Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Panel Session: Lessons Learned in Smart Grid Cybersecurity

TCIPG Industry Workshop
October 30, 2012

Jeff Dagle, PE
Chief Electrical Engineer
Advanced Power and Energy Systems
Pacific Northwest National Laboratory
(509) 375-3629
jeff.dagle@pnnl.gov

Outline

- Setting the context for challenges associated with control system security in the electricity sector
- Smart grid security considerations
  - Defining the “smart grid”
  - A discussion on synchrophasors and their security implications
- DOE efforts on securing ARRA smart grid investment grants
- The author’s perspectives on security and resilience
  - Issues for consideration

The Emerging Cyber Threat

- Industry has long history of planning for and coping with natural disasters and other reliability events
  - Through industry standard operating procedures, there is much effort expended to reduce likelihood of cascading outages leading to widespread blackouts
- Historically, cyber security focused on countering unstructured adversaries
  - e.g., individuals, untargeted malicious software, human error
- Very little protection against structured adversaries intent on exploiting vulnerabilities to maximize consequences
  - e.g., terrorist groups, organized crime, hostile nation states
  - Insider threat remains very challenging, can be used as part of structured threat vector
- New possibilities for widespread sustained outages resulting from cyber attack are now being contemplated
  - Currently, most of the emphasis is on compliance to mandatory cyber security requirements, e.g., NERC CIP
  - Some effort to expand thinking beyond minimum necessary requirements, e.g., the joint NERC-DOE effort on ***High Impact, Low Frequency Events***

Smart Grid Defined

- A smart grid uses digital technology to improve reliability, security, and efficiency of the electric system: from large generation, through the delivery systems to electricity consumers and a growing number of distributed-generation and storage resources.
- The information networks that are transforming our economy in other areas are also being applied to applications for dynamic optimization of electric system operations, maintenance, and planning.

