Improving Energy Infrastructure Security: Costs and Consequences

Alex Farrell[1], Hisham Zerriffi[2], Lester Lave[2], Granger Morgan[2]

[1]Energy and Resources Group, UC Berkeley

[2]Dept. of Engineering and Public Policy, Carnegie Mellon University

26th Annual Conference of the International Association for Energy Economics

Prague, Czech Republic

June 7, 2003

Part 1: Thinking about *Stress* in the Electric Power Sector

- Definition
  - Deliberate attack to create panic and political pressure
  - Other socially-created conditions that are not captured by traditional ideas of ‘reliability’

- NOT
  - Price shocks in international oil markets
  - Routine equipment failures
  - Weather-related outages
  - “Guards, gates, and guns”

Stress

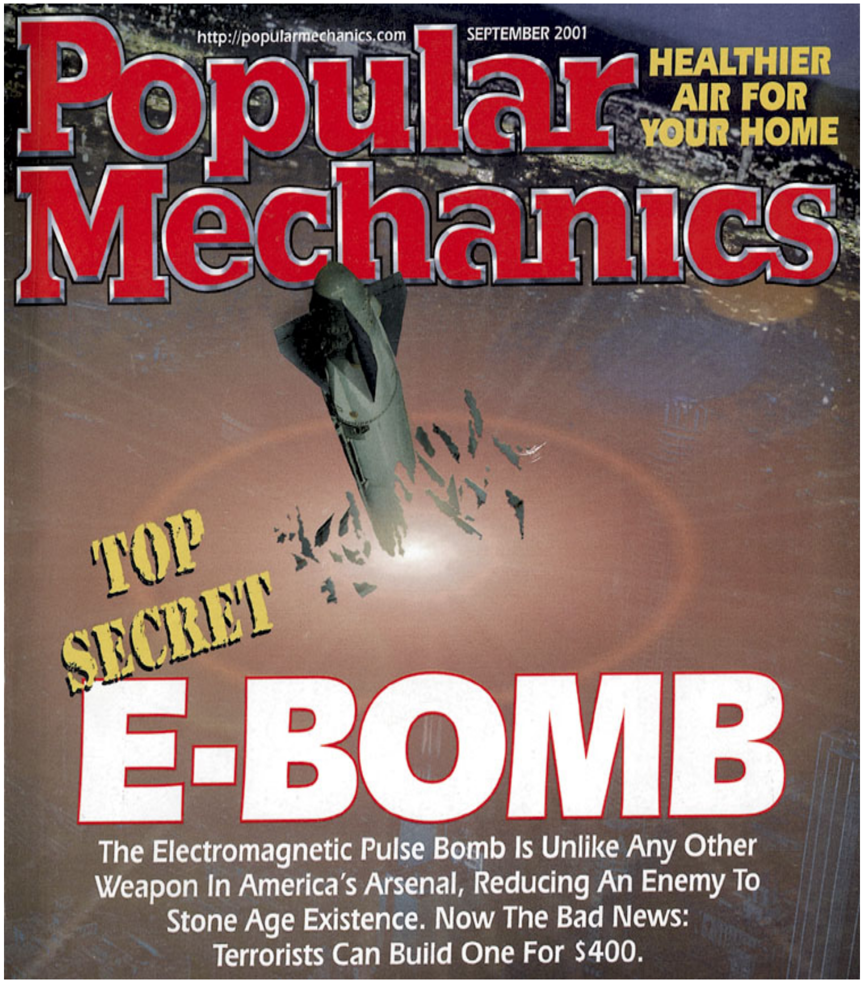
- Define
  - Conditions outside of “typical” reliability planning assumptions.
- Examples
  - Localized direct conflict damage (e.g. Columbia, or the U.S.)
  - System-wide direct conflict damage (e.g. Bosnia)
  - Inadequate investment/maintenance (e.g. India)
  - Incomplete institutional arrangements (e.g. Palestine)
- Literature
  - scarce

