

# **Darknet collaboration between Utilities and National Labs**

## ***Shaping the Future Development and Application of Faster Grid Analytics and Modeling.***

**David Wells**

*Senior Advisor Department of Energy, Office of Electricity*

October 2019

# Office of Electricity

- Provide national leadership to ensure a secure, resilient and reliable energy delivery system.
- Develop technologies to improve the infrastructure that brings electricity into our homes, offices, and factories.
- Support development of the federal and state electricity policies and programs that shape electricity system planning and market operations.
- Drive electric grid modernization and resiliency through research, partnerships, facilitation, and modeling and analytics.



# Many Threats Facing US Energy Infrastructure


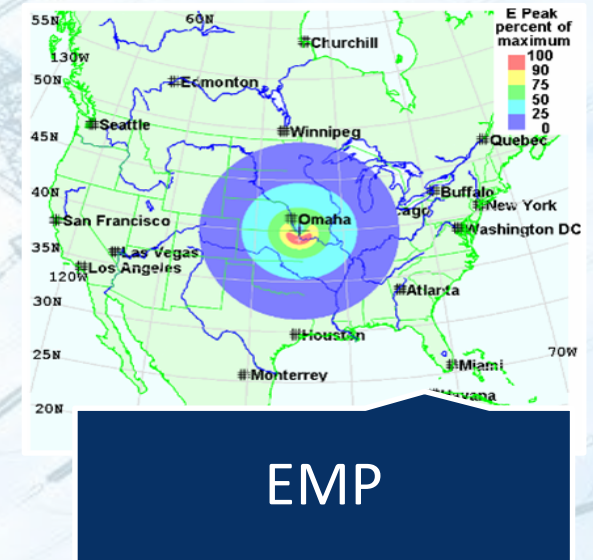
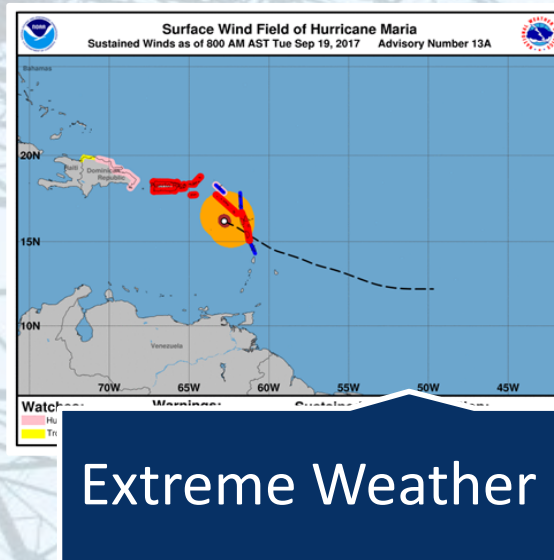


Diagram illustrating various cyber threats to energy infrastructure:

- Malicious Firmware Development
- SCADA Hijack (HMI/Client)
- Breaker Open Commands
- UPS Modification
- Firmware Upload
- KillDisk Overwrites

