SMART ULSS FORUM
"Electricity"

March , 2008

Patricia Hoffman
Principal Deputy Assistant Secretary
Office of Electricity Delivery and Energy Reliability
US Department of Energy
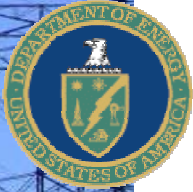
The Electric Grid is a Complex System with Unique Characteristics

Physically

§ Never holistically designed, grid developed incrementally in response to local load growth Today, there are:

  § 30,000 Transmission paths; over 180,000 miles of transmission line

  § 14,000 Transmission substations

  § Distribution grid connects these substations with over 100 million loads, i.e. residential, industrial, and commercial customers

§ Diverse industry w/o a common voice

  § 3,170 traditional electric utilities

  § 239 investor-owned, 2,009 publicly owned, 912 consumer-owned rural cooperatives, and 10 Federal electric utilities

Technically

§ Electricity flows within three major interconnections along paths of lowest impedance (at the speed of light); yet the grid is operated in a decentralized manner by over 140 control areas

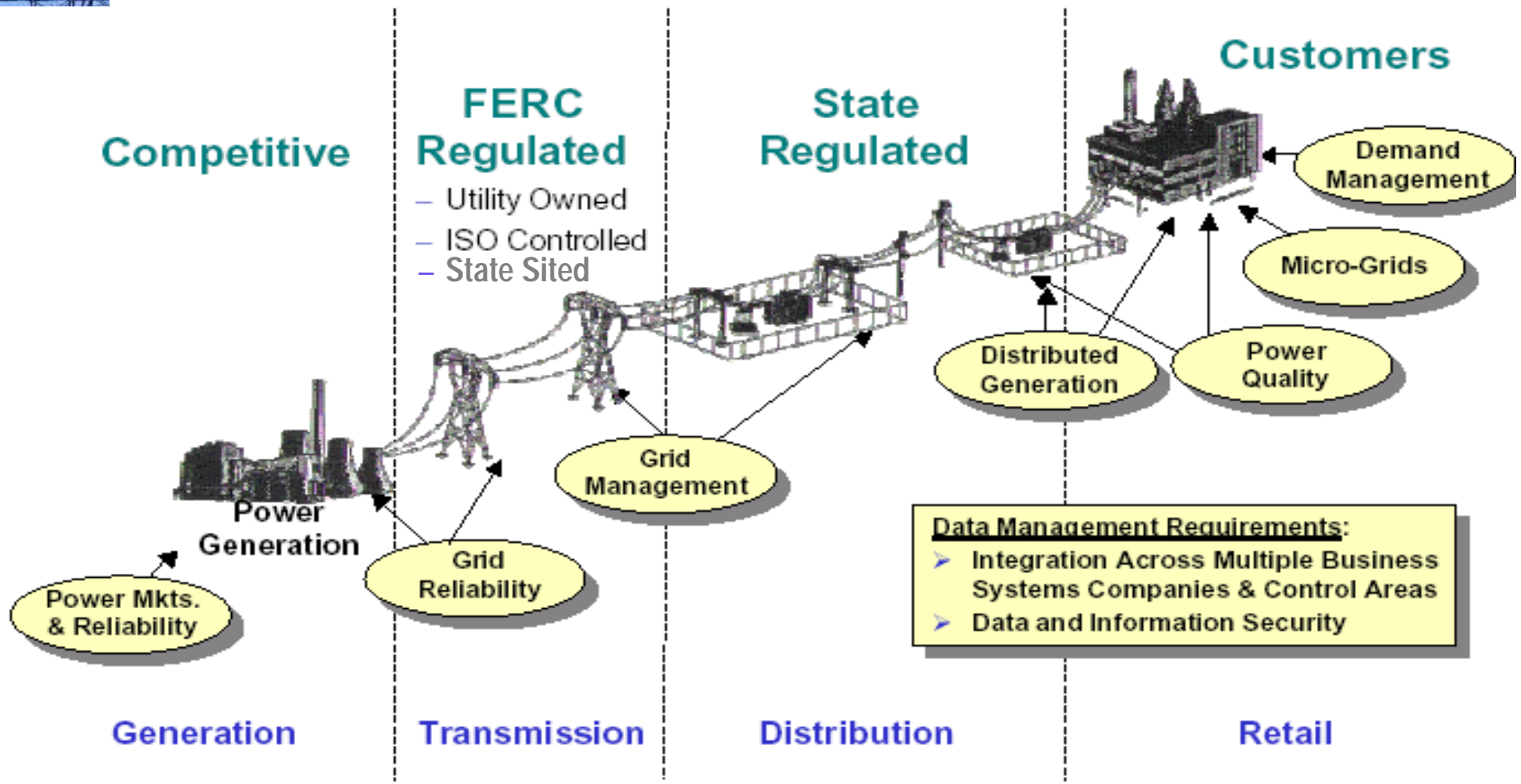§ Demand is uncontrolled; electricity is the ultimate "just-in-time" production process
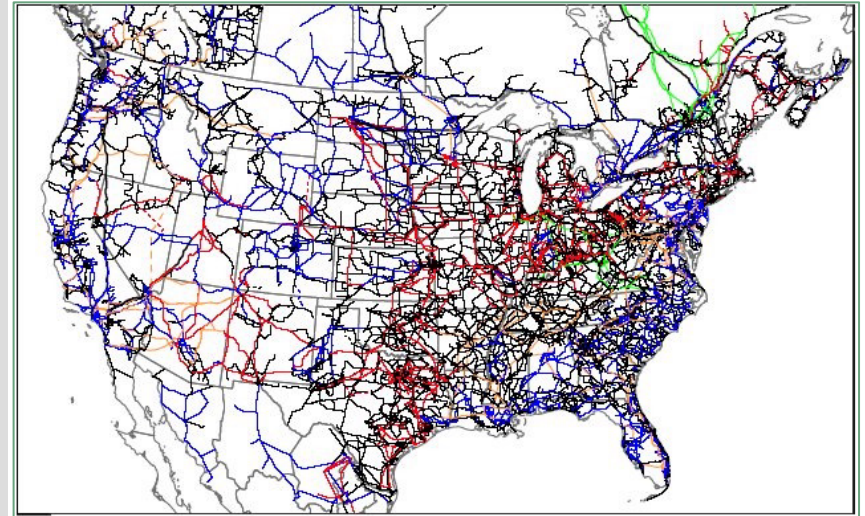
Uniqueness

