


CRITICAL INFRASTRUCTURES AT RISK: A Need for a New Conceptual Approach and Extended Analytical Tools

Wolfgang Kröger
Swiss Federal Institute of Technology Zurich (ETH)

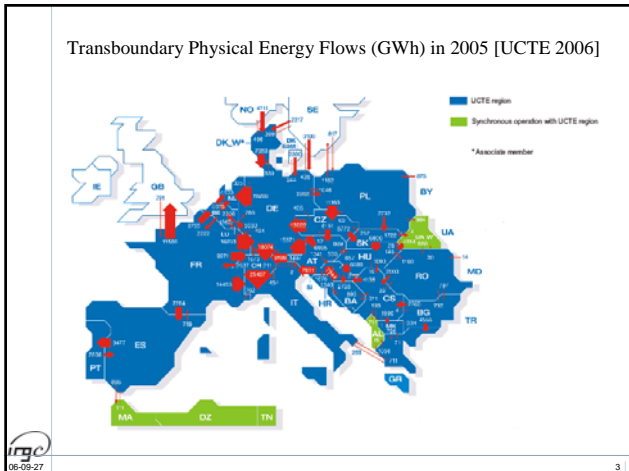
ESREL 2006 Lisbon
Monday, 18 September



International Risk Governance Council
9 Chemin de Balexert
Châtelaine
CH-1219 Geneva
Switzerland
+41 22 795 1730
www.irgc.org

Factors Which Have Promoted Tighter Integration, Greater Inter-dependency among, or Greater Vulnerability of Critical Infrastructures:

- Integration of smaller systems into larger systems (facilitated by modern ICT), thus increasing complexity and enabling transboundary propagation of disturbances
- Changes in the operating settings, including pressures which have squeezed out redundancy and thus reduced operating margins
- Use of off-the-shelf technology, including information and control systems, motivated by short-term economic efficiency
- Lack of adequate awareness of vulnerabilities, limitations to achievable reliability, low-probability-high-consequence failures, etc.
- Lack of adequate penalties or costs to private actors if, and when, system disruptions cause broader societal consequences
- Inadequacy of back-up measures to continue system operation when problems develop



What are (Critical) Infrastructures?

- A network of large-scale human-made systems that function synergistically to produce a continuous flow of services, essential for economic development and social well-being
- Designed to satisfy specific social needs but shape social change at much broader and complex level
- Subject to multiple threats (technical-human, physical, natural, cyber, contextual; unintended or malicious) and pose risks themselves
- Highly complex, inter-dependent, both physically and through a host of ICT ("system-of-systems"); subject to rapid changes
- Disruptions may cascade, even "normal" service interruptions cost industrialized countries a few percent of GDP
- Have no single owner/operator/regulator; are based on different goals/logics

Electric Power Supply Systems at Risk? Recent Major Blackouts

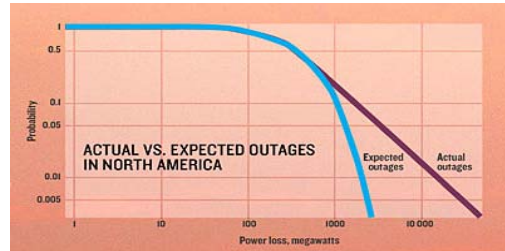
- August 14, 2003 – Great Lakes, NYC
- August 28, 2003 – London
- September 23, 2003 – Denmark / Sweden
- September 28, 2003 – Italy
- November 7, 2003 – Chile
- July 12, 2004 – Athens
- May 25, 2005 – Moscow
- June 22, 2005 – Switzerland (railway supply system)
- August 14, 2006 – Tokyo



Costs totalled up to USD 2 - 10 bn (US NE), people affected amounted to 60 millions (Italian), and recovery times varied from 2 - 4 (Swedish /Danish) to 5 - 9 hours (Italian cities) and more than a day (NYC, Detroit)



Analysis of Interruption Data



Cascading failures in the North American electricity grid have been more common than one might expect. Forty-six of the events between 1984 and 2000, or nearly three per year, involved losses of > 1,000 MW. The probability of smaller power losses follows an exponential curve, while for losses >500 MW is described by a power law typical for self-organized systems [compiled by J. Apt, 2004]



Lessons Learned from "Blackouts"



