



GovEnergy
www.govenergy.gov

The Premier Energy Training Workshop
and Trade Show for Federal Agencies

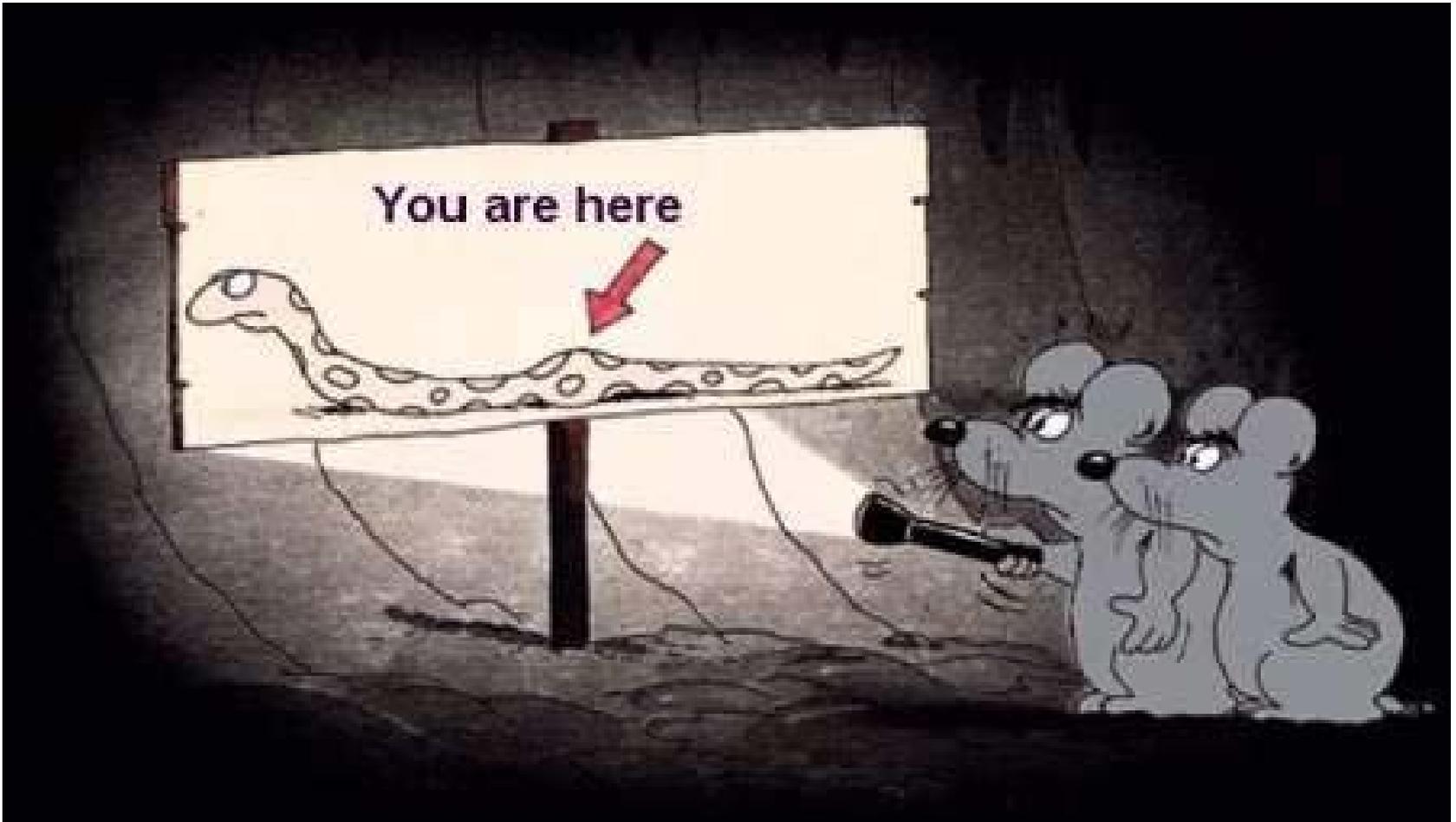


A River of Energy Solutions



Boeing's Information Solutions- Alan Greenberg

Welcome to the Wonderful World of Cyber



The Boeing Company

**Boeing
Defense, Space &
Security**



**Commercial
Airplanes**

***Boeing... More than an Aviation Company
Cyber Security is in Every System***

