

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security and Energy Security Challenges Ahead

North American Electric Reliability Corporation

September 29, 2009

Tim Roxey

Manager - CIP

to ensure
the reliability of the
bulk power system

An underpinning infrastructure

Access to sufficient and cheap energy fuels our modern economies and sustains our growing cities

- The bulk power system:
 - 164,000 Miles of Transmission lines
 - 150 BPS Control Centers
 - 16,756 Generators (5,253 Plants); 948,446 Megawatts (net summer capacity)
 - 3,028 Fossil Plants
 - 64 Nuclear Plants
 - 1,422 Hydro Facilities
 - 714 Renewable
 - Over 5,900 Electric organizations with 131 million customers

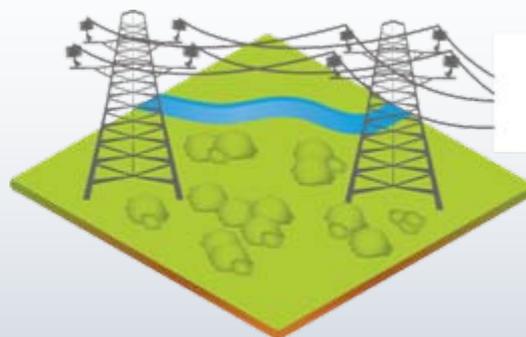


Highly complex and interconnected energy infrastructure

From edge to shining edge



Generation



Transmission



Distribution

5,000 plants

160,000 miles

Over 6,500,000 miles

65% of monthly bill

5% of average customer
monthly bill

30% of average customer
monthly bill

Employs approx. 120,000
people nationwide

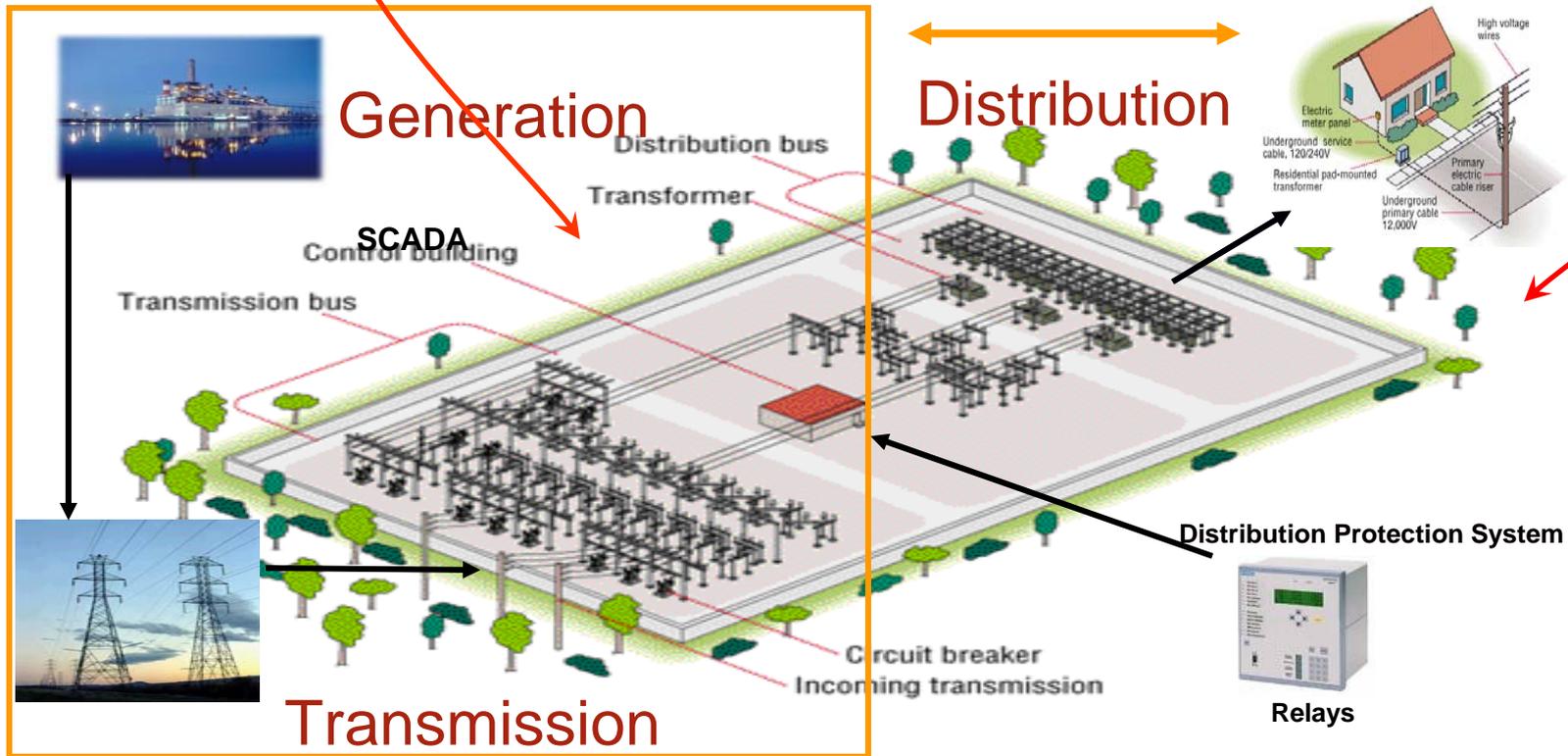
Employs approx. 15,000
people nationwide

