



EPRI

ELECTRIC POWER
RESEARCH INSTITUTE

Smart Grid, Cyber Security, and What's Next?

Annabelle Lee

Technical Executive – Cyber Security

Smart Grid Information Call

April 18, 2011

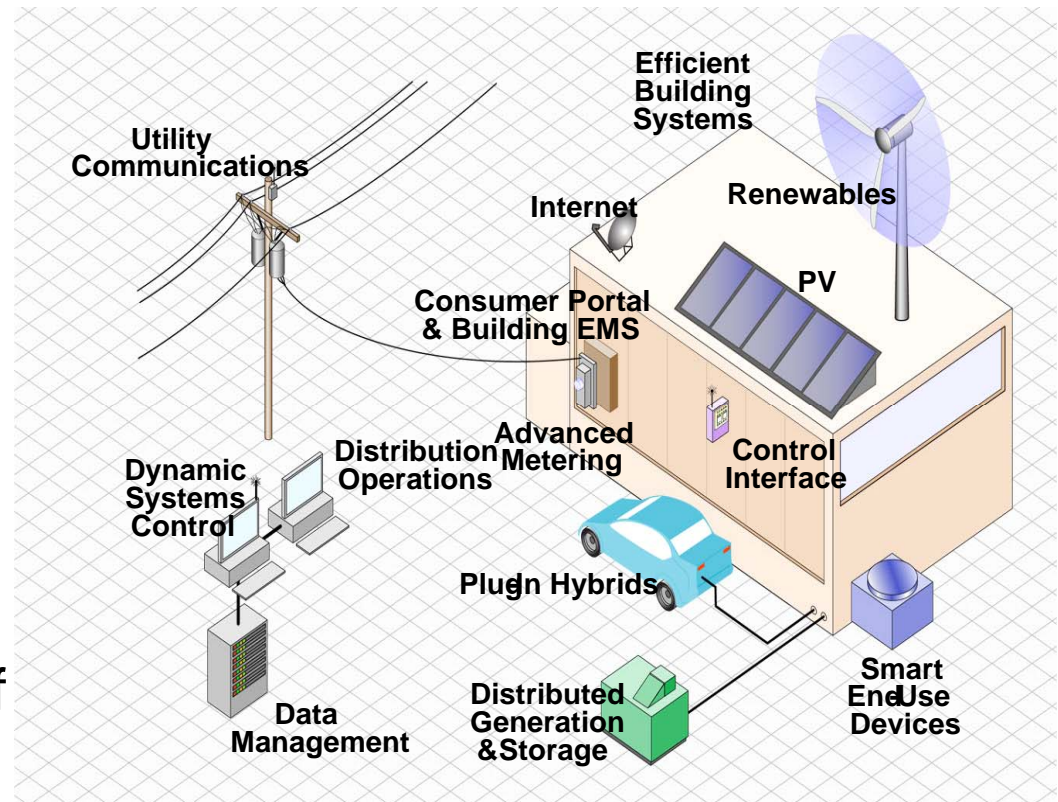
Recent events...



<u>What</u>	<u>Why it's important</u>
Stuxnet	Highly sophisticated attack on control systems hardware. Target specific through common USB attack vector.
WikiLeaks	Takes advantage of data breaches and the insider threat. Exposes national security and diplomatic information.
Night Dragon	Sensitive IP stolen from energy companies.
RSA SecurID	Security of 40M 2-factor tokens at risk after cyber-attack.

Trends Impacting Security

- Increasing interconnections at all levels
- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Insecure connections
- Widespread availability of technical information about control systems
- Increasing reliance on automation

