GRID, PHD

The Smart Grid, Cyber Security, and the Future of Keeping the Lights On

Kelly Ziegler
Chief Operating Officer
National Board of Information Security Examiners

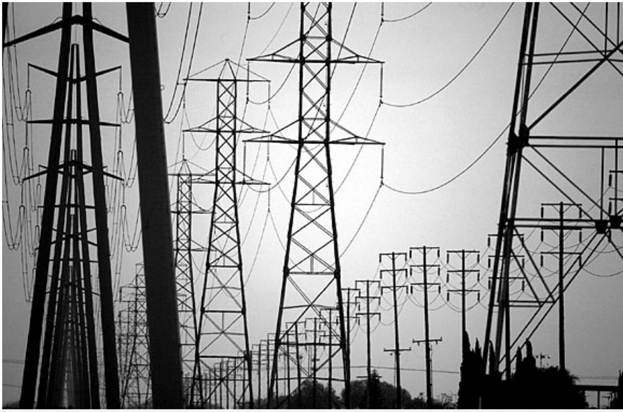
THE LEGAL STUFF

The views I will present today are my own and do not necessarily reflect the views of the National Board of Information Security Examiners (NBISE), its Board, Management, or Members.

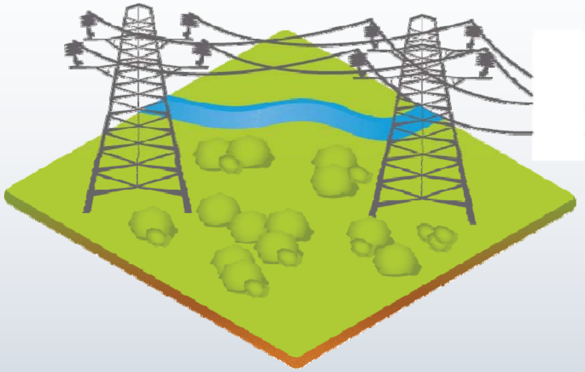
OVERVIEW

- The Grid: Common Background, Not Commonly Understood
- The Growth of the Smart Grid: Distribution, Transmission, the Chinese Wall, and Why it Matters
- Cyber Insecurity: The Smart Grid’s Mid-Life Crisis?
- The Road Ahead: FERC, NERC, NIST, and the Acronym Jungle

THE GRID: COMMON BACKGROUND

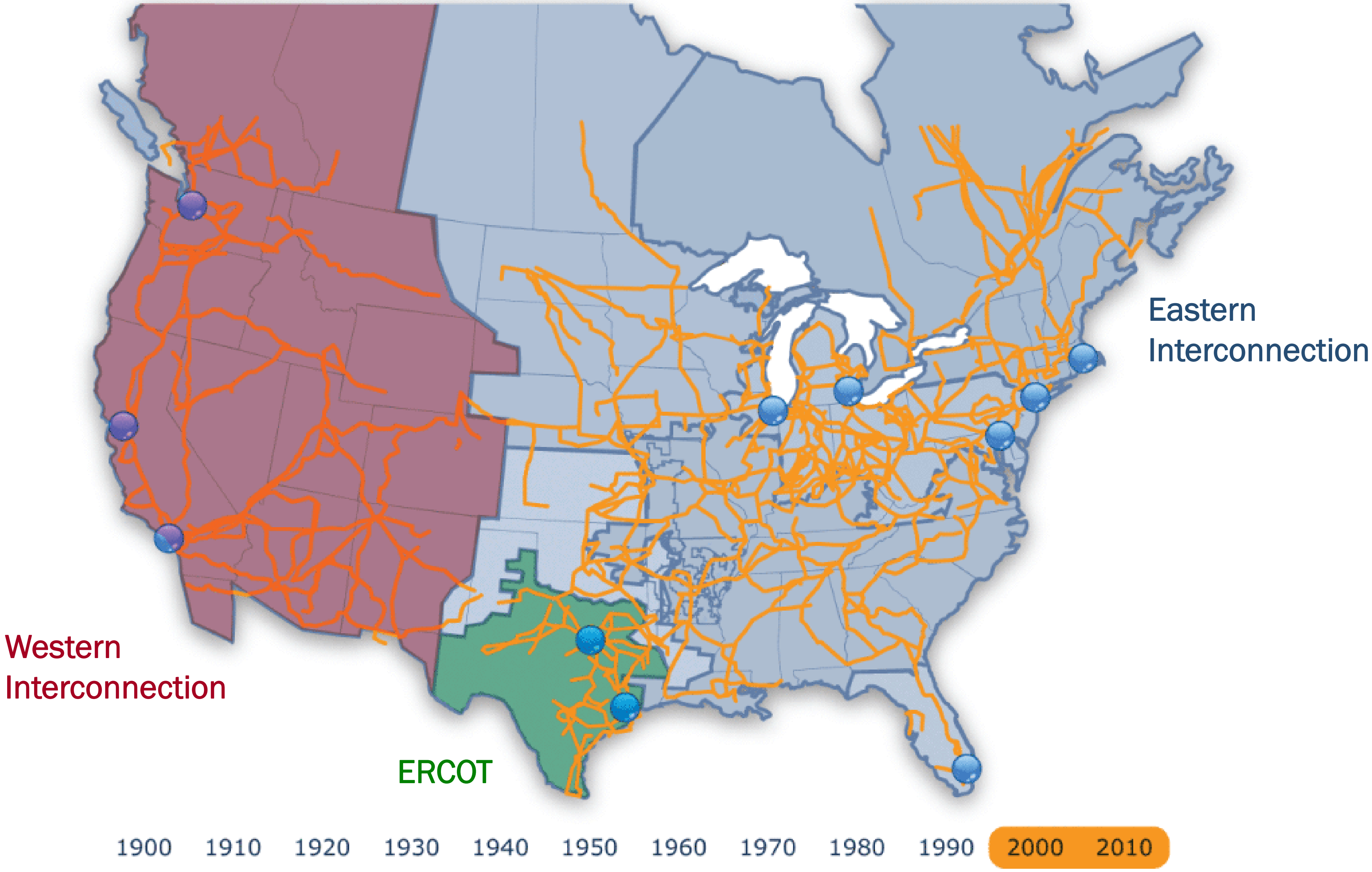


THE GRID: PARTS & PIECES



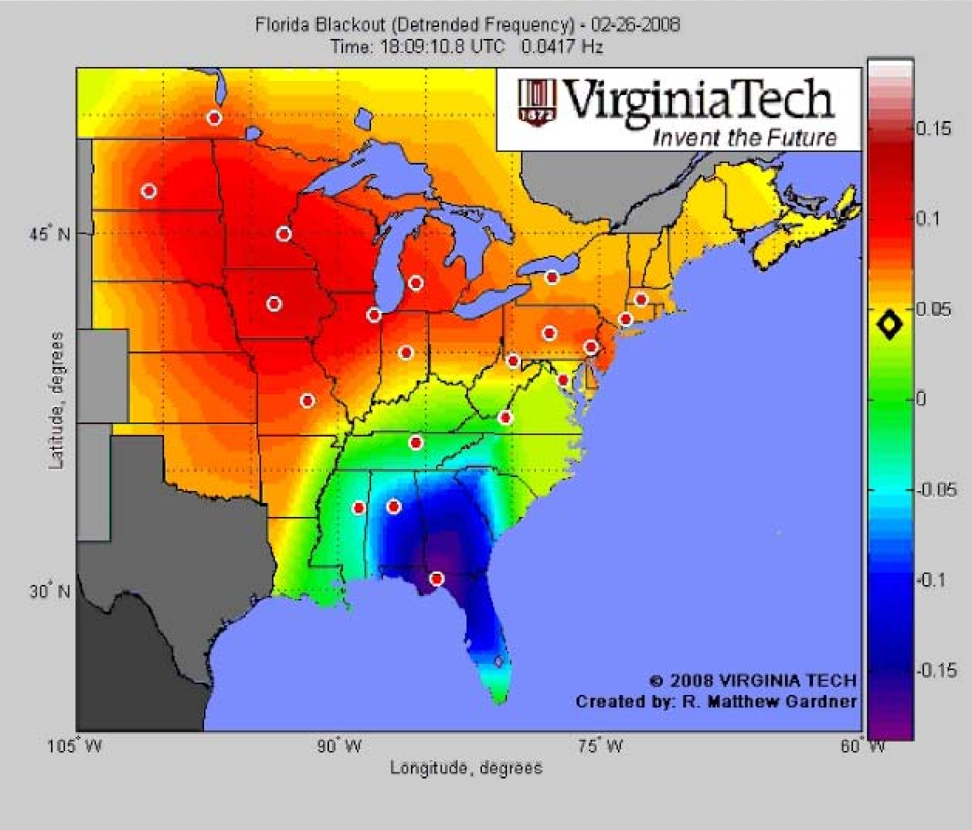
Generation	Transmission	Distribution
5,000 plants	160,000 miles	Over 1,000,000 miles
65% of monthly bill	5% of average customer monthly bill	30% of average customer monthly bill
Employs approx. 120,000 people nationwide	Employs approx. 15,000 people nationwide	Employs approx. 400,000 people nationwide

THE LARGEST MACHINE IN THE WORLD



THE LARGEST MACHINE IN THE WORLD

- Three Interconnections in United States
  - Eastern Interconnection, Western Interconnection, Texas (ERCOT)
- Changes happen faster than humans can react (measured in milliseconds)



Impacts from the 2008 February blackout in Florida were felt in Saskatchewan within 1 second.

