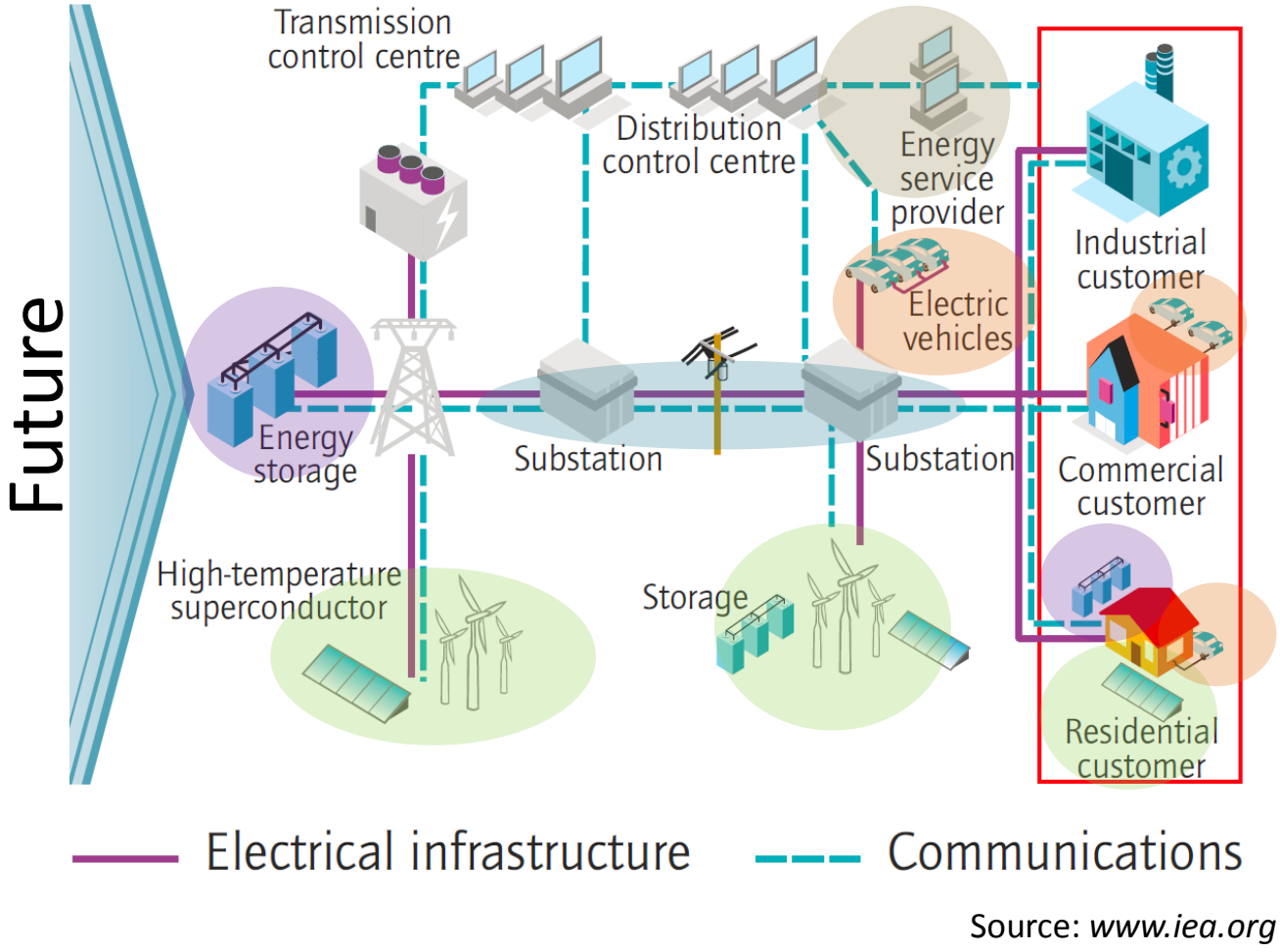
Setting up the Scene: Electrical Smart Grids Security and Dependability