Attack 1

**Cyber Attacks**

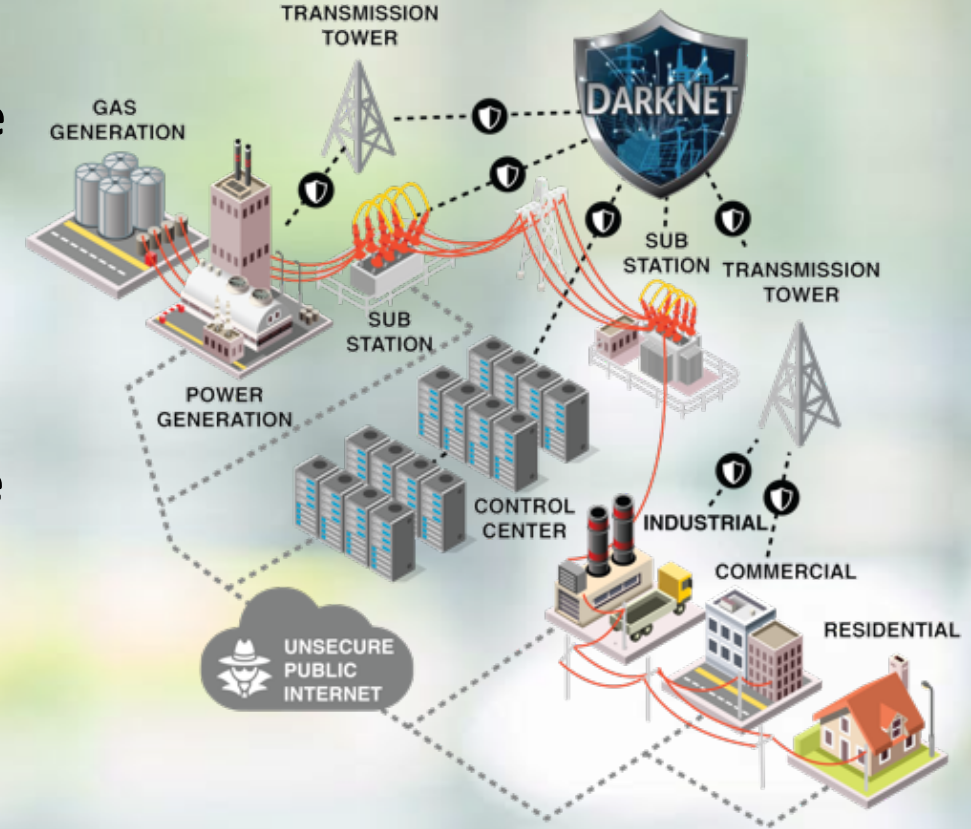


Ballistic Protection



# DarkNet: Project Scope

- Perform research, development and demonstration of the scalable designed architecture as “best practice, gold standard” communication network using existing infrastructure providing energy delivery systems grid data transport.
- Research and development of high fidelity and responsive sensing techniques and systems.
- Demonstration projects will include validation of the resilient network architecture and a network linking with substations within the Power Marketing Administrations (PMAs), pilot integration systems deployed in multiple sites, and utilization of the ORNL testing facility. The ORNL testing facility will be adapted to enable high speed sampling, measurement, and anomaly testing.



# Key Priorities

**Non GPS based Synchronization network supporting government owned substation assets conforming to Precision Timing Protocol 1588( PTP).**

**Verification of substation control cabling for accuracy, maintenance and affects over time and environment.**

**Revolutionizing Sensing Technology Utilization**

**Design an architecture based on internal synchronized timing source for all IT/OT related processes**

**Secure blockchain driven command and control system based on internal synchronization**

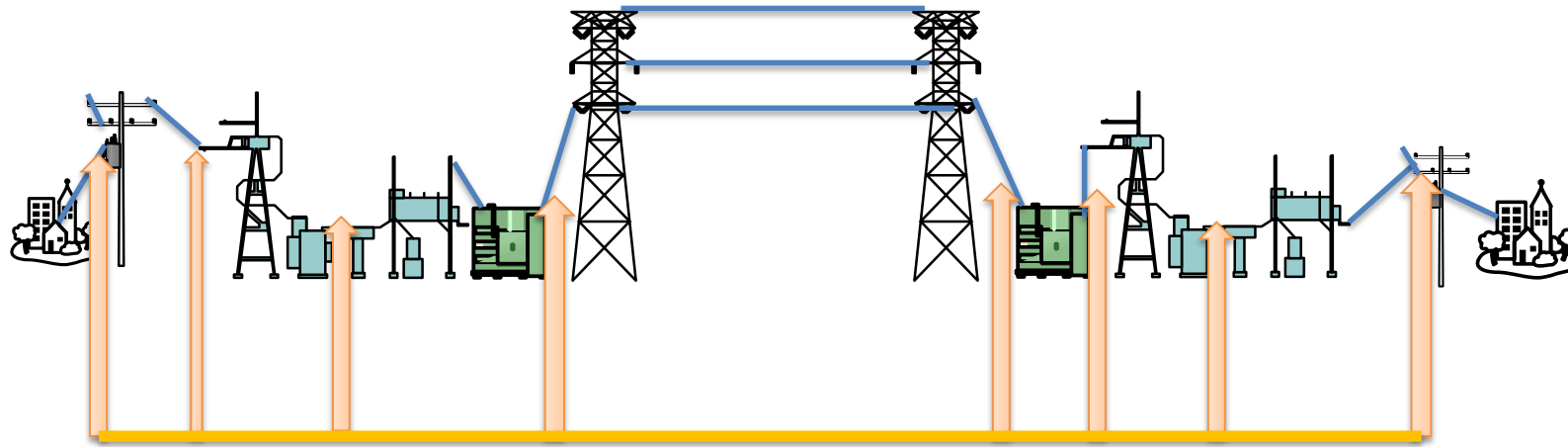
**Develop analytical signature open data base best practice standard for data collection and data interoperability**