Employs approx. 400,000
people nationwide

Power System Components

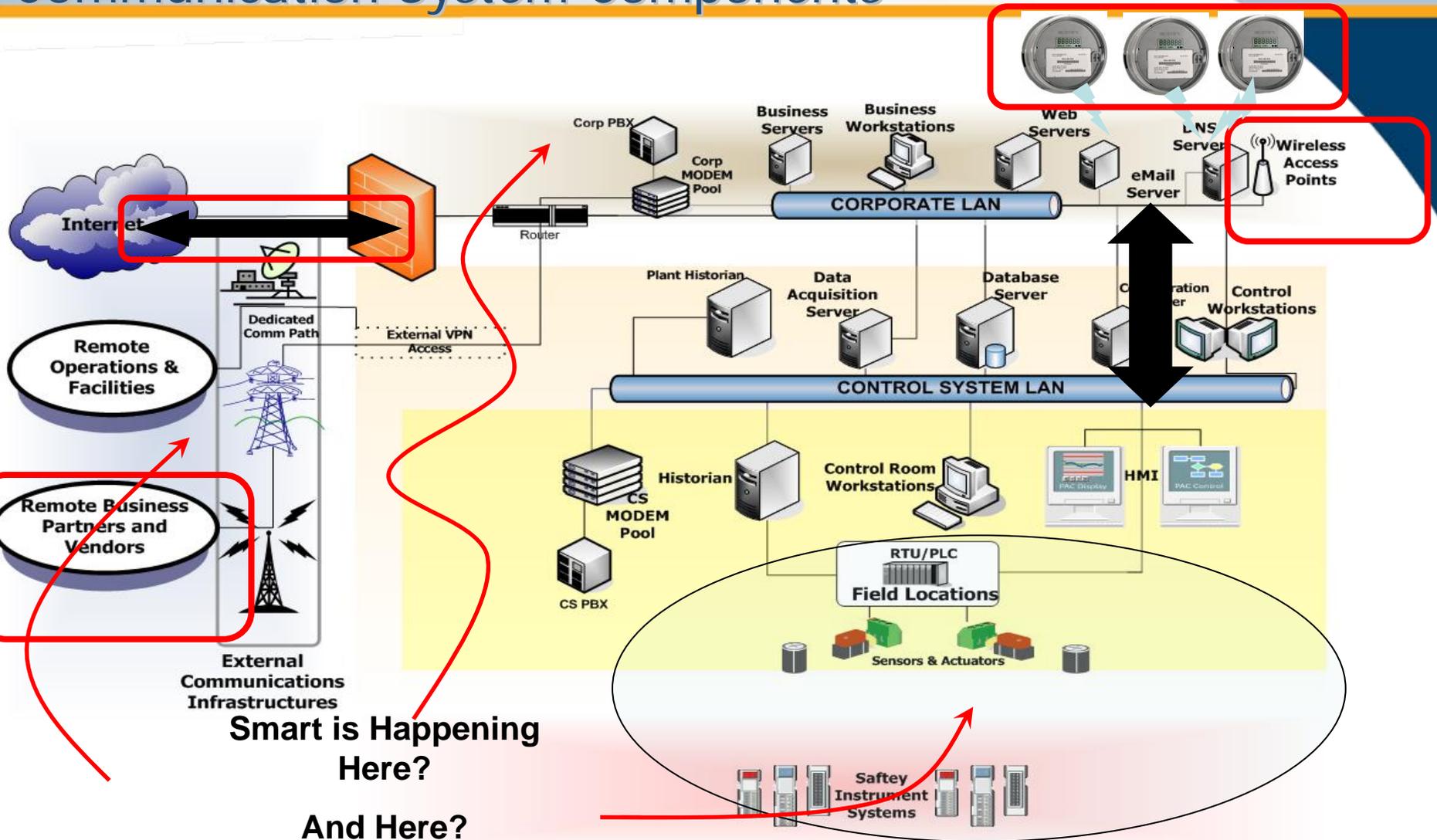
Smart is Happening Here?