§ Two things make electricity unique:

  1. Lack of flow control

  2. Lack of large-scale energy storage

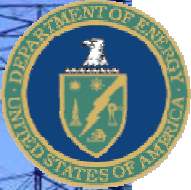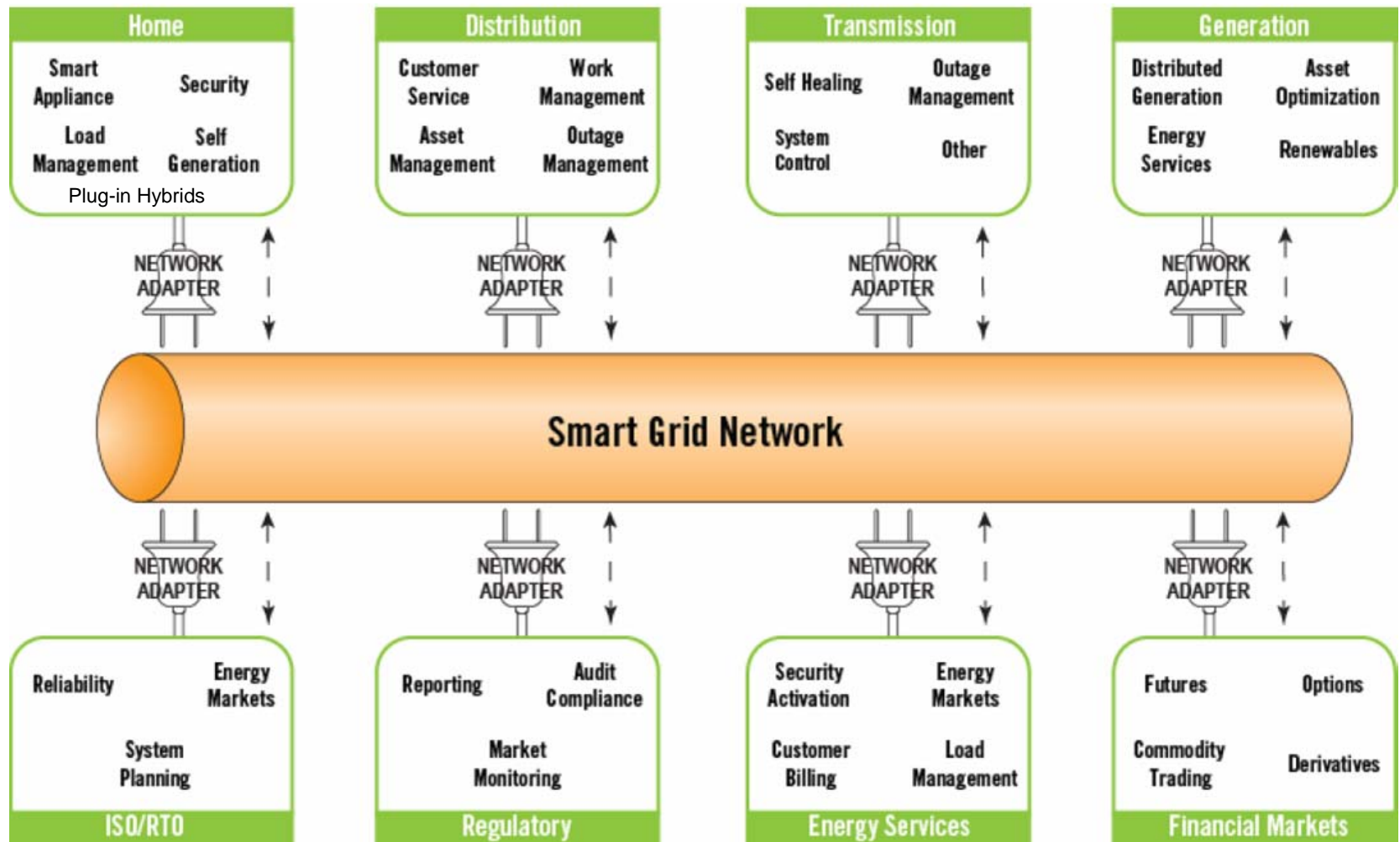§ *Change either of