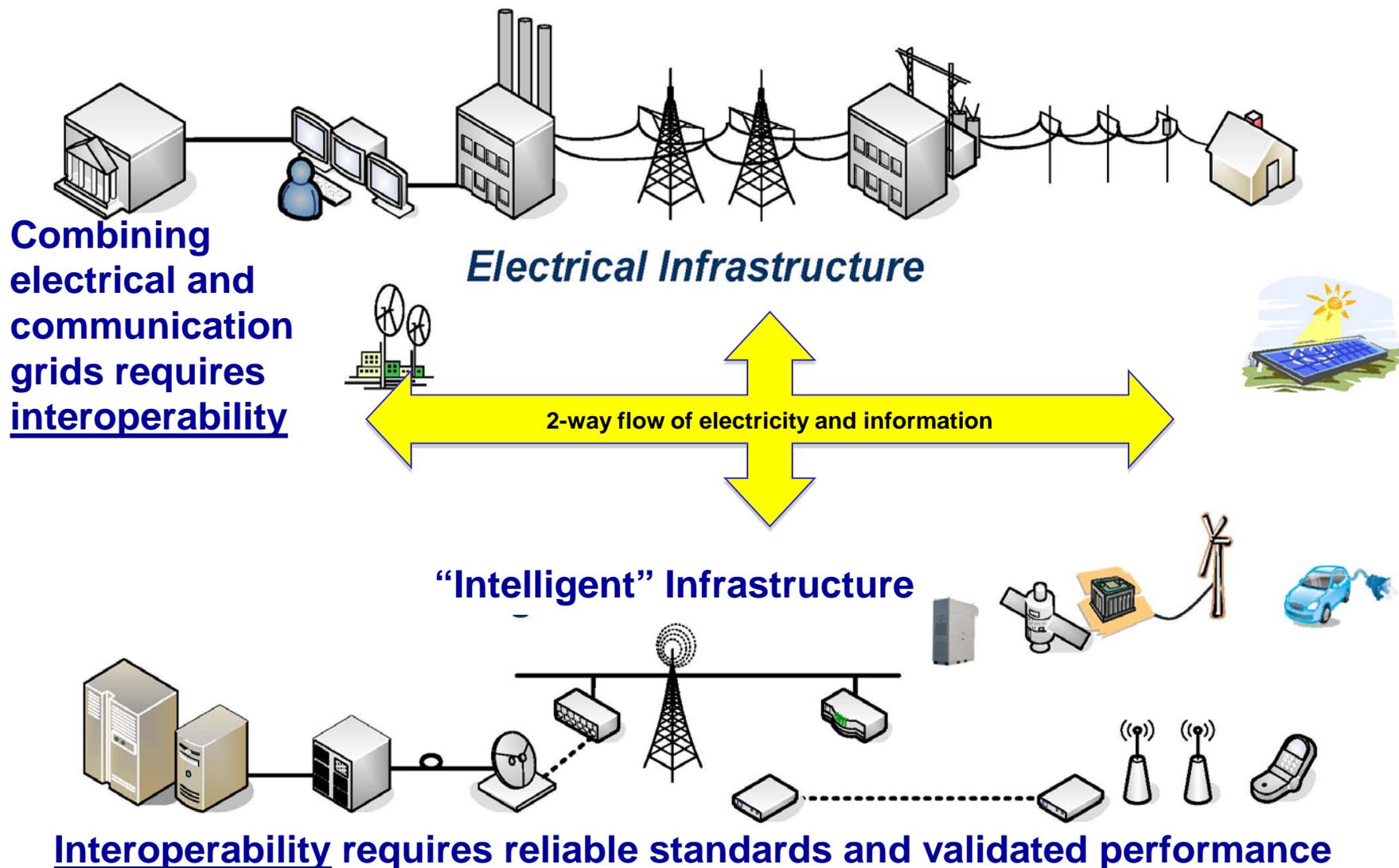
Boeing Lives the Global Cyber Challenge

- 240k user accounts, 2m extranet users/month on business portals & over 200k personal & 13,000 networks devices managed
- Moving over 76 PetaBytes per month (190Mb/month per employee)
- 580m transactions/day & over 500k viruses blocked/month
- Conducting Aggressive R&D to stay ahead of the threat
- Participating with the U.S. Government against cyber terrorism

