ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Analysis of Highly-integrated Systems

Methodological Uncertainties
Interdependencies among Complex Systems

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Spring Semester 2010
Prof. Dr. W. Kröger

Methodic uncertainties at the level of plant model

Fault Tree (CCF,HRA), Event Tree (scenarios, physical phenomena)

Adequacy of modeling approach: static approach vs. dynamic behavior; exclusion of certain failure types (e.g. human error of commission); system boundaries; unrealistic documents

- Quantification of the model
  - Data base: statistical basis
    - Engineered judgment
    - Generic
    - Plant specific
  - Population, relevance, uncertainty bands (→ error propagation)
  - Assumptions: rare event approximation, „cut-offs“, „binning“ (→sensitivity studies)
- Completeness of accident scenarios (→ large number) and model validity (→check against experiments and experience)

Required information for a FTA

Component level:

- Different relevant failure modes of individual units (to fix most relevant one)
- Relevant external "influences", e.g. environmental impacts
- For quantitative analyses: failure probabilities

System level:

- Precise definition of the operation mode in question and the system boundaries

Assignment of failure probabilities problems

- Lack of data (e.g. reliability figures of highly reliable tailor-made components in nuclear power plants, components designed to work under changing operating conditions in the chemical industry, etc.)
- Development of the database usually causes an extensive amount of work

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Spring Semester 2010
Prof. Dr. W. Kröger
Laboratory for Safety Analysis

Summary of the assumptions/preconditions

- A technical system consists of units (components)
- The units are both technically and logically connected
- The state of each unit follows a binary logic (true/false, on/off, intact/defect)

Available logic operators are:

- conjunction: AND ($\wedge$, $\cap$)
- disjunction: OR ($\vee$, $\cup$)

Labelling of the probabilities:

p_i: probability of survival of the *i*-th unit

q_i: probability of failure of the *i*-th unit

www.lsa.ethz.ch/education/vorl Risk Analysis of Highly Integrated Systems

Complicated vs. Complex

Complicated Systems (mechanical watches, aircraft, power plants, etc.)

- Components have well-defined roles and are governed by prescribed interactions.
- Structure remains stable over the time. Low dynamics.
- No adaptation. One key defect may bring system to a halt.
- Limited range of responses to changes in their environment.
- Decomposing the system and analyzing sub-parts can give us an understanding of the behavior of the whole, i.e. the whole can be reassembled from its parts.
- Problems can be solved through analytical thinking and diligence work.

Complex Systems (stock market, www, power grid, etc.)

- Rules of interaction between the components may change over time and may not be well understood.
- Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not always obvious.
- System responds to external conditions and evolves.
- Display organization without a central organizing principle (self-organization/emergence).
- Respond to and interact with their environment.
- Inadequate information about the state of the influencing variables, nonlinearities.
- Overall behavior cannot be simplified in terms of their building blocks. The whole is much more than the sum of its parts.

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Spring Semester 2010
Prof. Dr. W. Kröger
Laboratory for Safety Analysis

Critical Infrastructures in Switzerland

Sectors	Sub-sectors
Public Administration	Parliament, government, justice, administration
	Research institutes
	National cultural property
	Foreign representations and headquarters of international organisations
Chemical Industry	Production, transport, storage and processing of chemicals
Energy	Power supply
	Oil supply
	Natural gas supply
Waste Disposal	Wastewater
	Industrial and domestic waste
	Special waste
Financial Services	Banks
	Insurance companies
Public Health	Medical care and hospitals
	Medication
	Laboratories
Information and Communication Technology (ICT)	Telecommunications
	Information systems and networks
	Internet
	Instrumentation, automation and monitoring
	Radio and media
Water and Food	Food supply and food security
	Drinking water supply
Public Safety, Rescue and Emergency Services	Emergency organisations (police, fire service, emergency health care and rescue services)
	Protection & Support service
	Army
Transport	Road transport
	Rail transport
	Air transport
	Navigation
	Postal services and logistics