THE LAY OF THE LAND

- Reliability Coordinators

  Responsible for the Wide Area view of the electric grid and the operating tools, processes and procedures. Has authority to prevent or mitigate emergency operating situations in both next day analysis and real-time operations.

  - 14 in Eastern Interconnection
  - 2 in Western Interconnection
  - 1 in Texas

- Balancing Authorities

  Integrates resource plans ahead of time, maintains load-interchange-generation balance within a balancing area, and supports interconnection frequency in real time.

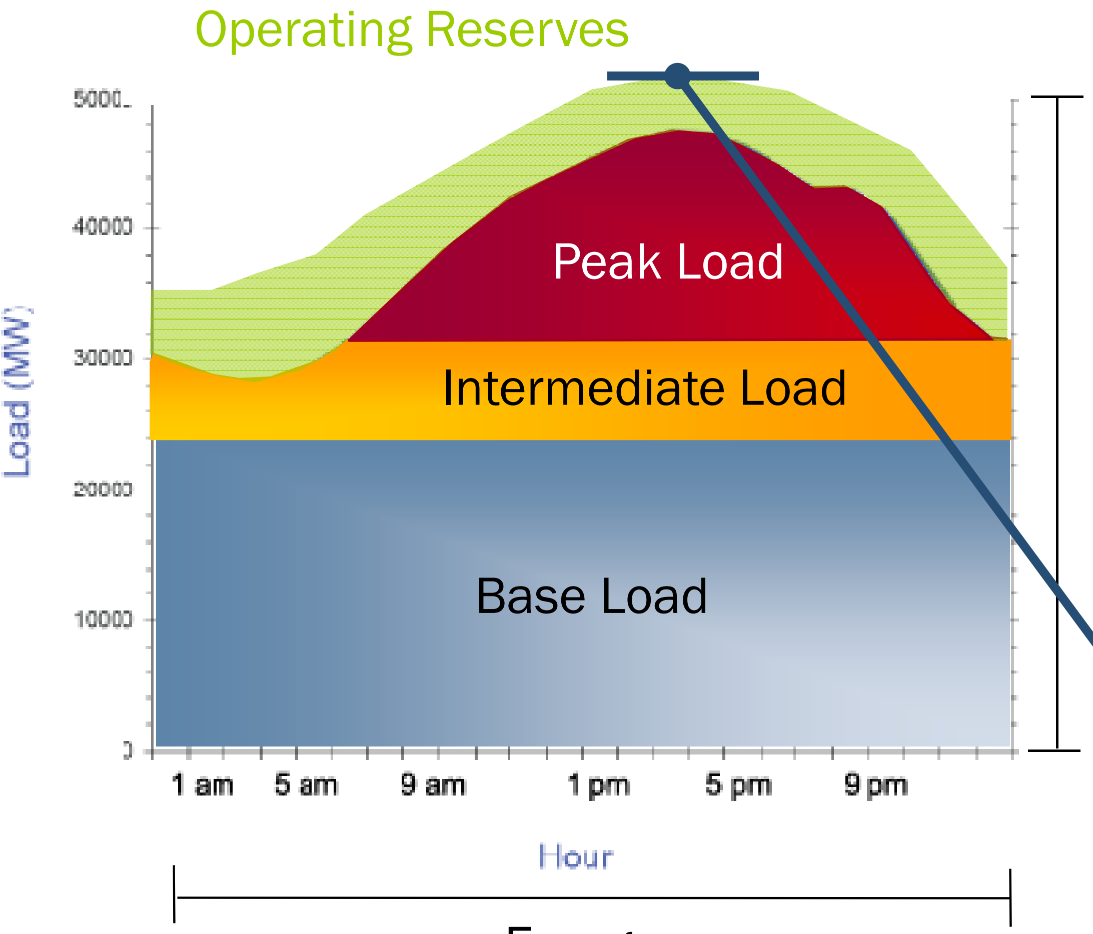
  - 97 in Eastern Interconnection
  - 34 in Western Interconnection
  - 1 in Texas

- Distribution System Operators

  Manages distribution systems at the local level.

THE BALANCE: SUPPLY & DEMAND

Typical Daily Demand Curve



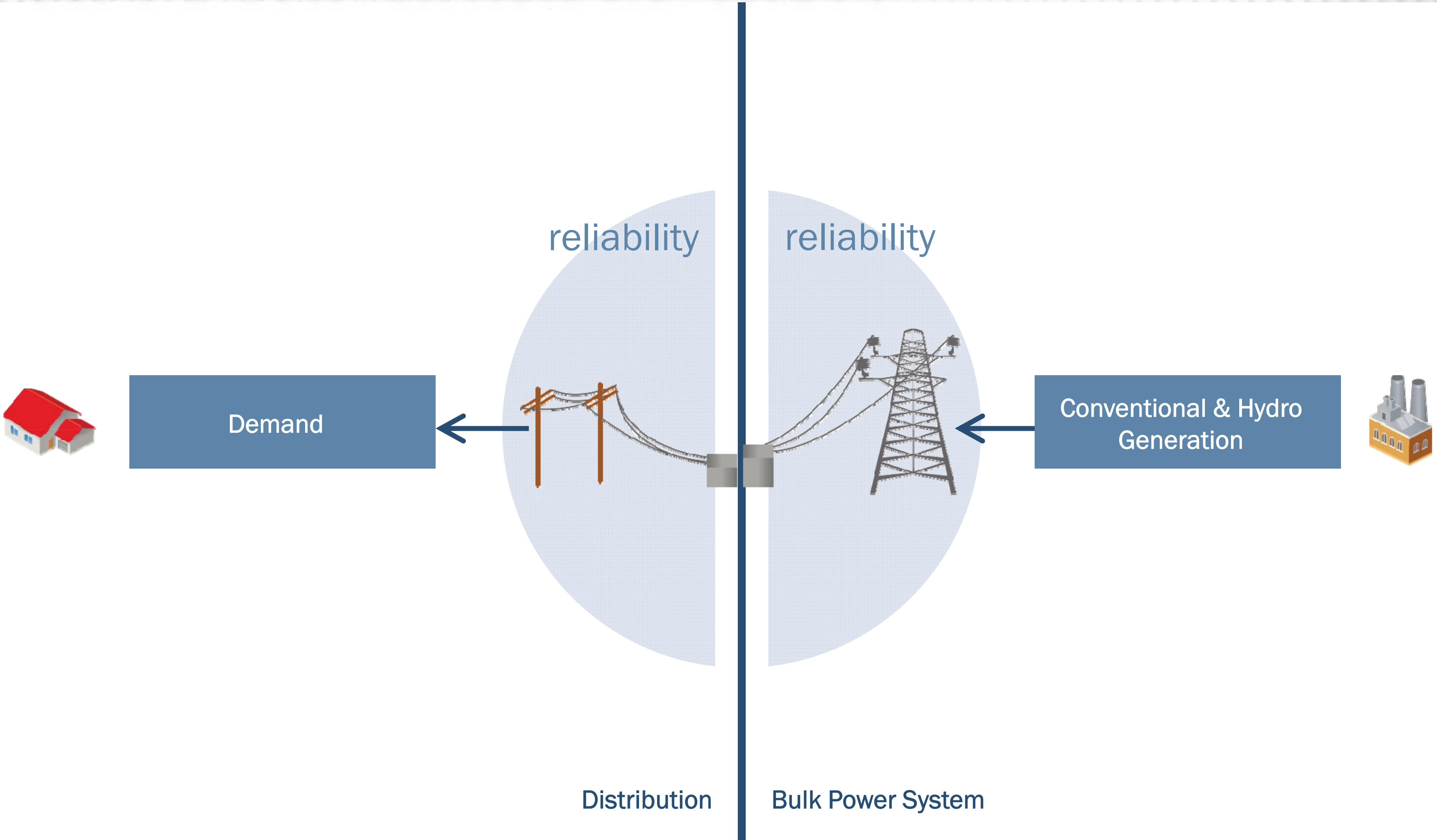
Capacity:
Instantaneous measure of electricity available at peak

System is designed to remain reliable during times of peak demand.