these and the grid delivery system will be transformed*
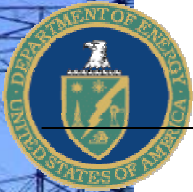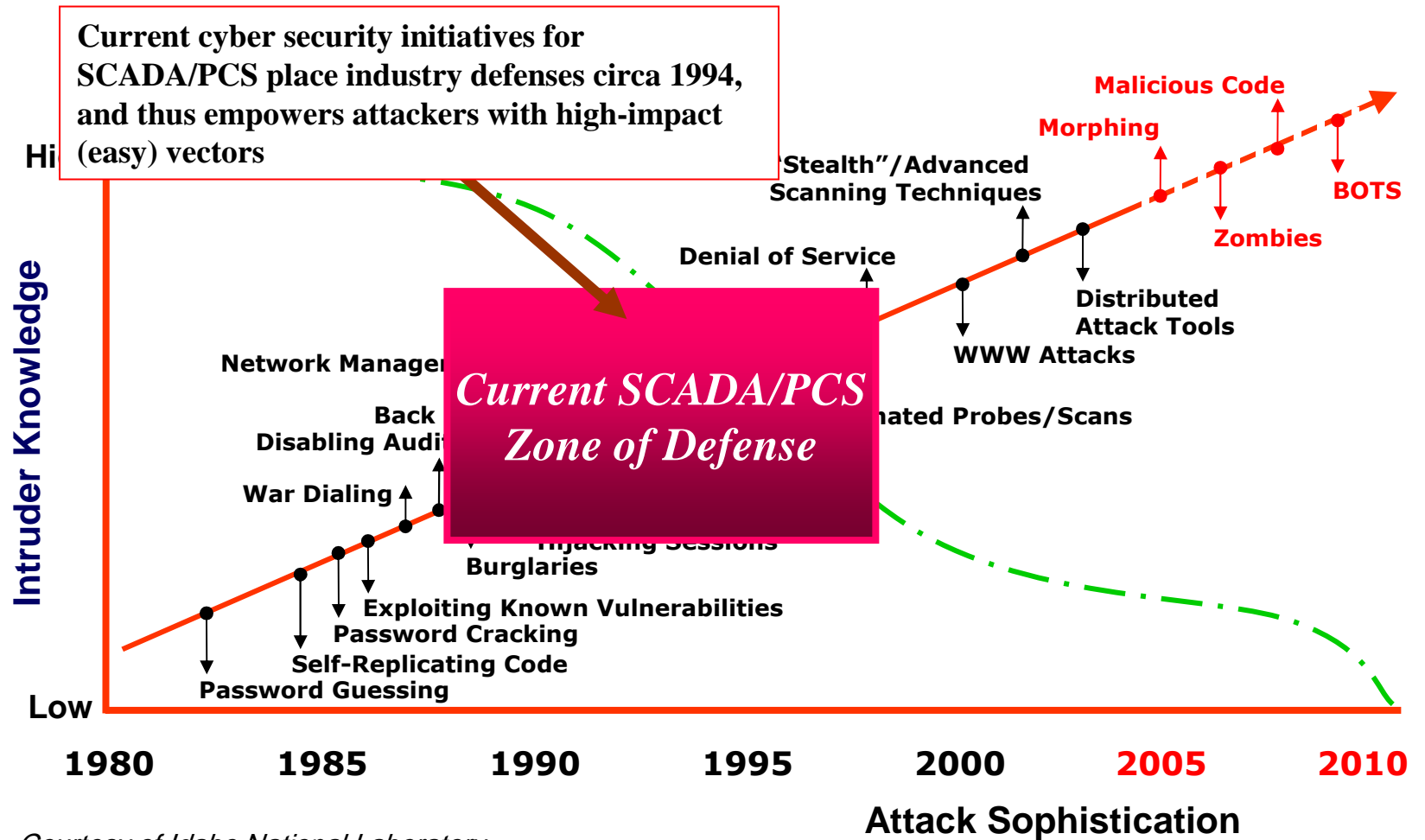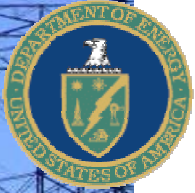
Electric Power Infrastructure

