U.S. DEPARTMENT OF ENERGY

Resiliency and Security of the Electric Power Delivery System

Patricia Hoffman
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy
www.OE.energy.gov

OE Strategic Plan

- **Mission**
  - Office of Electricity Delivery & Energy Reliability (OE) leads the Department of Energy's efforts to ensure a resilient, reliable, and flexible electricity system.
  - OE accomplishes this mission through research, partnerships, facilitation, modeling and analytics, and emergency preparedness.
- **Vision**
  - Through a mix of technology and policy solutions, OE will address the changing dynamics and uncertainties in which the electric system will operate. We will leverage effective partnerships, solid research, and best practices to address diverse interests in achieving economic, societal, and environmental objectives.

Resilience

"the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies"

- Presidential Policy Directive / PPD-8: National Preparedness

Build Capabilities to :

- Prevent: Reduce vulnerability or minimize impact
- Respond: Restore quickly while improving capabilities (e.g. Category 1 Hurricane – Category 2 Hurricane)

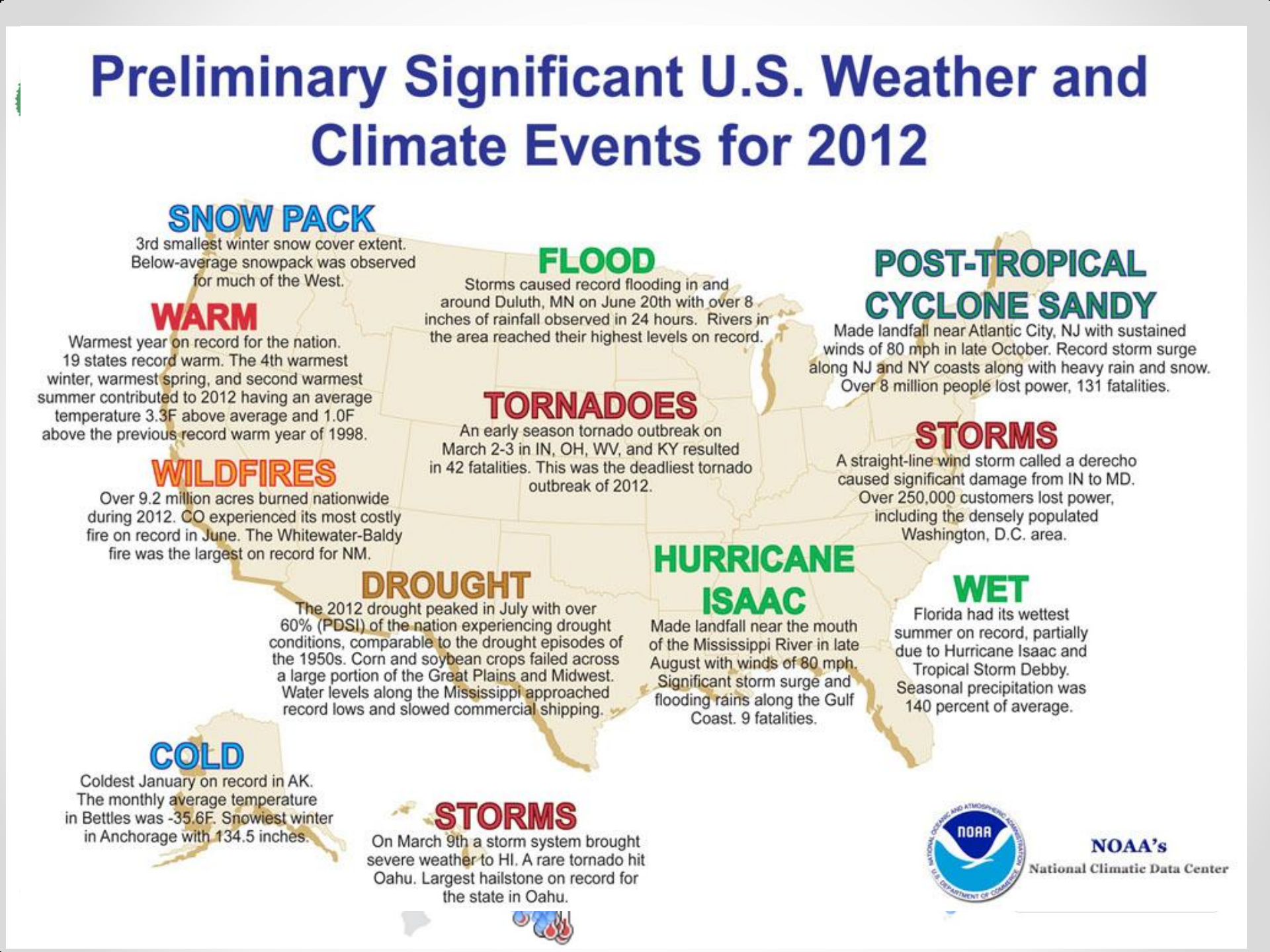
Utility Analytics and Standards Play a Critical Role