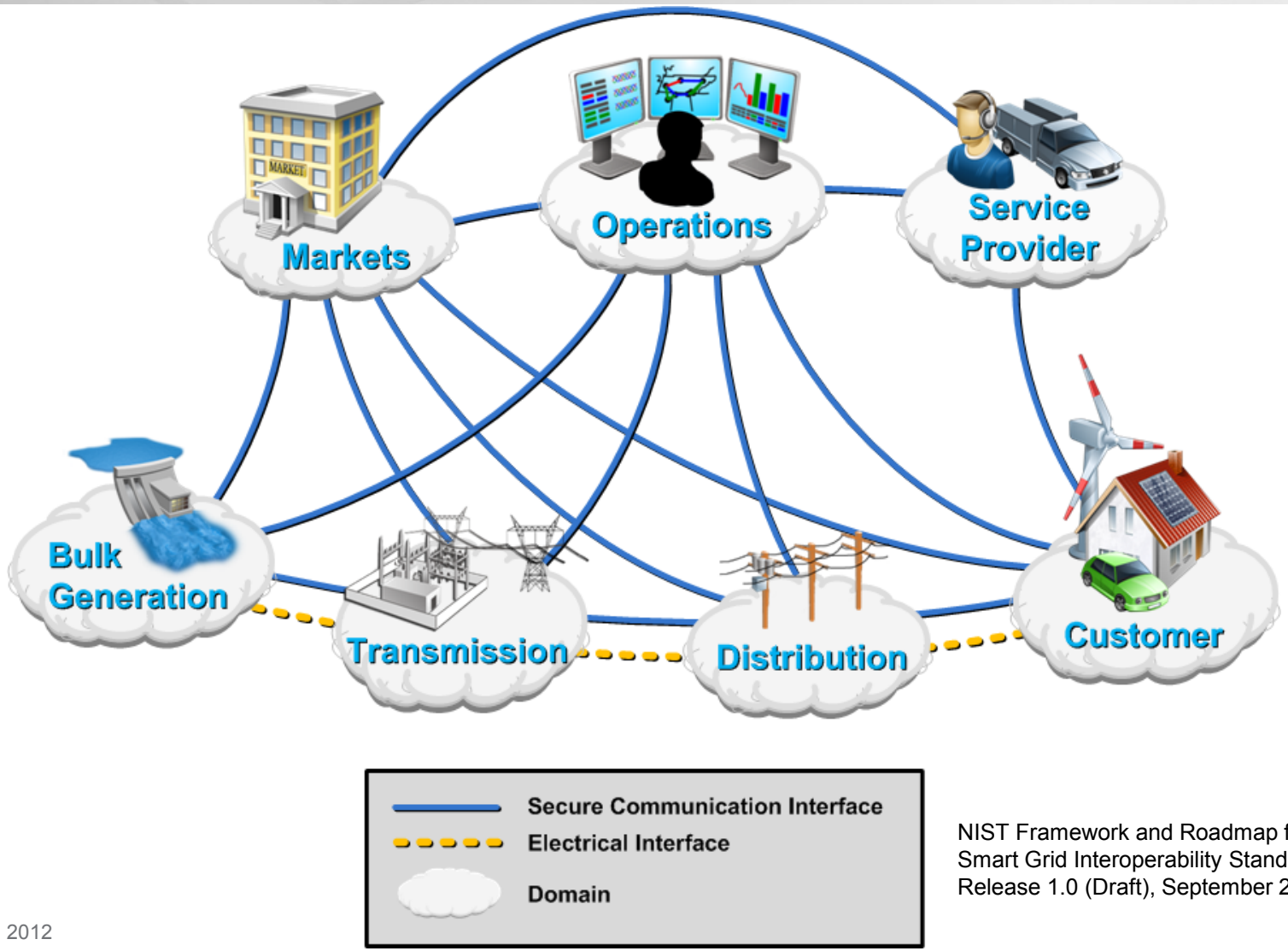
Smart Grid Vision

Bring digital intelligence & real-time communications to transform grid operations

- Demand-side resources participate with distribution equipment in system operation
  - Consumers engage to mitigate peak demand and price spikes
  - More throughput with existing assets reduces need for new assets
  - Enhances reliability by reducing disturbance impacts, local resources self-organize in response to contingencies
  - Provide demand-side ancillary services – supports wind integration

- The transmission and bulk generation resources get smarter too
  - Improve the timeliness, quality, and geographic scope of the operators' situational awareness and control
  - Better coordinate generation, balancing, reliability, and emergencies
  - Utilize high-performance computing, sophisticated sensors, and advanced coordination strategies

Communication and Information Technology will be Central to Smart Grid Deployment



NIST Framework and Roadmap for Smart Grid Interoperability Standards. Release 1.0 (Draft), September 2009

Smart Grid Cyber Security

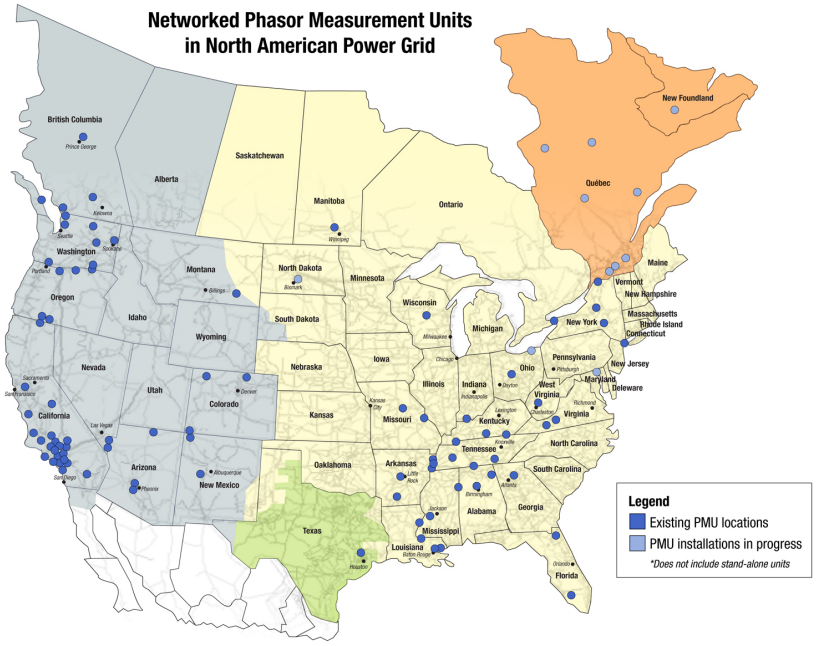
- The same information and communication technologies that enhance the resilience of the power system may also present a new set of vulnerabilities related to the control layer of the physical infrastructure
- If there are common modes of failure present in these control layers, there will necessarily be challenges to achieving full degrees of resilience in future smart grid deployments
- Because smart grid technologies transcend the scope of the FERC/NERC jurisdiction associated with the bulk electricity system, we cannot rely on existing mandatory cyber security standards and requirements