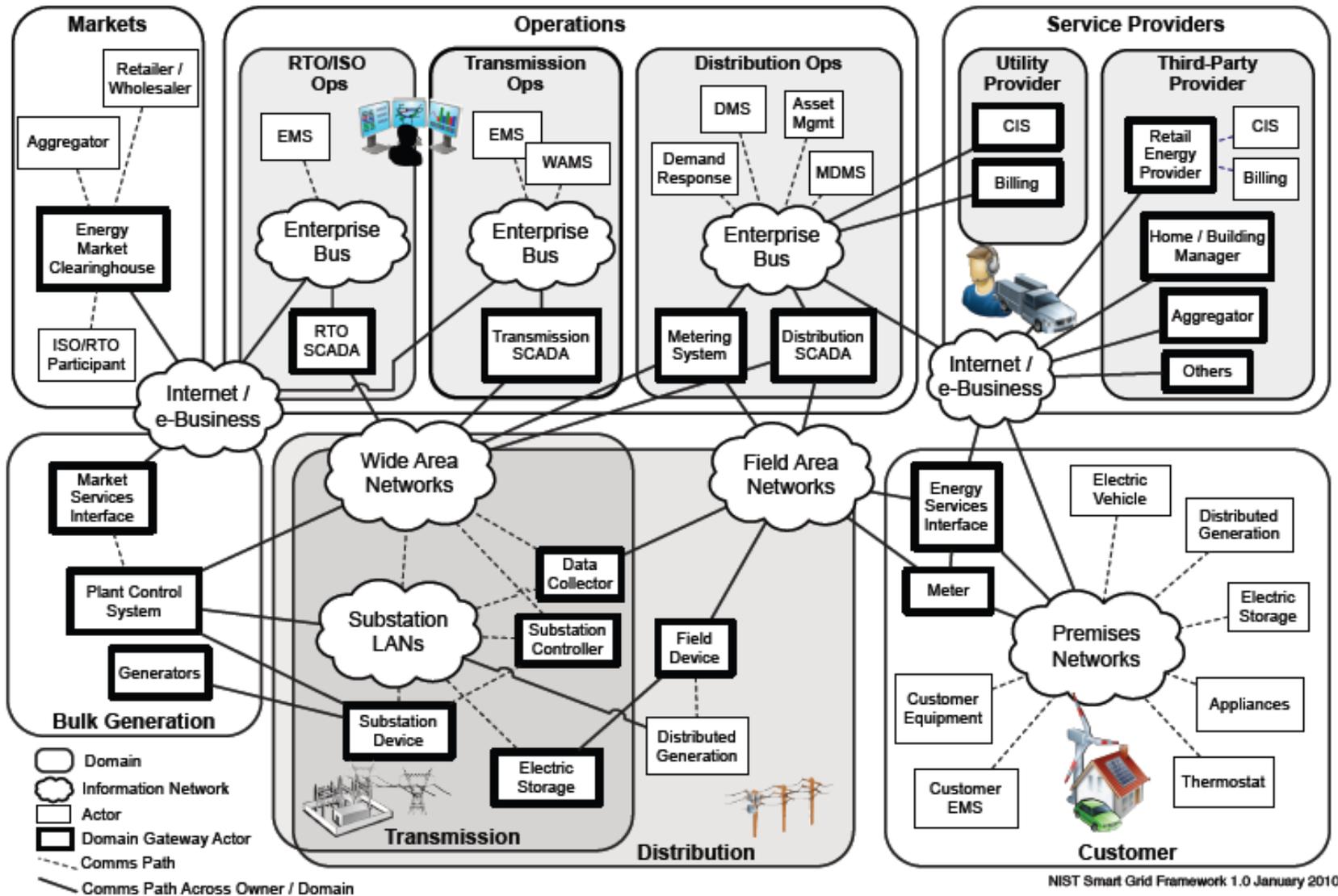


Boeing operates one of the largest virtual private network in the world

Smart Grid = Electrical Grid + Intelligent Infrastructure



Conceptual Reference Diagram for Smart Grid Information Networks

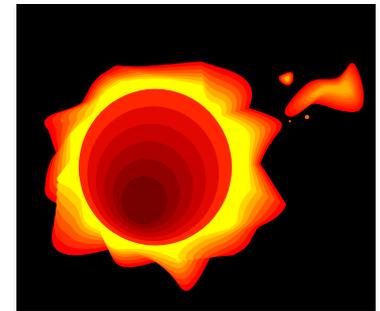


Challenges

- Timely actionable information sharing
- Adequate protection of information shared between public and private sectors
- New Regulatory Model
 - Compliance and risk management balance
 - “Safe Harbor” provisions in law and regulation
 - Efficient rate recovery process for cyber security costs
- Graded Cyber Security Requirements and Risk Management Processes
- Supply Chain Risk Management
- Survivability and Resilience
- Culture and Communication
 - Consumer education
 - Innovative and adaptive workforce
- Wide-Area Cyber Situational Awareness
 - Continuous Monitoring
 - Smart Grid cyber threats
 - Realistic analysis and response

Threats to the Grid

- Deliberate attacks
 - Disgruntled employees
 - Industrial espionage
 - Unfriendly states
 - Organized crime
- Inadvertent threats
 - Equipment failures
 - User/Administrator errors
- Natural phenomena
 - Weather – hurricanes, earthquakes
 - Solar activity



Increased Connectivity

★ Points of System Entry

Energy Consuming Equipment

Critical Loads



Non-Critical Loads



Housing



Electric Vehicles (Charging & Storage)



Distributed Energy Resources (DER)

Wind



Solar



Storage



Other



Distributed Generators



Geothermal Power



On-Site Peaker



Installation Utility Grid Interface

Intelligent Sub Station

Intelligent Transformer Vault (HTV)

Purchase/Demand Response/ Stability Support

Utilities – Energy Providers

Installation or Regional Networked Energy Operations Center (NEOC)

