


**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

**Laboratory for Safety Analysis**  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

# Risk Analysis of Highly-integrated Systems

## Methodological Uncertainties Interdependencies among Complex Systems



**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

**Laboratory for Safety Analysis**  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

## 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)

Spring Semester 2011 | Risk Analysis of Highly-integrated Systems | 2

**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich



Laboratory  
for Safety  
Analysis  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

## 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

Spring Semester 2011
Risk Analysis of Highly-integrated Systems
3

**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich



Laboratory  
for Safety  
Analysis  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

## 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:

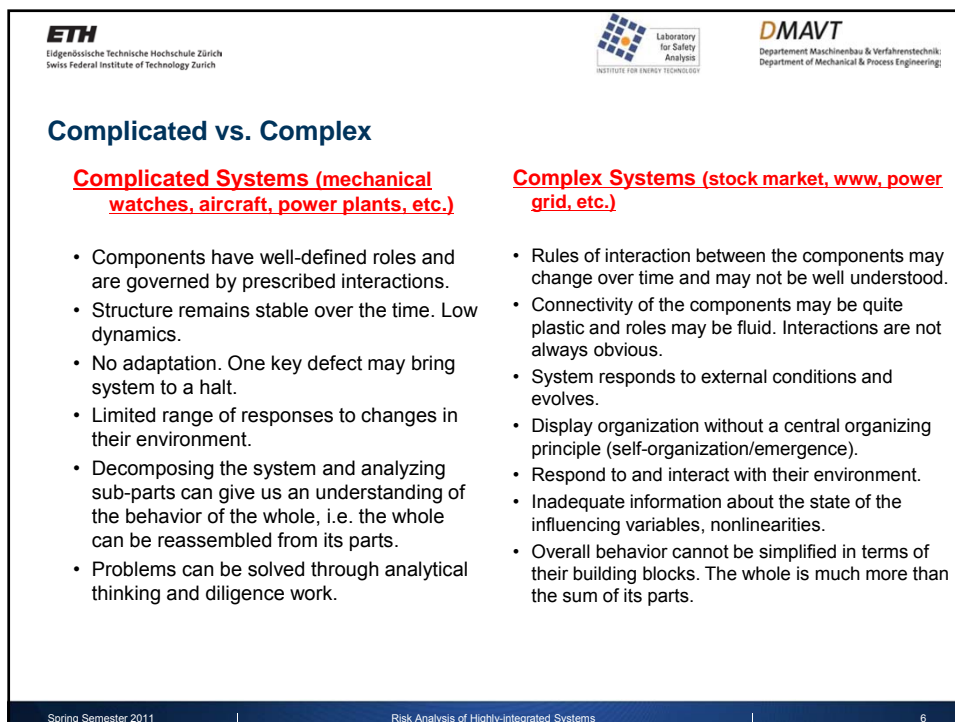
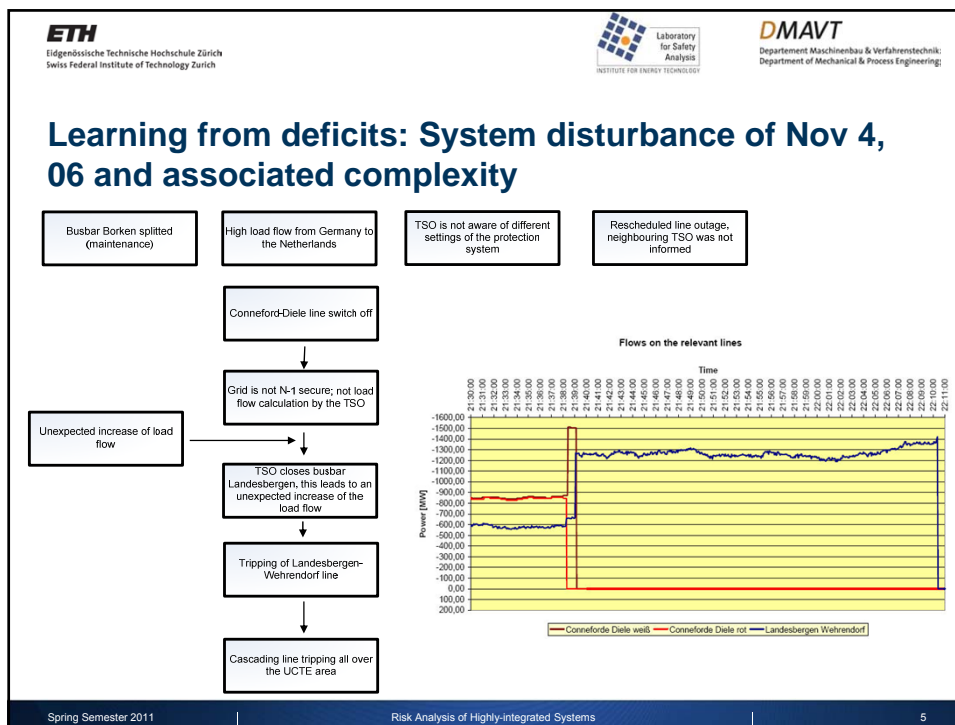
- conjunction: AND ( $\wedge$ ,  $\cap$ )
- disjunction: OR ( $\vee$ ,  $\cup$ )