Energy:
Electricity Produced over Time

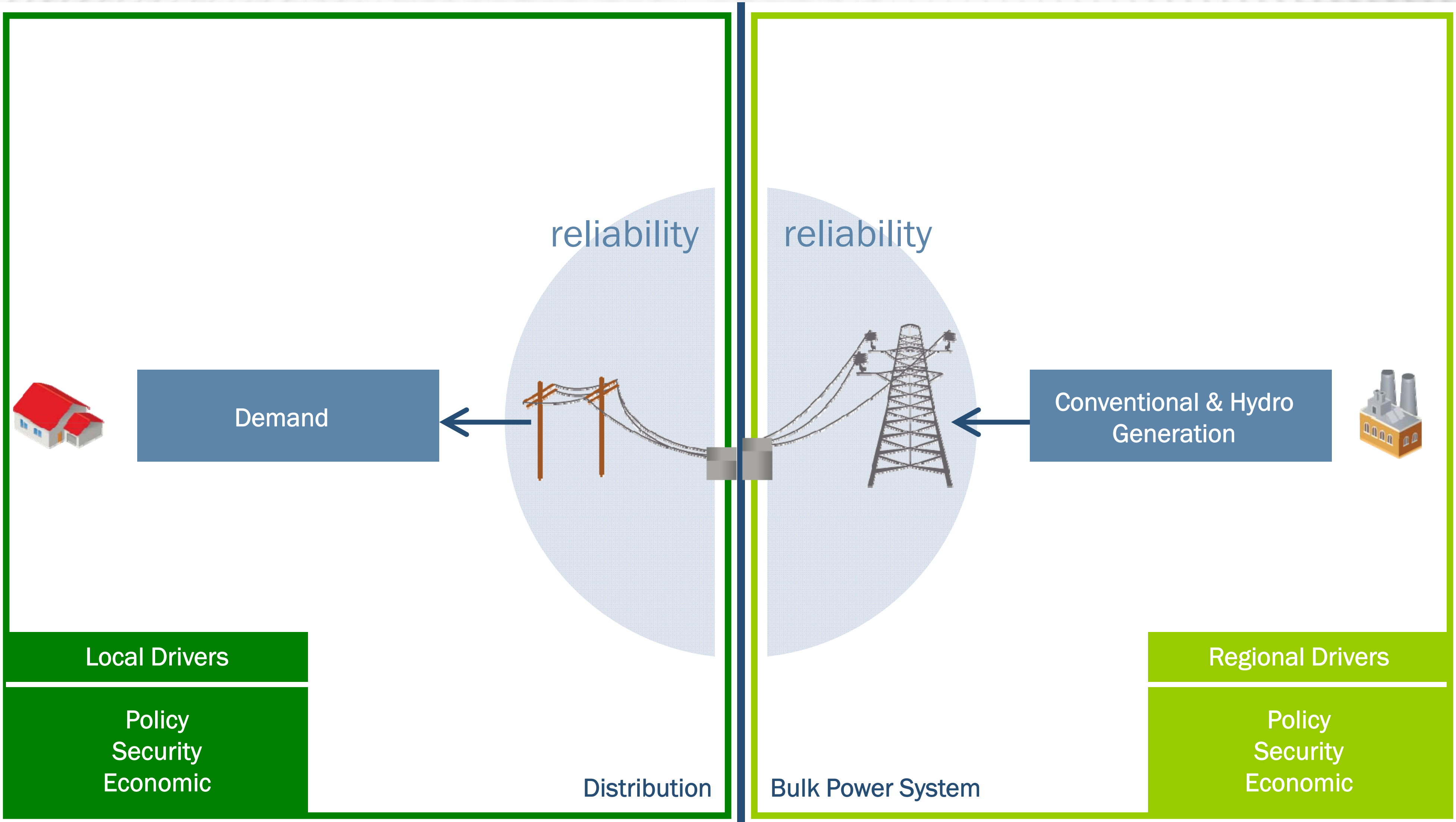
THE GROWTH OF THE SMART GRID

MEET THE CHINESE WALL



Over the past 60 years, we've divided the "grid" into two separate systems. Reliability requirements are different for each system.

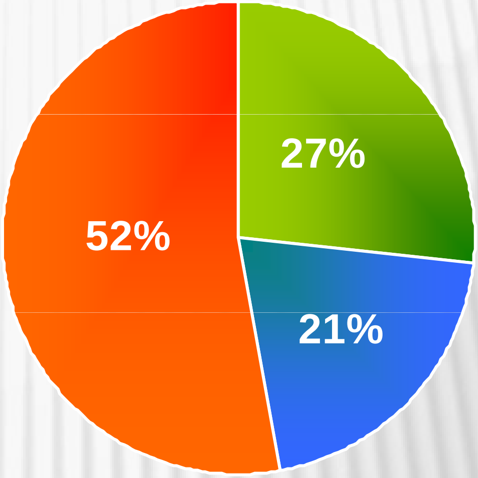
MEET THE CHINESE WALL



Policy and other drivers of development developed along the same line – factors that affected one system did not necessarily affect the other.

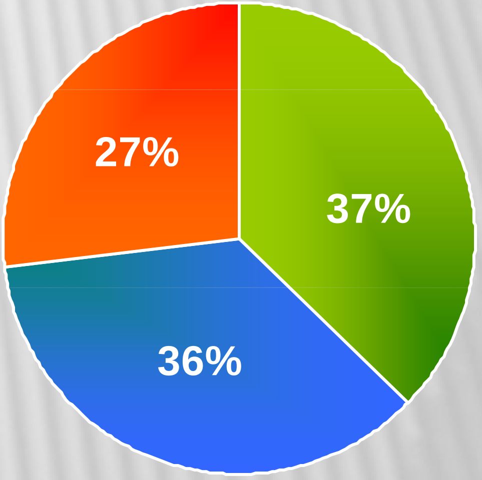
A CHANGING WORLD

- Home energy use: appliances, air conditioning, entertainment
  - Peak residential demand in Florida doubled in 5 years in the 1970's
  - Residential electricity use surpassed Industrial use in 1994
- Sporadic Industrial growth
  - Industrial use grew 16% in 1949
  - Use declined in 10 of the 50 years between 1957 and 2007