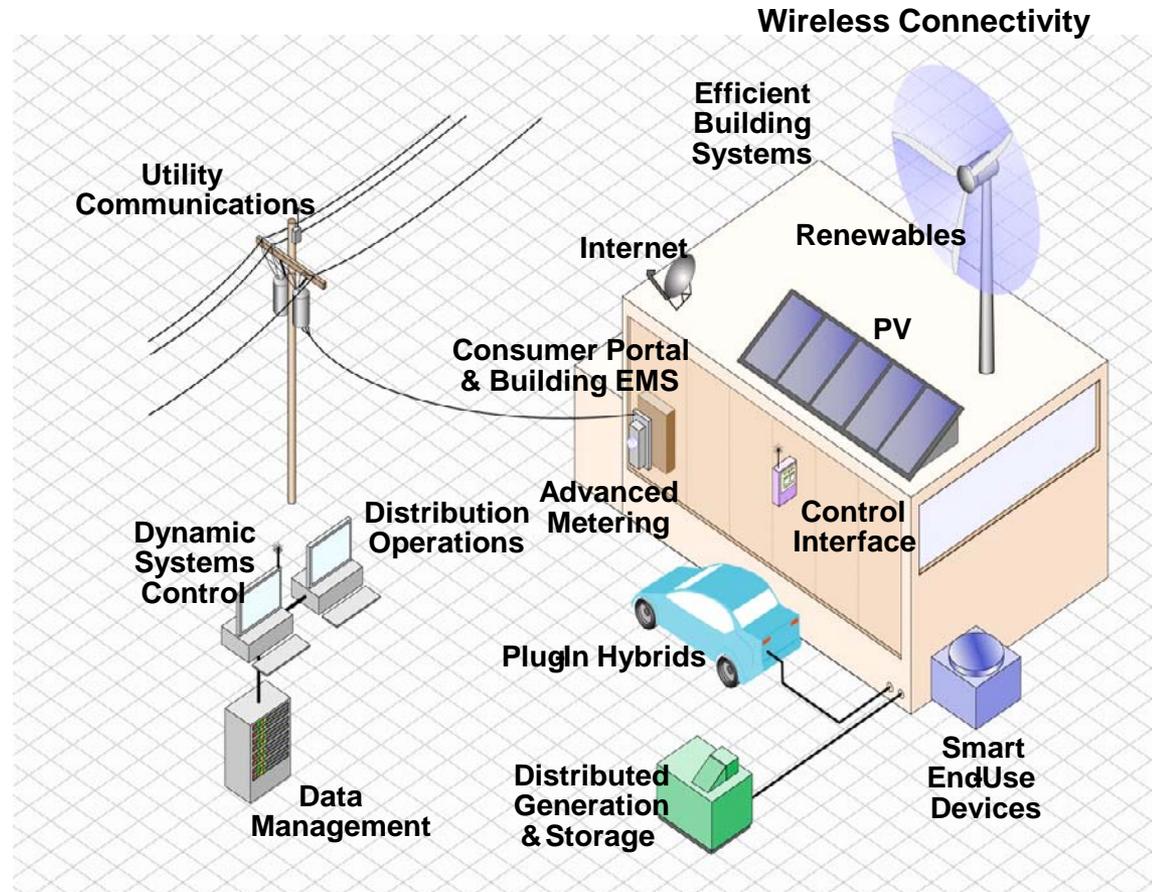
Energy Demand Driving Information



Every node on the System represents a Point of System Entry for an attack

Trends Causing Increased Risk

- 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



The Cyber Storm

SONY Playstations

Telegraph.co.uk

Home News Sport Finance

Technology News Technology Reviews

HOME > TECHNOLOGY > TECHNOLOGY NEWS

Cold war enemies Russia and China launch a cyber attack every day

abc NEWS

Hacked Drones: How Secure Are U.S. Spy Planes?

Pentagon Downplays Hacked Drones, Analysts Say Not So Fast

U.S. government sites among those hit by cyberattack

FT.com

Technology

FINANCIAL TIMES

FT Home > Companies > Technology

Front page

World

Companies

Energy

Industries

Twitter hijacked by 'Iranian Cyber Army'

By Tim Bradshaw, Digital Media Correspondent

Published: December 18 2009 12:23 | Last updated: December 18 2009 12:23

North Korean hackers blamed for sweeping cyber attack on US networks

North Korean hackers may have stolen US war plans

Files outline South Korea and Washington's strategy in event of

Pro-Iranian hackers hit Twitter and opposition websites

STUXNET



Software & Web

< Back to the top page



Cyber criminals eye file sharing networks: Kaspersky Lab

Cyber crime poses threat to e-commerce

Aurora



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Recommendation to Industry

AURORA Mitigation — Protection and Control Engineering
Practices and Electronic and Physical Security Mitigation
Measures

October 13, 2010

Advisory - Initial Distribution: June 21, 2007 (Superseded by Recommendation)

[Why am I receiving this? >>](#)

[About NERC Alerts >>](#)

Status:

Acknowledgement Required by October 18, 2010
Reporting Required by December 13, 2010 and every six
months thereafter until mitigation plan is completed.