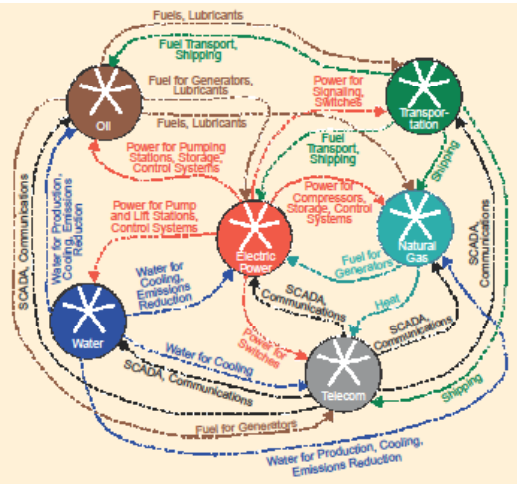
www.lsa.ethz.ch/education/vorl Risk Analysis of Highly Integrated Systems

Concepts and Definitions

Dependency: *A linkage or connection between two infrastructures,* through which the state of one infrastructure influences or is correlated to the state of the other. That is, infrastructure *i depends on j* through the link, but *j does not depend on i through the* same link.

Interdependency: *A bidirectional relationship* between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. That is, infrastructure *i depends on j through some links, and j*
likewise depends on *i through other links.*

Examples of Dependencies and Interdependencies among Critical Infrastructures [Rinaldi]



Four general "types of interdependencies":

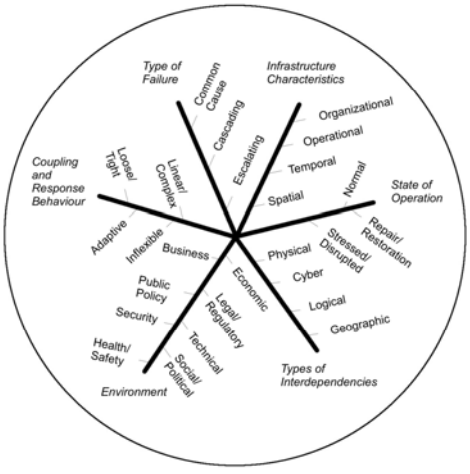
• **physical interdependencies** - the state of each is dependent on the material output(s)/flows(s) of the other, e.g., a pipeline network provides gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network;

• **geo-spatial interdependencies** - elements are in close spatial proximity and a local environmental event affects components across multiple infrastructures, e.g. earthquake, flooding or a fire;

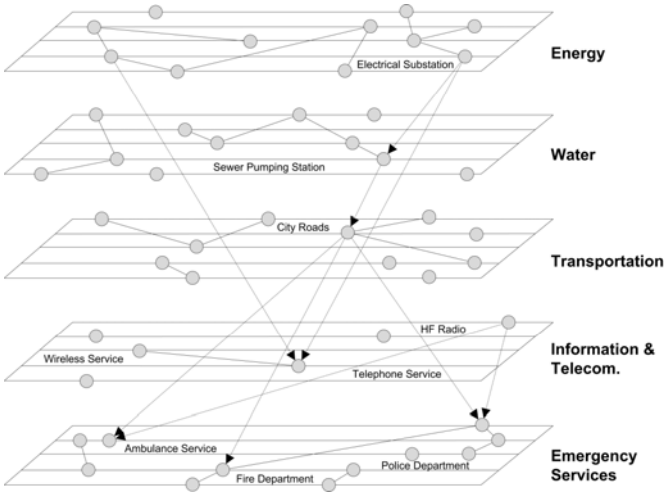
• **informational interdependencies** - connect infrastructures to one another via electronic, informational links, e.g. a supervisory control and data acquisition (SCADA) system monitors and controls elements of the electric power grid - likewise it may provide pieces of information or intelligence supporting another infrastructure or a decision making process elsewhere;

• **logical interdependencies** - exist between infrastructures that do not fall into one of the above categories.