Communications Integration

Cyber Threat Trends

Attacker sophistication has decreased due to proliferation of Easy-to-Use (automated) attack tools

Current cyber security initiatives for SCADA/PCS place industry defenses circa 1994, and thus empowers attackers with high-impact (easy) vectors

Intruder Knowledge (vertical axis, Low to High)

Attack Sophistication (horizontal axis)

High

Low

- Malicious Code
- Morphing
- BOTS
- Zombies
- "Stealth"/Advanced Scanning Techniques
- Denial of Service
- Distributed Attack Tools
- WWW Attacks
- Network Management
- Automated Probes/Scans
- Back
- Disabling Audits
- War Dialing
- Hijacking Sessions
- Burglaries
- Exploiting Known Vulnerabilities
- Password Cracking
- Self-Replicating Code
- Password Guessing

Current SCADA/PCS Zone of Defense

1980   1985   1990   1995   2000   2005   2010

Courtesy of Idaho National Laboratory

Resiliency/N-X Contingency

Isolation of critical
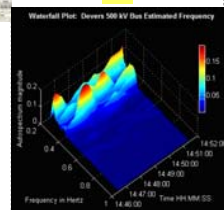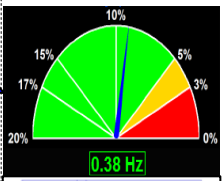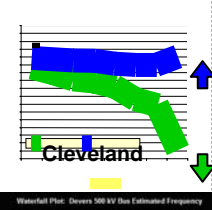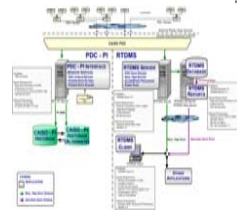services-MUST RUN

Backup, Diversity and
Redundancy
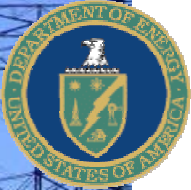
Recovery

**Phasor Measurements, Real Time Wide-Area Situational Awareness,
Visualization, Infrastructure Monitoring, Alarming, and Control**

GOAL

Industry Approach to Phasor Technology Research and Applications:

• 1996 Western Interconnection Blackouts • 2003 Northeast Blackout	§ TVA Super PDC § IEEE 37.118 § NIST SynchroLab	• Real Time Dynamics Monitoring System	• CAISO Operating Engineers Workstation • Baselining Static Angles in East	• Small Signal Stability Monitoring § Intelligent Alarming § State Estimation § Adaptive Islanding	§ EIPP -> NASPI § WECC WAMTF § Research Roadmap

§ Visualization

§ State Estimation

§ Mode Monitoring

§ Alarming

§ Real Time Controls

PROBLEM IDENTIFICATION

INFRASTRUCTURE DEVELOPMENT
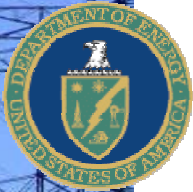
VISUALIZATION FOR WIDE-AREA SITUATIONAL AWARENESS

FORENSIC ANALYSIS/ BASELINING

APPLICATIONS

INDUSTRY ADOPTION

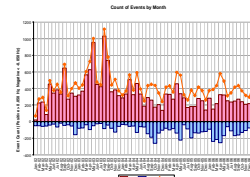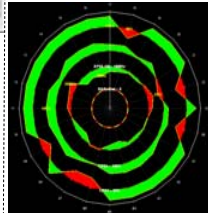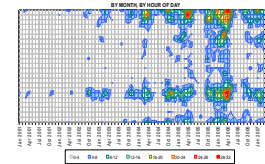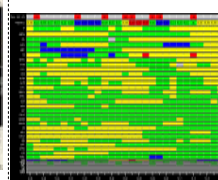# Reliability Metrics and Compliance Monitoring Tools

Visualization, Compliance, Monitoring, Infrastructure, Real Time Wide-Area Standards Compliance and Situational Awareness

Common Wide-Area, Real Time Monitoring Platform – Standards Compliance, Key Metrics for Reliability Intelligent Alarms, Reports, and Event Analysis Situation Awareness Visualization Dashboards for NERC, DOE, and FERC

1999 Low Frequency Events on Eastern Interconnection	Wide-area visualization infrastructure	Wide-area real time ACE-Frequency monitoring tool	Interchange Error (AIE) Monitoring	Performance standards research, validation, field trials	CPS-BAAL monitoring and analysis
• Declining System Performance	• Relational time-series database	• Suppliers performance for AGC and frequency response	• Wide-area Inadvertent Monitoring	• Resources adequacy load-generation analysis and assessment	• Research for situational awareness for resource adequacy
• Frequency Excursions					

PROBLEM IDENTIFICATION	INFRASTRUCTURE DESIGN	VISUAL-IZATION	WIDE-AREA MONITORING	FORENSIC ANALYSIS	COMPLIANCE MONITORING
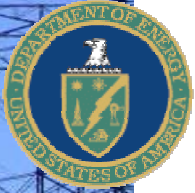
Characteristics
(Now and Future)

§ Interoperability

§ Flexible (generation diversity, disruptive technologies)

§ Reliable: N-X contingency (X=1, 2, etc)

§ Eco-centric (Impact)

§ Provider of Last Resort?

§ Human behavior (hybrids, demand response)