- Physical Access Points Numerous and Diverse And Here?



Bulk Power System

Communication System Components

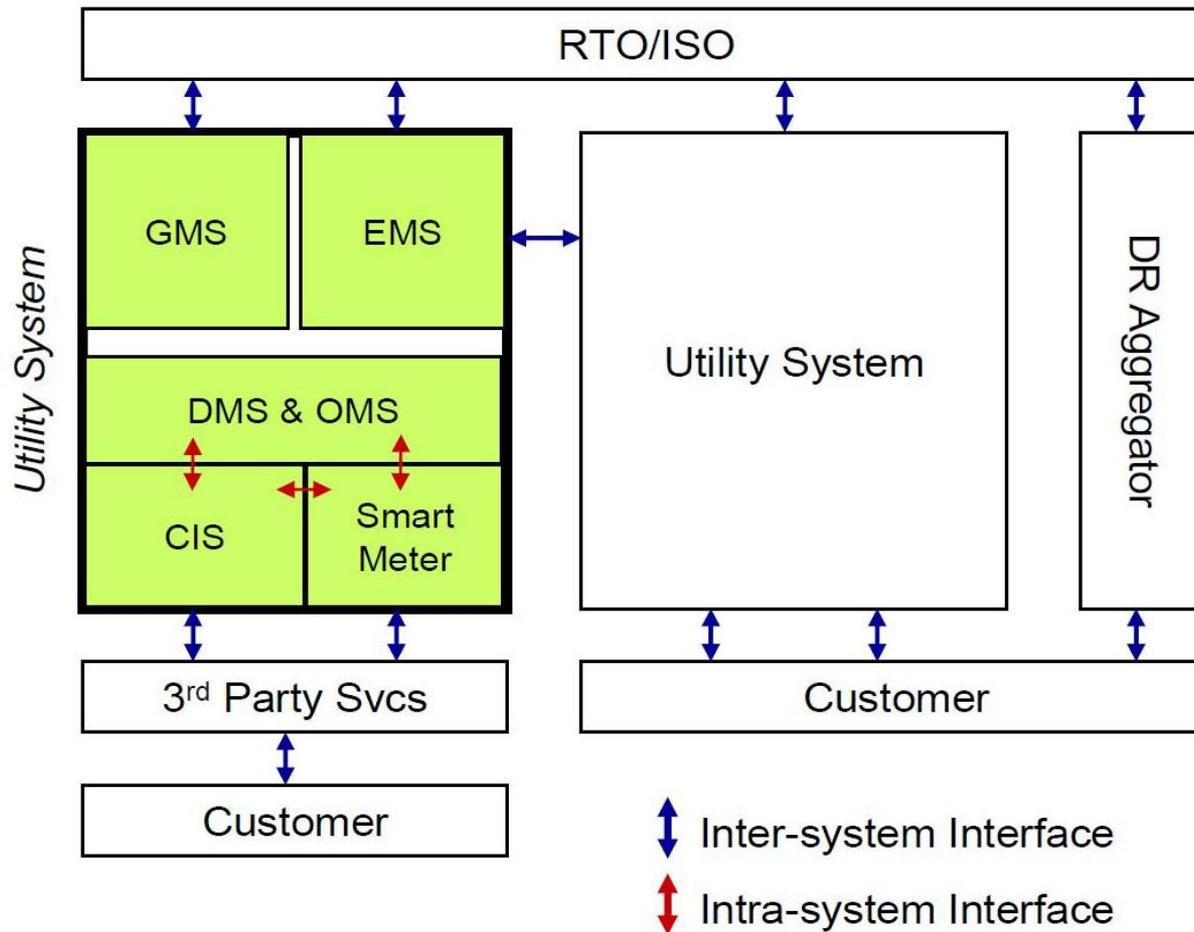


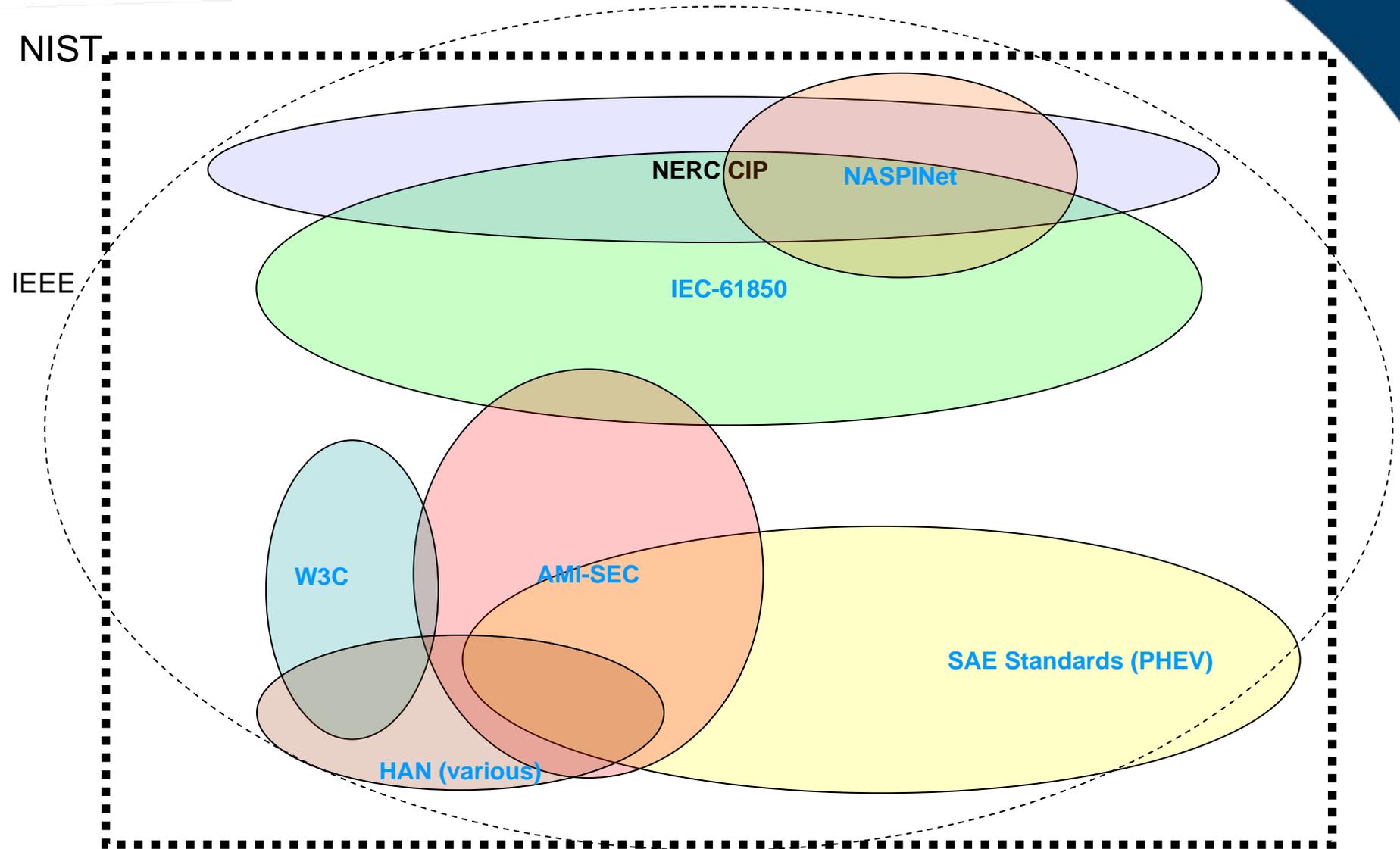
Smart is Happening Here?