North American SynchroPhasor Initiative

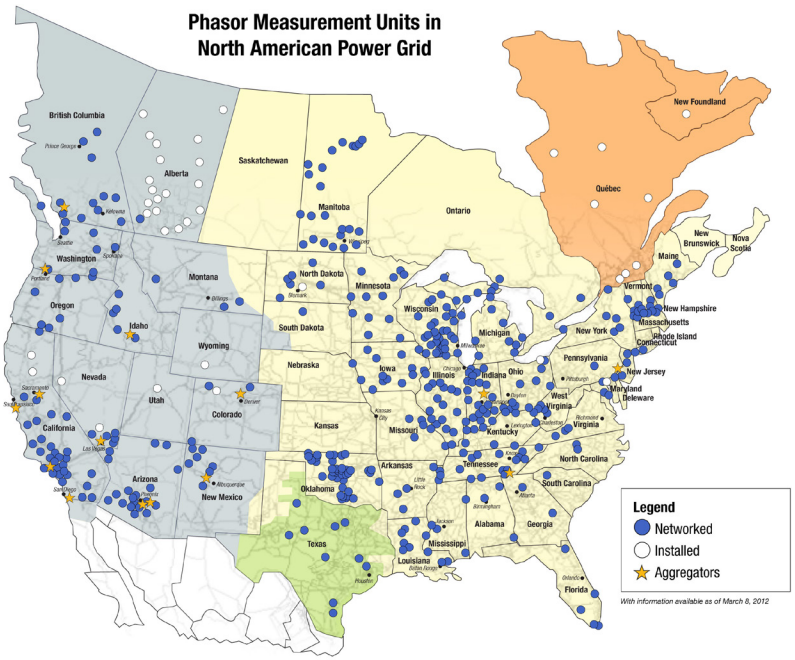
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

DOE and NERC are working together closely with industry to enable wide area time-synchronized measurements that will enhance the reliability of the electric power grid through improved situational awareness and other applications

