The Protection of Critical Infrastructures: Concept, Evolution and Complexities

Opening Keynote

11st MAS ETH SPCM Forum
Zurich, Switzerland

04 April 2008

Professor Saifur Rahman
Director
Advanced Research Institute
Virginia Polytechnic Inst & State University, U.S.A.
www.ari.vt.edu

Asymmetric Threat and Risk Environment

Asymmetric Threat

Risk Environment

Randomness
Asymmetric Threat and Risk Environment

What is Critical Infrastructure
An European Perspective

- Energy
- Transportation
- Water supply
- Information & communication
- Emergency services
- Law enforcement
- Financial services
- Health care
- Food supply
- High vulnerability industries
Critical infrastructures are vulnerable to cascading failures

- Natural Hazards
  - Hurricanes
  - Snowstorms
  - Earthquakes
  - Floods
- System Failures
  - Sabotage
  - Equipment Breakdown
  - Human error

A Plan for CIP

- Analyze the likelihood of the event
- Offer a resiliency planning to bring back normalcy
- Prioritize the actions needed to minimize the impact of the event
- Set up a rescue/recovery plan
Recent Hurricane Damages in the United States

- Need to address the potential for natural disasters
- Put forward the concept of resilience in addition to protection
- Climate change induced impacts

Source: Department of Energy, highlighting Rita's projected path and the site of offshore oil platforms and refineries in the Texas and Louisiana area.
Hurricane Katrina, August 2005

Hurricane Katrina heading for the Gulf Coast

Impact of Katrina on Refinery Availability

Gulf of Mexico damaged oil rig

A submerged oil refinery in Alabama
Impact of Katrina in New Orleans, Aug 2005

80% of the city is left under water with no power, no gas, no medical services, no drinking water, telephone or food supply.

These damages could have been prevented if the levee condition could be monitored.

Global impacts of natural disasters (1980 to 2004)

Trends in insured share

**Insured share of total losses (by hazard)**

- Storm (mean = 44%)
- Flood (mean = 7%)
- Other (mean = 10%)
- Non-WR (mean = 9%)


System Failures
Electric Power Grid Failures

- August 2003 blackout affected over 50 million people in northeastern USA and eastern Canada

U.S. Northeast Blackout, Aug 2003
Pre-Blackout
Cascading outages could have been prevented if the first power-line failure could be detected.

**Italian & Swiss Blackout - Sequence of Events (28 September 2003)**

- Loss of 28,000 MW
- Recovery in Southern Italy after 20 hours

Source: www.europeanenergyforum.eu
Italian & Swiss Blackout - Causes (28 September 2003)

- Lack of co-ordination between bordering TSOs
- Inappropriate evaluation of the situation after the first line outage

(Swiss-Italy)

Source: www.europeanenergyforum.eu

European Incident (4 November 2006)

Source: www.europeanenergyforum.eu
**European Incident (4 November 2006)**

**Facts**

- Triggering events started in Northern Germany
- Splitting the UCTE System into three areas
- Power imbalances in each areas
- Load shedding > 17 000 MW (15 million households)
- No blackout
- Restoration about one hour

Source: www.europeanenergyforum.eu

---

**Alaska pipeline shut down, Aug 2006**

Oil pipeline in Prudhoe Bay, Alaska, has been indefinitely shut down due to oil leak

The Alaska pipeline would not have been shut down if the corrosion could be detected earlier.
Infrastructure Protection

US Naval Base in Norfolk, Virginia
Asset Protection

Norfolk, VA

Hampton Roads Military Facilities in Virginia, USA
Protection of Infrastructures

Needed Inputs Upstream

Protection of Infrastructures

Recipients of Services Downstream
Complexities and Interdependencies

- **Private Ownerships** (over 85% of the infrastructure in the US is privately owned)
- **Competitiveness**
- **Regulations**
- **Profit Motive**
Local Ownership to Supplement Protection

- Involve local communities to take ownerships
- Involve host governments in cross-jurisdiction projects
- Provide additional services/benefits to local communities
Oil companies build pipelines literally in people's front yards.

Nigeria lost $4 billion in 2006 for damage (sabotage) to pipelines, loss of supply and security expenses.
CIP: Past, Present and Future

- **Past:** Vulnerability Assessment at the Organization/Facility Level

- **Present:** Past 9/11 – Three G’s (Gates, Guards, Guns)

- **Future:** Resiliency

---

Resilience as a means for CIP

- Resilience refers to the capacity of infrastructure, service and social systems potentially exposed to hazards from technical, natural or intentional events to adapt either by resisting system degradation or by readily restoring and maintaining acceptable levels of functioning, structure and service following an event.
Resilient physical and social systems must be robust, redundant, resourceful, and capable of rapid response.

Resilience and its Four Qualities

- **Robustness**: the inherent strength or resistance in a system to withstand external demands without degradation or loss of functionality.
- **Redundancy**: system properties that allow for alternate options, choices, and substitutions under stress.
- **Resourcefulness**: the capacity to mobilize needed resources and services in emergencies.
- **Rapidity**: the speed with which disruption can be overcome and safety, services, and financial stability restored.

Value of Resilience

Adding redundancy is another strategy to make critical infrastructure more resilient.

Challenges if Private-Public Partnership

- Planning and Preparedness
- Information sharing between governments and the private sector
- Relationship of regulator / regulated
- Corporate return on investment in Homeland Security
- Anti-trust concerns for collaborating corporations
- Prioritization of response and recovery

David J. Duecker, 2007
Conclusions

- Improve system resiliency by:
  - Identifying vulnerability & threats
  - Adding redundancy to protect critical nodes

- Increase the acceptance of large energy infrastructure projects by:
  - Involving local people & government to take ownership
  - Designing infrastructures for multi-purpose use

Contact Information

Name: Prof. Saifur Rahman
Affiliation: Virginia Tech, USA
Phone: +1-703-528-5500
Email: srahman@vt.edu
Web site: www.ceage.vt.edu

Questions or Comments?
Enhancing the resiliency of critical infrastructures

- Information sharing on operations and assets, priority setting, and resource allocation.
- Detailed knowledge of infrastructure interdependencies, critical assets and the extent of their vulnerabilities.
- Readiness of both the public and private organizations to ensure the privacy of data and liability protection.

5-step Process for Resilience Planning

1. List assets take inventory
2. Perform network analysis - identify critical nodes and links
3. Identifying threats and vulnerability of each critical components
4. Analyze the fault tree model using an event tree (vulnerability analysis)
5. Budget analysis - compute optimal resource allocation (risk assessment)
What are Critical Energy Infrastructures?

- Electric power generation, transmission, distribution
- Coal mining and transportation
- Natural gas/Oil production, transportation and storage
- Hydrogen production, delivery and storage

Global Insured Losses from weather related natural catastrophes, 1970-2005

- 2005: Hurricanes Katrina, Rita & Wilma, USD 65bn
- 2004: Hurricanes Charley, Frances, Ivan & Jeanne, USD 29bn
- 1999: Storms Lothar & Martin, USD 10bn
- 1992: Hurricane Andrew, USD 22bn