And Here?

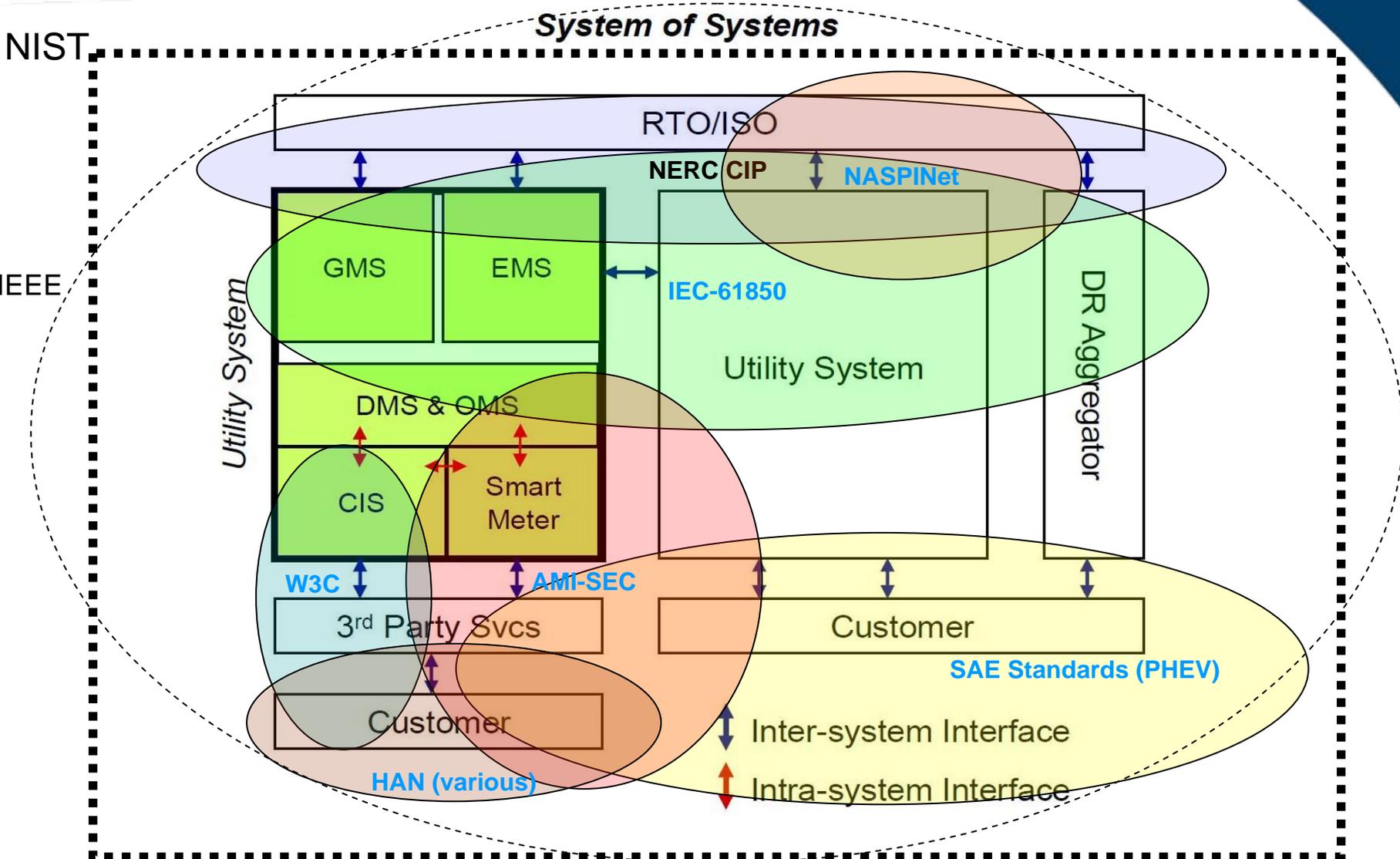
And Here?