Labelling of the probabilities:

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

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

Spring Semester 2011
Risk Analysis of Highly-integrated Systems
4



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

Spring Semester 2011

Risk Analysis of Highly-integrated Systems

7

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

ETH

Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

DMAVT

Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

## Concepts and Definitions

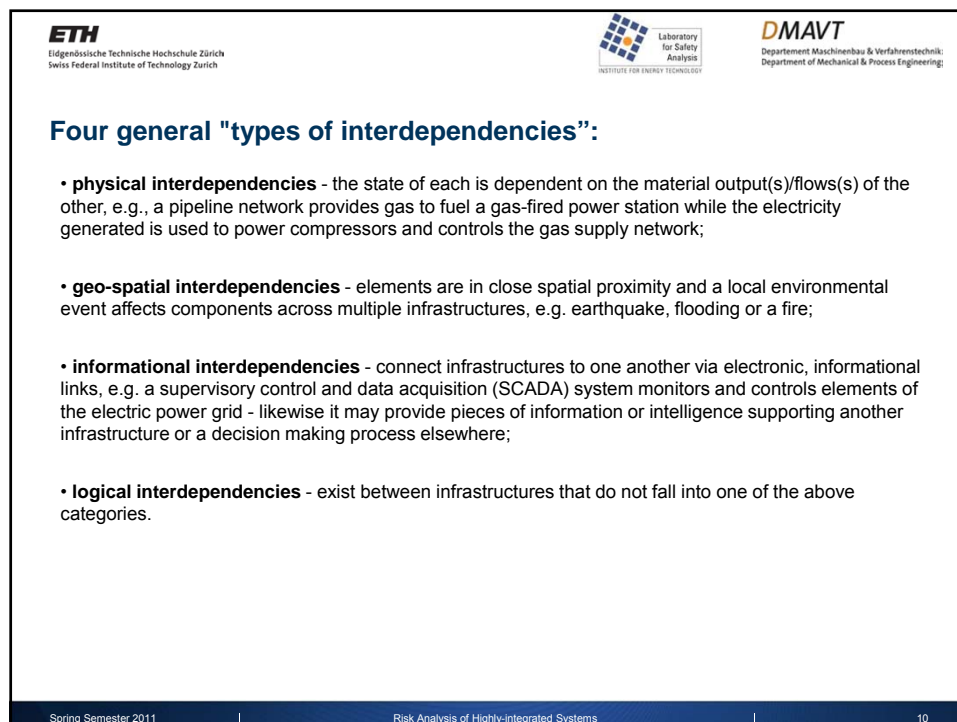
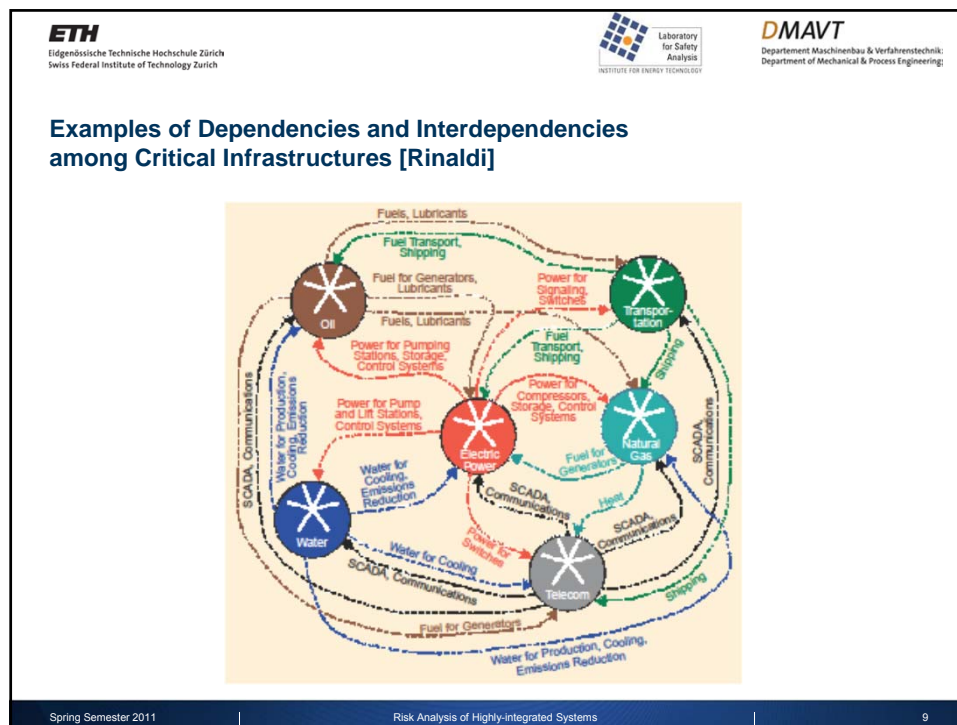
**Dependency:** A linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other. That is, infrastructure  $i$  depends on  $j$  through the link, but  $j$  does not depend on  $i$  through the same link.