**Secure communications between substations and control center via QKD**



# Synchronization /Timing

- Transformers /Substations don't move around positioning isn't a priority
- Transformers don't care about time
- Transformers need to be synchronized on information



## Comms measurement path synchronization is key

3 stages to timing and controlling a rolling anomalies

- Time stamp ( time stamp applied as close in time to the measurement taken)
- Consistent Latency ( required to achieve the Synchronization)
- Synchronization ( to effectively know the anomalies are the same across the area)

# Sensor Integration with PTP & Time chain of custody

## Integrating PTP

- initial testing on Linux-based microcontroller boards
- identifying substation devices and architecture

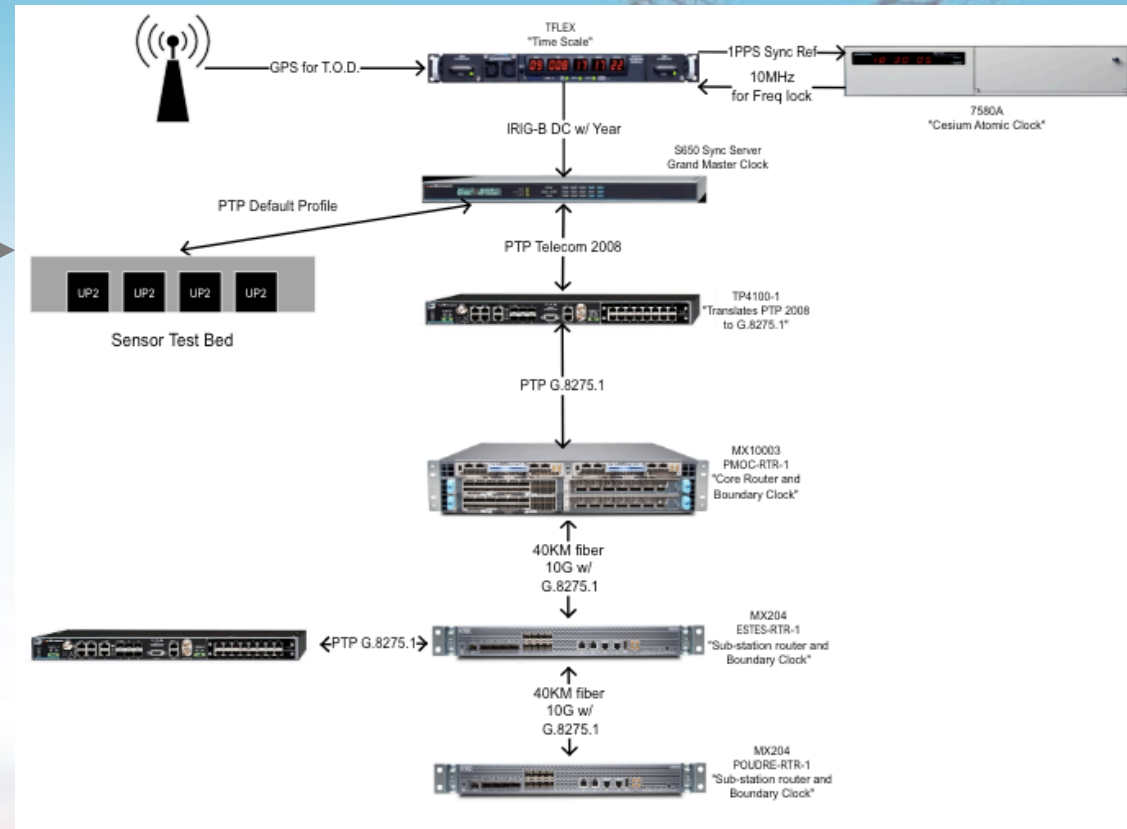
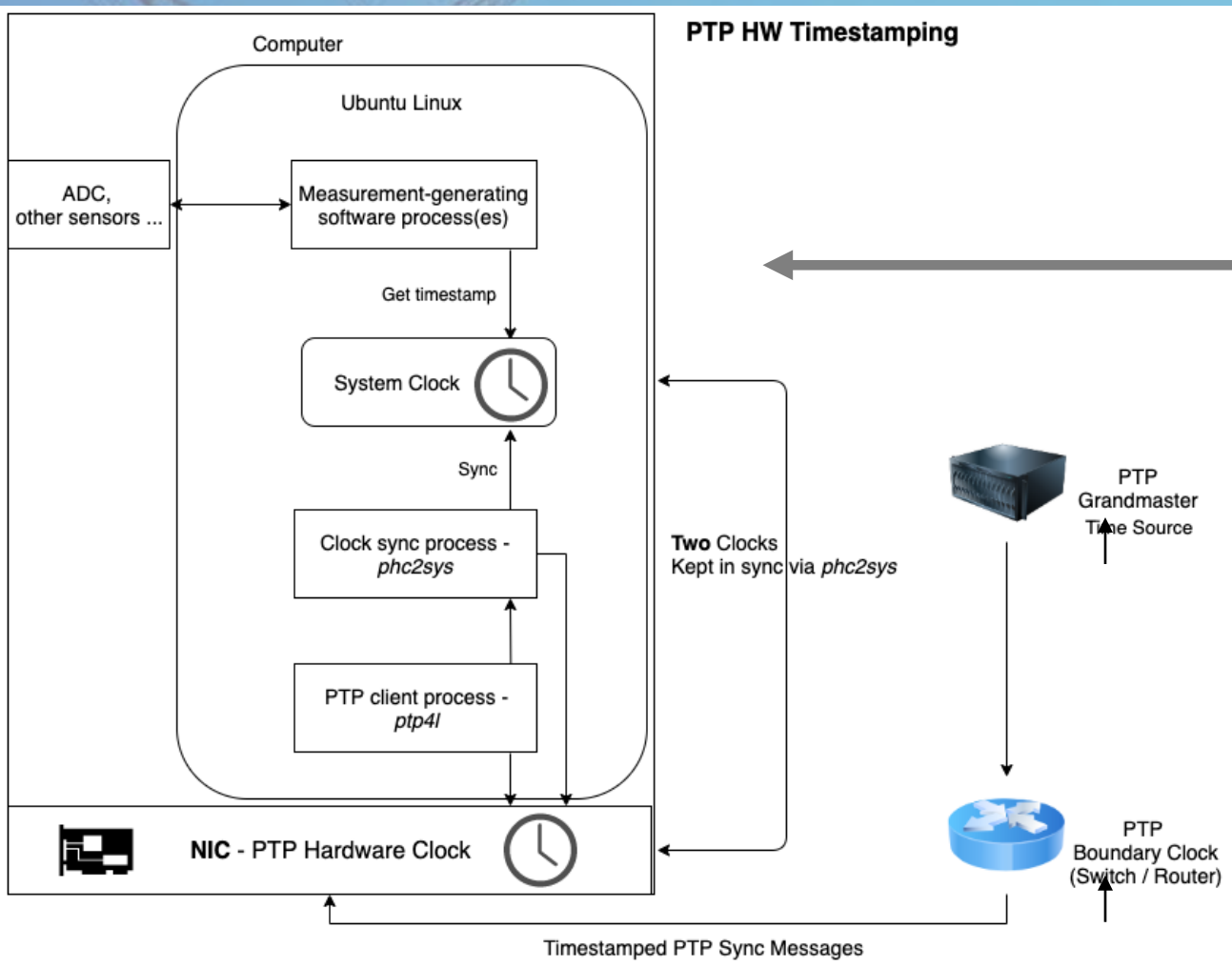
## Configuring PTP Clients

- software vs. hardware timestamping support
- Linux kernel support, utilities

## Characterization of timing

- Latency and offsets from master clock
- Network and software timestamping jitter

# PTP HW Timestamping



Lab Scale PTP Network





# Best Practices for Substation Communications Infrastructure

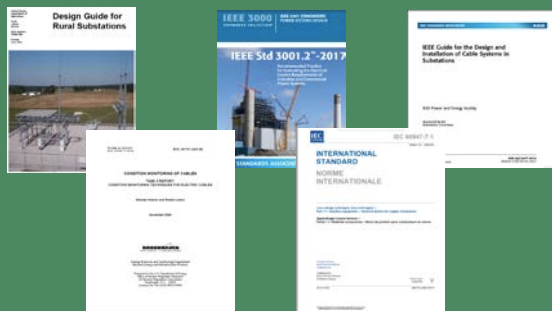
Management of best practices for the support and implementation of critical infrastructure relating to DOE assets within a substation. Management of best practices for the support and implementation of critical infrastructure relating to DOE assets within a substation.

