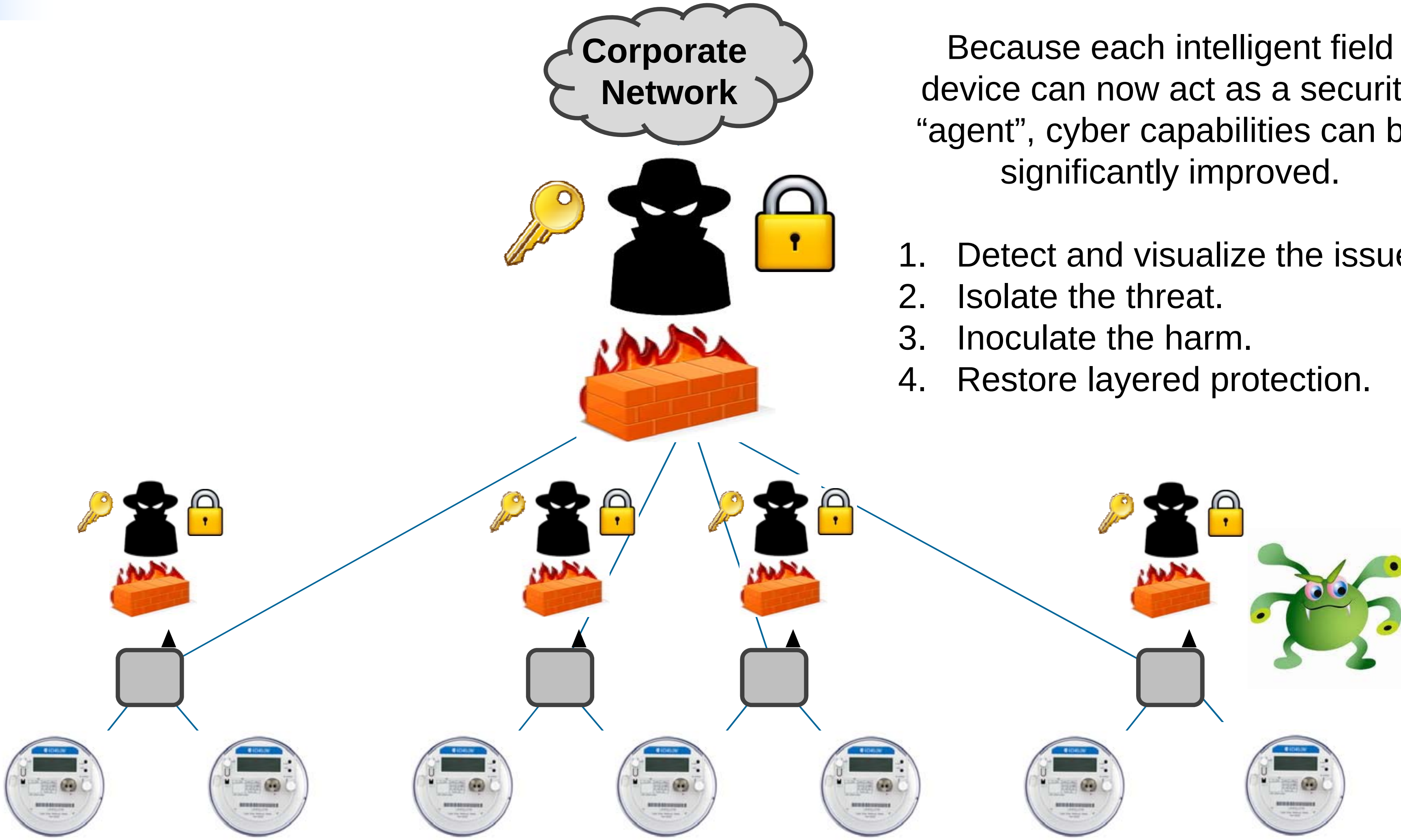
While a central, corporate network may survive, the security of field assets can be compromised.



For example, STUXNET is malware that targets SCADA and is spread via USB drive across a trusted network.

Modern attacks are aware of (and can defeat) common firewall and encryption techniques.

A Distributed, Standards-Based, Inter-Operable System Also Provides Significantly Enhanced Cyber Security Capabilities