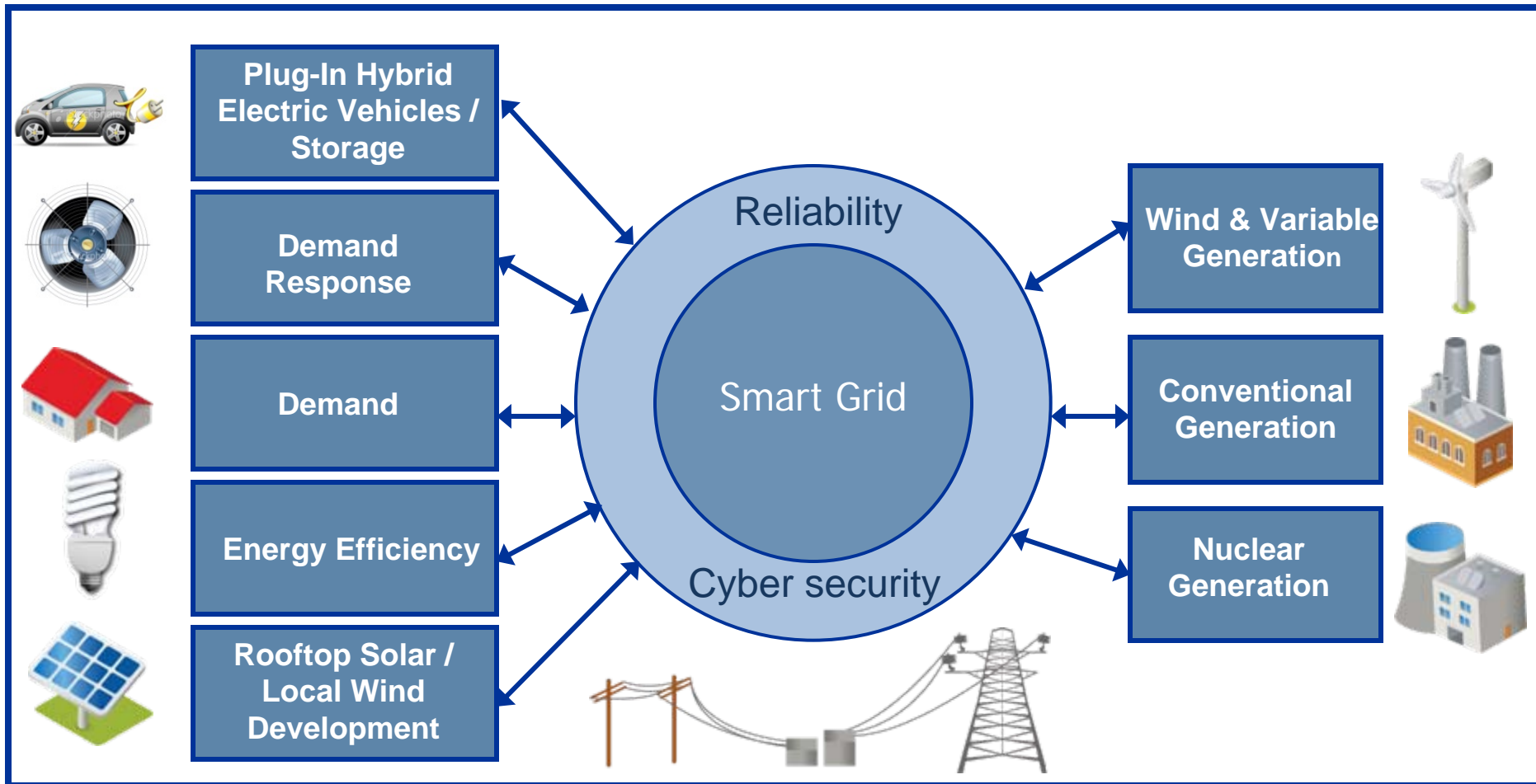


Trends Impacting Security (2)

- Open protocols
 - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- Common operating systems
 - Standardized computer platforms increasingly used to support control system applications
- Interconnected to other systems
 - Connections with enterprise networks to obtain productivity improvements and information sharing
- Reliance on external communications
 - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- Increased capability of field equipment
 - “Smart” sensors and controls with enhanced capability and functionality



21st century: Smart Grid and Beyond...



Building the 21st century grid requires a comprehensive and coordinated approach – looking at the grid as a whole, not as component parts.

FERC Technical Conference

- EISA directed FERC to "institute a rulemaking to adopt such standards as may be necessary to ensure Smart Grid functionality and interoperability, after NIST's work has led to consensus in the Commission's judgment."
- October 6, 2010:
 - NIST identified five foundational families of standards as ready for consideration by regulators
 - Standards are fundamental to Smart Grid interoperability
 - And to priorities identified in the Commission's July 16, 2009 Smart Grid Policy Statement

FERC Technical Conference (2)

- Technical conference announcement:
 - The purpose of the conference is to obtain further information to aid the Commission's determination of whether there is "sufficient consensus" that the five families of standards posted by NIST on October 6, 2010, are ready for Commission consideration, as directed by section 1305(d) of EISA.
- Technical conference held January 31, 2011
 - Thirteen speakers and George Arnold from NIST
- Five families of standards:
 - IEC 61970 and IEC 61968: Common Information Models
 - IEC 61850: Facilitates substation automation and communication
 - IEC 60870-6: Facilitates exchanges of information between control centers.
 - IEC 62351: Addresses cyber security of communication protocols