**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.

Spring Semester 2011

Risk Analysis of Highly-integrated Systems

8



**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

### Dimensions for describing infrastructure interdependencies [Rinaldi et al.]

Spring Semester 2011 | Risk Analysis of Highly-integrated Systems | 11

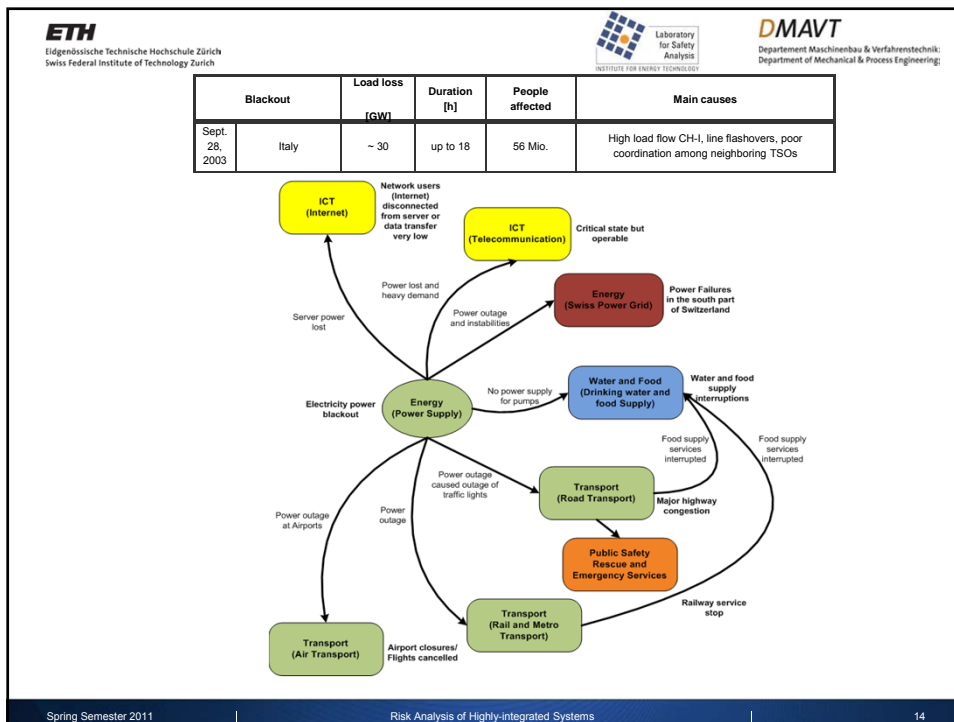
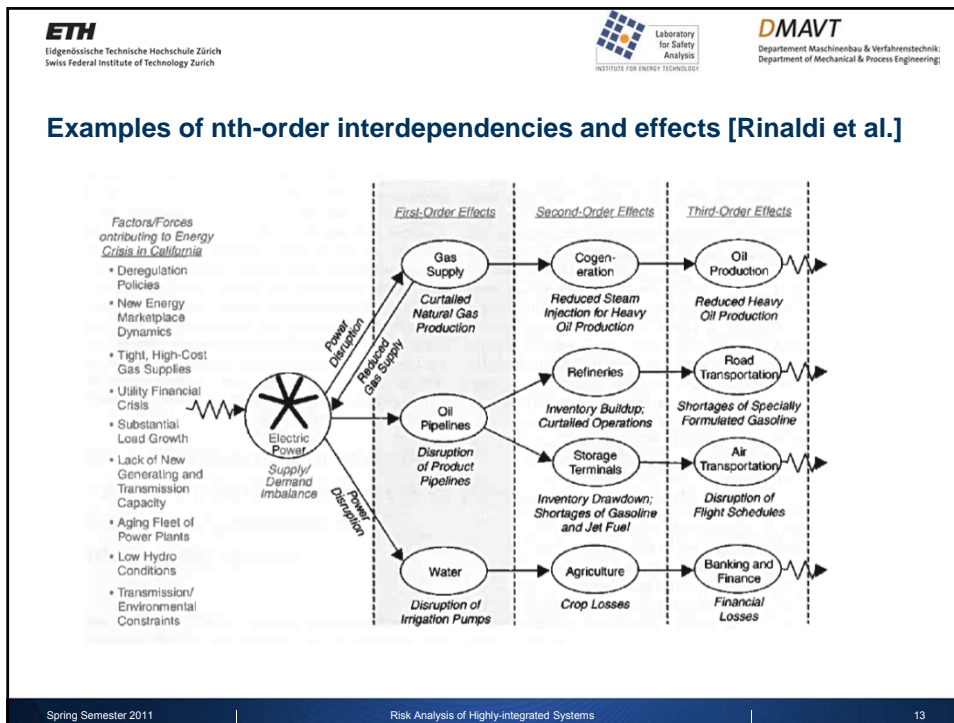
**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Departement Maschinenbau & Verfahrenstechnik  
Department of Mechanical & Process Engineering

### Infrastructure interdependencies (Hurricane Katrina)

Spring Semester 2011 | Risk Analysis of Highly-integrated Systems | 12



**ETH**  
Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

**Laboratory for Safety Analysis**  
INSTITUTE FOR ENERGY TECHNOLOGY

**DMAVT**  
Department Maschinenbau & Verfahrenstechnik:  
Department of Mechanical & Process Engineering

## Illustrating (inter)dependencies: Telco mini-blackout

Major telecommunication service node affected in Rome, 2 January 04 :

- At 5:30 breakage of a cooling water pipe of air-conditioning plant caused flooding of the first floor (cables of nodes located beneath)
- Telco devices for voice services were flooded (connecting different operators for fixed and mobile services)
- Fire Brigade arrived at 7:30 for pumping out water, technicians had to shut down the air-conditioning plant before repair
- Several devices failed for short circuit, main power supply got lost
- Emergency diesel generators failed to start due to flooding
- Batteries provided power to supply still working devices, finally for five minutes last working devices were not powered at all.

Source IRRIS

Spring Semester 2011 | Risk Analysis of Highly-integrated Systems | 15