Common pattern identified and clear confirmation of systemic nature of the risks involved:

- Each system has been developed in the past 50 years with a view to assuring "mutual assistance". These systems are now operated often beyond the original design parameters, mainly due to market liberalization
- Minor single events (e.g. tree flashover due to inadequate tree-cutting or line-overload) may snowball into massive problems for a highly burdened electrical power system with long transmission distances
- Malfunction of critical equipment (possibly due to inadequate diagnostics) and behaviour of protective devices complicated the management of these events; available system automation turned out to be insufficient
- Most aggravating factors were human-related and contextual, including a general lack of situational awareness of potentially far-reaching failures and short-term emergency preparedness
- The impacts on other infrastructures and our societies are significant although in the studied incidents the affected population reacted calmly



The Creation of the International Risk Governance Council: Why (reasoning)?



- Experienced events demonstrate higher-correlation, risks have become transboundary
 - Example: Mydoom computer virus generated 100 mio infected e-mails worldwide in its 36 hours and slowed overall internet performance by approx. 10%
 - and new and changed traditional risks have emerged
 - Examples: Negative side-effects of future applications of nanotechnology, infections diseases (H1N5 influenza pandemic)
- Necessarily narrow interests of government, business, academia, civil society and NGOs must be transcended



Who are we (mission)?

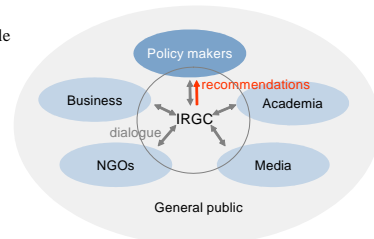
IRGC is an independent organisation whose purpose is to help the **understanding and management of global risks** that impact on human health and safety, the environment, the economy and society at large by

- developing **concepts of risk governance** that have relevance across different fields, organisations and countries
- **anticipating major risk issues** and improving the understanding and assessment of them and the ambiguities involved
- providing **recommendations** to key political decision makers

Focus on Risk Governance

- Interaction with the totality of actors and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken
- Reflection of the need for the principles of good governance, i.e. accountability, transparency, effectiveness, efficiency and strategic vision/focus

Working Principle



Successes („Products“) so far

- In **June 04** our Inaugural Conference was held in Geneva (170 delegates from 29 countries)
- In **September 05** our General Conference was held in Beijing at the invitation of the Chinese government (300 delegates from 32 countries)
- In **September 05** our White Paper No.1 on 'Risk Governance – Towards an Integrative Approach' was published
- In **June 06**, our White Paper No.2 on 'Nanotechnology Risk Governance' was published
- In **July 06**, IRGC's multi-stakeholder conference 'The risk governance of nanotechnology' was held in Zurich at the invitation of Swiss Re (130 delegates from 24 countries)
- In **October 06**, our White Paper No. 3 on 'Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures' will be published
- **Delivery planned for 2007:**
 - Recommendations for strategic preparedness for an influenza pandemic
 - Report on 'Regulation of Deep Geological Sequestration of CO₂'
 - Launch of new projects
 - General Conference in Lisbon, 8-10 October 2007

Potential New Projects

- Sequestration of CO₂ (with extended scope to include ocean sequestration) – seeking to develop recommendations for an international regulatory framework
- Risk governance of innovative technology – aiming to develop recommendations for the governance and regulation of innovation which account for its characteristics
- The risks of loss of ecosystem services – formulating a new approach to govern the degradation of ecosystem services and generating policy recommendations
- Best practice in natural disaster risk management - examining approaches to issues such as early warning, prevention, coping capacity, crisis management
- Vulnerabilities of critical infrastructures to 'upset conditions' (i.e. pandemics, earthquakes, weather, terrorist attacks) and instructions to deal with emergencies
- Assessing vulnerabilities of transcontinental gas transport systems (with the intention to take a full spectrum of threats/disruptive events and coupling effects into account)
- Global risk governance options for selected nanotechnology applications and the political barriers to their implementation

IRGC's Study on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures

Focus on Western industrialized countries, on five interconnected networks:

- electric power and gas supply
- information and communication services – particularly as provided by the Internet as well as ICT used for industrial control
- urban water supply and waste water treatment and
- rail transport