Nuno Neves
nuno@di.fc.ul.pt
Univ. of Lisboa, Faculty of Sciences, LASIGE

Smart Electrical Grid



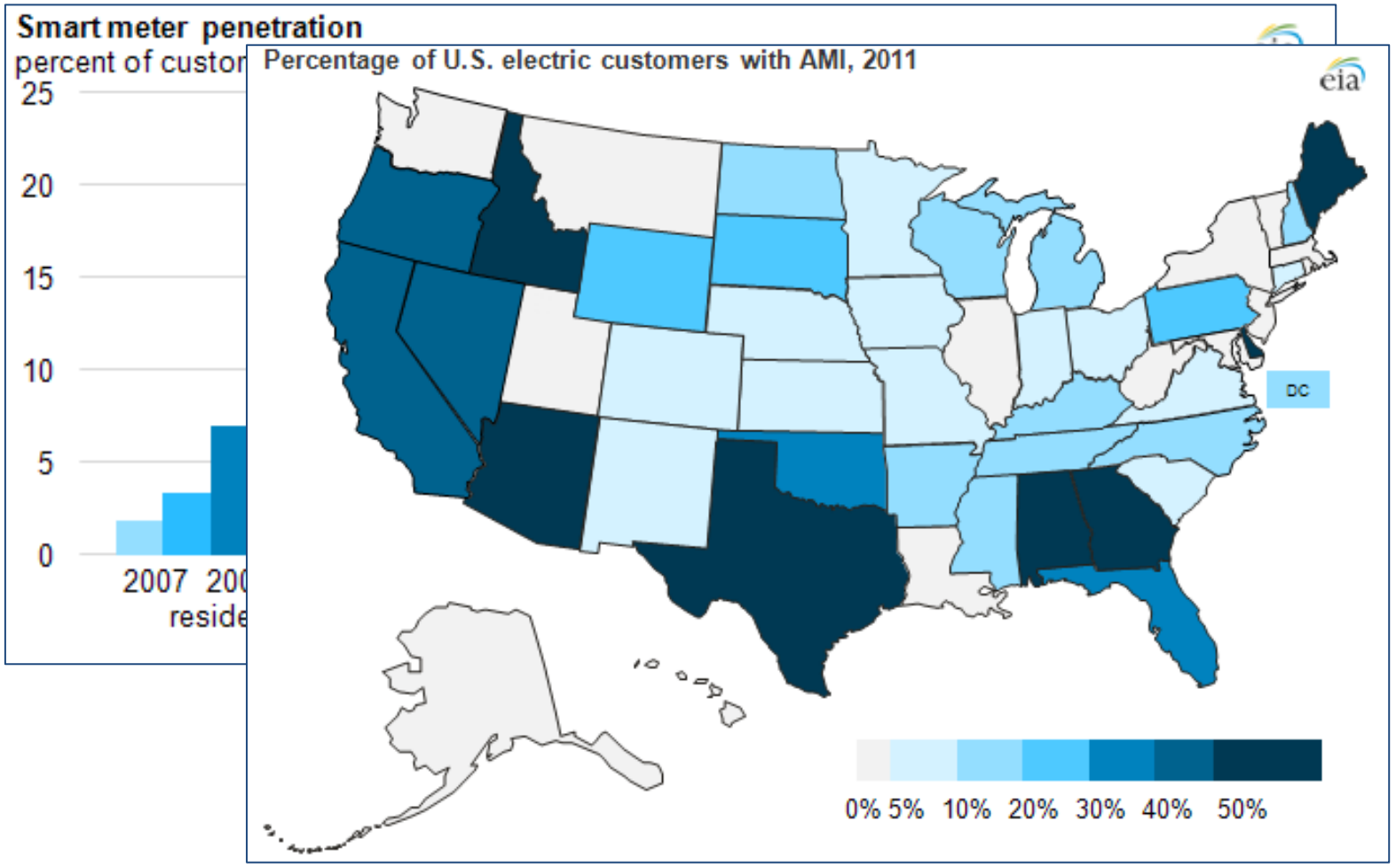
- Flexible & distributed generation
- Storage capability
- Electric mobility
- Sophisticated comms infrastructure
- Markets & regulation

Source: *www.iea.org*

Some Benefits

- Enables informed participation by customers
  - detailed information is given on electricity use, permitting decisions to be made on how to spend energy, which can be influenced by new forms of energy pricing and other incentives
- Optimizes asset utilization and operating efficiency
  - better load modeling and real-time monitoring ensures effective and efficient power generation (demand response management); condition-based maintenance
- Supports diverse generation and storage options
  - integration of renewable energy production and storage; accommodate multiple decentralized energy sources, reducing transmission losses
- Enables new products, services and markets
  - opportunities for differentiated offering (e.g, power quality) and dynamic pricing schemes
- Resilience to disturbances (e.g., natural disasters and attacks)
  - real-time monitoring allows for self-healing actions, e.g., by isolating problematic areas