Reliability

- Restoration of power supply from single-point failures under well-defined conditions
- OECD power systems are *extremely* robust in the face of weather and equipment failures
- Great Northeast Blackout of 1965
- Southern Ontario ice storm of 1998
- 2000 North American Reliability Council (NERC) major incidents
  - 26 due to weather (mostly thunderstorms)
  - 12 operator error or maintenance error
  - 12 equipment failures
  - 2 forest fires (largest – NM, 660,000 people, <4 hours)

Stress is not Weather

- Repeated
- Threats to repair personnel
- Focused on damaging crucial infrastructure
  - Transformers
- High-hazard facilities
  - Dams and locks
  - Nuclear power plants (spent fuel)
  - Cooling towers
  - Electro-magnetic pulse
- Cyber attacks on electronic data collection and control systems (SCADA)
  - Internet-based
- Insider attacks



Institutions for reliability

- Reliability and security are both public goods – role for government
- Institutions that promote reliability
  - State-owned enterprises
  - State public utility commissions
  - Monopoly franchise – incentives for transmission investment
  - NERC
  - EPRI
  - NRC
    - 1999 review: “significant weaknesses” in 27 of 57 facilities
    - Red Team exercises: staff are briefed about timing and detailed plans
    - Nuclear industry pushing for ‘self-regulation’

- What are the institutions that will promote security?

Failure in complex, engineered systems

- Complex systems seem to have more large-scale disruptions than a normal distribution, or even a log-normal distribution, would suggest.

- Failure detection in an unbounded system (incompletely observed) may be slow and difficult.

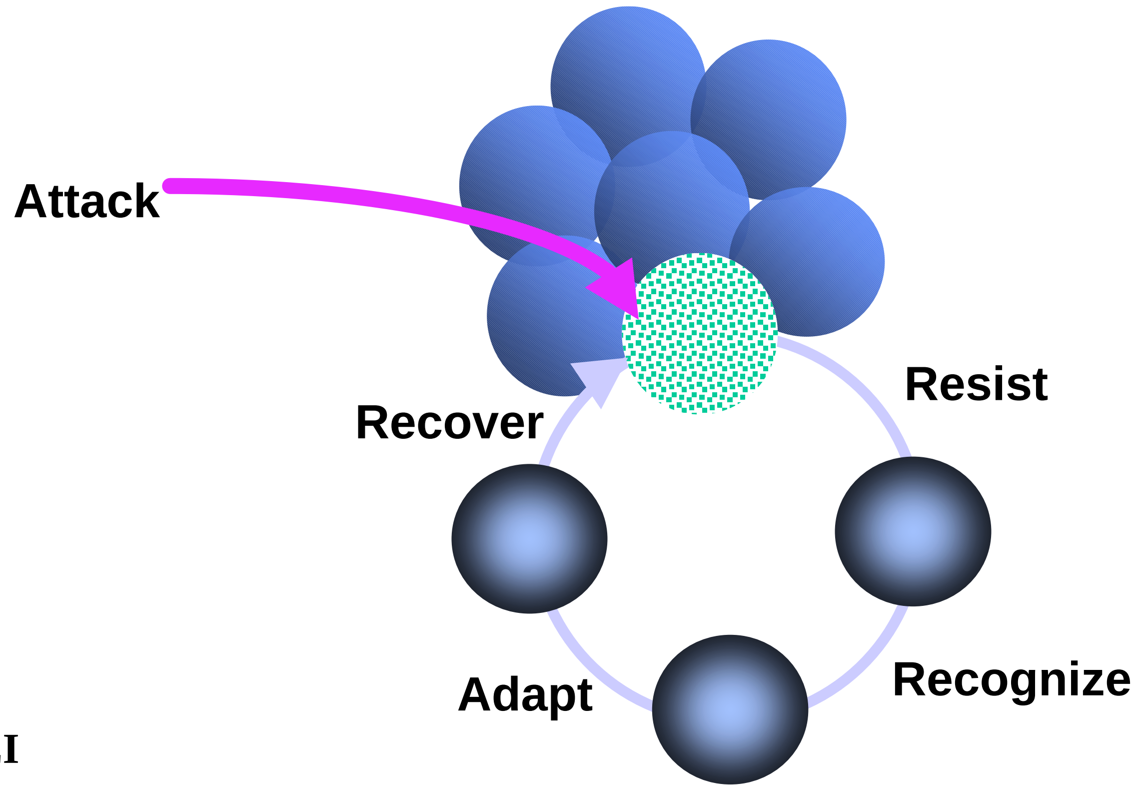
- Suggests that the only strategy it to accept that vulnerabilities will always exist, that failures (even large ones) will always occur.