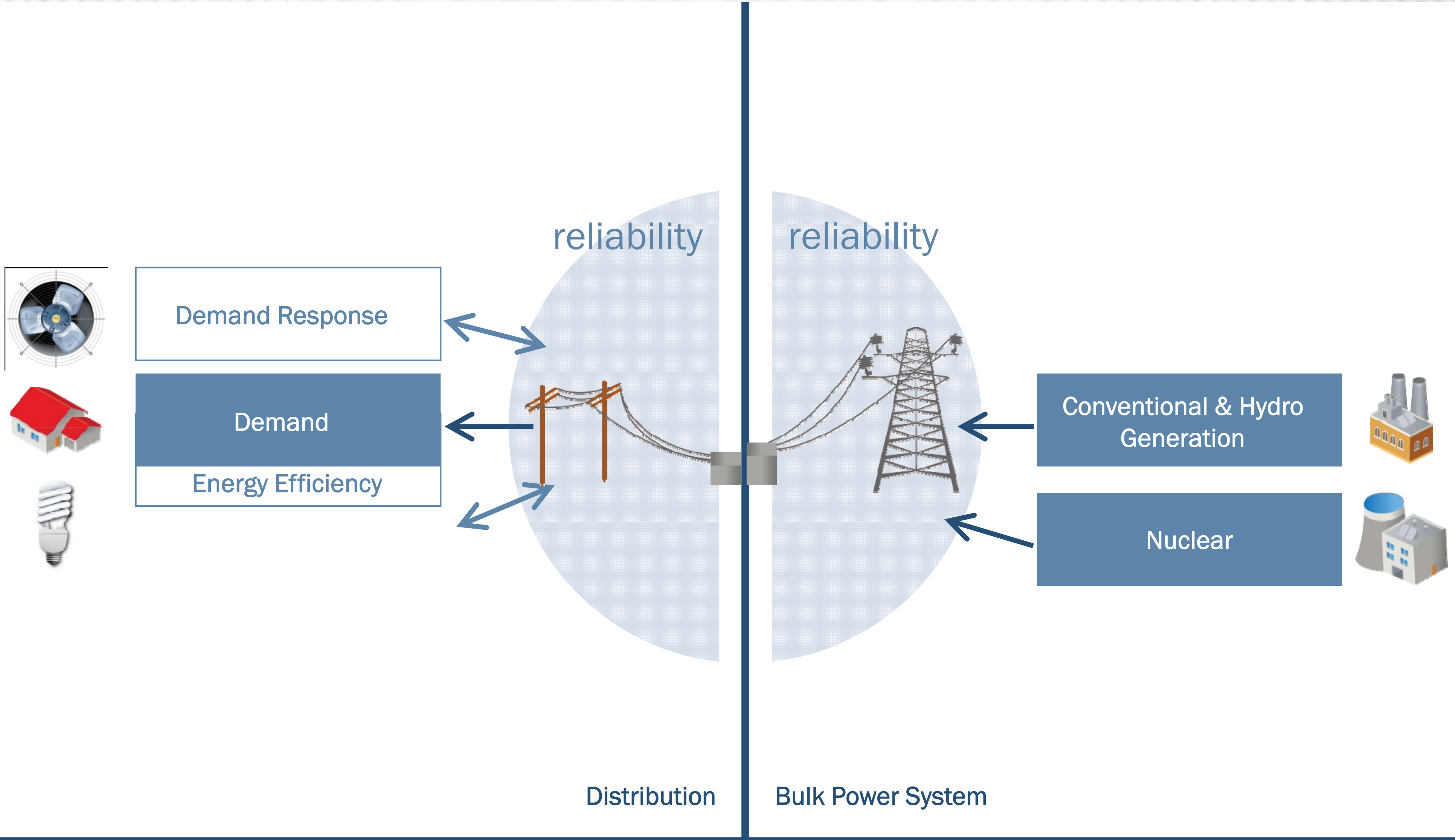
Energy Use by Sector 1956
Total Use:
540 million MWH

Energy Use by Sector 2007
Total Use:
3.8 billion MWH



🟧 Industrial
🟦 Commercial
🟩 Residential

ENTER: THE SMART GRID AS A YOUTH



As new resources were added in the 1970's and 80's, bulk system reliability became more dependent on distribution-level assets like demand response and energy efficiency. This began to blur the line between the bulk power system and the distribution system.

SMART GRID: THE FORMATIVE YEARS

- As communications and computing technology advances, a transformation begins to build within the utility sector
  - Automatic Meter Reading
  - Distribution Automation
  - Distributed Generation
  - Demand Response
  - SCADA, Control Systems, & Sensing

AUTOMATIC METER READING

- Deployed earliest on major industrial and commercial locations
- More detailed, hourly, and time-of-use billing
- Fewer meter readers
- Various configurations
  - “Drive-by” meter reading
  - Power Line Carrier
  - “Mesh” networks
  - Cellular
  - Broadband over Power Line

DISTRIBUTION & TRANSMISSION SYSTEM AUTOMATION

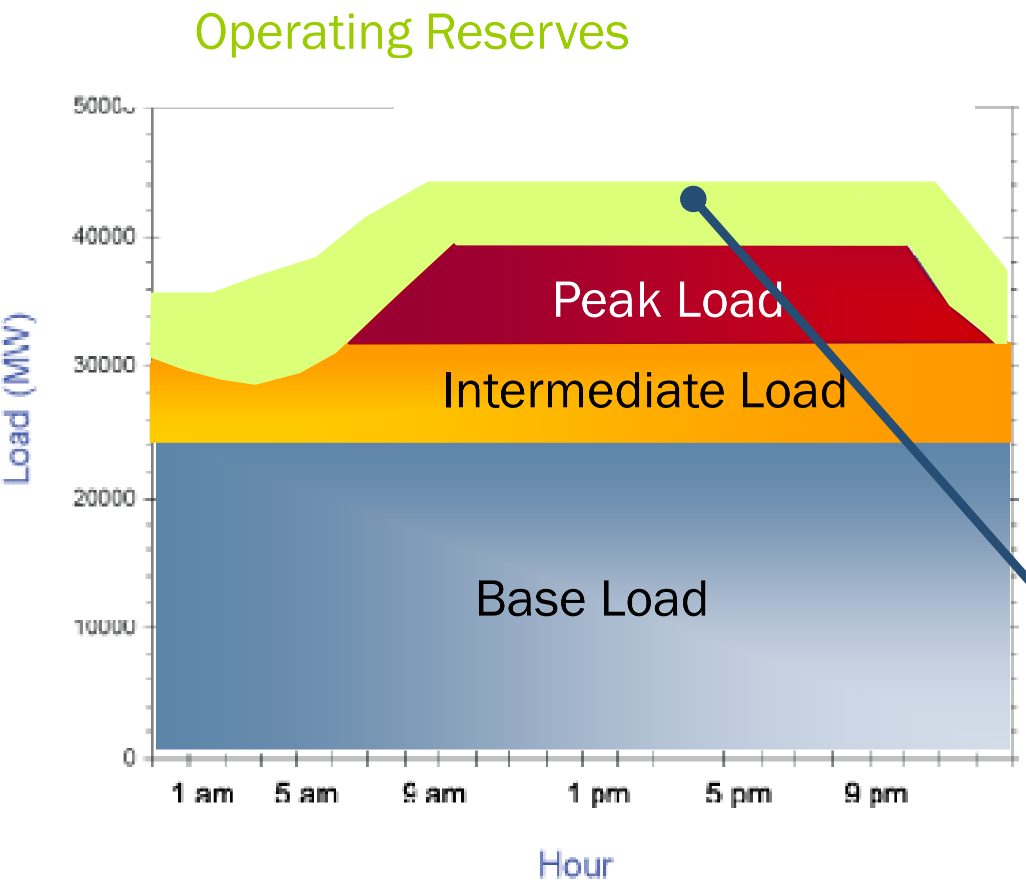
- Allows operators greater control and management of the distribution system
- Easier maintenance & storm restoration
- Greater safety
- “Self-healing” “micro-grids”

DISTRIBUTED GENERATION

- Small generating units serving load locally
- Backup generators
- Avoids line losses
- Requires remote control and operation

DEMAND RESPONSE: A PRIMER

Typical Daily Demand Curve



Demand Response is designed to “shave” peak demand and manage the overall load profile.