- Measurement control lead installation standards
- Low voltage installation standards
- Outdoor vendor communications plant standards
- Communications best practices for installation and maintenance
- Secure network best practices

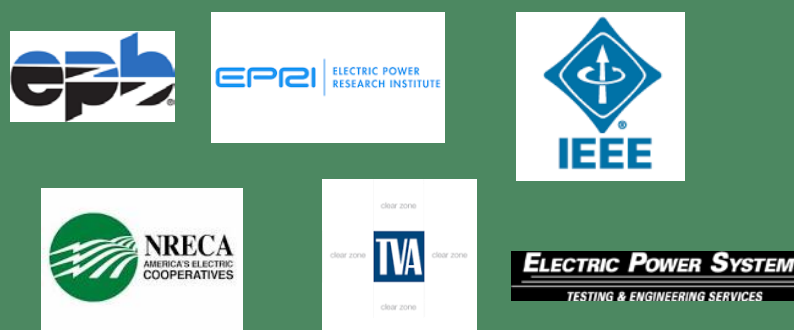


# Best Practice Guide

## Existing standards and Best Practices



## Industry Engagement



## Testing Best Practices



## Lab and Field Testing

### Lab Testing (ORNL)

- New Cables (10, 12, 14)

### Field Testing (EPS/NRECA)

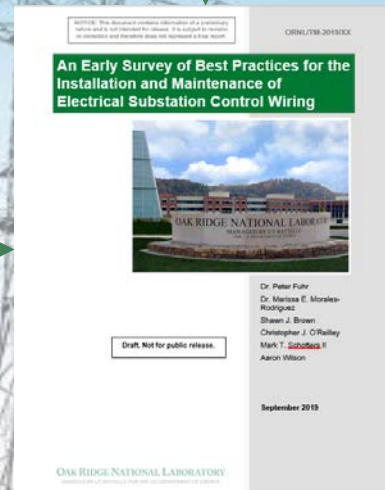
- 7 Climate Zones

### Climate Testing (EPRI)

- New Cables

### Other Data Sources

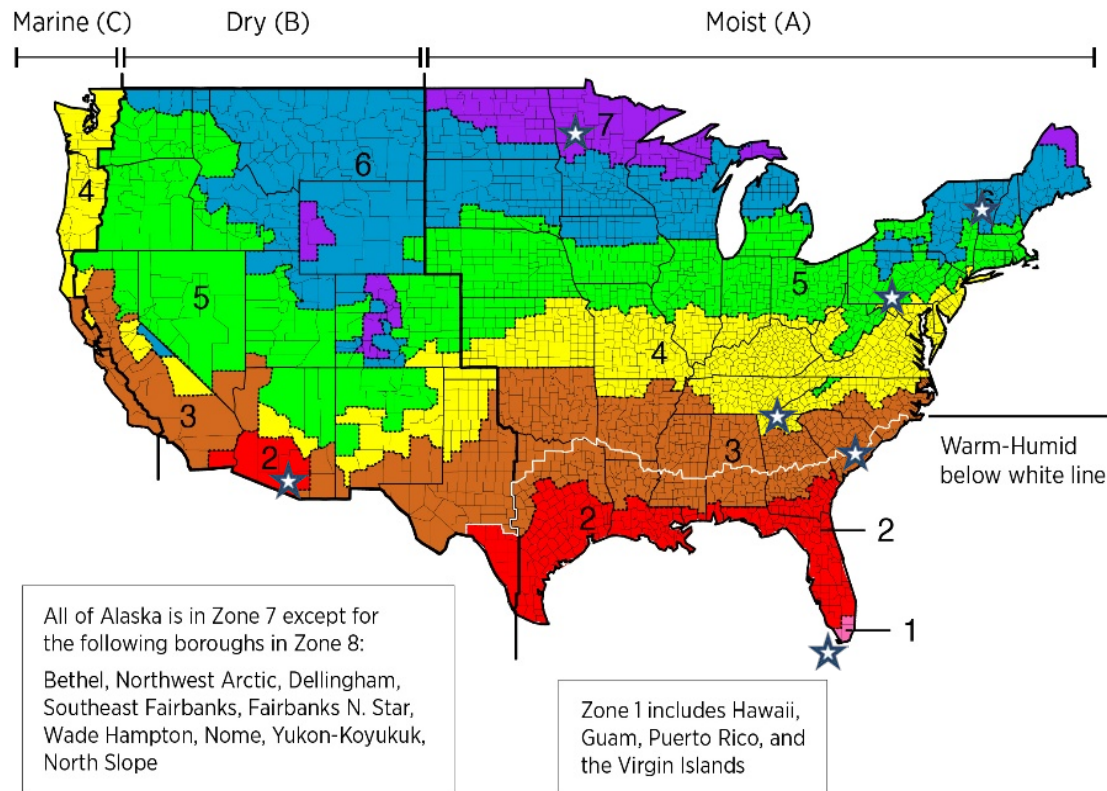
- Survey of current practices (EPS, NRECA, EPRI)
- Aged Cables (EPB, EPS, NRECA)
- Other test data (EPS)