Assuming that the basic resources (fuels, water, etc.) for their operation are available

Overarching goal and project audience:

- Provide pertinent information to senior decision makers and end-user groups, raise wider awareness of critical big picture issues
- Address contradictory aims or trade-offs and – where appropriate – stimulate means to improve risk governance

Summary of objectives:

- Examine selected critical infrastructures from both the physical / technical and socio-economic / organisational perspective
- Explore the vulnerabilities and main drivers behind this tighter integration including political and institutional shortcomings
- Develop proposals for strategies that might reduce vulnerabilities and recommend policy options



13

Stress Factors: Discrepancy between System Design and Trading / Operational Practices within Synchronized UCTE-Grid

Historically:

Self-sufficient, vertically integrated utilities serving native (national) load; interconnection at corporate level designed to:

- Provide mutual support in maintaining system reliability, set security and reliability standards
- Share generation reserves to increase economic efficiency
- Allow international trade (limited coordinated exchanges)

Currently

(liberalisation, political development – extension towards Eastern Europe)

- Drastically higher (and uncoordinated) cross-border trades (Italian imports increased by factor 10 from 1970 to 2002)
- Unbundling of the generation-transmission-distribution chain, of electricity traders and transmission system operators
- Transmission systems run closer to the limits (little investment in new transmission capacity, environmental concerns)
- Security criteria ("N-1 rule") still the same
- Institutional structure within UCTE quite the same (decentralized control blocks)



14

Assessment Matrix for the Five Infrastructures Selected for this Study

Colours are used for our initial judgement: Red corresponds to high, green to low, yellow to in-between; transitions from one colour to another indicate changes/trends.

			Electricity	Gas	Railways	ICT	Urban Water
Infrastructure characteristics	Complexity	Physical	Red	Green	Yellow	Red	Green
		Organisational	Yellow	Green	Yellow	Red	Green
		Speed of change	Red	Green	Yellow	Red	Green
	Dependence (interconnectedness)	On other infrastructures	Red	Green	Yellow	Red	Green
		For other infrastructures	Red	Green	Yellow	Red	Green
		Intra-structure	Red	Green	Yellow	Red	Green
	Vulnerability	ICT control	Red	Green	Yellow	Red	Green
		External impact*	Red	Green	Yellow	Red	Green
		Technical/human failures	Red	Green	Yellow	Red	Green
	Market environment	Cyber attacks	Red	Green	Yellow	Red	Green
Terrorist target		Red	Green	Yellow	Red	Green	
Inadequacy of control		Red	Green	Yellow	Red	Green	
Criticality	Degree of criticality - factors	Scope**	Red	Green	Yellow	Red	Green
		Magnitude	Red	Green	Yellow	Red	Green
		Effects of time	Red	Green	Yellow	Red	Green
	Overall degree of criticality	Red	Green	Yellow	Red	Green	



* Natural hazards, construction work, etc.
** Potential of cascading trans-national effects

15

Issues for Further Consideration

The rank of reliability and security of electricity supply within our society, and the question of what constitutes adequate levels of, need to be addressed from a broad perspective including – inter alia -

- **Technical fixes** (adding generation and transmission paths, reactive power support, proper maintenance, alignment of protection schemes and settings, closer to real time system monitoring and simulation, improved situational awareness, scenario-based operator training in contingency recognition and response)
- **Special issues** (improved modelling capabilities, professional accident investigations, refrain from use of Internet (without adequate security), optimal size of the synchronous grid, integration of dispersed intermittent generators (wind, solar))



16

Some More Specific Policy Recommendations (I/II)

The Electric Power Supply System

In the EU internal market Directives and Regulations, national legal and regulatory authorities as well as provisions are still all market-focused. Reliability criteria are often traded-off against other factors in liberalised markets. Therefore:

- Security of continuous supply should be addressed more explicitly and become a new overarching principle. Strategies to ensure an appropriate level of protection and resilience need to be promoted
- Top-down political decision and rule making processes should be revisited to include an appropriate level of technical analysis and dialogue with stakeholders, not only embracing all major players (including end-user groups) but also addressing key challenges (e.g. tariff structures to ensure adequate investments)



17

Some More Specific Policy Recommendations (II/II)

Communication and Information (Internet)

