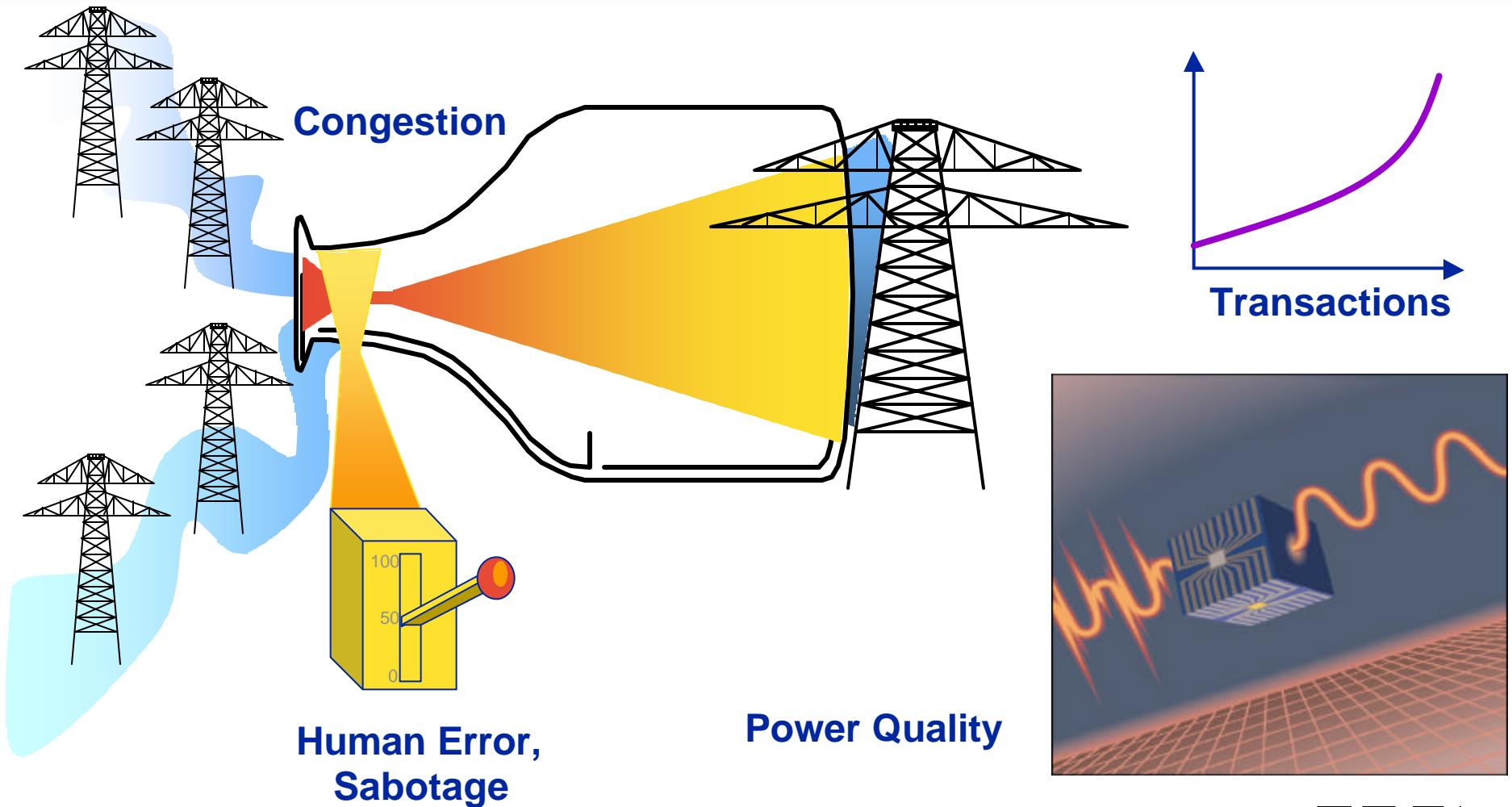


Electricity Infrastructure Security



Steve Gehl
Director, Strategic Technology
EPRI
November 28, 2001

Power Delivery Vulnerability, circa 9/10/2001



Background: Growing Problems with the Grid

- Power delivery infrastructure and institutions have sometimes failed to meet the needs of a digital economy
 - Reliability Problems -- 1996, 1998, 1999
 - Western States Power System “Crisis” -- 2000, 2001
- Technical issues posed by terrorist threats and attacks are similar to these reliability problems