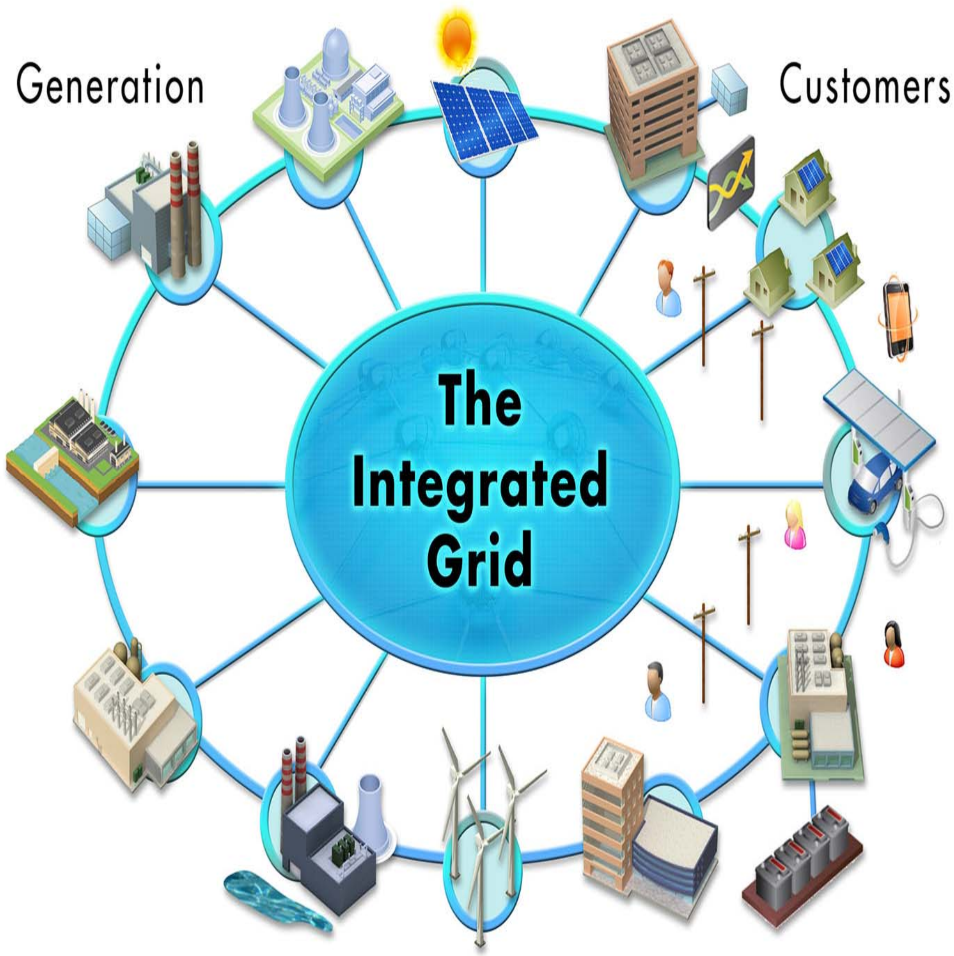


Because each intelligent field device can now act as a security "agent", cyber capabilities can be significantly improved.

1. Detect and visualize the issue.
2. Isolate the threat.
3. Inoculate the harm.
4. Restore layered protection.

Why is this Important for Duke Energy?

- Provides accurate control and alleviates intermittency of distributed energy resources
- Provides the ability to scale independently, as needed, without needing a system wide rollout
- Takes cost out of the business by reducing integration time and effort
- Allows Duke to be at the forefront of developing new regulations and policies

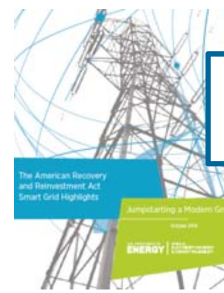


Questions / Discussion

Bio – Bob Yinger

- Consulting Engineer position in SCE's Advanced Technology group - focused on Smart Grid implementation
- 37 years experience with SCE working in research:
  - Solar and wind energy development
  - Communications technologies
  - Electronic metering
  - Substation and Distribution automation
  - Inverter behavior and integration
- P.I. and Chief Engineer – Irvine Smart Grid Demonstration
- BSEE Calif State Univ, Long Beach, P.E in electrical engineering, member of IEEE

Pages 80-85



Pages 63-64

Communications and Cyber Security: Foundations of the Modern Grid

Irvine Smart Grid Demonstration

Bob Yinger

Advanced Technology

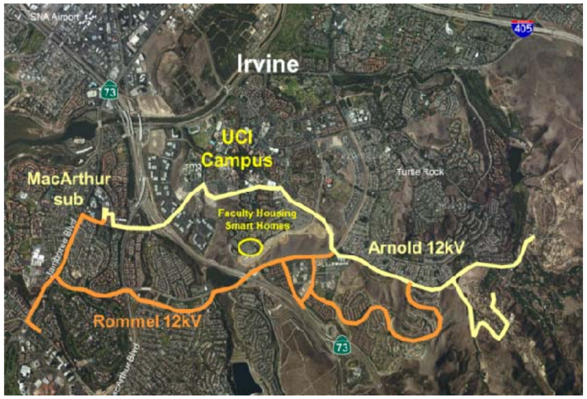
Southern California Edison

October 28, 2014

Charlotte, NC

Project Description

- Objective: Build and operate a cross-section of what the smart grid may resemble within 10 years
- Location – Irvine, CA (UC Irvine area)
- Key sub-projects:
  - **Zero net energy homes with storage**
  - Solar car shade with storage and EV charging
  - Distribution volt/VAR control system
  - **Advanced distribution circuit protection system**
  - IEC 61850 substation automation using Substation Configuration Language
  - **Advanced common cyber security services** and back office systems
  - Workforce of the future



Project Successes - Field Area Networks

- Implemented 4G public cell communications for data collection and control of in-home equipment
- Constructed distribution protection system assisted by low latency unlicensed radio network