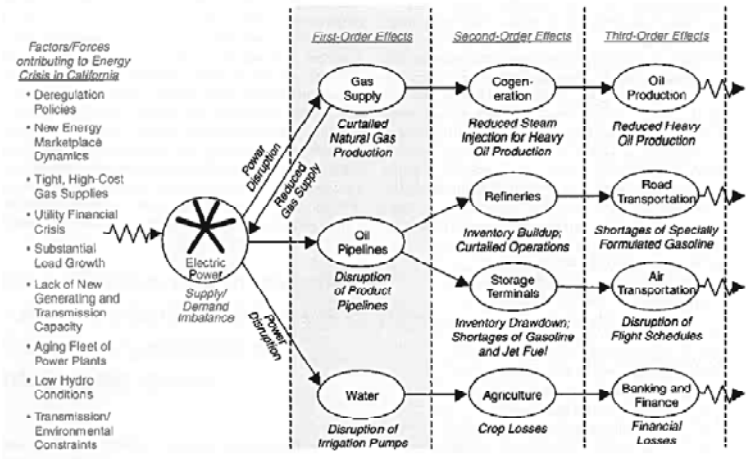
Dimensions for describing infrastructure interdependencies [Rinaldi et al.]



Infrastructure interdependencies (Hurricane Katrina)

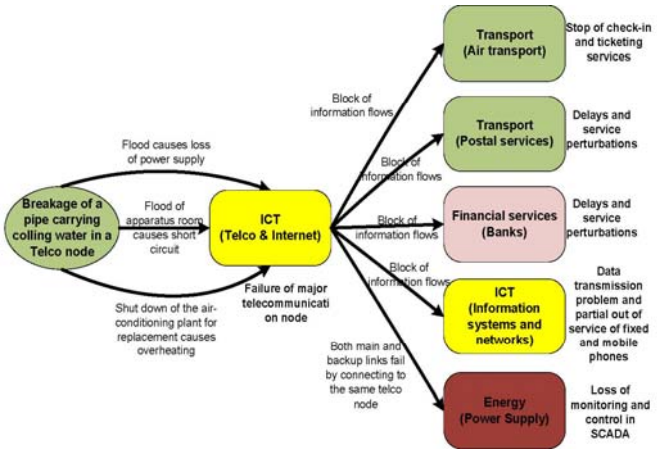


Examples of nth-order interdependencies and effects [Rinaldi et al.]



Blackout		Load loss [GW]	Duration [h]	People affected	Main causes
Sept. 28, 2003	Italy	~ 30	up to 18	56 Mio.	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs

Infrastructures affected by the mini telecommunication blackout in Rome, 2004



Failures (negative impact) that arise from interdependencies can be classified as follows:

(1) One event causing failure or loss of service of more than one infrastructure, such as areal external events (earthquakes, floods, extreme weather conditions, etc.), due to spatial proximity (called *common cause initiating events*);

(2) Failure of one infrastructure causing failure or loss of service of at least another infrastructure, e.g. rupture of mains of the water supply system (called *cascade initiating events*);

(3) Failure or loss of service resulting from an event in another infrastructure, e.g. failure of gas lines due to loss of main electricity supply if compressors are electronically driven (called *cascade resulting events*);

(4) Failure or loss of service of one infrastructure escalating (domino effect) because of failure of another affected infrastructure, e.g. failure of the electric power system leading to failure of the SCADA system and by this affecting restoration of the electric power system (called *escalating* events).

Events being neither one of these four types maybe called independent. The types of non-independent events are not mutually exclusive.

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Spring Semester 2010
Prof. Dr. W. Kröger

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

Course material:

http://www.lsa.ethz.ch/education/vorl

www.lsa.ethz.ch/education/vorl Risk Analysis of Highly Integrated Systems