- Non-storability and system balancing in electric power systems make this even more problematic

Survivability offers a coherent framework

Carnegie Mellon University
Software Engineering Institute

Survivability **is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.**



Source: Howard Lipson, SEI

Survivability

- Fundamental assumption: No individual component of a system is immune to all attacks, accidents, and design errors.
- Goal: The <u>mission</u> must survive, not any individual component, not even the system itself.
- Contrasts with the ‘fortress’ model of system security – failures can be catastrophic
- Survivability is an *emergent property* of a system.
- Contrast to “fortress” model

Example – Traffic Lights

- Major problem during blackouts: traffic accidents
- Backups available
  - LED lights, solid-state switches, batteries
- “Fortress-type” thinking:
  - Blackouts will not occur, so don’t plan for operation during them
  - All loads on the same circuit
  - Blackouts lead to accidents and create gridlock for police, etc.
- Survivability thinking:
  - Recognize: open breakers upon power failure
  - Adapt: operate on battery power
  - Recover: re-connect when power is restored.

- But who pays?

Restructuring

- Changes (reduces mostly) the role of many reliability institutions
- Incomplete restructuring makes incentives for investment in transmission system unclear
- May result in poor incentives for transmission investment
- Data sharing is problematic
- Key issue – WHO PAYS FOR SECURITY?
- Must be resolved before security issues can be resolved.

Part 2: Analysis of Stress

- How do different system architectures affect reliability and survivability?
  - Large central generation
  - Distributed generation
- How do sensitivities change?
- What are the costs?

- Possible advantages of DG
  - Law of large numbers in generation
  - Less reliance on electricity T&D
  - Fuel switching
  - Advantages of gas T&D
    - Underground
    - Storage
    - Operational simplicity

Method

- Stochastic reliability model using IEEE Test System
  - Modify to include DG
  - Modify to represent stress (Stress Adjustment Factor – SAF)