- http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

Emergency/Significant Events

- Significant event that causes (Climate or Criminal/Terrorism):
  - Prolonged outage (> X weeks)
  - Mass disruption
  - Economic impact (loss of $$, price volatility)
- Thresholds (Risk):
  - Restoration greater than X weeks or X days
  - Price of delivered electricity – abnormal
- Success Measures:
  - Track performance/events (Assess performance and provide recommendations)
  - Exercises
  - Modeling / Simulations

Preliminary Significant U.S. Weather and Climate Events for 2012



SNOW PACK

3rd smallest winter snow cover extent. Below-average snowpack was observed for much of the West.

WARM

Warmest year on record for the nation. 19 states record warm. The 4th warmest winter, warmest spring, and second warmest summer contributed to 2012 having an average temperature 3.3F above average and 1.0F above the previous record warm year of 1998.

WILDFIRES

Over 9.2 million acres burned nationwide during 2012. CO experienced its most costly fire on record in June. The Whitewater-Baldy fire was the largest on record for NM.

COLD

Coldest January on record in AK. The monthly average temperature in Bettles was -35.6F. Snowiest winter in Anchorage with 134.5 inches.

FLOOD

Storms caused record flooding in and around Duluth, MN on June 20th with over 8 inches of rainfall observed in 24 hours. Rivers in the area reached their highest levels on record.

TORNADOES

An early season tornado outbreak on March 2-3 in IN, OH, WV, and KY resulted in 42 fatalities. This was the deadliest tornado outbreak of 2012.

DROUGHT

The 2012 drought peaked in July with over 60% (PDSI) of the nation experiencing drought conditions, comparable to the drought episodes of the 1950s. Corn and soybean crops failed across a large portion of the Great Plains and Midwest. Water levels along the Mississippi approached record lows and slowed commercial shipping.

STORMS

On March 9th a storm system brought severe weather to HI. A rare tornado hit Oahu. Largest hailstone on record for the state in Oahu.

HURRICANE ISAAC

Made landfall near the mouth of the Mississippi River in late August with winds of 80 mph. Significant storm surge and flooding rains along the Gulf Coast. 9 fatalities.

POST-TROPICAL CYCLONE SANDY

Made landfall near Atlantic City, NJ with sustained winds of 80 mph in late October. Record storm surge along NJ and NY coasts along with heavy rain and snow. Over 8 million people lost power, 131 fatalities.

STORMS

A straight-line wind storm called a derecho caused significant damage from IN to MD. Over 250,000 customers lost power, including the densely populated Washington, D.C. area.

WET

Florida had its wettest summer on record, partially due to Hurricane Isaac and Tropical Storm Debby. Seasonal precipitation was 140 percent of average.

NOAA's National Climatic Data Center

The Calm After the Storm: Lessons Learned from Hurricane Sandy

Recommendations

- Establish standards and guidelines for fuels facilities
- Strengthen resiliency and hardening of the system
- Consider alternative system configurations for critical facilities
- Revise current building and rehabilitation codes

DOE's "Next Steps"

- Continue meeting with stakeholders to examine areas for improvement
- Continue improving communications channels with energy stakeholders
- Continue identifying what can be done to facilitate access to critical supplies for restoration of critical services
- Continue facilitating communication of policies and practices which support preparedness and resilience

NEXT GREAT IDEA

The Rush to Resilience: 'We Don't Have Decades Before the Next Sandy'

RICHARD FLORIDA NOV 09, 2012 3 COMMENTS

In an era of disruptions so significant that we refer to them in a single-name shorthand (think: 9/11, Katrina, Fukushima, Haiti, Sandy) what gives communities their ability to bounce back? And what does it mean for the way we build (and rebuild) cities? To explore these topics, we invited two leading thinkers who are working at the forefront of resilience — Andrew Zolli and Jonathan Rose — into a dialogue.