The Threat



- Electric power systems constitute *the* fundamental infrastructure of modern society and therefore an inviting target for three kinds of terrorist attacks:
- Attacks upon the system
 - Power system itself is primary target with ripple effect throughout society
- Attacks by the system
 - Population is the actual target, using parts of the power system as a weapon
- Attack through the system
 - Utility networks provide the conduit for attacks on other critical infrastructures

The Dilemma

- How to make the electricity infrastructure more secure without compromising the productivity advantages of highly interconnected networks
 - **Centralization/decentralization:** Enhance resilience through simultaneous top-down and bottom-up decision making
 - **Dependence on communications:** Protecting the electricity supply requires enhancing security of associated communications
 - **Accessibility and vulnerability:** Comprehensive physical protection is not possible; probabilistic vulnerability assessment offers strategic guidance in where and how best to deploy security resources

What kind of Security is Ultimately Needed?

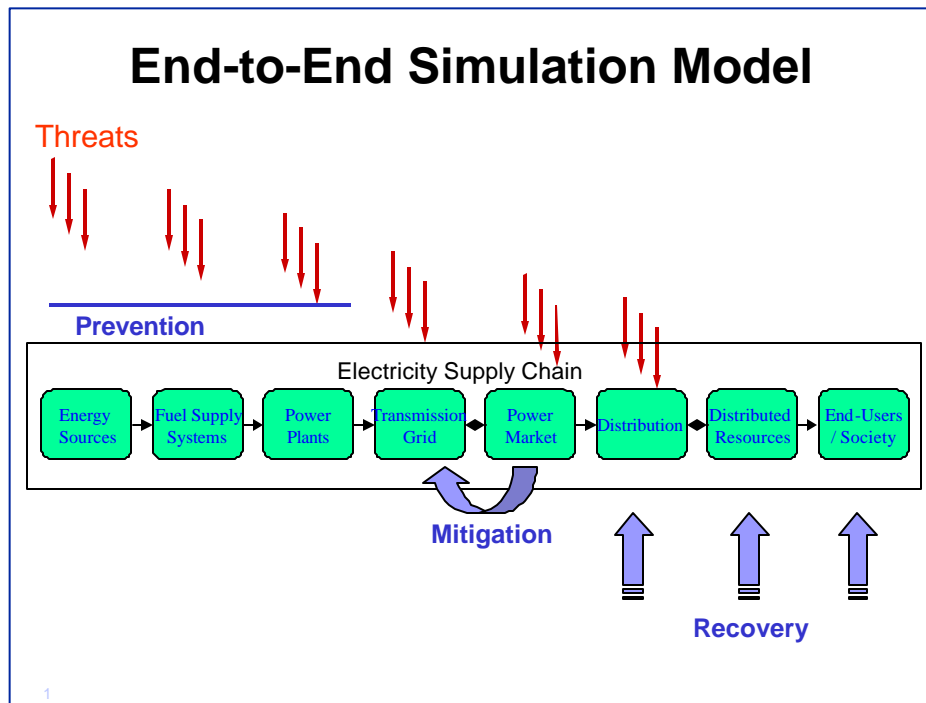


- The grid must be made secure from cascading damage
- Conduits for attack must be monitored, sealed off, and “sectionalized” under attack conditions
- Critical controls and communications must be made secure from penetration by hackers and terrorists
- Ongoing security assessments will be needed to ensure the industry stays ahead of changing vulnerabilities