FERC Technical Conference (3)

- Questions posed to presenters
- Unanimous agreement among speakers that the standards are not ready for adoption
- Additional questions posted on the website after the technical conference
 - Web site
 - <http://www.ferc.gov/docs-filing/elibrary.asp>
 - Under docket search, enter RM-11-2
 - Initial comments submitted by April 8, 2011
 - Comments on comments due **April 22, 2011**

Analysis of Submitted Comments

- 35 organizations/individuals submitted comments
 - Asset owners/operators
 - State PUCs and NARUC
 - Trade associations
 - Vendors
 -
- General comments
 - The general consensus was that the process can benefit from a more robust review by reliability and security experts who are capable of assessing the functionality of technologies as well as their capability to address cyber threats. (SCE)
 - ...the CPUC is concerned that the proposed standards have not sufficiently met appropriate functionality, interoperability and cyber-security criteria.

Analysis of Submitted Comments (2)

- General comments

- It is also important to recognize that cyber security standards are different from traditional electric utility standards. Cyber threats and vulnerabilities are constantly changing. Cyber security controls and responses must therefore be regularly monitored and augmented to address those changes. (SMUD)
- Without appropriate standards, there is potential for technologies developed or implemented with sizable investments to become prematurely obsolete or to be implemented without measures necessary to ensure reliability and security, including cyber security. (EEI)
- Similarly, SDG&E has consistently raised concerns that the adoption of prescriptive cyber security standards runs the risk that such standards will ultimately prove to be insufficiently responsive to, robust against, and anticipatory of emerging threats.

Analysis of Submitted Comments (3)

- General comments:
 - NERC respectfully requests that the Commission: ...4) investigate the use of “defense-in-depth” and risk assessment to address cyber security implications of smart grid applications.
 - Part of this additional work should involve ensuring that the standard provides adequate levels of cyber security and that it has been proven in real-world scenarios.
(ISOs/RTOs)
 - Most troubling from FPL’s perspective is the lack of an adequate record regarding rigorous consideration of cyber security and system reliability impacts that may result from the Commission’s adoption of the five families of standards.
 - While it is essential that the standards include cybersecurity protocols, the evolving nature of cyber threats will require adjustments, responsiveness, and adaptable risk management in and beyond the standards.
(NARUC)

Analysis of Submitted Comments (4)

- General Comments
- ..regulating cyber security is not only unwise but could increase the likelihood of a successful cyber attack. As with interoperability standards, rigorous cyber security depends on industry's ability to respond quickly and without regulatory intervention to new and emerging threats. (AT&T)

Specific Comments

- *Whether the criteria for the Commission's evaluation should differ for interoperability and functionality, and the extent to which cyber security is an element of each.*
 - Functionality of a standard/protocol cannot be divorced from its cyber security and interoperability attributes, because they are all intertwined. (SCE)
 - Realistically, cyber-security and interoperability are at odds. Perfect security precludes any interoperable functionality; perfect interoperability makes security extremely difficult. (NRECA/APPA)
 - The appropriate cyber security reviews should be performed, regardless of whether considered an aspect of interoperability or functionality. (EEI)

Specific Comments (2)

- SDG&E considers risk-based cybersecurity reviews and testing to be an important element of the evaluation of any standards without regard to whether the standard addresses interoperability or functionality.
- Clear guidance needs to be considered should security mechanism failures impact the operational integrity of the Smart Grid.

Systems must be resilient with respect to security failures (SISCO)

Moving Forward...

- Address interconnected systems – both IT and control systems
 - Cyber security needs to be addressed in all systems, not just critical assets
 - Augment existing reliability controls, as applicable
 - Build upon current base of organization and system policies, procedures, and technical mitigations
- Continuously assess the security status
 - Regression testing
- Acknowledge there will be some security breaches
 - Focus on response and recovery
 - For example, isolate/quarantine infected devices
 - *Fail secure*
 - Address both safety and security

Moving Forward... (2)

- Build Security In!
 - Confidentiality, integrity and availability – implement best practices
- Apply IT/telecomm security lessons-learned from the past 40 years
- Train and educate
 - Address advanced persistent threats (APTs)
 - Social engineering tactics
- Cyber security supports both the reliability and privacy of the Smart Grid
- Compliance DOES NOT equal security



alee@epri.com

Together...Shaping the Future of Electricity