Zolli's new book, *Resilience: Why Things Bounce Back*, written with Ann Marie Healy, is a must-read primer on the field of resilience research, examining the capacity of everything

NJ SPOTLIGHT
WHERE ISSUES MATTER

PSE&G Wants $4 Billion to Bring Power Grid Into 21st Century

Scheme would substitute new ratepayer subsidies for ones now expiring, masking real costs to customers

By **Tom Johnson**, **February 21, 2013** in **Energy & Environment** | *5 Comments*

Is it time to invest nearly $4 billion in ratepayer subsidies to help modernize the power grid to avert widespread outages from extreme weather, such as Hurricane Sandy?

If the state's largest utility gets its way, the answer is "Yes," at least according to a filing yesterday with the New Jersey Board of Public Utilities. The proposal -- courtesy of Public Service Electric & Gas -- is likely to kindle a fiery debate over how the state should respond to Sandy and at what cost to consumers.

The filing comes at a time when the state's utilities are under enormous pressure to reduce long outages caused by extreme weather, while the Christie administration is struggling to find ways to reduce energy bills, which typically rank among the highest in the nation. Tough choices abound all around.

Related Links

Report from American Society of Civil Engineers

But PSE&G executives argue that with natural gas prices at historic lows and surcharges related to the deregulation of the energy industry in New Jersey lapsing in the next few years, it's possible to ramp up the resiliency of the power grid without spiking residential customers' bills.

It is a scenario that some find highly unlikely.

"If you think a $4 billion filing will not affect ratepayers, then you believe in fairy dust," said Stephen Goldenberg, an attorney for the New Jersey Large Energy Users Coalition, a group that could be burdened by big increases in their electric bills if the filing is approved. Goldenberg noted he has yet to review the filing.

"I don't know how ratepayers can afford it," agreed Stephanie Brand, director of the New Jersey Division of Rate Counsel, which represents consumers and businesses in utility rate cases. "It's really troubling from a ratepayer perspective."

R&D Priorities- Terrorism Report

- Development of high-voltage recovery transformers
- Development and demonstration of advanced computational system intended to support more rapid estimation of system state and broader system analysis
- Development of visualization system for transmission control centers to support informed operator decision making and reduce vulnerability to human errors
- Development of dynamic systems technology and demand response demonstrations to allow interactive control of consumers and consumer loads
- Development of multilayer control strategies that include capabilities to island and self-heal the power system
- Development of improved energy storage that can be deployed as dispersed systems

"R&D Priorities , mid- long term time frame" Pg 79/97 of Terrorism and Electric Power Delivery System

OE Priorities

- Research and Development ($ 71.6 million)
  - Energy Storage
  - Microgrids/Active Distribution System (DG, EV, Transactive Control)
  - Cyber Security
  - *Flow Control*
  - *Asset Management/Predictive Failure*
- Smart Grid Deployment ($4 Billion ARRA)
  - Meters, phasors and other sensors
  - Outage management systems
  - Transmission Visualization
  - Transactive control, Volt/VAR, System efficiency,
  - Storage, Distributed Generation, EV
  - Rates and Consumer Behavior Studies
  - Cyber Security
- Energy/Grid Modeling and Analytics ($24.6 million)
  - Visualization
  - Predictive Modeling
  - *Next Generation EMS*
- Infrastructure Security and Energy Restoration ($6 million)
  - Emergency Preparedness Response and Restoration
  - Physical and Cybersecurity Awareness
  - Global Energy Assurance
- National Electricity Delivery ($7 million)
  - Transmission Planning
  - NEPA/Environmental Impact
  - Technical Assistance
  - Energy/Water nexus