EPRI's *Electricity Infrastructure Security Assessment*

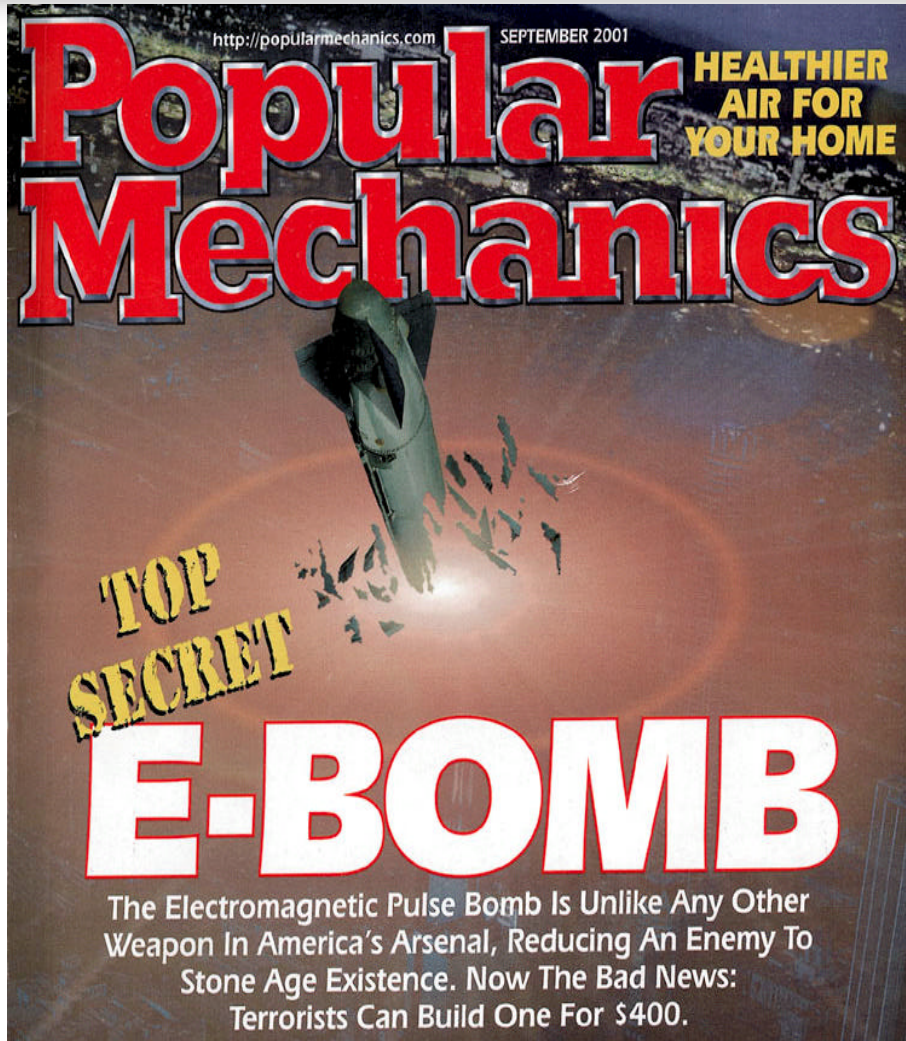
- Two volumes:
 - Vol 1: out to 18 months
 - Vol 2: 18 months to 5 years
- Purpose
 - To provide a preliminary assessment by EPRI of potential terrorist threats to the U.S. electricity system, along with some suggested countermeasures
- Emphasis
 - How advanced technologies can be used to protect critical infrastructures
 - Physical security issues are left to individual utilities

Probabilistic Vulnerability Assessment



- First priority is to assess system vulnerabilities and determine most effective countermeasures
- Short term: Preliminary Probabilistic Risk Assessment (PRA) using existing system models
- Long term: Comprehensive Probabilistic Vulnerability Assessment (PVA) based on new, End-to-End Simulation Model and threat matrix – producing a Vulnerability Index

Examples of Threats



- Threats on the power system
 - Terrorists gain access to critical cyber systems through Internet
 - Countermeasures: Develop secure systems to replace Internet connections
- Threats by the power system
 - Terrorists use power plant cooling towers to disperse CB agents
 - Countermeasures: Determine scope of threat, install sensors to detect CB agents, develop methods to destroy agents
- Threat through the power system
 - Terrorists build “E-bombs” using widely available designs
 - Countermeasures: Develop shielding for critical equipment and detection devices to quickly identify grid areas affected

Some Discussion Questions

- How real do you believe the “of-by-through” threats are in terms of damaging the power system?
- If these threats are credible, how well does the *Vulnerability Assessment* address the issues?
- How best can the industry (and EPRI) mount a response?
 - Public-private partnership?
 - Enabling legislation??
 - Industry-funded “Electricity Infrastructure Security Initiative”