

Secure Communications for the Digital Grid

Christine Hertzog

Sr. Technical Advisor – ICT/Cyber Security

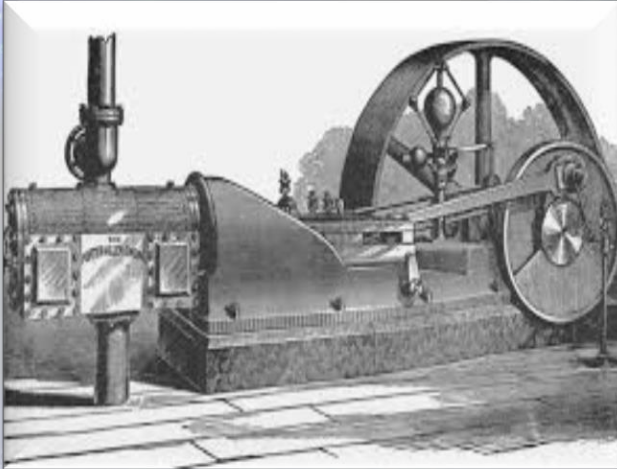
NASPI Technical Workshop

April 2018



How We Work Revolution 4.0

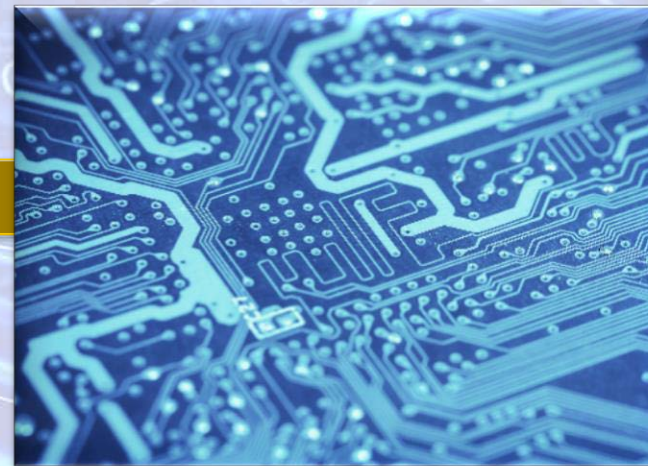
1.0 – Water and Steam



2.0 – Electricity / Mass Production



4.0 –Cyber/Physical Convergence

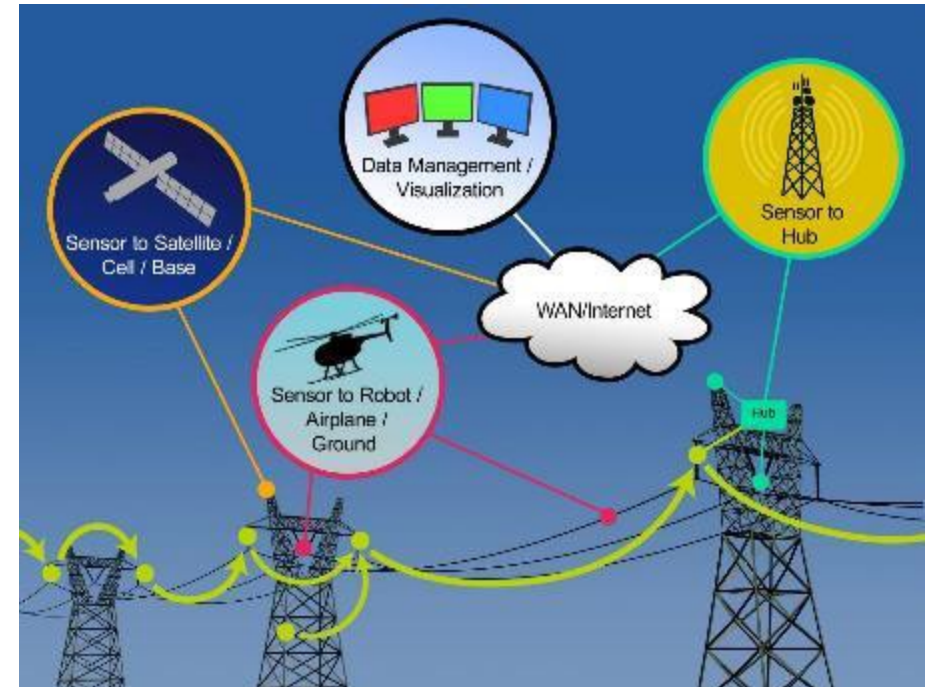
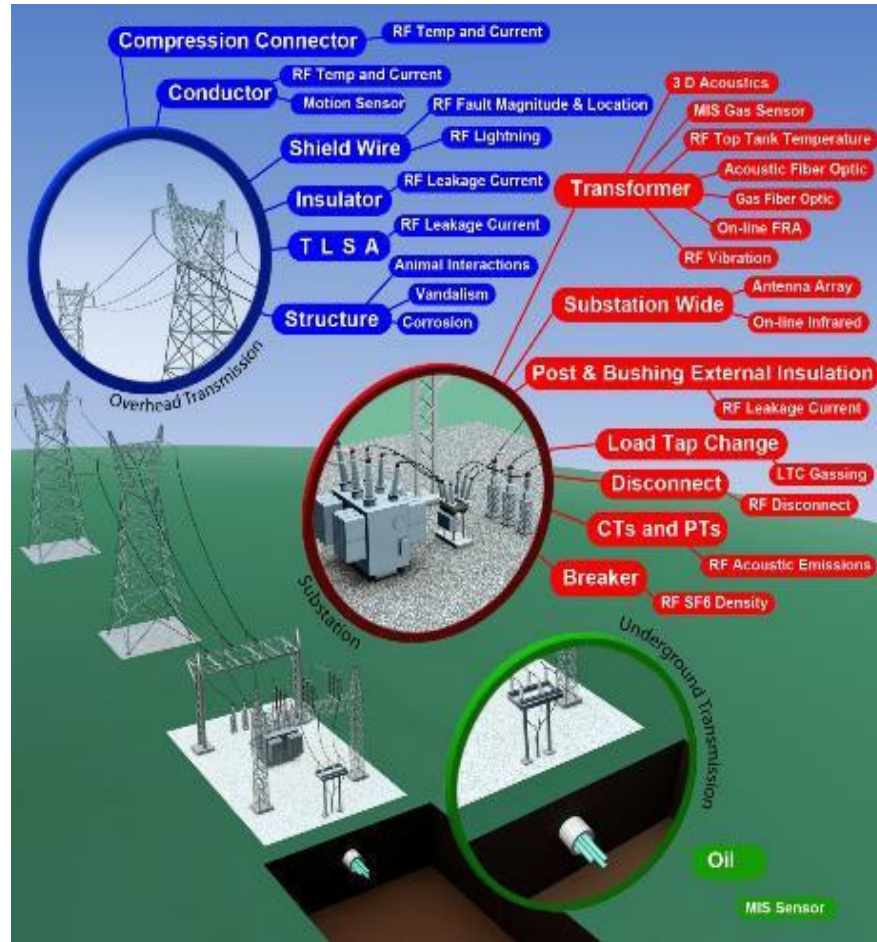