NOTE: FY 2012 numbers, *Italics represents future areas*

Storage

Southern California Edison Storage Project

A Tehachapi Wind Field

8MW Storage Plant under Construction

Goals/Objectives:

- Validate the performance and effectiveness of lithium-ion technology
- Demonstrate the integration of intermittent wind energy
- Develop a smarter, more efficient electrical grid
- Advance market readiness of utility-scale storage

Key Milestones:

- Completion of energy storage system manufacturing plan (November 2011)
- Installation of battery and inverter completed (June 2012)
- Two year demonstration complete (December 2014)

Anticipated Benefits:

- Create/retain jobs
- Improve power quality
- Increase system reliability
- Integrate more clean, renewable energy
- Foster energy independence

http://www.smartgrid.gov/sites/default/files/socal-edison-oe0000201-final.pdf

OE Microgrid Efforts

To date, the majority of the DOE microgrid work has been on demonstrations

FY 2012 and prior

- Renewable and Distributed Systems Integration (RDSI)
- Consortium for Electric Reliability Technology Solutions (CERTS)
- The Distributed Energy Resources Customer Adoption Model (DER-CAM)
- Test Beds and Laboratory Efforts
- Energy Surety Microgrids (ESM)
- Smart Power Infrastructure Demonstration for Energy, Reliability, and Security (SPIDERS)
- Standards Development – Interconnection and Interoperability

FY 2012 and beyond

- **Microgrid Development/Active Distribution System**
- RD&D to reach 2020 performance targets on costs, reliability, system energy efficiencies, and emissions

Smart Grid

Customer Systems

Oklahoma Gas and Electric (OGE)

Time-of-use and variable peak / critical peak pricing with in-home customer device use enabled **up to 30% peak demand reduction (which could offset a new peaking plant)** and **lowered customer bills by up to $150**

Distribution

Electric Power Board of Chattanooga

Advanced automated circuit smart switches and sensor equipment will enable **40% reduction in customer outage minutes** – worth $35 million/year to customers

AMI

Talquin Electric Cooperative (TEC)

Smart meter installations are saving hundreds of thousands of dollars in misreporting (from manual reading) and **saving an expected $200,000/year from 5,500 avoided truck rolls**

Transmission

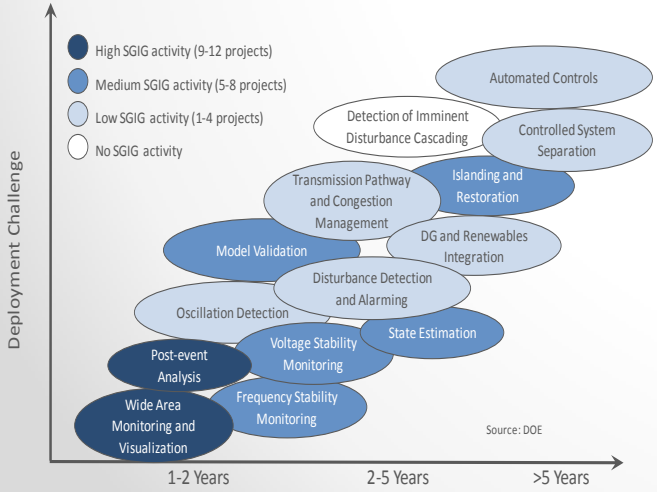
Western Electricity Coordinating Council (WECC)

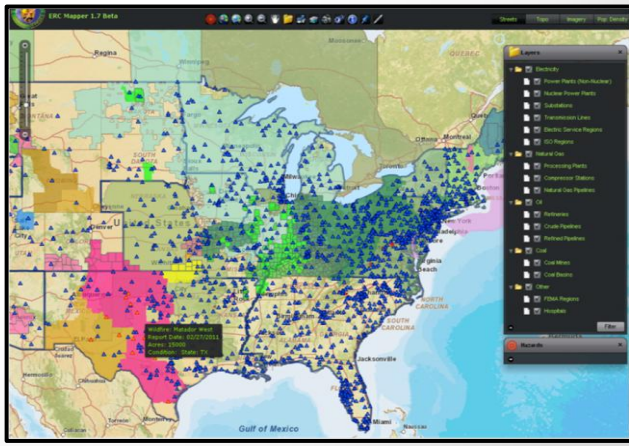
18 transmission owners **installing and connecting 341 PMUs and 62 PDCs** to modernize transmission in the Western Interconnection