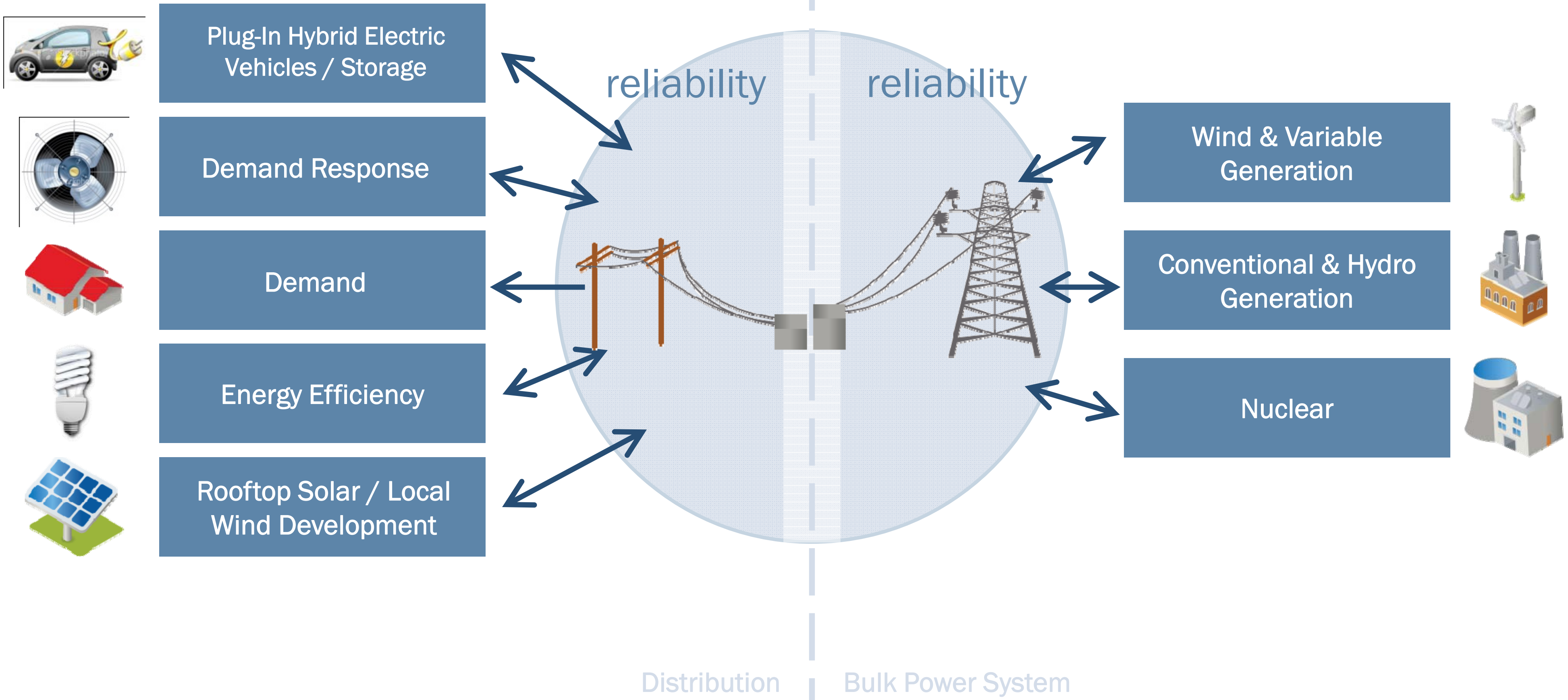
DEMAND RESPONSE: A PRIMER

- Communicating devices that control major appliances (e.g. home air conditioning systems) and major industrial systems
- Provide participating customers a reduced rate or discount for allowing the utility to curtail usage during peak times
- Critical Peak Pricing and Time of Use rates provide alternate options

SCADA, CONTROL SYSTEMS, & SENSING

- Sophistication of computer based control systems increases exponentially
- Enables operating efficiencies: allows system operators to do more with less
- Critical to market development and maturation

THE SMART GRID GROWS UP


Plug-In Hybrid Electric Vehicles / Storage
Demand Response
Demand
Energy Efficiency
Rooftop Solar / Local Wind Development
reliability
reliability
Wind & Variable Generation
Conventional & Hydro Generation
Nuclear
Distribution
Bulk Power System

The development and successful integration of these resources will require the industry to break down traditional boundaries and take a holistic view of the system with reliability at its core.

GRID, PHD

- An end-to-end system: generator to consumption
- Two-way flow of energy and information across multiple interfaces
- Smart appliances to synchro-phasors to vehicles

2010 All Electric Chevrolet Volt

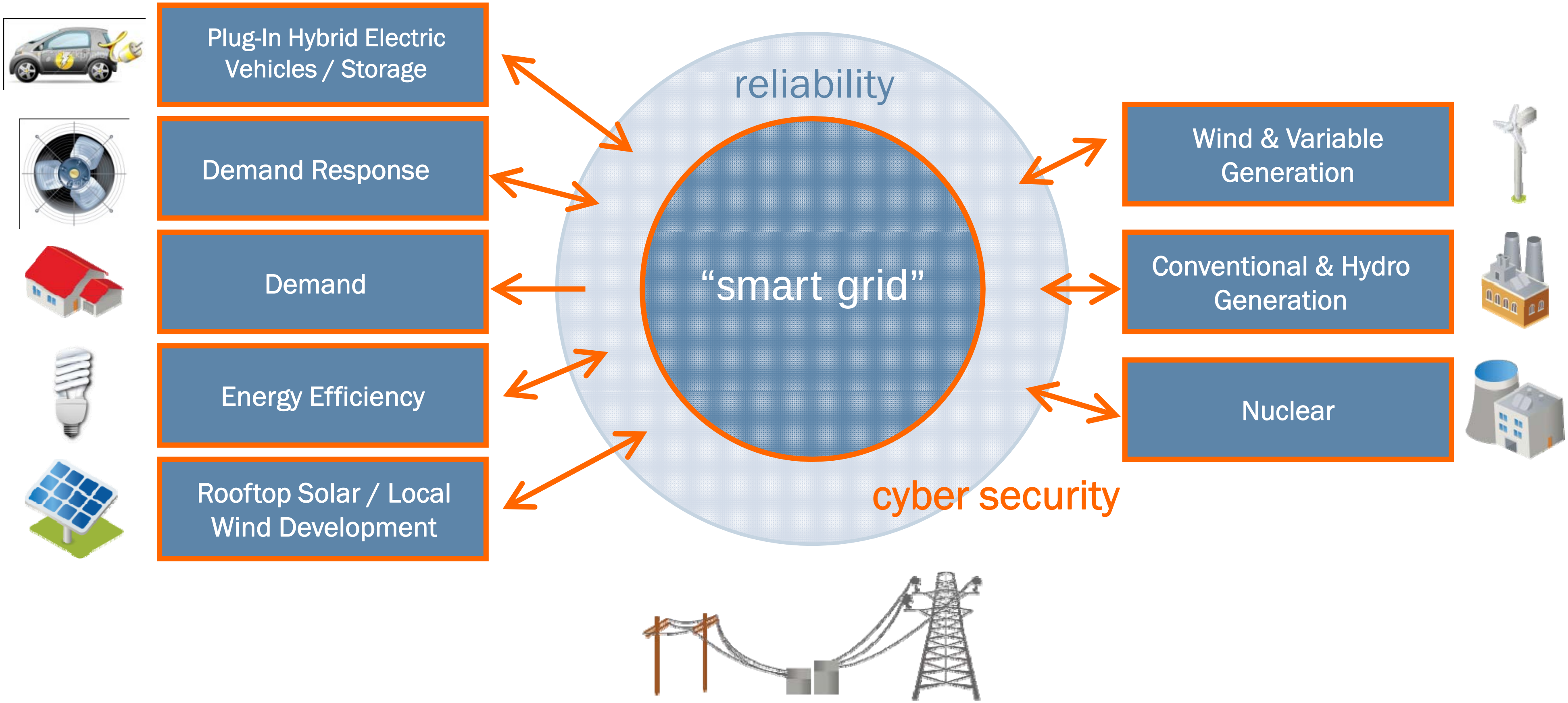
Courtesy of General Motors

GRID, PHD: THE VITALS

- 85% of Relays now Digital
- 33 Million Smart Meters Installed by 2011
- 250 Million to be Installed by 2015
- 4% of Demand Met by Demand Response Resources

CYBER INSECURITY

CYBER INSECURITY: SMART GRID'S MID-LIFE CRISIS?


Plug-In Hybrid Electric Vehicles / Storage
Demand Response
Demand
Energy Efficiency
Rooftop Solar / Local Wind Development
reliability
"smart grid"
cyber security
Wind & Variable Generation
Conventional & Hydro Generation
Nuclear

Cyber security is one of the most important concerns for the 21st century grid and must be central to policy and strategy. The potential for an attacker to access the system extends from meter to generator.