3.0 – Information Technology

Secure Communications Networks

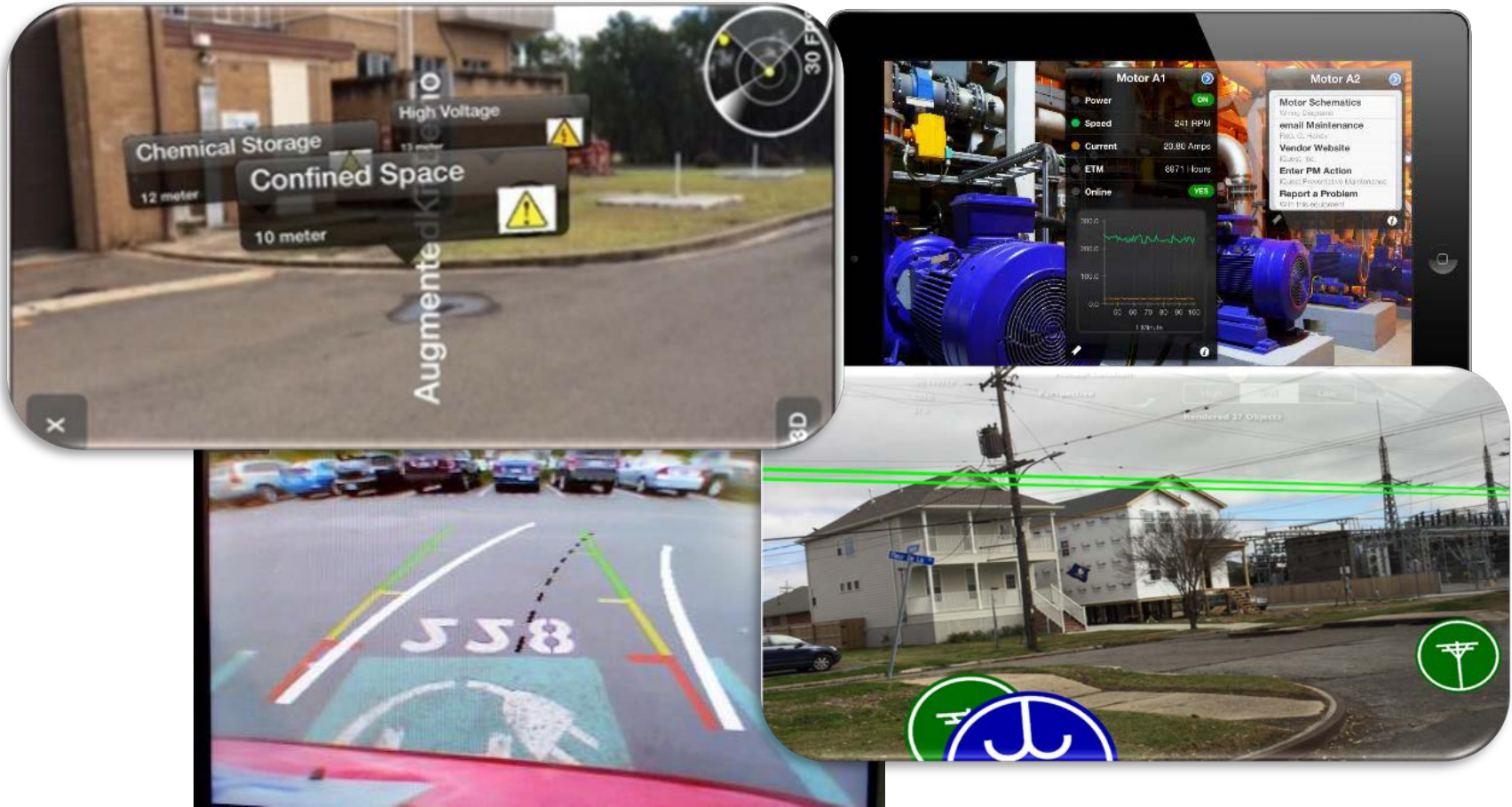


Sensored Infrastructure



- New data sources
- New data transport requirements
- New data storage needs
- New data correlations
- New data valuations
- One constant - **VERACITY**

Digital Workforce



- Augmented Reality
- Wearable technologies
- Emphasis on standards and interoperability