Grid Modeling and Energy Analytics

- Modeling and Simulation for Emergency Response and Restoration (Energy Resiliency and Risk Analysis
  - Energy Risk "Criticality" Analysis Project
  - Expand Eagle- I's Capability
- Predictive Modeling and Controls for Cascading Events (System Dynamics)
  - Synchrophasor (visualization, operator tools and next generation EMS)
  - Implement recommendations from the 2003 and 2011 Blackouts.
- Energy Reliability Assessments.

Data consistency, Model convergence, CIM standards are important issues.

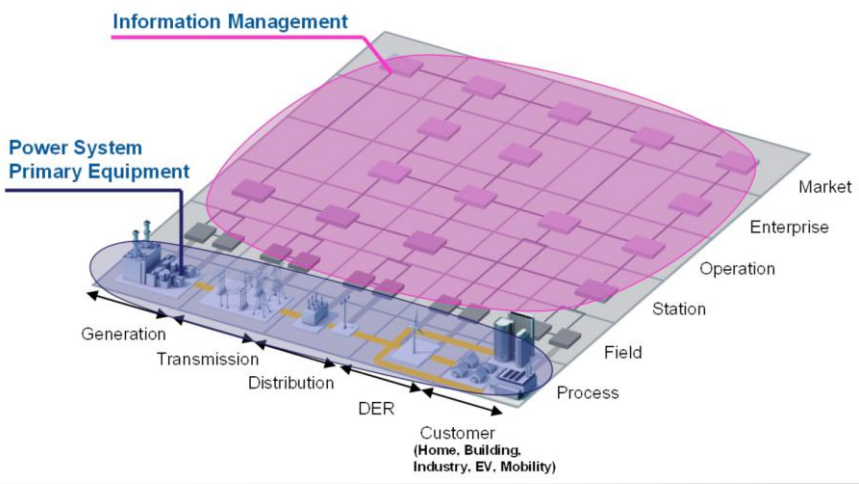




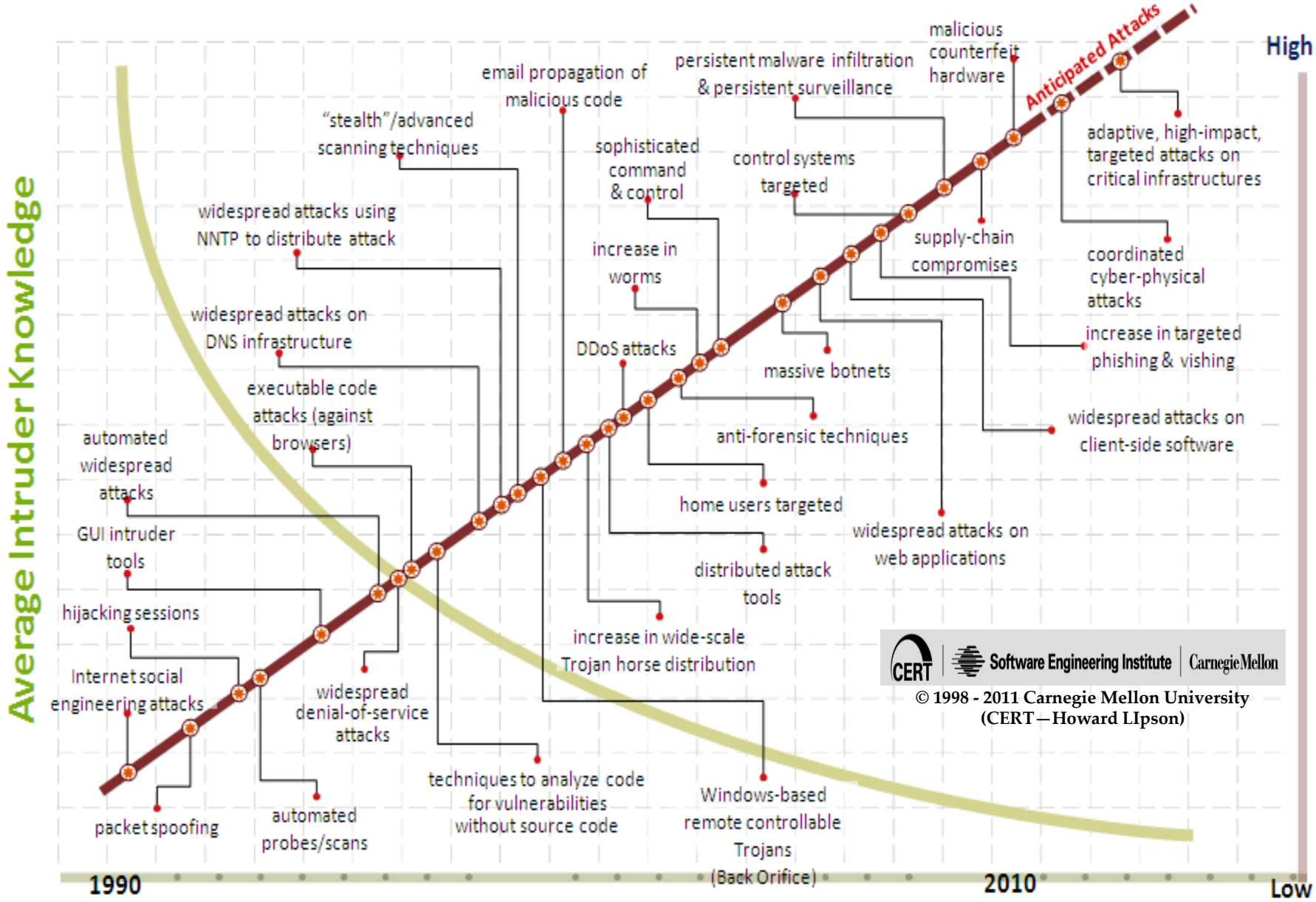
Cyber Security Framework

Comprised of Capability and Risk Management

- Risk Management (analyze risk)
- Asset Configuration Management (inventory, architecture, software upgrades
- Identity and Access Management (role base access for application and physical access
- Threat and Vulnerability Management (new IT, OT technologies)
- Situational Awareness (Monitoring tools, intrusion detection tools)
- Information Sharing and Communications
- Event and Incident Response (Detect and Respond)
- Supply Chain and External Dependencies Management
- Workforce Management



Attack Sophistication vs. Intruder Technical Knowledge



Situational Awareness

- Situational awareness activities may include:
  - Performance of logging
  - Monitoring logs
  - Aggregating monitoring information
  - Developing a "Common Operating Picture"

- Example MIL Progression for "Monitor the Function"
  - MIL1 – Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data)
  - MIL2 – Alarms and alerts are configured to aid the identification of cybersecurity events
  - MIL3 – Continuous monitoring is performed across the operational environment to identify anomalous activity

Incident Response

- Incident response activities may include:
  - Analyzing incidents to identify patterns and trends
  - Logging, tracking and reporting incidents
  - Performing root-cause and lessons-learned analysis

- Example MIL Progression for "Plan for Continuity"
  - MIL1 – The sequence of activities necessary to return the function to normal operation is identified
  - MIL2 – Recovery time objectives for the function are incorporated into continuity plans
  - MIL3 – Recovery time objectives are aligned with the function's risk criteria

Example: Shodan

Description: Readily available search engine that identifies configuration of industrial control systems connected to the internet

Attack Vector	Capability
Internet Accessible assets	A network (IT and/or OT) architecture is used to support risk analysis
Remote Access	Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring
Brute Force Attack	Anomalous access attempts are monitored as indicators of cybersecurity events
Known Vulnerability Exploits	Cybersecurity vulnerability information is gathered and interpreted for the function

US-CERT ICS Alert: http://*www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf*

Example: Night Dragon

Description: Coordinated attack by Advanced Persistent Threat using multiple attack vectors with the goal of data theft