NEW REALITIES

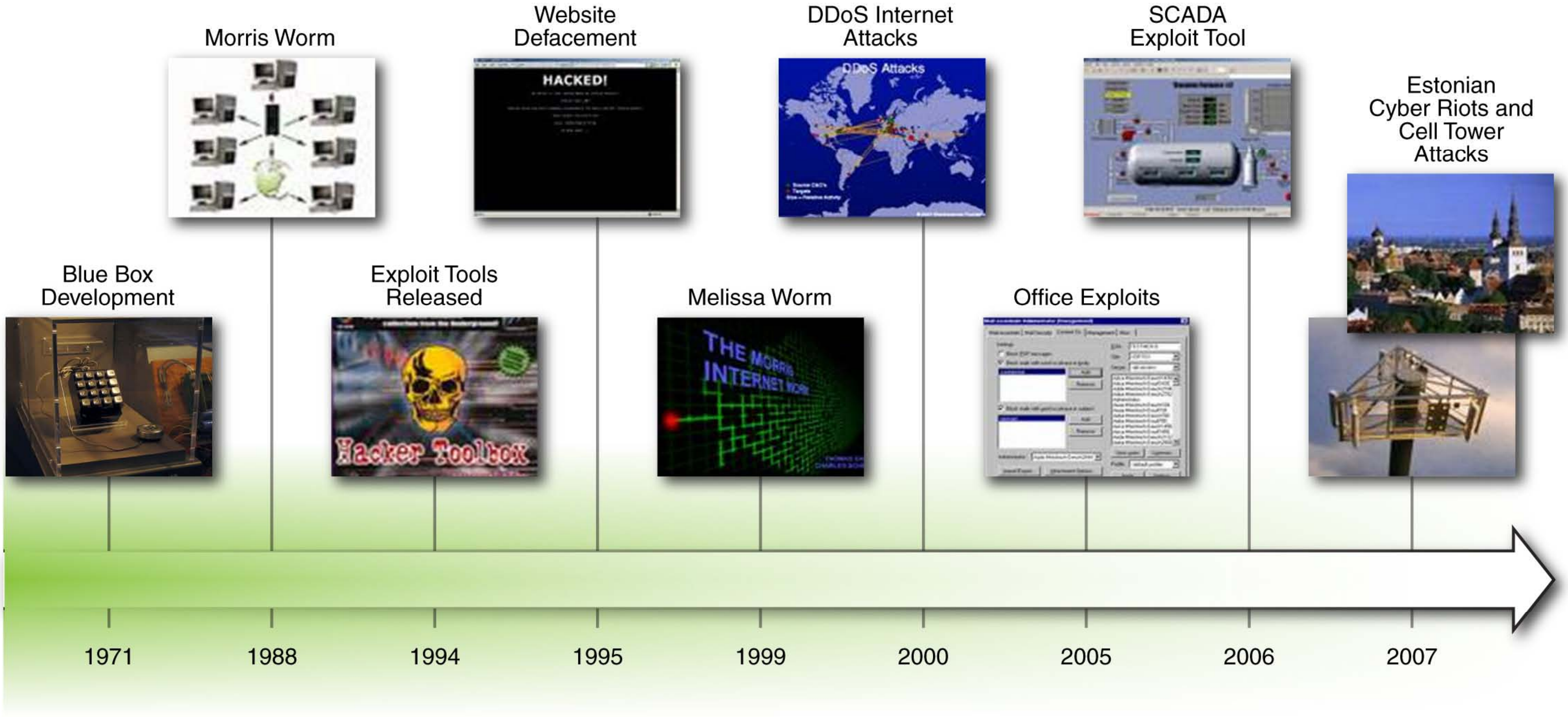
1900 - 2001

- Few homeland threats
- Perceived security
- Limited digital technology change
- Ample human and material resources

2001 - Present

- Threats increasing
- Recognized national security issue
- Aging infrastructure undergoing technology revolution
- Limited new investment

CYBER SECURITY: THE PACE OF CHANGE



Morris Worm

Website Defacement

DDoS Internet Attacks

SCADA Exploit Tool

Estonian Cyber Riots and Cell Tower Attacks

Blue Box Development

Exploit Tools Released

Melissa Worm

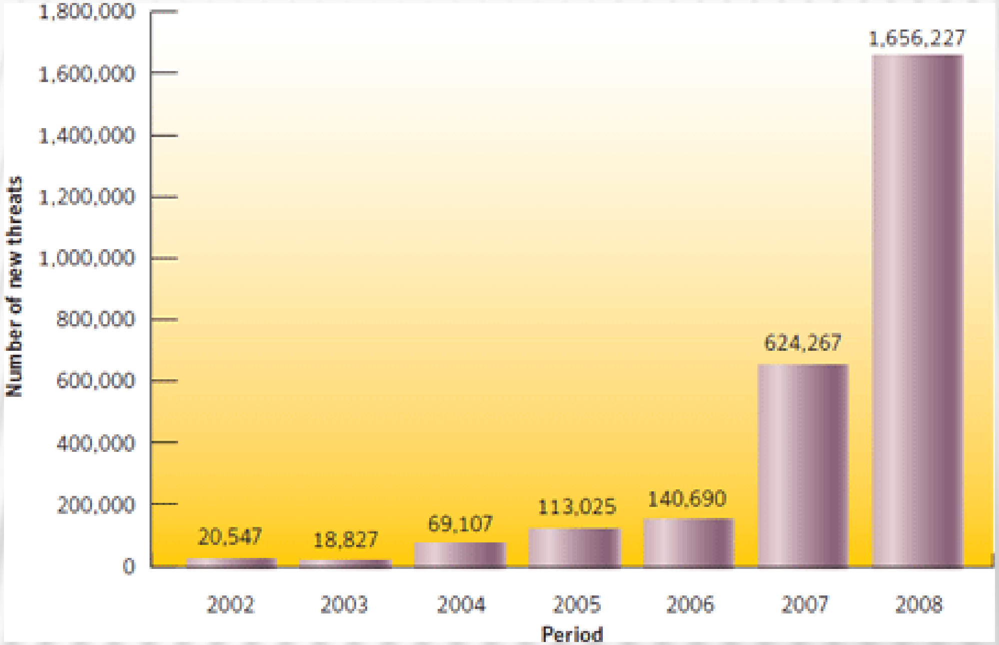
Office Exploits

1971 1988 1994 1995 1999 2000 2005 2006 2007

"It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

President Obama, May 2009

A GROWING THREAT



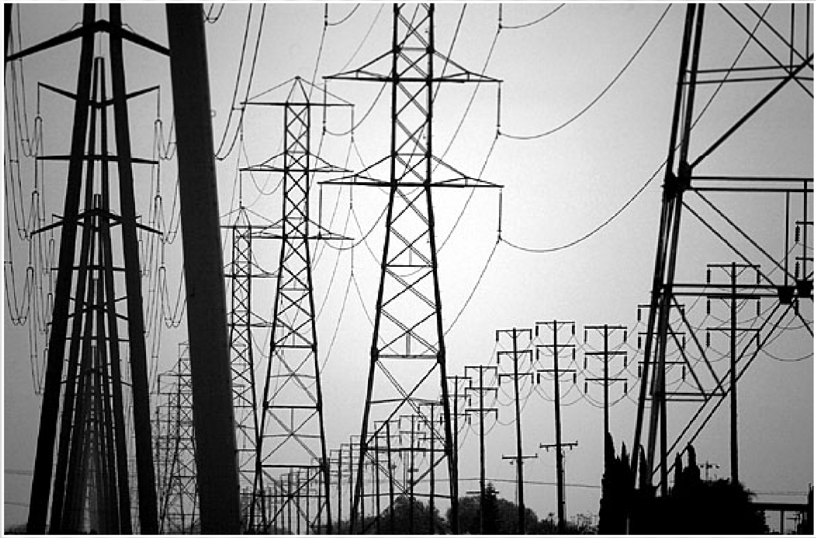
New malicious code signatures

Source: Symantec Corporation

THE SOFT UNDERBELLY

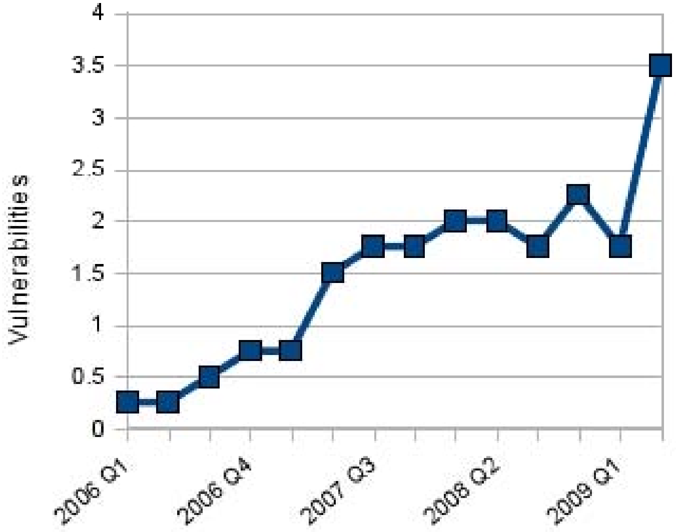
Cyber Security has presented a new set of threats to the bulk power system that are fundamentally different from other concerns system operators deal with on a daily basis.