Surprises – Field Area Networks

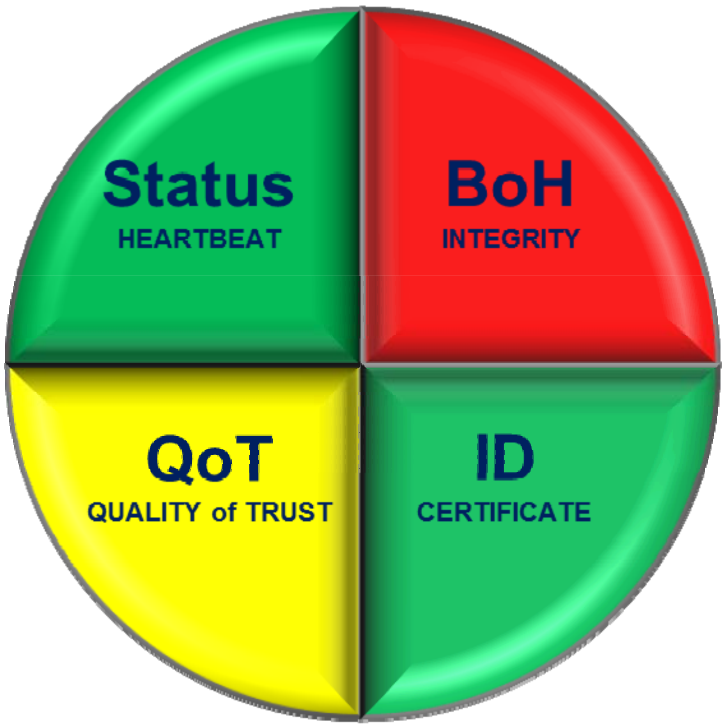
- 4G cell radio coverage not as good as expected causing data dropouts
  - Experimented with better antennae
  - Relocated equipment
- Low latency radios were hard to find and did not have coverage expected
  - Explored several systems that did not meet our needs
  - Vendor RF coverage claims are optimistic

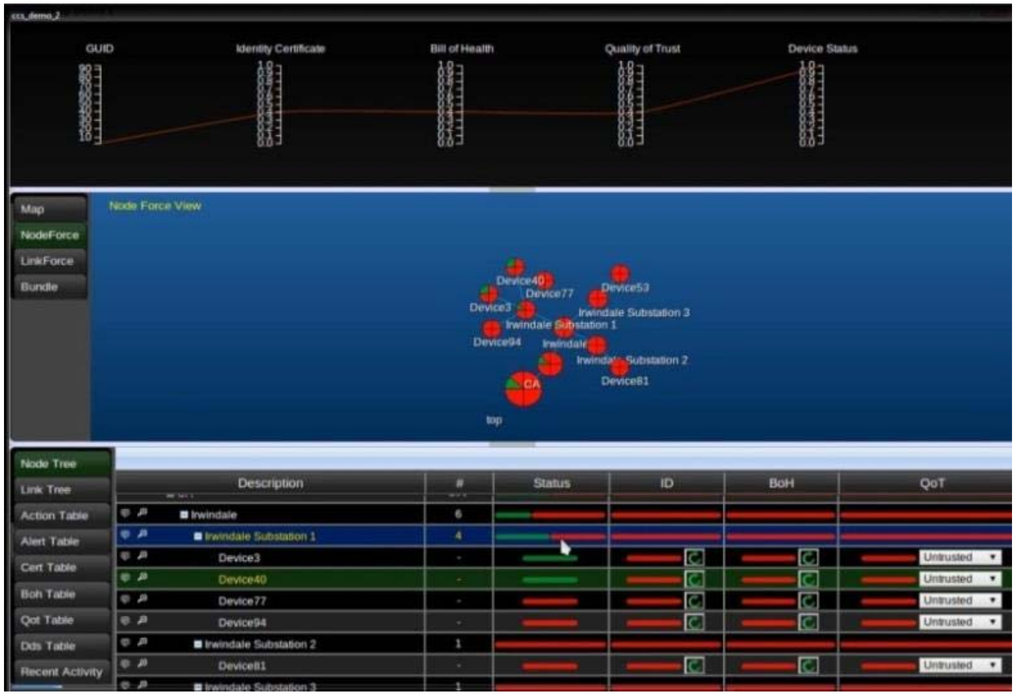
Reaching Beyond – Field Area Networks

- Radio bandwidth for private systems is not available or expensive which limits deployments to the unlicensed band or public networks
  - Can the FCC set aside bandwidth for utilities?
- Getting good radio coverage is difficult in the real world
  - Mesh networks can route around obstacles
  - Try to avoid engineering each link
  - Models just give indication of RF coverage
  - Trade-off deterministic latency for “good enough” latency
  - Antenna aesthetics are a big deal in underground areas

Project Successes – Cyber Security

- Implemented advanced centralized cyber security system
- Provided end-to-end security from back office to field equipment and substation automation system