Attack Vector	Capability	
Social Engineering	Cybersecurity awareness content is based on the organization's threat profile, users are educated	
Default Hardware Configuration	The design of configuration baselines includes cybersecurity objectives	
Known Vulnerability Exploits	Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organization-defined frequency	
Lack of awareness	Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings)	

ES-ISAC Industry Advisory: http://www.esisac.com/Public%20Library/Alerts/Night%20Dragon.pdf

R&D Success Story: Lemnos Interoperable Configuration Profiles

Configuration Profiles Improve Electricity Delivery Systems Security and Interoperability

- **Secure channels for routable data communications** through Internet Protocol Security (IPSec) virtual private networks (VPNs)
- **Secure web communications and terminal connection** using the Transport Layer Security (TLS) cryptographic protocol to provide communication security over the Internet and Secure Shell (SSH) for public-key cryptography to authenticate a remote terminal user
- **Centralized Certificate Revocation** using the Online Certificate Status Protocol (OCSP) to obtain the revocation status of a digital certificate
- **Central authentication and authorization** using the Lightweight Directory Access Protocol (LDAP) for accessing and maintaining distributed directory information services over an IP network
- **Central log collection** using Syslog for notification, traceability, and trouble shooting

***EnerNex Corporation**, Sandia National Laboratories, Schweitzer Engineering Laboratories, Tennessee Valley Authority*

Ten vendors of power grid devices have implemented the Lemnos solution for cybersecurity of energy sector routable communications!

CEDS Success Story: exe-Guard

Protects substation servers and communication processors against malware and unauthorized changes

- Whitelisting solution for embedded Windows and Linux® devices
- Protects against malware at the device level
- Maintains settings and configuration integrity
- Minimizes application of security patches
- Addresses CIP-007-R4, which requires asset owners to employ malicious software prevention tools on assets
- Minimizes the CIP-007-R3 requirement for security patch management

Technical Approach

- Develop a software solution for embedded Windows and Linux Systems
- Build on the Code Seal research conducted by Sandia National Laboratories
- Leverage deny by default/whitelist approach

For more information:
https://www.controlsystemsroadmap.net/Efforts/Pages/exe-Guard.aspx

Project Team: ***Schweitzer Engineering Laboratory****, Dominion Virginia Power, Sandia National Laboratories*

Examples of DOE National Laboratory R&D to enhance cybersecurity in energy sector

1. **High-Level (4th Gen) Language Microcontroller Implementation** – Idaho National Laboratory is implementing a high-level fourth generation programming language for use with microcontrollers that limits direct access to device memory and hardens microcontrollers against low-level cyber attacks

   Partners: *Siemens Corporate Research*

2. **Control Systems Situational Awareness Technology Interoperable Tool Suite** – Idaho National Laboratory is developing a situational awareness tool suite for control systems

   Partners: *Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho*

3. **Automated Vulnerability Detection for Compiled Smart Grid Software** – Oak Ridge National Laboratory is developing a system for conducting cybersecurity vulnerability detection of smart grid components and systems by performing static analysis of compiled software and device firmware

   Partners: *Software Engineering Institute, University of Southern Florida, EnerNex Corporation*

4. **Next Generation Secure, Scalable Communication Nework for the Smart Grid** – Oak Ridge National Laboratory is a developing a wireless technology that is robust, secure, scalable for smart grid applications using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming

   Partners: *Pacific Northwest National Laboratory, Virginia Tech, OPUS Consulting, Kenexis Consulting.*

5. **Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector** – Pacific Northwest National Laboratory is demonstrating that a bio-inspired solution using lightweight, mobile agents (Digital Ants) can be deployed across multiple organizational boundaries found in smart grid architectures to correlate activities, produce emergent behavior, and draw attention to anomalous condition

   Partners: *Wake Forest University, University of California-Davis, Argonne National Laboratory, SRI International*.