April 2007



March 2012



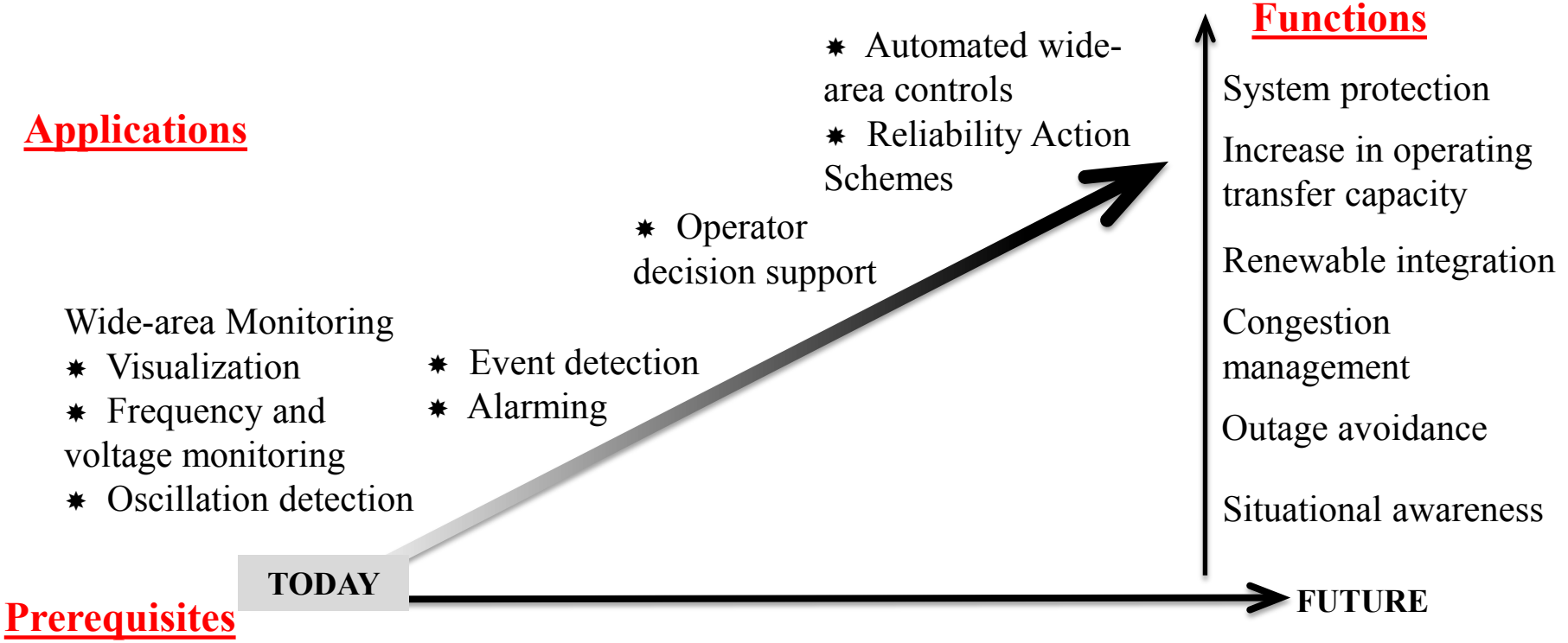
"Better information supports better - and faster - decisions."

NASPI North American SynchroPhasor Initiative

CERTS Consortium for Electric Reliability Technology Solutions

NERC North American Electric Reliability Corporation

REAL-TIME SYNCHROPHASOR APPLICATIONS AND THEIR PREREQUISITES



Prerequisites

ANALYSIS	Good data collection	Interconnection-wide baselining	Pattern detection	Model validation – system & elements	System studies
COMMUNICATIONS	Interoperability standards	High availability, high speed	Appropriate physical & cyber-security	Redundant, fault-tolerant	
USERS	Familiarity		Good visual interface	Training	

Security of Synchrophasors

- Synchrophasors are becoming part of the bulk electric system and will require physical and cyber security
  - ***But these systems shouldn't be treated any differently than other forms of measurement and control telemetry***
- Synchrophasor systems will coexist with other bulk electricity system (BES) cyber infrastructure and will have similar dependencies on common communications and network elements
- System designers and owners are leveraging emerging cyber-security standards and technologies
- Currently available phasor applications require further data analysis, software refinement and operational validation to be fully effective; many are in advanced development and testing and are not in full operational use
  - Therefore, many of these systems are not currently considered critical cyber assets
- Due to nature of continuous, high-volume data flows, new technology will likely be required for measurement, communications, and applications
  - Technology anticipated to undergo rapid change and refinement over the next several years