Surprises – Cyber Security

- All existing systems in use when the project started seemed too "siloed" or were not scalable
  - Turned to tech transfer from the DoD
- While some standards existed, they did not cover the range of cyber security we wanted
  - Built centralized system to ease administration
  - Provided overview of whole system to allow threats on several fronts to be correlated

Reaching Beyond – Cyber Security

- Security risk = Probability of attack x Impact
- Grid modernization increases the places cyber attacks can take place (more connected devices)
- Need to push for open standards in the cyber security area so products will be interoperable
- Plan to meet future requirements of NERC CIP
- Scalability is critical because of the number of smart endpoints being installed on the grid
- Need to support legacy equipment with “bump in the wire” solution

Questions

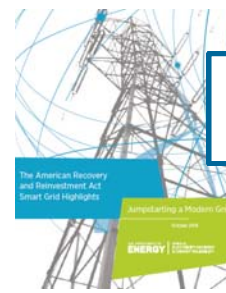
Bob Yinger
Advanced Technology
Southern California Edison
Robert.Yinger@sce.com

Presenter Bio:
Joe Nowaczyk, Director, SRP

- 30 years at SRP
- Variety of experiences including, Strategic Planning, Resource Planning, Marketing, Metering & Field Customer Services Substation and Transmission Line Design & Construction, Gas Fired Generation Engineering, Substation Maintenance, and more..
- Director of Electronic Systems for 7 years including, Communications, Control, and Protection Systems.

Joe Nowaczyk

Pages 78-79



Pages 52-54

ELECTRIC POWER RESEARCH INSTITUTE

U.S. DEPARTMENT OF ENERGY

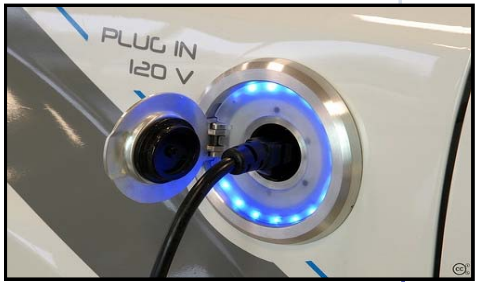
Communications & Cyber Security: Foundations of Modern Grid

The Smart Grid Experience: Applying Results, Reaching Beyond

October 27-29, 2014
Charlotte, NC

Smart Grid Demonstration – SRP FAN Pilot:

- Background
- SRP Field Area Network (FAN) Pilot
- Proposal

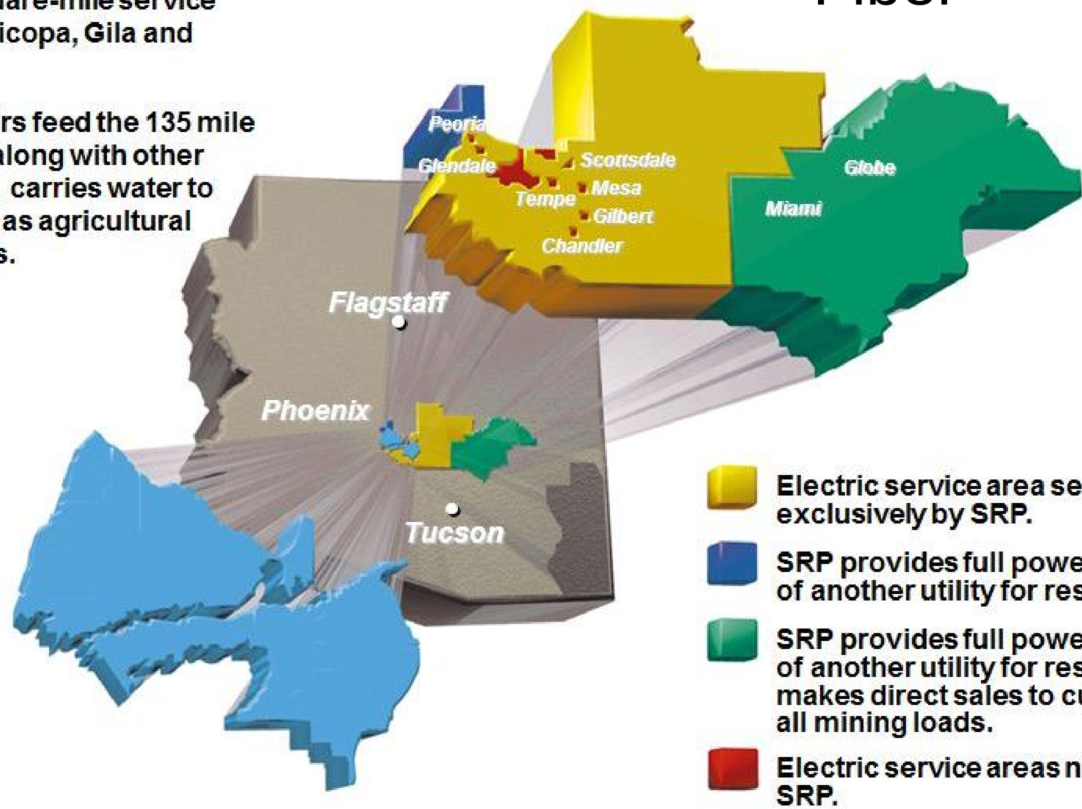


Background:
SRP Territories

The Salt River Project Agricultural Improvement and Power District provides electricity to power users in a 2,900 square-mile service area in parts of Maricopa, Gila and Pinal Counties.