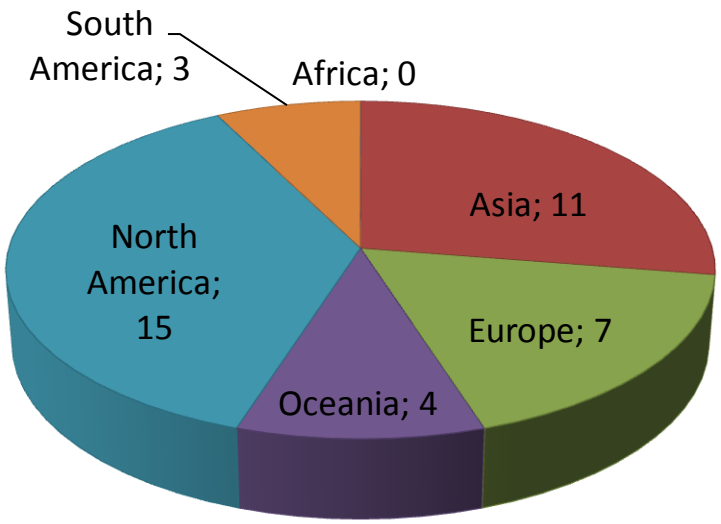
Deployment of Smart Grid



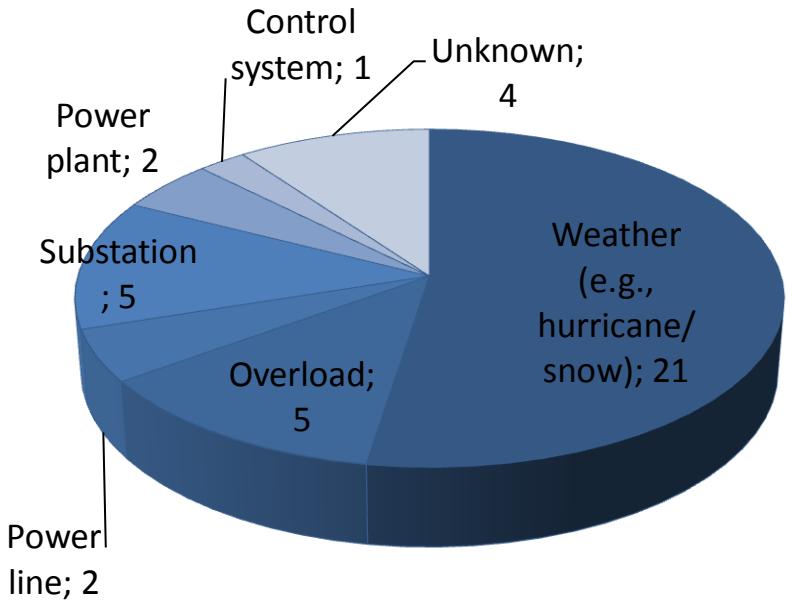
Source: *U.S. Energy Information Administration*

High Impact Blackouts (2010-14)

Number of blackouts



Geographic Distribution



Failure Cause

<u>High impact blackouts</u>: 1) at least 1,000,000 person-hours of disruption;
2) at least 1000 people affected for more than 1 hour;

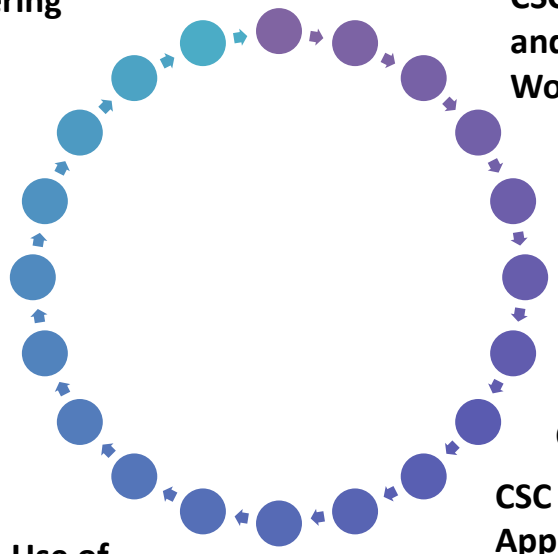
Security Standards and Best Practices

- International Electrotechnical Commission (IEC)
  - IEC 62443: Technical Specification - Industrial Communication Networks - Network and System Security
  - IEC 62351: Power Systems Management and Associated Information Exchange – Data And Communications Security
- North American Electric Reliability Corporation (NERC)
  - CIP series of standards
- National Institute of Standards and Technology (NIST)
  - NISTIR 7628: Guidelines for Smart Grid Cyber Security
- International Organization for Standardization (ISO)
  - ISO/IEC 27002:2005: Information technology —Security techniques — Code of practice for information security management
  - ISO/IEC 27011:2008: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
  - ISO/IEC TR 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry
- European Network and Information Security Agency(ENISA)
  - Proposal for a List of Security Measures for Smart Grids