- Security is not a typical system design requirement
- Minimal security at substations and along transmission lines
- Wide range of security programs
- Utilities seldom train against directed & structured threats
- Current system restoration plans do not assume total loss of critical items

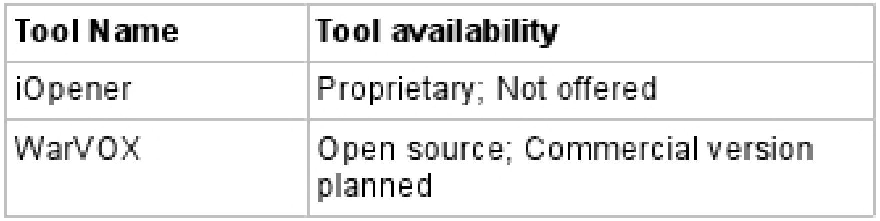


VULNERABILITIES: A SNAPSHOT

ICS-Specific Vulnerabilities

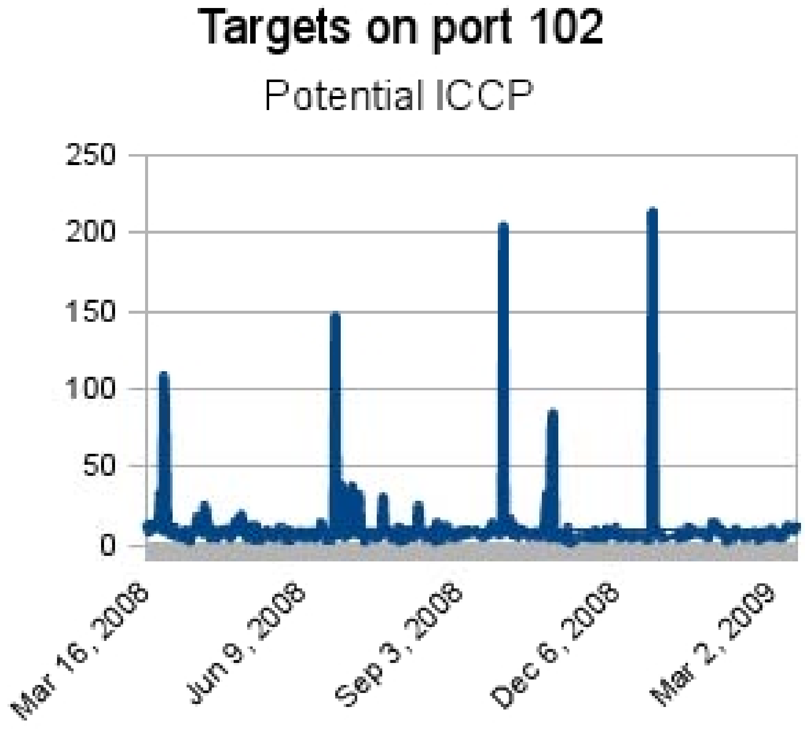


ICS-Attack Tools

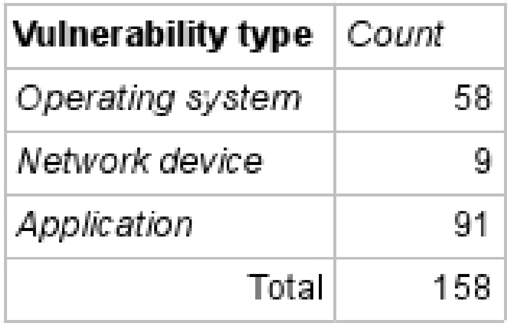


Tool Name	Tool availability
iOpener	Proprietary; Not offered
WarVOX	Open source; Commercial version planned

Electric ICS Port Probes



Vulnerabilities that can affect ICS

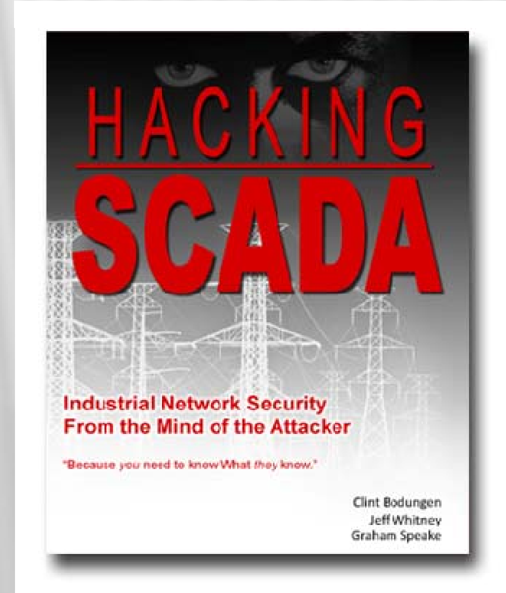


Vulnerability type	*Count*
Operating system	58
Network device	9
Application	91
Total	158

Source: Critical Intelligence – info@critical-intelligence.com

PUBLIC DISCLOSURES

- CIA discloses they have information of cyber attacks against power system controls outside the US.
  - Resulted in multi-city outage
  - Extortion as the prime motivation
- US Power companies have been penetrated
  - Media reports & government officials
- Connectivity to substations & digital hardware exist
  - Market Surveys (modems, SCADA, Internet, wireless, etc…)
  - Restoration time is critical, Availability is priority
- Websites, presentations and books devoted to hacking our systems
- CNN Aurora disclosure & video
- April 2009 Wall Street Journal Article: “Spies in the Wires” and Advanced Persistent Threats


HACKING SCADA
Industrial Network Security
From the Mind of the Attacker
"Because you need to know What they know."
Clint Bodungen
Jeff Whitney
Graham Speake

PUBLIC DISCLOSURES

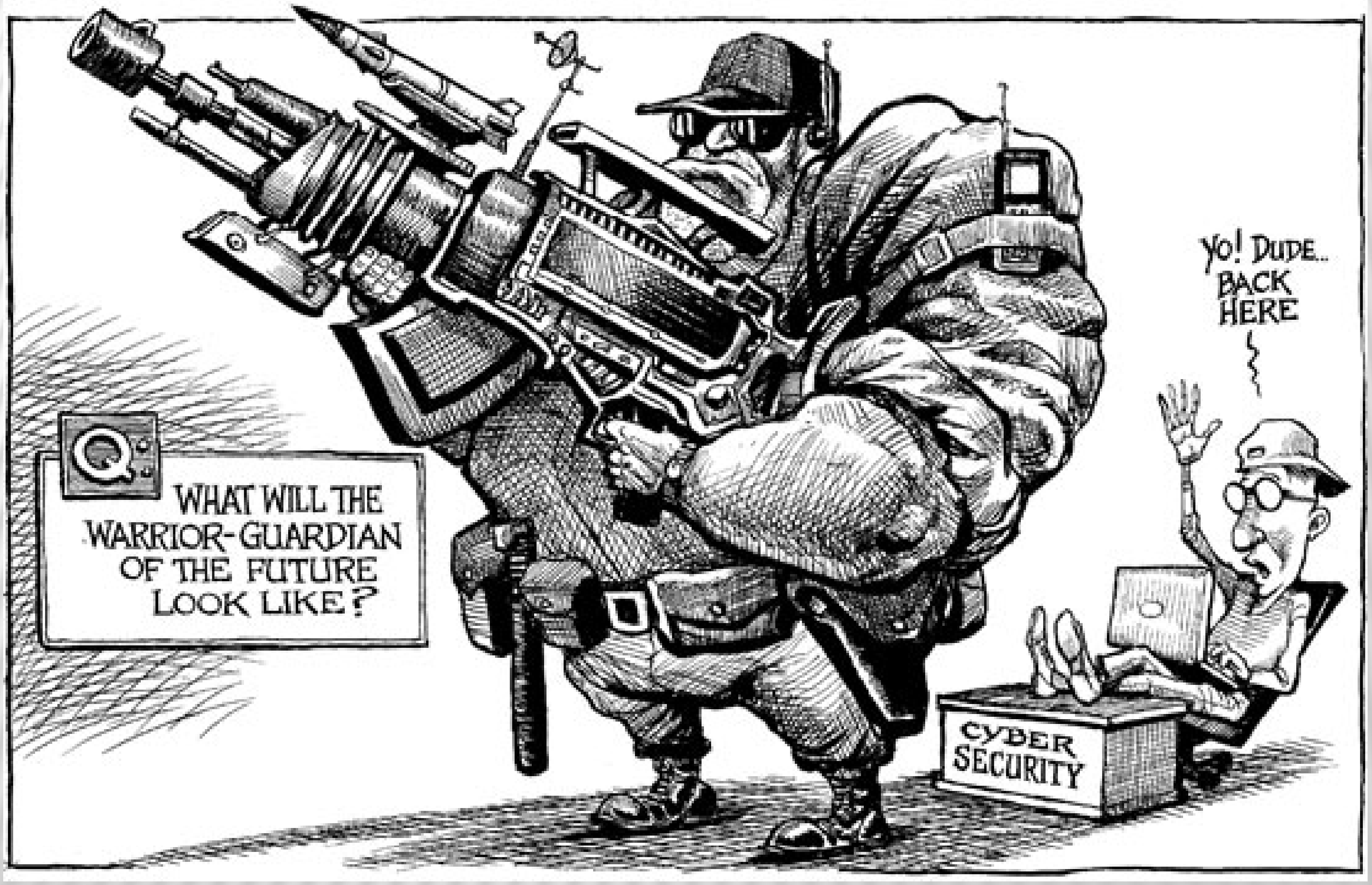
- “Cyber spies have penetrated the U.S. electrical grid and left behind software systems that could be used to disrupt the system.” Current and former national security officials
- “The Russians and Chinese have attempted to map our infrastructure.” Senior intelligence official
- U.S. Intelligence agencies detected the “intrusions,” not the companies in charge of the infrastructure. Officials
- “There are intrusions and they are growing.” “There were a lot last year.” Former DHS official
- “Utilities are reluctant to speak about the dangers.’’ PJM