System of Systems





Complexity - Overlay Everything



- Power System Components
 - Micro-generation, Portable generation, Variable generation -
 - Home based – dispatched thru metering
 - Portable generation – Vehicles
 - Variable generation – Wind and Solar
 - On boarding new generation
 - Transmission and congestion Issues
 - Supply Chain Issues
 - Limited or Absent Domestic Manufacturing
- Communication System Components
 - Aggregated Impacts
 - Not just N-1 Maybe N- 10,000
 - Common vulnerable underlying OS's and applications
 - Attack Surface – Lots of vulnerable points to enter

- Operational Components
 - Legacy issues with both Inter and Intra System Interfaces
 - Cyber Security – as an after thought in the rush to get an installed base
 - Interoperability between various deployed solutions
 - Supply Chain Issues
 - Limited or Absent Domestic Developers
- Standards and Regulatory Components
 - Many different bodies developing standards and Regulations
 - Span of applicability between BPS Standards
 - States typically have distribution
 - Federal Level typically has BPS
 - Certain organizations typically have device level

- **Power Systems**
 - Build security in – don't add it on – at the device level
 - Protect the vulnerability researcher
 - Develop agreed upon testing practices
 - Develop flexible architectures and designs to allow correction of unknown challenges more easily in the future.. avoid legacy problems

- **Communications Systems**
 - Build security in – don't add it on
 - Ensure interoperability
 - Protect the vulnerability researcher

- **Operational Systems**
 - System functions should be prioritized
 - Ensure interoperability
 - Need to communicate and educate so buyer and supplier have common expectations
 - New technology should be provided with test and development kits or systems for security testing

- **Standards and Regulations**
 - Incentivize interoperability
 - Need to improve the standards so compliance does not limit technology progression