SRP reservoirs feed the 135 mile canal system that, along with other smaller waterways, carries water to eight cities, as well as agricultural and urban irrigators.

- Microwave
- Fiber



- Electric service area served exclusively by SRP.
- SRP provides full power requirements of another utility for resale.
- SRP provides full power requirements of another utility for resale. Project makes direct sales to customers for all mining loads.
- Electric service areas not served by SRP.
- SRP's irrigated area.

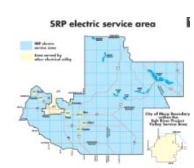
North

FAN Pilot:
Current Environment

- Different applications are utilizing different communications solutions
  - Distribution Feeder Automation (DFA) – Unlicensed 900MHz
  - Water SCADA – Licensed and Unlicensed 900MHz
  - Capacitor Control (VOLT/VAR) – 150MHz Licensed Paging System
  - Field Emergency Communications – 150MHz Licensed Paging System
  - Trunked Radio – 900MHz Licensed Land Mobile Radio System
  - AMI – 900 MHz Unlicensed Mesh, Commercial Cellular Backhaul
  - Vehicle Location – Commercial Cellular
  - Truck Mounted Laptops – Commercial Cellular
  - Power Quality Meters – Commercial Cellular

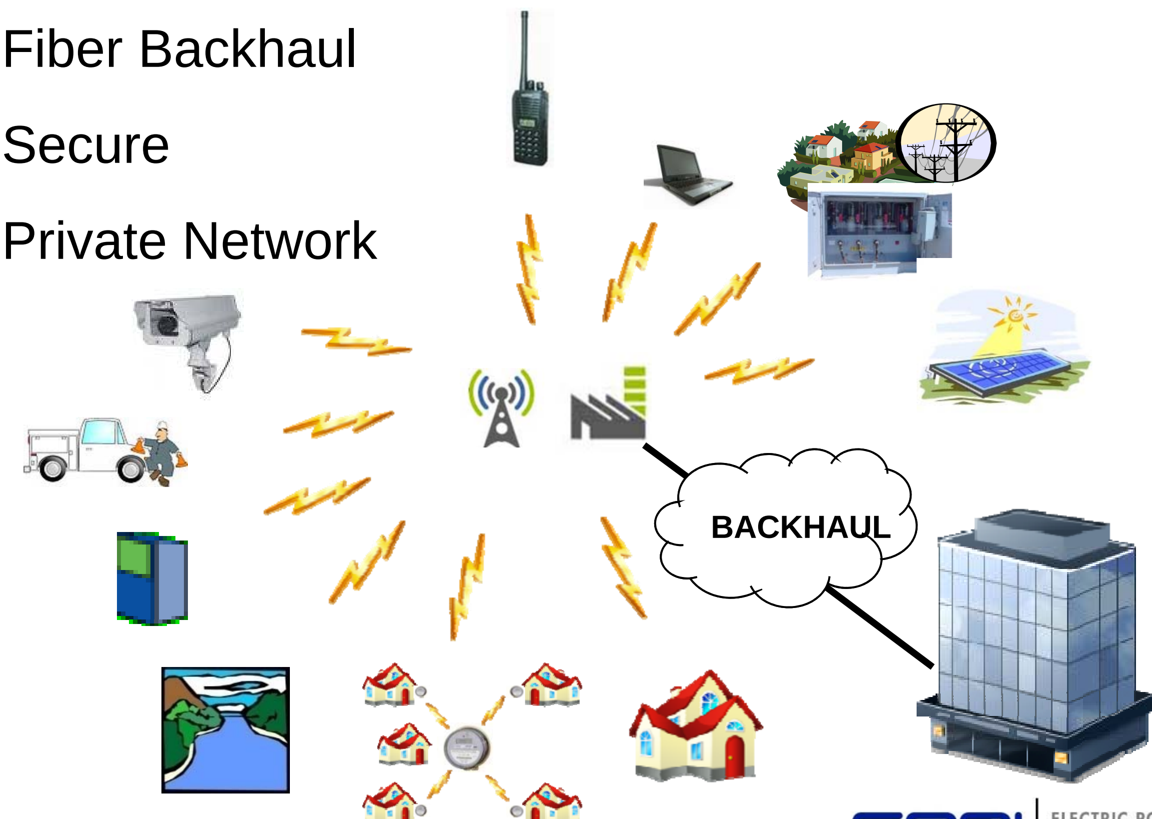
FAN Pilot:
Future Business Drivers

- Future grid automation and customer programs will bring proliferation of intelligent electronic devices (IEDs) to the field requiring communications.
  - DFA expansion supporting reliability improvements
  - Renewable energy resource integration
  - VOLT/VAR optimization for power quality & reduced losses
  - Remote fault indication to improve outage response
  - Distribution and meter data for real-time operations
  - Automation of water delivery infrastructure
  - Remote video surveillance to mitigate risks