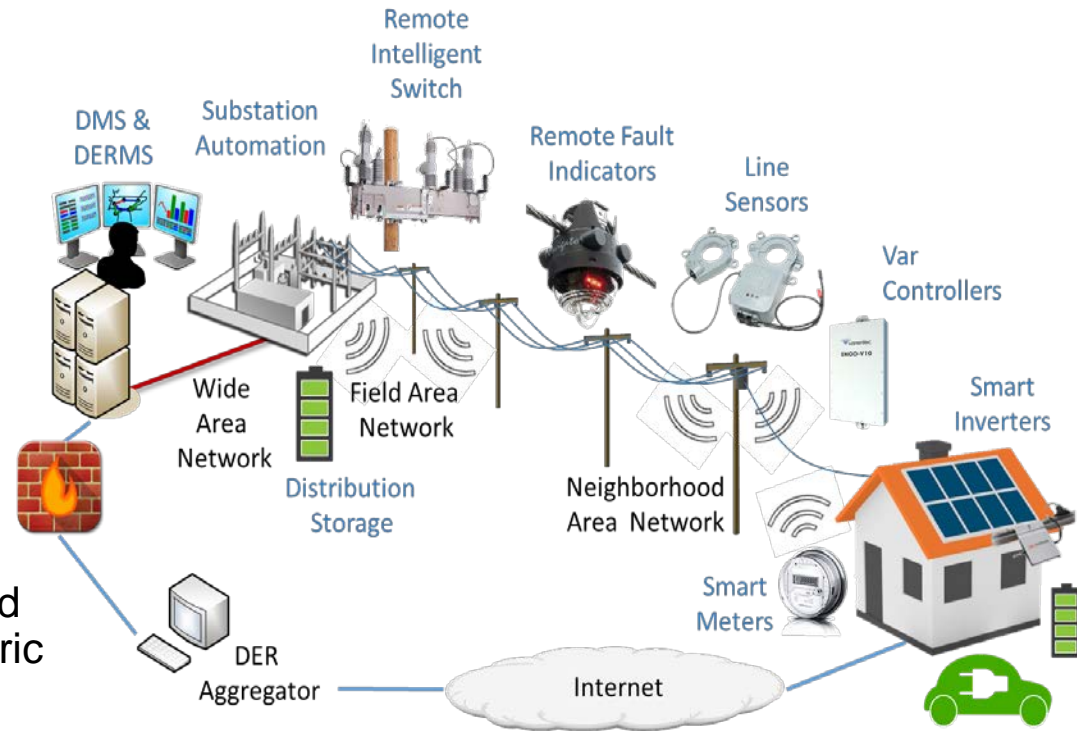
Securing Data Transport and Storage

Transmission & Distribution

- Operations and Maintenance
 - Real-time situational awareness
 - Dynamic supply / demand balancing with DER (DERMS)
 - Data – 5Vs
 - Increasingly **strategic communications**

Increasing Security Threats

- Increasingly numerous and advanced cyber security threats targeting electric utilities
- Deployment and rapid maturing of malware focusing on power delivery systems
- Ukraine aftermath - ISOC, IDS/IPS, and security architecture R&D fill some of the most urgent needs in the region



Mission-Critical Networks

Key Requirements

- Reliable – 24x7 uptime
- Resilient – graceful degradation
- Flexible – multi-purpose
- Secure – mitigate vulnerabilities