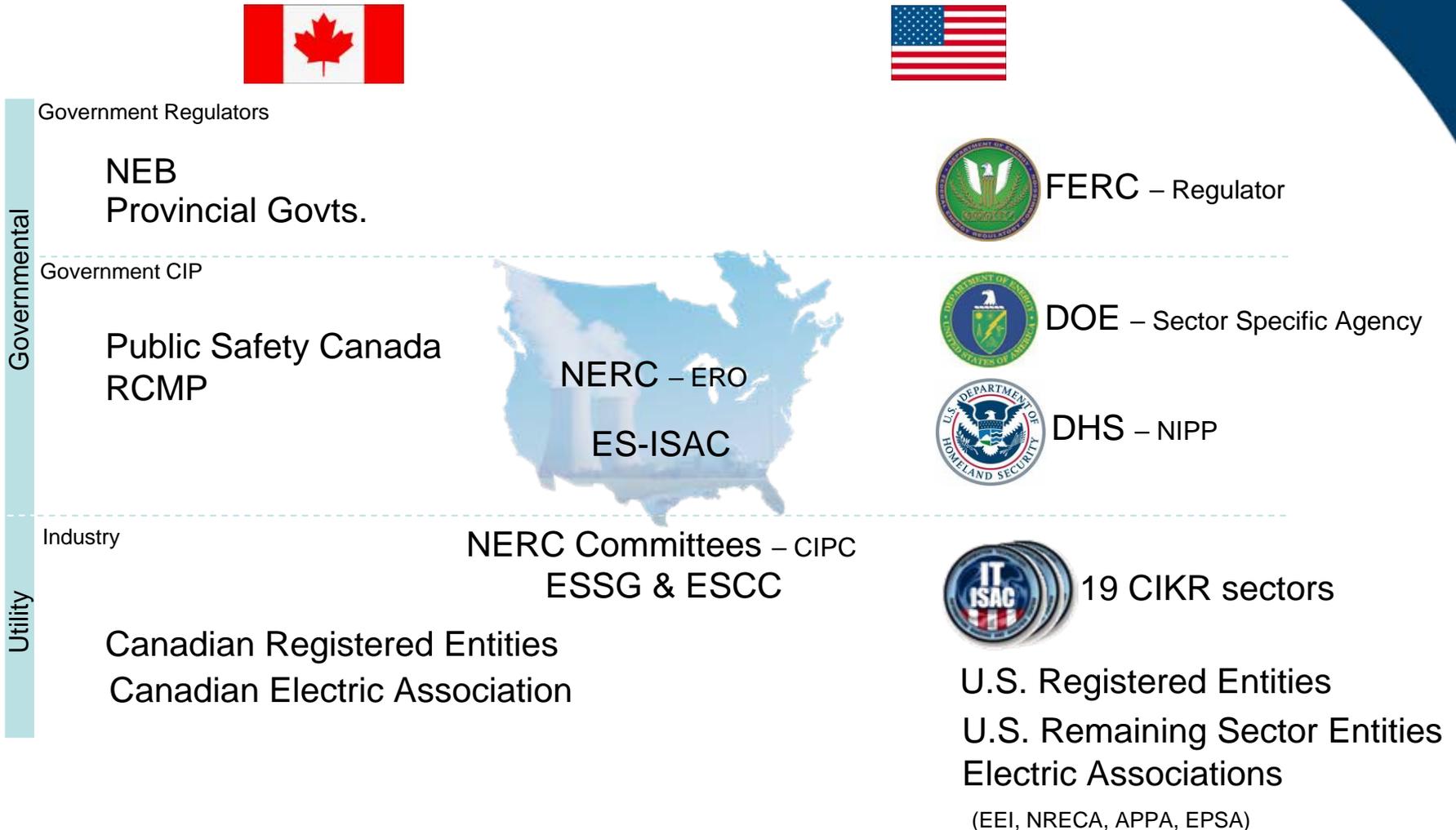
- Number one overall issue - stop inherent machine to machine trust
 - In the beginning we “hard wired” all circuits from the “button to the device”. Security was assured and could be verified by hand over hand system walk-downs
 - Today – virtual computers - operate virtual systems – through vast networks – with common vulnerabilities – controlling real devices
- Challenge Implicit Trust – It Should become explicit trust.

The North American Goal

Art credit: "Report of the commission to assess the threat to the U.S. from electromagnetic pulse attack, 2008"



BPS CIP Organization Map



* Organization descriptions provided – enclosed document