Cyber Security ARRA Activities *Critical* to Smart Grid Success

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

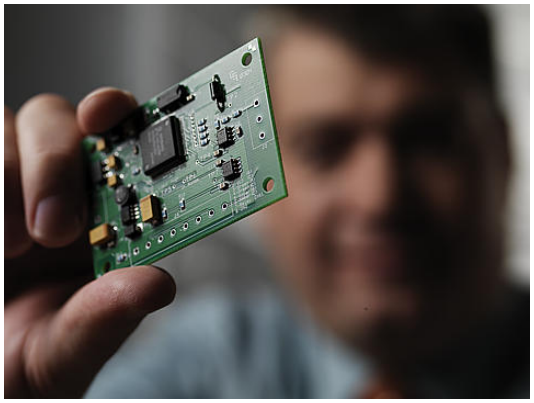
- Organized interagency group (DOE, NIST, FERC, DHS, others) for development of cyber security requirements in the funding opportunity announcement
- Cyber security - major factor in technical merit review
- Separate subject matter expert team provided independent reviews
- DOE's team of subject matter experts reviewed and approved the cyber security plans
- Annual site assessments currently underway

"DOE may not make an award to an otherwise meritorious application if that application cannot provide reasonable assurance that their approach to cyber security will prevent broad based systemic failures in the electric grid in the event of a cyber security breach."

Smart Grid FOA

www.ARRASmartGridCyber.net

Provide a resource enabling Smart Grid Investment Grants (SGIG) and Smart Grid Demonstration Projects (SGDP) to understand the baseline principles and practices necessary to implement cyber security in the deployment of smart grid technologies



Cyber Security Plan

- ARRA projects committed to a technical approach to cyber security that included a plan to provide a summary of:
  - the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact),
  - cyber security criteria utilized for vendor and device selection,
  - relevant cyber security standards and/or best practices that will be followed, and
  - how the project will support emerging smart grid cyber security standards.
- A strong Cyber Security Plan will:
  - provide commitment to the organization's cyber security assessments, evaluations, and threat analyses,
  - provide assurance that a defensive strategy will be created, appropriate security controls, will be selected, and mitigation methodologies based on risk-informed processes will be implemented, and
  - document that all systems are installed, tested, and operated with appropriate and diligent cyber security.

Identifying Risks of Implementing Smart Grid Systems (an All Hazards Approach)

- Complexity
  - Introduces potential vulnerabilities
  - More access points (increased exposure)
  - Difficult to manage a complex system
- Power system would be more vulnerable to communication (or software) disruptions
  - Denial of service (e.g., unintentional load shedding)
  - Potential for common failure modes across connected systems
  - Software/system integrity (e.g., firmware, logic bomb, supply chain, etc.)
- Intelligence gathering tool for the adversary
- Potential for breach of customer privacy
- Implementation issues
  - Inappropriate or premature mandating of technologies that aren't appropriate for the application
  - Potential for technology obsolescence

Mitigating Smart Grid Implementation Risks

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Develop security controls
  - Policies, procedures, control baselines, reference architectures, conformance and interoperability testing, certification
- Need built-in (rather than bolt-on) security
- Apply good security practices
  - Follow best practices, established standards when available
- Apply defense-in-depth concepts
  - Redundancy, zones, proxies, role-based authority, etc.
- Instill a culture of security
  - Training, awareness, adequate resources, management support
- Develop transition strategy that maximizes interoperability, security, reliability, etc.
- Forensics and enforcement
- Establish trusted technology supply chain

Infrastructure Resilience

- Ability to reduce the magnitude and/or duration of disruptive events
- Resilient infrastructure can anticipate, absorb, adapt to, and/or rapidly recover from a disruptive event
- Best when all-hazard “disruptive events” that were not envisioned beforehand do not create systemic failure

Concluding Remarks

- The power grid is exceptionally complex, and extraordinarily reliable
  - Most customer outages are due to issues with radial distribution feeders vs. the networked transmission grid
- Hierarchal control strategy provides good tradeoff between reliability and efficiency
- As advanced technology is being considered for deployment, need to consider unintended consequences (e.g., cyber security)
- Robustness and resiliency are enhanced by considering all threats to the power system
  - An “all-hazards” approach
- Historically little attention has been given to addressing multiple contingency scenarios
  - Need to consider cost-effective risk mitigation solutions