- Until research efforts, under way to develop much more secure Internets in the future, are successful, the public Internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure. Instead, dedicated communication lines and/or systems, should be employed that involve no logical link to publicly accessible computer systems and networks



18

CYBER EXAMPLES

In 1982, CIA Exploited Software Transferred to Soviet Union That Operated Pumps, Turbines, & Valves of Pipeline. Caused Software to Malfunction and Reset Pump Speeds and Valve Settings. Result was Largest Non-Nuclear Explosion and Fire Ever Seen From Space. 3 Kilotons TNT Equivalent – Hiroshima Was 14-20 Kilotons TNT

In 2000, Disgruntled Rejected Employee Used Radio Transmitter on 46 Occasions to Hack Into Controls of Sewage Treatment Plant and Released 264k Gallons of Raw Sewage into Rivers & Parks

In 2003, Slammer Worm Affected Business Network of Ohio Nuclear Plant and Spread to Operations Network. Caused Computerized Panel Used to Monitor Crucial Safety Indicators to Fail. Minutes Later Plan Process Computer Crashed.

27-Sep-06

© Jody R. Westby
Global Cyber Risk LLC
February 24, 2006

Reflections on Deficits of “Classical” Methods for Risk Analysis

- High complexity and interconnectedness of modern “system-of-systems” cannot be adequately modelled
- All kind of human factors including malicious behaviour not sufficiently covered
- Dynamic, or even non-linear behaviour of systems has to be handled; scenario-generating capabilities are too limited
- Full spectrum of triggering events/threats, including cyber attacks and acts of terrorism, cannot yet be taken into account
- Independence from ‘contextual factors (market organisation, safety culture, socio-political environment, etc.) assumed



20

ETH
 Eidgenössische Technische Hochschule Zürich
 Swiss Federal Institute of Technology Zürich

Laboratorium für
 Sicherheitsanalyse
 INSTITUT FÜR ENERGIELEKTRIZITÄT

The Italian Blackout Sept 28, 2003 – Contextual Factors

- **Discrepancy between commercial and physical flows**
 The generation dispatch realized in FR for the contractual energy export to IT led to high loads on the transit lines in CH. The resulting high phase angle differential over the failed Mettlen-Lavorgo line impeded its timely re-closure
- **Insufficient coordination and information exchange** among the adjacent TSOs (CH-IT-FR) due to economic, technical and historical reasons
- **Non-compliance of Italian generators with the technical rules of connection to the transmission network**
 After the disconnection from the UCTE grid 21 out of 50 large thermal generation units were shedded before the nominal 47,5 Hz frequency threshold was reached, impeding the successful island operation in IT

13.03.06 / 44. Tutzing Symposium Wolfgang Krieger / ETH Zürich / krieger@maiv.ethz.ch 21

ETH
 Eidgenössische Technische Hochschule Zürich
 Swiss Federal Institute of Technology Zürich

Laboratorium für
 Sicherheitsanalyse
 INSTITUT FÜR ENERGIELEKTRIZITÄT

The Agent-based Modelling Approach (I/II)

An Agent...

- ❑ is an autonomous software object
- ❑ has different states and attributes
- ❑ may interact and cooperate with one or several other agents (multi-agent system)
- ❑ follows given rules of behavior (deterministic or stochastic) and can strive for a goal
- ❑ has a memory and resources

The basic concept

23.03.06 / CNPQ / Rome Wolfgang Krieger / ETH Zürich / krieger@maiv.ethz.ch 22

ETH
 Eidgenössische Technische Hochschule Zürich
 Swiss Federal Institute of Technology Zürich

Laboratorium für
 Sicherheitsanalyse
 INSTITUT FÜR ENERGIELEKTRIZITÄT

The Agent-based Modelling Approach (II/II)

The Electric Power System as a Multi-agent System

- ❑ Agents represent both technical (e.g. generators) and non-technical components (e.g. grid operators, consumers, traders)
- ❑ Complex event chains (e.g. cascading failures) as well as emergent system behavior are derived by defining the behavioral rules of each agent and observing their interplay (i.e. the overall system performance) by simulations

Modelling the electric power system as a multi-agent system

13.03.06 / 44. Tutzing Symposium Wolfgang Krieger / ETH Zürich / krieger@maiv.ethz.ch 23