# Control Lead Wiring Testing Procedures

## Field Testing – EPS / NRECA

- Field testing control leads at 7 NRECA Cooperative Utilities
- Coordination with NRECA and EPS – mitigate disruption to utility

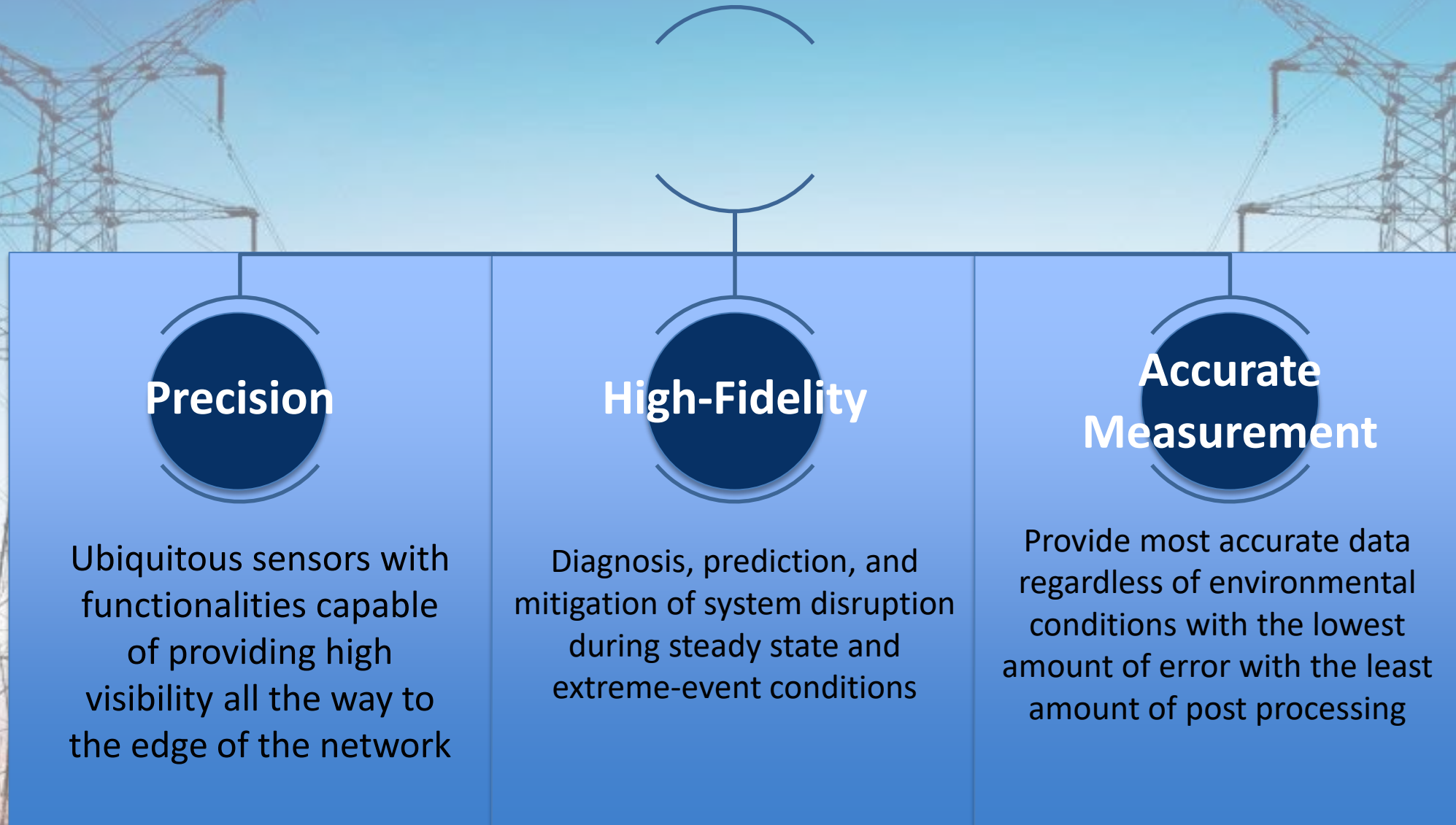


- Zone 1: Florida Keys Electric Co-op (FL)
- Zone 2: Arizona G&T (AZ)
- Zone 3: Coastal Electric (SC)
- Zone 4: EPB/TVA (such as the Ridgedale or Oglethorpe jointly owned substations) TN/GA
- Zone 5: Allegheny Electric Co-op (PA)
- Zone 6: Vermont Electric Co-op (VT) or Flathead Electric Co-op (MT)
- Zone 7: Otter Tail Power (MN)

EPS, NRECA, and EPRI - provide additional testing data, cable samples, and survey question results from members / customers