Example Security Best Practices

The Critical Security Controls for Effective Cyber Defense (Version 5.0)

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ



CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 2: Inventory of Authorized and Unauthorized Software

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Malware Defenses

CSC 6: Application Software Security

CSC 7: Wireless Access Control

CSC 8: Data Recovery Capability

CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps

CSC 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

CSC 11: Limitation and Control of Network Ports, Protocols, and Services

CSC 12: Controlled Use of Administrative Privileges

CSC 13: Boundary Defense

CSC 14: Maintenance, Monitoring, and Analysis of Audit Logs

CSC 15: Controlled Access Based on the Need to Know

CSC 16: Account Monitoring and Control

CSC 17: Data Protection

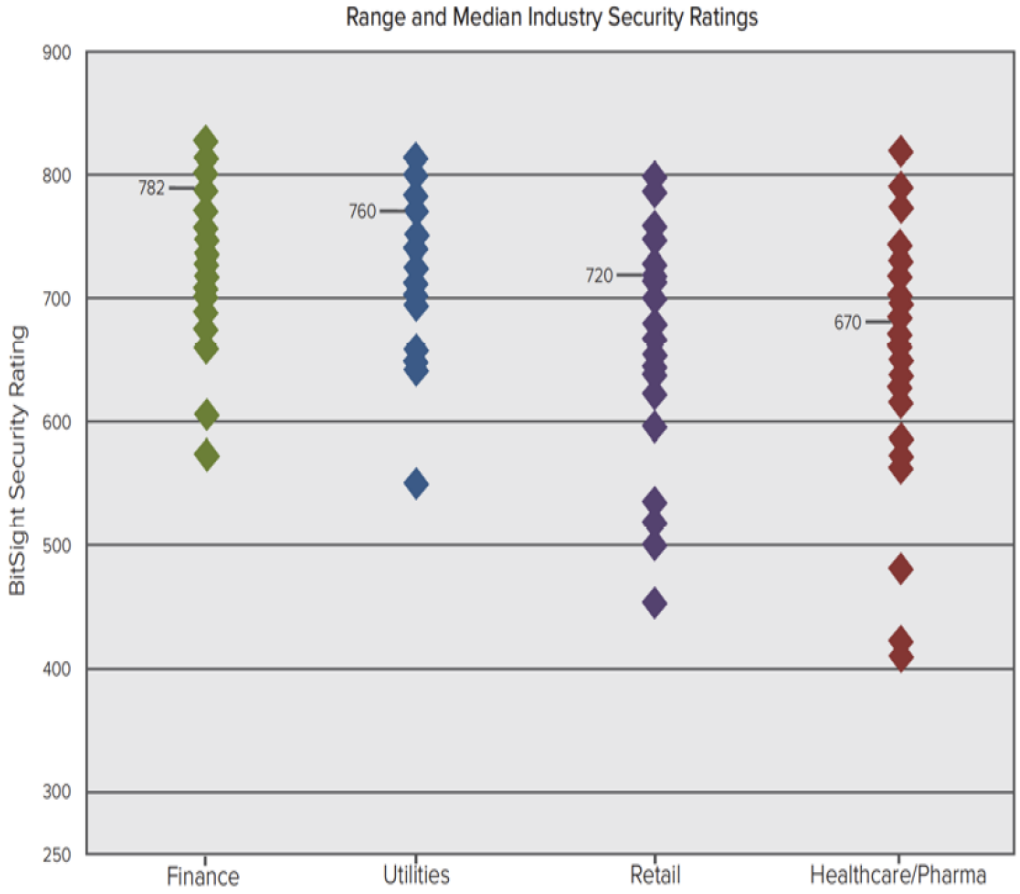
CSC 18: Incident Response and Management