Examples of Applied R&D to Enhance Energy Sector Cybersecurity

1. **Watchdog** – Schweitzer Engineering Laboratories is developing a Managed Switch for the control system local area network (LAN) that performs deep packet inspection using a white list configuration approach to establish a set of known, allowed communications

   Partners: *CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory*

2. **Padlock** - Schweitzer Engineering Laboratories is developing a security gateway to help protect field device communications and sense physical tampering to enhance cyber and physical security at the distribution network level. The low-power, low-cost Padlock Gateway will establish encrypted communication between central stations and filed devices while enabling strong access controls, logging, and secure communications with transparent access to the serial port of the existing energy system protection device

   Partners: *Tennessee Valley Authority, Sandia National Laboratories*

3. **Role Based Access Control -Driven (RBAC) Least Privilege Architecture for Control Systems** – Honeywell International is developing a role based access control driven least privilege architecture for energy delivery systems

   Partners: *University of Illinois, Idaho National Laboratory*

4. **SIEGate** – Grid Protection Alliance is developing a Secure Information Exchange Gateway (SIEGate) that provides secure communication of data between control centers

   Partners: *University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D.*

5. **Smart Grid Cryptographic Key Management** – Sypris Electronics is developing a cryptographic key management system scaled to secure communications for the millions of smart meters within the smart grid advanced metering infrastructure

   Partners: *Purdue University Center for Education and Research in Information Assurance and Security, Oak Ridge National Laboratory, Electric Power Research Institute*

Putting it all together

Office of Electricity Delivery and Energy Reliability (OE)

- **Office Leading Vision View**
- **Office with Subject Matter Expertise**
- **Outstanding Relationships with Energy Industry**
- **OE Research Used in Industry Practice**

Cybersecurity

- **Cybersecurity is a shared responsibility**
- **Supply Chain issues**
- **Situational Awareness is a near-term priority**

Resiliency

- **System Flexibility (generation, load)**
- **Supply Chain**
- **Predictive failure/asset management**

Response

- **Improved Outage Management Systems**
- **Utility Analytics/information**
- **Interdependencies/Risk (gasoline, other critical infrastructure)**

Grid Modernization

- **Building Off Success of Smart Grid Investment Grants**
- **Whole System Approach**
- **Active Distribution System**
- **Predictive Analysis**


Chattanooga

The New York Times

Business Day
Technology

Fastest Net Service in U.S. Coming to Chattanooga

John Rawlston/Chattanooga Times Free Press

EPB workers installed fiber optic cable around Chattanooga last year. The utility began offering high-speed broadband a year ago.

By STEVE LOHR
Published: September 12, 2010

Friday, January 25, 2013 · 12:22 p.m.

Nooga.com

Home | Business | Government | Lifestyle | Opinion | Sports | Weather

BUSINESS

Gig City becomes partner in White House initiative to promote, utilize high-speed Internet

By Chloé Morrison Published Wednesday, June 13th 2012

John Rawlston/Chattanooga Times Free Press

EPB workers installed fiber optic cable around Chattanooga last year. The utility began offering high-speed broadband a year ago.

By STEVE LOHR
Published: September 12, 2010

Local Stocks

Mohawk Industries, I... 101.42 (+0.7
mhk

CBL & Associates Pro... 21.30 (+0.0
cbl

Miller Industries, Inc. 15.57 (+0.0

CBS News | CNET | SmartPlanet | TechRepublic | ZDNet

smartplanet

sp Home | Business | Technology | Innovation

Aerospace \ Architecture \ Cities \ Design \ Education \ Energy \ Finance \ Food \ Government \ Healthcare \ Sci

Home / Blogs / Technology / Thinking Tech

Follow this blog:

Chattanooga powers smart grid with a gigabit network

By Mari Silbey | May 1, 2012, 5:35 AM PDT

Home | Business

BUSINESS

Gig City becc
promote, uti

By Chloé Morrison Published

EPB workers installed fiber optic cable
year ago.

By STEVE LOHR
Published: September 12, 2010

Local Stocks

awk Industries, I... 101.42 (+0.7

& Associates Pro... 21.30 (+0.0

ler Industries, Inc. 15.57 (+0.0

published Thursday, July 21st, 2011

EPB grid attracts Cisco Systems to Chattanooga

by Ellis Smith
view bio »

font size print email share comment

EPB workers installed fiber optic cable year ago.

By STEVE LOHR
Published: September 12, 2010