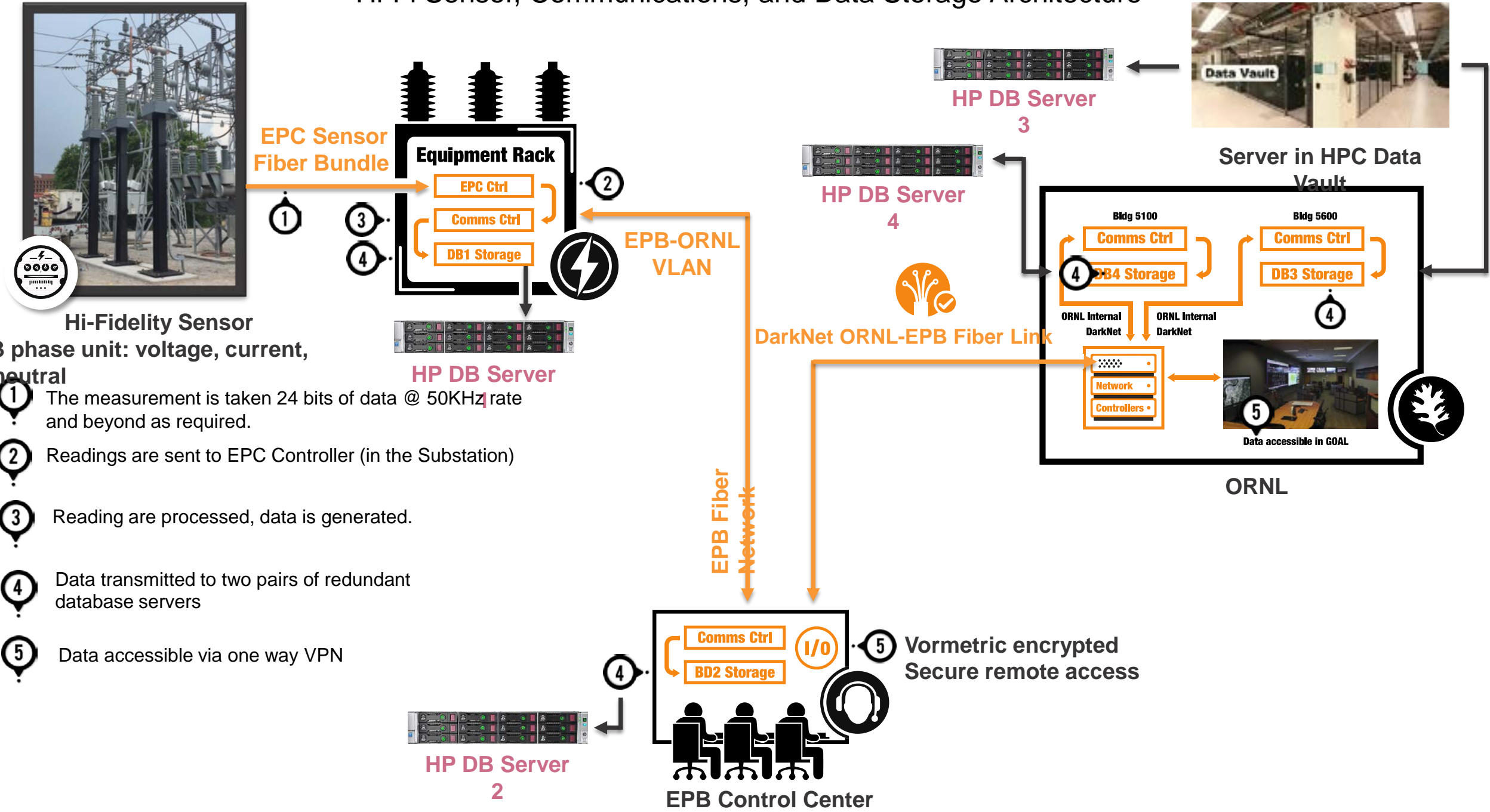


# Sensors Development



# EPC @ EPB

# Hi-Fi Sensor, Communications, and Data Storage Architecture



**Hi-Fidelity Sensor**  
**3 phase unit: voltage, current, neutral**

- 1 The measurement is taken 24 bits of data @ 50KHz rate and beyond as required.
- 2 Readings are sent to EPC Controller (in the Substation)
- 3 Reading are processed, data is generated.
- 4 Data transmitted to two pairs of redundant database servers
- 5 Data accessible via one way VPN

HP DB Server 3

HP DB Server 4

HP DB Server

HP DB Server 2

EPB Control Center

Server in HPC Data Vault

ORNL

Data accessible in GOAL

Vormetric encrypted Secure remote access

DarkNet ORNL-EPB Fiber Link

EPB Fiber Network

EPC Sensor Fiber Bundle

EPB-ORNL VLAN

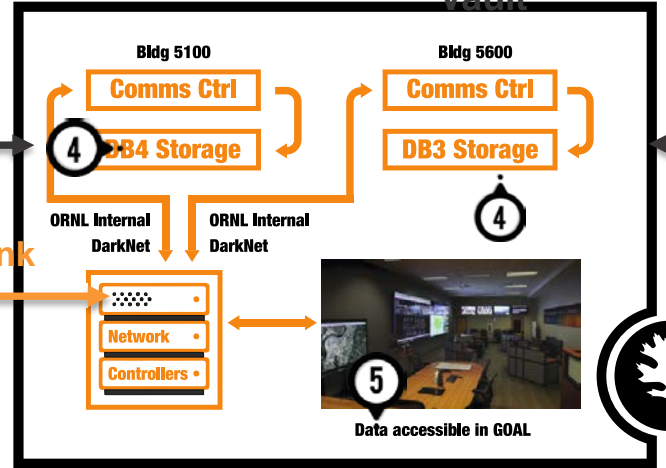
Equipment Rack

EPC Ctrl  
 Comms Ctrl  
 DB1 Storage

Bldg 5100  
 Comms Ctrl  
 DB4 Storage

Bldg 5600  
 Comms Ctrl  
 DB3 Storage

Network  
 Controllers



# Signature Library Goals

---

- Predictive Maintenance
  - Preparing for problems before they happen instead of simply dealing with the aftermath
- Anomaly Detection
- Supervised learning algorithm to detect and label different issues as they are seen in the data.
- Develop data collection requirements; lab scale under controlled environment, and field test
- Development of signatures classification algorithms and testing



# Validation of Grid Signature Library

Validation of a Signature Library framework using advanced sensors – their performance characterization – and Library utilization for Event Detection. Of specific interest will be the integration of field-deployed hi-fidelity sensors for studying various grid operations.

- Verification of Secure Network Transport of Hi-Fidelity sensor measurements into Signature Library,
- Data Collection, and Formatting for Classifiers Training,
- Verification of Consistency with the NAERM Data Architecture ,
- Integration and Verification of “Data-at-Rest & Data-in-Motion” Advanced Sensor Measurements into Library,
- Library Verification: Initial correlation-based analytics using operational data



## David Wells

*Senior Advisor*

*Department of Energy*

*Office of Electricity*

David.wells@hq.doe.gov