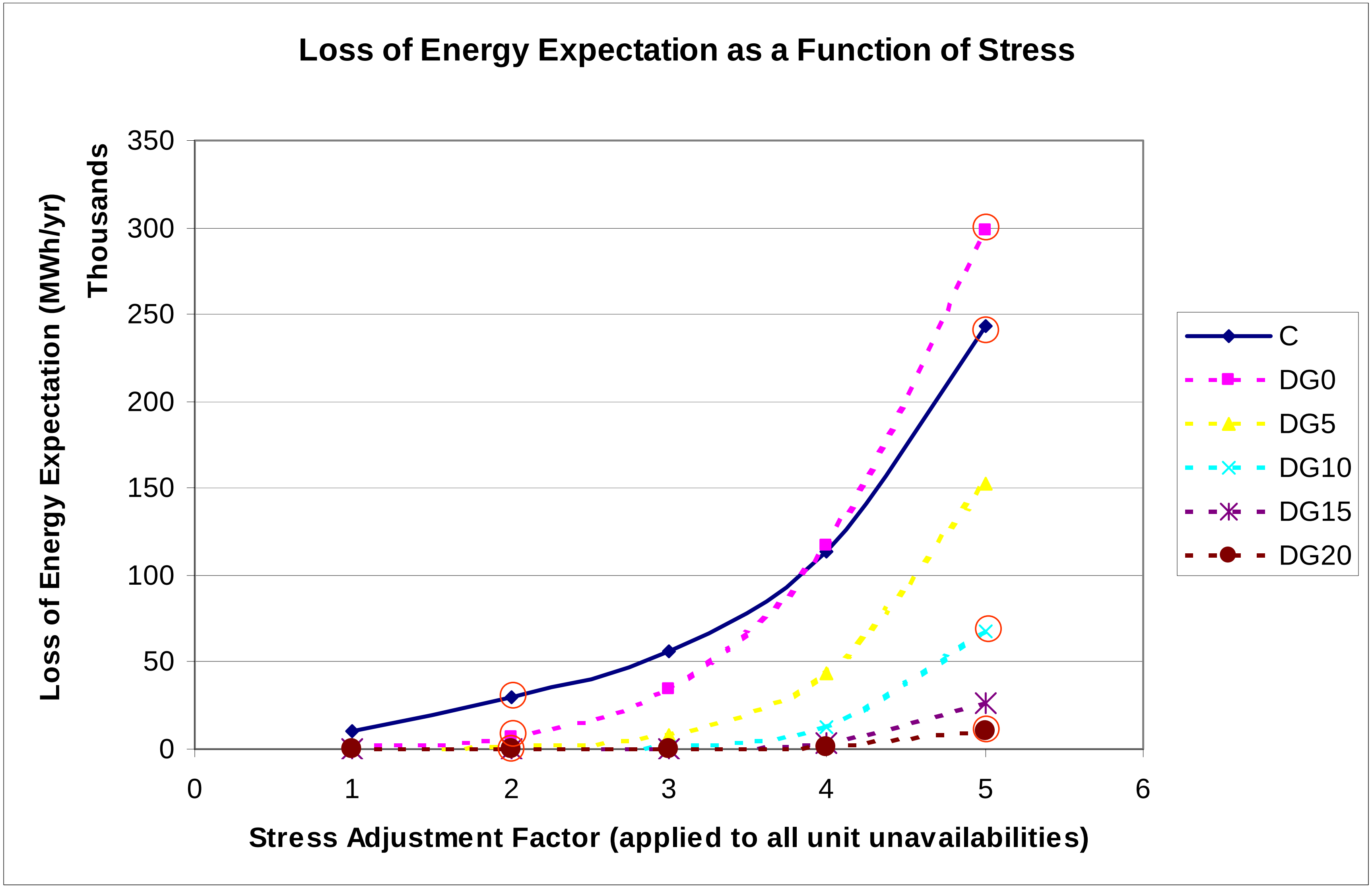
- Cost model to estimate the costs of energy supply, outages