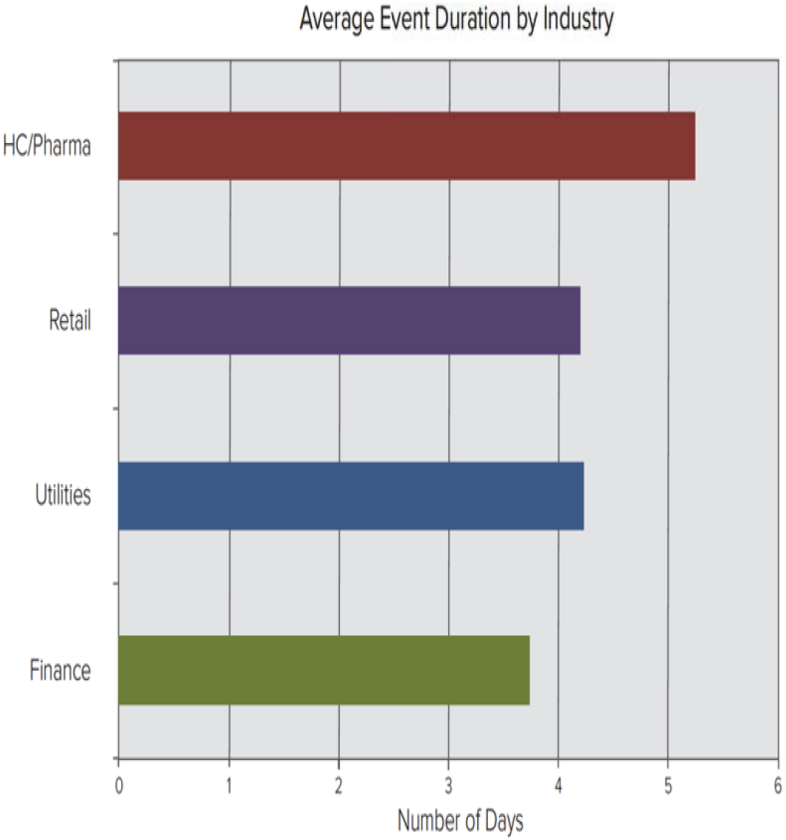
CSC 19: Secure Network Engineering

CSC 20: Penetration Tests and Red Team Exercises

Improvements are Visible!

Utilities rank well in security incidents than other sectors





<u>BitSight Insights Volume 4, May 2014</u> : Uses data observed externally to rate the security performance of companies in the Standard & Poor's 500; ***82% of the companies suffered a security*** *compromise between Apr 2013 – Mar 2014*

Targeted Attacks (or Advanced Persistent Threats) (1)

BitSight report is encouraging but only indicates that (large) electrical utilities have catch up with other sectors with regard to common threats, like worms, port scanning, botnets

- *Mandiant Report, Exposing One of China's Cyber Espionage Units, Feb 2013*
  - … single organization of operators that has conducted a **cyber espionage campaign** against a broad range of victims **since at least 2006**
  - … intrusions against **nearly 150 victims** over seven years
  - … APT1 is likely **government-sponsored**
  - … this group as "APT1" and it is **one of more than 20 APT groups** with origins in China

➢ *Bloomberg, June 2014: Chinese hackers targeted 23 natural gas pipeline companies over seven months beginning in December 2011, and breached at least 10, according to a U.S. DHS*
➢ *May 2014 : Eventually, five members of the group described in this report were indicted for economic espionage by the US*

Targeted Attacks (or Advanced Persistent Threats) (2)

- *CrowdStrike Intelligence Report, PUTTER PANDA, June 2014*

  … widespread espionage campaigns, Chinese threat actors are **targeting companies and governments in every part of the globe**

  … Unit 61486 is … is headquartered in Shanghai, China … tracking this particular unit since 2012, under the codename PUTTER PANDA, and has documented activity **dating back to 2007**

  … steal corporate trade secrets, primarily relating to the **satellite, aerospace and communication industries**

  … actively tracks and reports on **more than 70 espionage groups**, approximately **half of which operate out of China**

These security threats are particularly worrisome from the perspective that electrical utilities manage a **critical infrastructure** with not only a very strong economic, but also, a high societal impact

Security & Dependability Challenges

- Support for risk modeling and evaluation in power grid assets
  - to prioritize where to apply security controls
- Privacy concerns from society at large
  - detailed data collection by smart meters enables unprecedented eavesdropping (e.g., which movie are you watching tonight?)
- Architectures and protocols
  - taking into consideration the operational requirements (e.g., real time) and economic constraints of utility companies, but addressing a wide range of failures
- Vulnerability detection and mitigation on smart appliances
  - new techniques and solutions (e.g., SCADA protocols; Phasor Measurement Units**;** smart metering protocols; power line communication protocols)