FAN Pilot:
SRP Unified FAN Vision

- System Characteristics:
  - Broadband
  - Ubiquitous Two Way Communication
  - Fiber Backhaul
  - Secure
  - Private Network

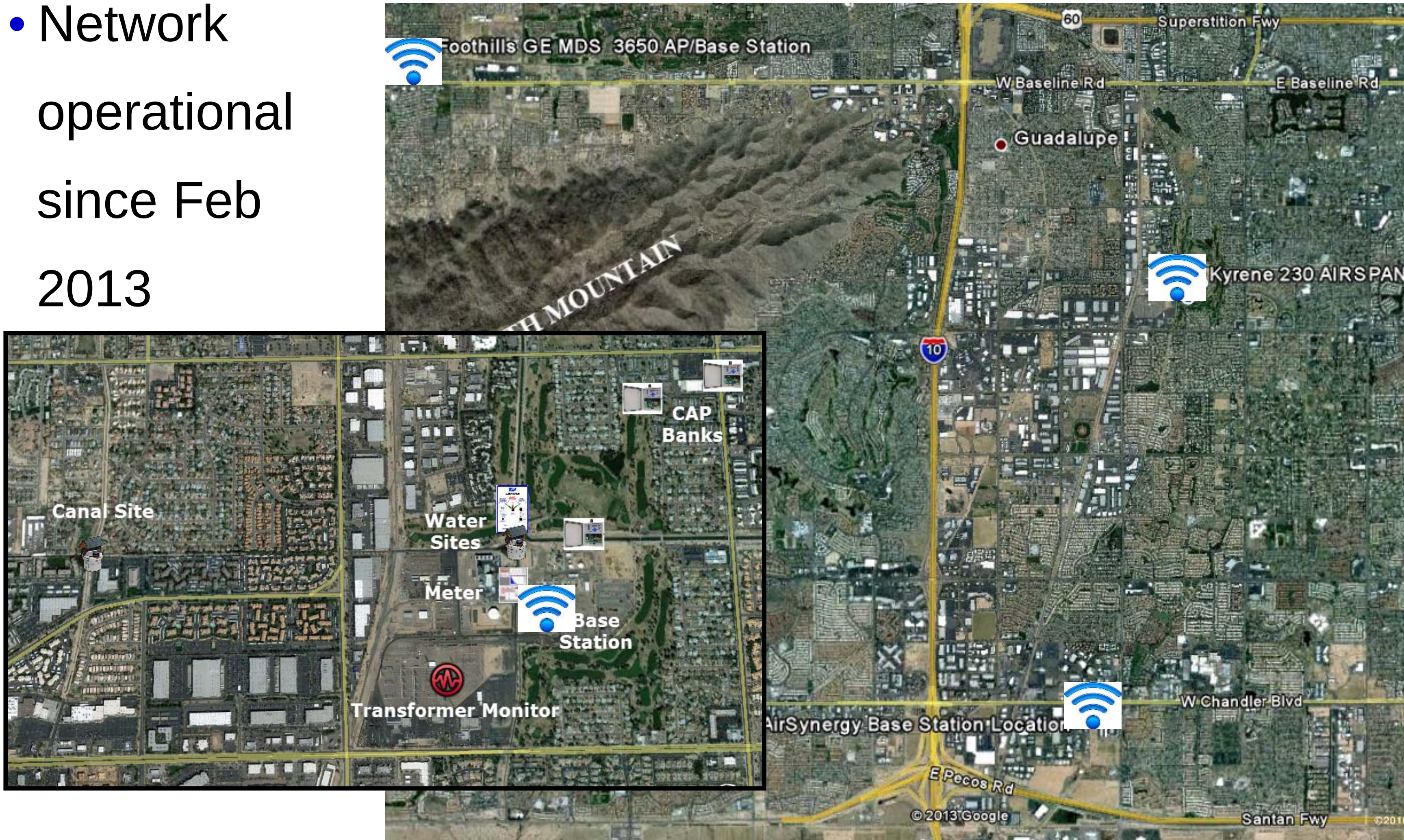


FAN Pilot:
SRP FAN Pilot Objectives

- SRP, in partnership with EPRI, launched a FAN Pilot in May 2012 with the goal to define a strategy for next generation field area communications
  - Implement base stations at three locations
  - Define requirements, integrate, and test 2-way communications for various end user applications
  - Assess technology (WiMAX vs. LTE, RF spectrum & cyber security)
  - Evaluate alternative public/private models
  - Assess the business case
  - Develop strategy & proposal

FAN Pilot:
SRP FAN Deployment

- Network operational since Feb 2013



FAN Pilot:

Implementation Models

	Public	Private	Hybrid	PSBN
Availability	Green	Yellow	Yellow	Red
Scalability	Green	Green	Green	Yellow
Traffic Prioritization/SLA	Red	Green	Yellow	Red
Fault Tolerance/Resiliency	Yellow	Green	Yellow	Green
Cyber Security Control	Yellow	Green	Yellow	Yellow
Service Coverage Control	Yellow	Green	Yellow	Yellow
Network Customization	Red	Green	Yellow	Yellow
Capital Expense (CAPEX)	Green	Red	Yellow	Yellow
Operational Expense (OPEX)	Red	Yellow	Yellow	Yellow