Telecom Research

■ Telecom Planning Framework

- Develop and expand traffic modeling from telecom planning framework

■ Software Defined Networking

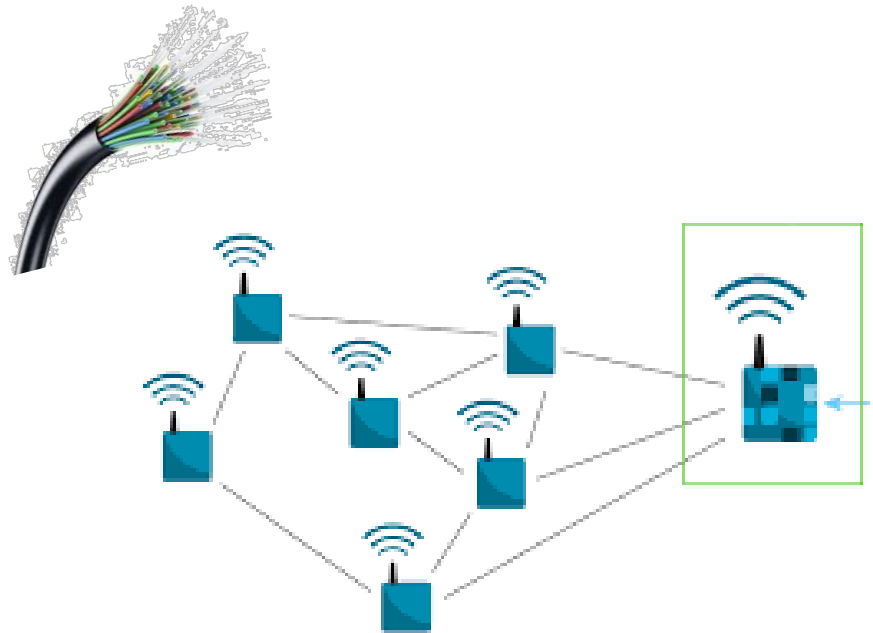
- SDN benefits (security, resiliency, flexibility, economics) to OT network in the field

■ Wide Area Networks

- 5G fiber deployments and partnering opportunities for utility operational needs
- Timing - packet networks and latency requirements

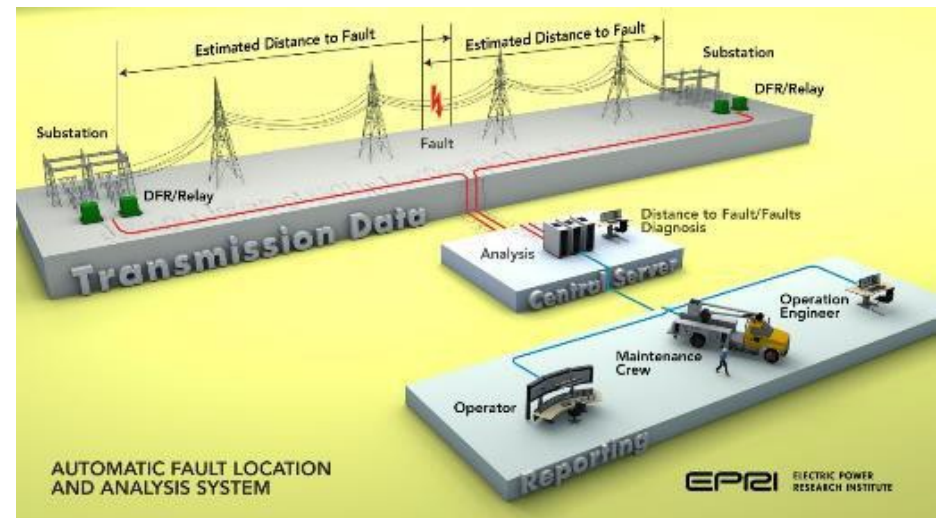
■ Field Area Networks

- Prioritization support and peer-to-peer communication



Analytics – Building Data Value Through Data Management

- Standard data formats
- Useful data correlations
- Data quality – avoid garbage in/garbage out
- Standards and Common Information Model



EPRI Cyber Security R/D/D



Industry Collaboration and Technology Transfer

- Industry Collaboration and Technology Transfer
- Cyber Security White Papers

IT/OT Security Convergence

- Situational Awareness
- Incident Response
- Threat Management
- Asset and Configuration Management



Business Process Challenges for Security Operations

- Security Architecture
- Cyber Security Metrics
- Cyber Security Compliance
- Cyber Security Risk Management