- Gas T&D
- Mixed architectures
- Heterogeneity of local loads
- Power flows

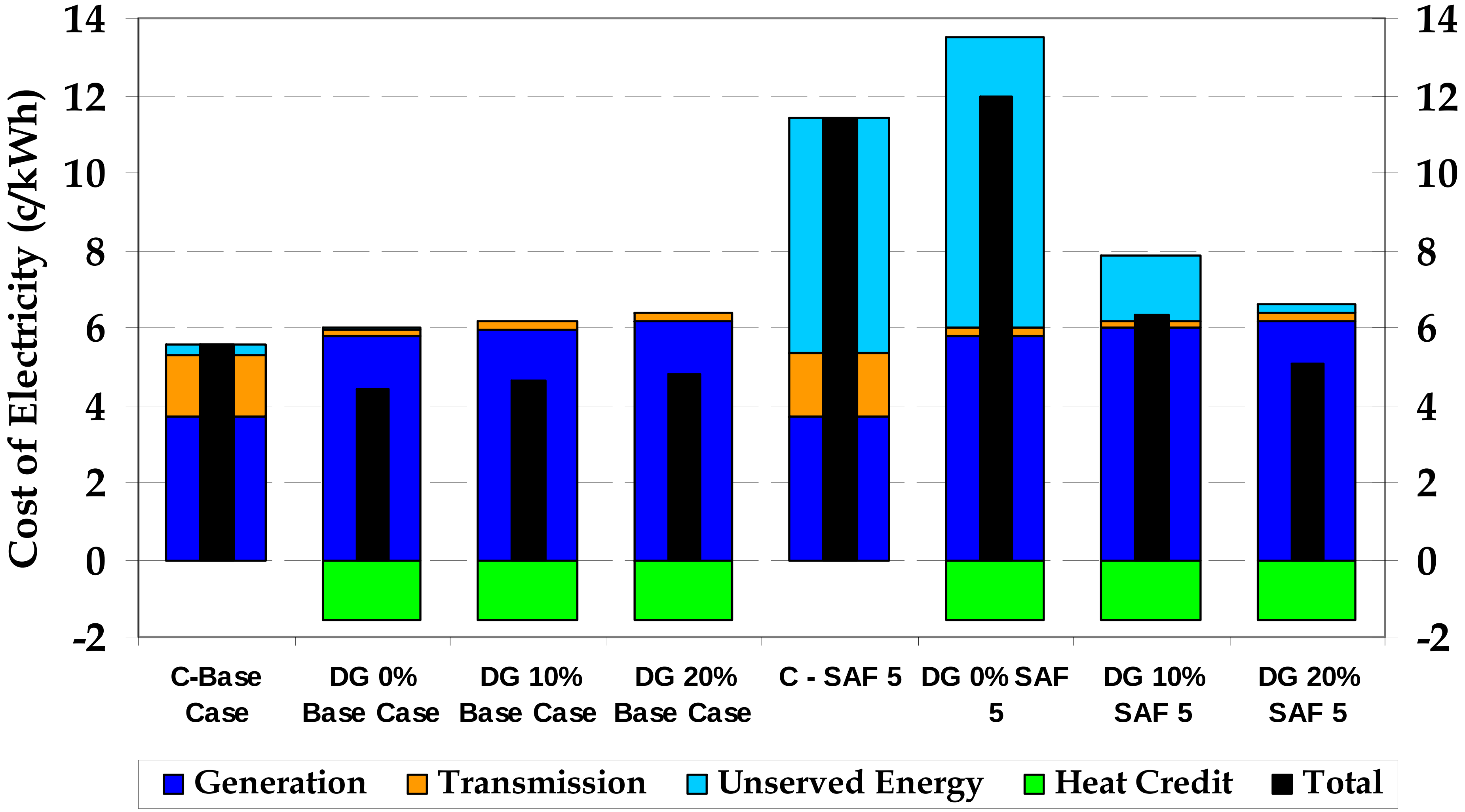
System Architectures

Scenario	Number of Units	Unit Sizes (MW)	Total Capacity (MW)	Capacity Reserve (percent)
C (Centralized System)	32	12-400	3,405	19.5
DG0 (Minimum System)	5700	0.5	2,850	0
DG5	5985	0.5	2,992	5
DG10	6270	0.5	3,135	10
DG15	6555	0.5	3,277	15
DG20 (Match Centralized)	6840	0.5	3,420	20

Loss of Energy Expectation



Cost of Electricity



Thanks to

- **UC Berkeley, Committee on Research**
- **Carnegie Mellon Electricity Industry Center**

  www.cmu.edu/electricity

References

Farrell, Lave and Morgan (2002) “Bolstering the Security of the Electric Power System” *Issues in Science & Technology*. **XVIII**(3):49-56. Spring

Lipson and Fischer (1999) “Survivability-A new technical and business perspective on security” Proceedings of the New Security Paradigms Workshop. Caledon Hills, ON: ACM

Zerriffi, Dowlatabadi and Farrell (2002) “Electricity and Conflict: Advantages of a Distributed System” CEIC Working Paper 02-01.

Cowart (2002) “Electrical Energy Security: Policies for a Resilient Network” Montpelier, VT: Regulatory Assistance Project. 7.