Green = Best, Yellow = Moderate, Red = Worst

FAN Pilot:
Scenario Evaluation

	Lic. LTE	3.65 WiMAX	WIFI Mesh
Spectrum	🟢	🟡	🟡
Technology Longevity	🟢	🟡	🟢
Equipment Availability	🟡	🟢	🟢
Total Cost of Ownership	🟢	🟡	🔴
Labor Resources	🟢	🟡	🟡
Cyber Security	🟢	🟡	🔴

	Lic. LTE	3.65 WiMAX	WIFI Mesh
Total Capital Cost	~$8M	~9.5M	~25M
Base Stations	30	128	3450

FAN Pilot:
Pilot Conclusions

- SRP is well positioned with backhaul, geography, real estate, and experience
- Unification of existing wireless systems is feasible
- Numerous application benefits enabling grid modernization & optimization
- Private is better than public networks
- Long Term Evolution (LTE) is preferred
- Licensed spectrum is preferred
- Strategy to deploy private field area networks common in utility industry

FAN Pilot:
Business Case Conclusion

A private wireless broadband network will enable application benefits and cost optimization

- Enables advanced grid automation & customer programs
- FAN decision similar to fiber build out strategy
- Private provides improved reliability and competitive NPV
- Unified platform needed in advance of project requirements
- Economy of scale optimizing cost and security architecture
- Private promotes use while public promotes minimization
- Large number of potential SRP customers
- Supports capital based funding model versus O&M

FAN Pilot:
Pilot Surprises

- Numerous Wireless Internet Service Providers (WISPs) Utilizing 3.65GHz
- FCC Database Inaccuracies
- Security vulnerability discovered related to rogue WiMAX base stations
- Gathering application requirements is challenging.

<u>Changes</u>

- Initially planned on leasing 1.4GHz
- Had to use 3.65GHz due to spectrum holder of 1.4 going bankrupt

FAN Pilot:
Lessons Learned

- The Phoenix area has a 3.65GHz user group for coordinating the use of 3.65GHz. There's no information on this on the FCC website. Coordinating with the users group would be important for any additional deployments of 3.65GHz. We discovered this when we interfered with local WISP. Action was taken and the issue was addressed coordinating through the users group.
- The 3.65GHz band would be challenging to deploy throughout SRP's service territory as the bulk of SRP's distribution system is underground. 3.65GHz would be better as an intermediate wireless backhaul solution from fixed clients that allowed for higher antenna heights. There would also be the potential for others to start deploying 3.65GHz and interfere with our system as we did with the WISP.

FAN Proposal:

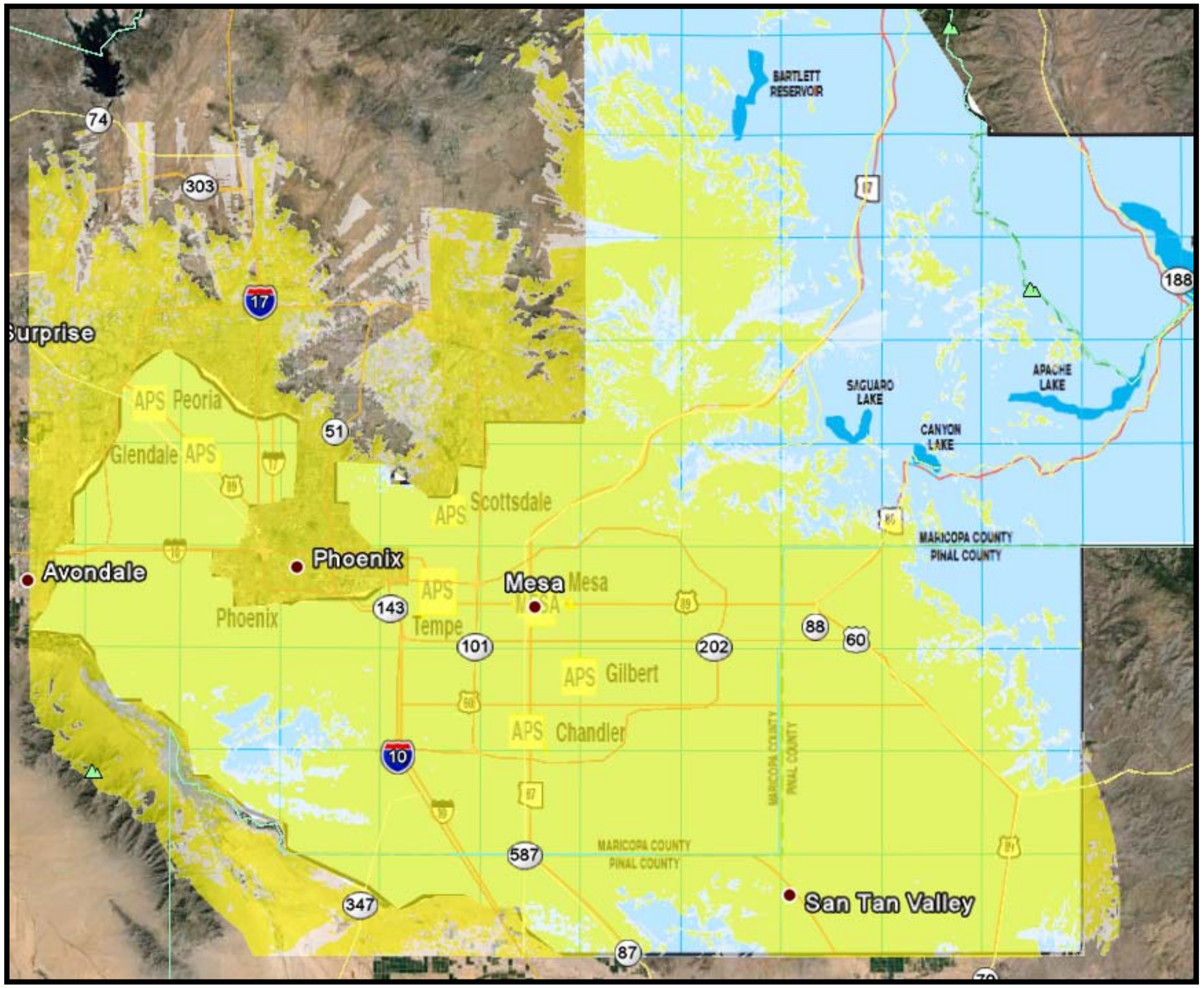
SRP FAN Proposal

Implement a private broadband network utilizing licensed spectrum as a strategic asset to get in front of future communications needs.

- Two new labor resources for O&M required
- Outdoor wireless coverage for power and water
- Long Term Evolution (LTE) – 30 sites
- Focus on reliability, performance & cyber security
- End point devices not included (Support is included)
- Requires licensed spectrum acquisition

FAN Proposal:
SRP FAN Proposed Wireless Coverage

- ~2,000 Square Miles
- 10Mbps
- 9K-15K devices



Yellow = Fixed outdoor wireless coverage, Blue = SRP Service Territory

FAN Proposal:
Potential FAN Applications

Distribution Feeder Automation (DFA)	Water SCADA (Gatekeepers)
Remote Fault Indication (RFI)	Water Measurement
VOLT/VAR Optimization	Substation/Plant Monitoring
Conservation Voltage Reduction	Renewable Generation SCADA
Aviation Light Monitoring	Physical Security & Surveillance
Power Quality Meters	Advanced Meter Infrastructure

FAN Proposal:
Implementation Risks

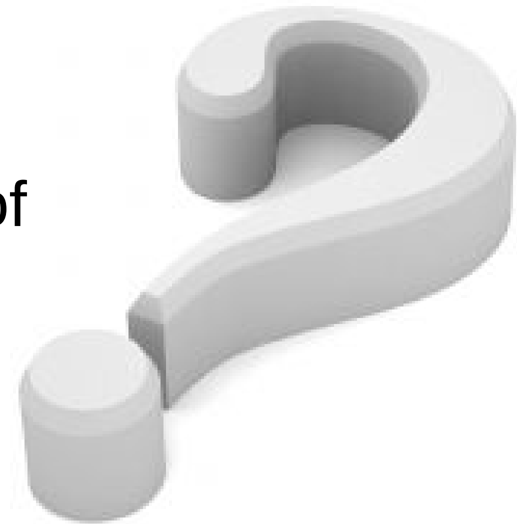
Risk	Impact	Mitigation
Availability of Licensed Spectrum	Lack of spectrum for procurement would eliminate the licensed option from consideration.	Research and test other scenarios while continuing pursuit of licensed spectrum
LTE Device Availability	Immaturity or lack of availability of "LTE Advanced" compatibility, re-banding in licensed frequency obtained and/or limited equipment availability would impact schedule.	Extend schedule to 3 years to allow the market to mature. WiMAX equipment could be considered as alternative to LTE.
Application Coordination	Large scale CPE deployments could strain resources. Difficult coordinating multiple budgets around FAN availability could create schedule issues.	Extend schedule to 3 years to allow coordination of end-user application plans. Work with stakeholders to ensure effective resource planning
Resource Constraints	Resources may be constrained due to conflicting priorities and availability causing delays.	Extend schedule to 3 years to avoid peak workloads currently anticipated in FY15. Add additional positions to cover ongoing support requirements. Ensure effective resource planning.

Questions / Discussion

Discussion Questions

- How is your communications/telecom group organized within your utility? How does that impact the development (planning and funding) of an integrated communication network?

- In weighing the pros and cons of public network operators vs private communications infrastructure for a FAN, what are your most important considerations?



Discussion Questions

- When considering hybrid types of communications networks, what are the primary factors leading to a multiple technology selection?

- When considering standards for communications and/or cyber security, what are the gaps between promise and reality? What are the lessons learned?

Together…Shaping the Future of Electricity

Tim Godfrey

650-855-8584

tgodfrey@epri.com