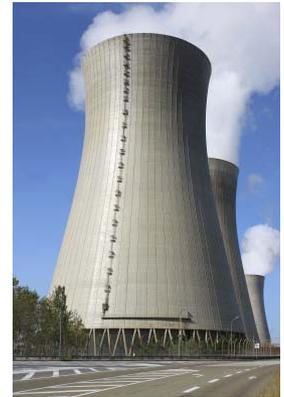


SENSITIVE: Internal Use Only (Do Not Distribute Outside
Your Company)

[More on handling >>](#)

Stuxnet

- First publicly disclosed control systems rootkit, but certainly won't be the last...
- USB vector; focused on “air-gapped” networks
- Highly sophisticated; infects everything, then rewrites PLC logic and hides
- Undermines integrity of control system
- Most regulations wouldn't have stopped it
- No 100% security against determined adversary



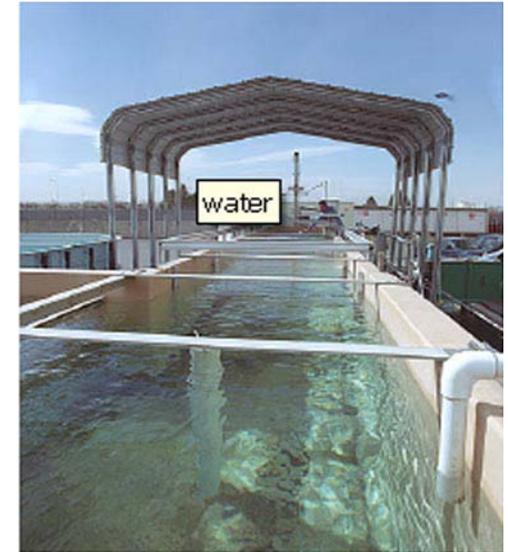
There's An App For That

- “Get mobile access to your control system via an iPhone, iPad, Android and other smartphones and tablet devices. The Ignition Mobile Module gives you instant access to any HMI / SCADA project created with the Ignition Vision Module.”



Maroochy Waste Water-Wireless

- Event
 - More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds
- Impact
 - Loss of marine life, public health jeopardized, \$200,000 in cleanup and monitoring costs
- Specifics
 - SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water
 - Used OPC ActiveX controls, DNP3, and ModBus protocols
 - Used packet radio communications to RTUs
 - Boden used commercially available radios and stolen SCADA software to make his laptop appear as a pumping station
 - Causes as many as 46 different incidents over a 3-month period (Feb 9 to April 23)



Lessons learned

- Change log-ons after terminations
- Investigate anomalous system behavior
- Use secure radio transmissions

Davis Besse Nuclear Power Plant- Patching and Network Connectivity

- Event
 - August 20, 2003 Slammer worm infects plant
- Impact
 - Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)
- Specifics
 - Worm started at contractors site
 - Worm jumped from corporate plant network and found an unpatched server
 - Patch had been available for 6 months



Recovery time:

SPDS – 4hours 50 minutes

PPC – 6 hours 9 minutes

Lessons learned

- Secure remote (trusted) access channels
- Defense-in-depth strategies, FWs and IDS
- Critical patch installation needs to drive trusted agent status

Energy Independence and Security Act

Defines ten national policies for the Smart Grid:

1. Use digital technology to improve reliability, security, and efficiency of the electric grid
2. Dynamic optimization of grid operations and resources, with full cyber-security
3. Integration of distributed renewable resources
4. Demand response and demand-side energy-efficiency resources
5. Automate metering, grid operations and status, and distribution grid management
6. Integrate “smart” appliances and consumer devices
7. Integrate electricity storage and peak-shaving technologies, including plug-in electric vehicles
8. Provide consumers timely information and control
9. Interoperability standards for the grid and connected appliances and equipment
10. Lower barriers to adoption of smart grid technologies, practices, and services.

US Grid Stakeholders Supporting Securing Critical Infrastructure

- Government-Industry-Academia Working on Cyber Security
 - Standards-NISTR 7268
 - Laws
 - Implementations
 - Pilot Projects
- Building a Risk Management Approach



Public Utility Commissions



Questions ??????????