Securing Emerging Grid Technologies & the Multi-Party Grid

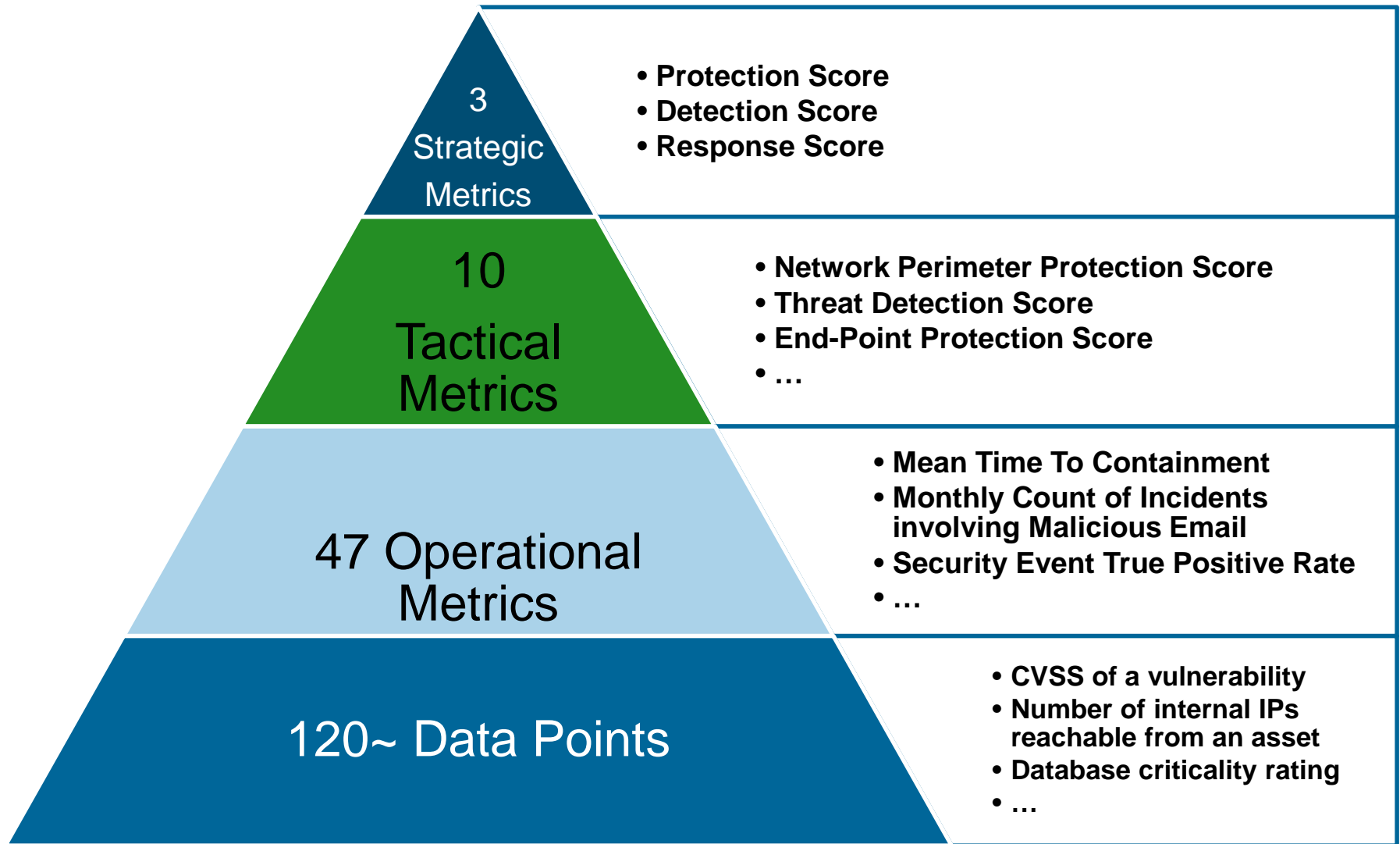
- ICT and Cyber Security for DER Integration Supplemental

Cyber Security Research Activities

- Timing Security
 - GPS, NTP, PTP
- IDS/IPS Solution Assessments
- Multi-party grid
- ICS Forensics
- Integrated Threat Assessments
- ISOC
- IoT/IIoT convergence
- Metrics
- Architecture
- Standards



Security Metrics Research



The Digital Grid Major Trends

- *Secure Communications Networks*
 - *Sensored Infrastructure*
 - *Digital Workforce*



Together...Shaping the Future of Electricity