AURORA: THE SIGNIFICANCE

THE GREATEST THREAT

- The potential for an intelligent cyber attacker to exploit a common vulnerability that impacts many assets at once, and from a distance
  - Common or single point of failure
  - Universal points for commands/action
  - Data & network concentrations
    - Convergence of safety and control
  - Inherent trust in the system and between components
  - Growing system complexity
    - Develop flexible models and architectures
    - Reverse the convergence of safety/protection and control systems
  - Remove silos and integrate cybersecurity into operations
    - Training operators to observe and consider

GRID'S NEW SECURITY DETAIL



Cartoon credit: The Economist 2009

THE ROAD AHEAD

ADDRESSING CYBER INSECURITY

- Requires a different approach, that must include:
  - Constant vigilance
  - Urgent action (as technologies change, threats arise, and vulnerabilities are identified)
    - information must be distributed to the individuals who need it most as quickly and securely as possible
  - Layered defense (CIP Standards, Active risk identification & management, Communications)
  - Involved risk decision making model
    - Identify, measure, and manage risk, scope and pinpoint specific issues, and determine the timeframe in which they must be addressed.

COMPETING PRIORITIES

- The most efficient system operates exactly at its operating limits with no redundancy
  - Every component is critical
  - Every component utilized to its maximum
  - Very economical as long as nothing breaks
- A resilient system has sufficient redundancies in the right places to withstand losses of any component
  - No one component is critical
  - Components far from their operating limits
  - Very robust but expensive to build and operate

THE QUESTIONS

- How to manage risk?
  - Risk management in the business world is highly dependent on the ability to assign a probability to a given outcome
  - How would one calculate the probability of a cyber attack?
- Who benefits?
  - If asset owners determine they have appropriately managed risk, they may not see the benefit in creating more protection
- Who pays?
  - Unfunded mandates can result in significant impacts to individual businesses, industries, and society (i.e. higher electricity prices)
  - Funded mandates require public trade-offs

A HOLISTIC APPROACH

Leadership & Culture

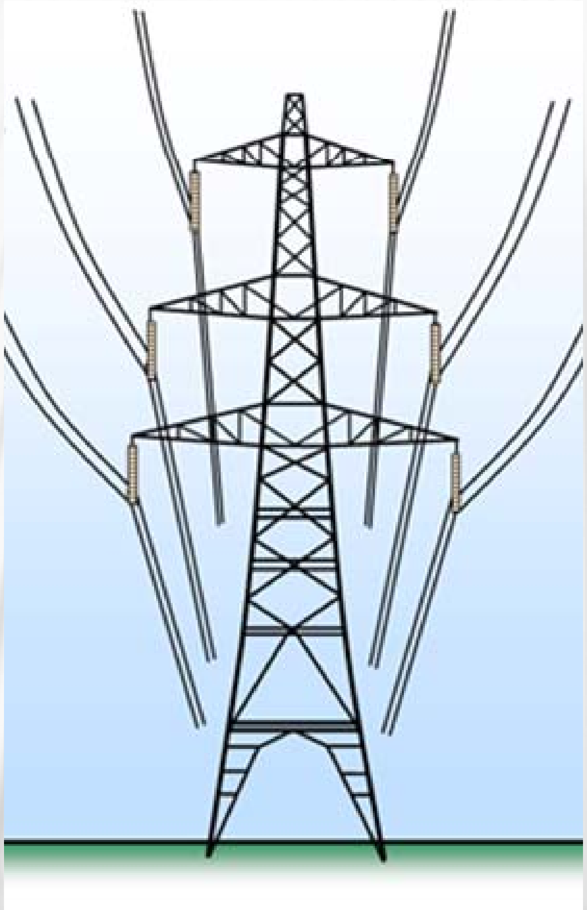
Skilled people

Bi-directional communications

Dynamic & resourced security operations

Awareness & Coordination

Foundational standards



System Resilience & Capacity

WORKFORCE DEVELOPMENT

- Educate the workforce on the importance of cyber security
- Ensure broad adoption of cyber security best practices in daily activities
- Develop certification programs for Industrial Control Systems & SCADA Personnel

NBISE
NATIONAL BOARD OF INFORMATION
SECURITY EXAMINERS

TECHNOLOGY DEVELOPMENT

- Improve security of existing assets
  - Better security management
  - Built in – not bolt on – protection
- Develop forensics tools
- Develop system operating tools and techniques to allow for graceful degradation of functionality
  - Develop capability to allow systems to shed non-critical applications

STANDARDS & BEST PRACTICES

- Standards for operations, equipment, and planning should take cyber security into account
- Must begin to look at the system differently, take into account the potential for an attacker to successfully disable, destroy, or misuse multiple assets at once
- NERC, NIST, etc…

NERC/FERC: CIP STANDARDS

- The critical infrastructure protection standards approved through Order No. 706 are a sound starting point for the electric industry to address cybersecurity.
- Designed as a foundation for sound practices
  - "Good housekeeping" requirements intended to help protect asset owners from unstructured cyber threats
- NERC's Reliability Standards development process enables the progressive and continuous improvement of Reliability Standards.
- Important milestone to help ensure grid reliability by improving the resiliency of control system cyber assets and enhancing their ability to withstand cyber-based attacks

LIMITATIONS

- The CIP Reliability Standards alone cannot eliminate the threat of a cyber disruption of critical national infrastructure
    - NERC has jurisdiction only to propose reliability standards for the bulk power system
        - CIP Reliability Standards cannot address other critical assets – such as telecommunications systems, for example, or electricity distribution systems
    - The open process by which Reliability Standards are developed, while demonstrably successful in producing standards that have significantly enhanced the reliability of the grid, may not be ideally suited to sensitive subject matter where confidentiality is required
    - Standards take time to modify (foundational but static)
        - Specific cyber security risk can be very dynamic
        - Compliance can’t be at the expense of developing necessary and more flexible security management approaches

NEXT STEPS

- Must improve public-private sector cooperation, information sharing
- Must ensure executive support and a positive culture of security and compliance is instituted
- Must take a holistic approach including utilities, asset owners, policy makers, and equipment manufacturers

- Must fully recognize the gravity of this concern

Question & Answer

Contact:

Kelly Ziegler
Chief Operating Officer
National Board of Information Security Examiners
Kelly.ziegler@nbise.org
973.766.3276

"It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation." **President Obama, May 2009**