

# Risk Analysis of Highly-integrated Systems

Dozent: Prof. Dr. W. Kröger, [kroeger@mavt.ethz.ch](mailto:kroeger@mavt.ethz.ch)  
Assistenz: Patrick Probst, [probst@mavt.ethz.ch](mailto:probst@mavt.ethz.ch)  
Cen Nan, [nan@mavt.ethz.ch](mailto:nan@mavt.ethz.ch)



# Risk Analysis of Highly-integrated Systems

Fundamentals I: key terms, analytical goals and focal points, notion of system complexity, set of failures, hazards and threats, management tasks



## Introduction to the topic with a specific case:

### Italian Blackout, September 28, 2003

- 3:00 AM Italy imports 6.9 GW, 25% of the country's total load, 300 MW more than scheduled
- 3:01 Trip of the 380 kV line Mettlen-Lavorgo (highly loaded) caused by tree flashover; overload of the adjacent 380 kV line Sils-Soazza
- 3:11 ETRANS (CH) informs GRTN (I): Request by phone to reduce the import by 300 MW (not enough)
- 3:21 GRTN reduces import by 300 MW
- 3:25 Trip of the Sils-Soazza line due to tree flashover (at 110% of its nominal capacity); the Italian grid loses its synchronism with the UCTE grid; almost simultaneous tripping of all the remaining connecting lines
- 3:27 Breakdown of the Italian system, which is not able to operate separately from the UCTE network (instabilities); loss of supply
- 9:40 PM Restoration of the Italian system completed



### Impact on Population - strong

- People affected: 56 Million
- Hundreds of people have been trapped in elevators.

### Economic Losses - moderate

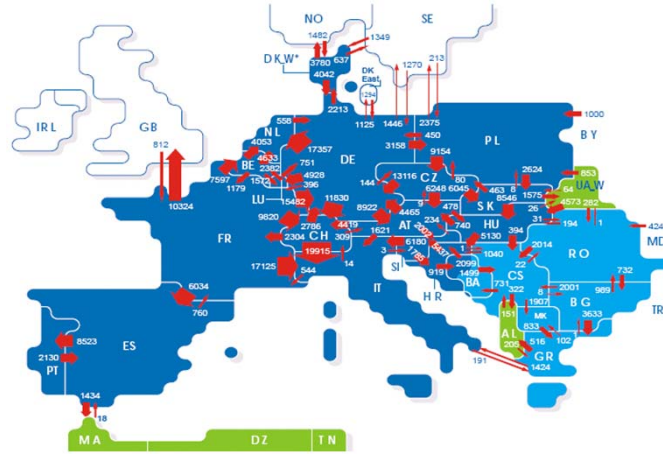
- About 120 million €
- Several hundred k € due to the interruption of continuously working industries .

### Impact on Dependent Critical Infrastructures - varying

- Transportation: ~110 trains , 30'000 passengers, Subways in Rome and Milan. Flights cancelled or delayed. Outage of traffic lights partly led to chaotic situations in major cities, no severe accidents.
- Water supply: Interruptions for up to 12 hours.
- I & C: Telephone and mobile networks in a critical state. Internet providers shut down their servers (data transfer rate went down to 5% of normal).
- Hospitals: No serious problems due to the use of diesel-driven generators..

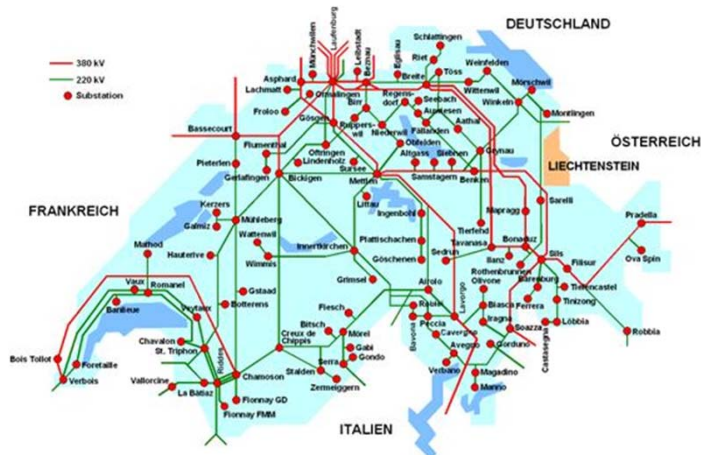


## Highly integrated Systems: (1/2)



Transboundary energy flows (GWh) in 2004 [UCTE 2006]

## Highly integrated Systems: (2/2)



swissgrid

## Risk as a Central Term

Problems to solve:

- Identification
- Assessment
- Management

of **threats and risks** to technical installations in a context by applying methodologies of natural and engineering sciences.

Factual (“calculated”) risk – as opposed to the perceived risk – calls for

- Verification
- High degree of independence from observer / analyst
- Proper application of a specific methodology
- Presentation of results with indication of uncertainties

## Definition of Factual (mathematical) Risk

**General**

- Possibility that damage results from a state or process.

**Risk**

- Measure for hazards. It is a function of the frequency  $F$  of an undesirable event and the consequences  $C$  (ISO/IEC Guide 73, 2002: combination of the probability of an event and its consequence).

**Usual calculation (“insurance formula”) without aversion**

- $Risk = f(F, C) = F \cdot C$  respectively  $\sum_i F_i C_i$  (for more than one event)

**Weighted risk**

- In order to consider the so called aversion, the consequences are weighted above a certain threshold value  $a$  using a coefficient  $\alpha > 1$  (between 1.2 and 2)

$$Risk = \begin{cases} F \cdot C & : C < c_i \\ F \cdot C^\alpha & : C \geq c_i \end{cases}$$

- For infrastructures (in addition) also the frequency of service interruption with its resulting consequences for the people concerned.

## Systematics of Factual (mathematical) Risks

### Statistical risk

- Basis: available, directly usable data, e.g. [number of accidents/year];
- Experience from a large number of similar events.
- Collection of directly usable observations on system/event level.

### Real risk

- Basis: a complete sample of all possible information and data of an event
- After prolonged observation (infinite) a complete set of data is available, provided circumstances/conditions remain unchanged. Not determinable!

### Predicted risk

- Basis: failure scenarios and models for the prediction of rare or not yet occurred events, e.g. fault tree analysis
- Events are assessable by using the probability of their occurrence
- Use of observations (statistical data) at component's level

## More 'Risk' Terms

### Maximum acceptable risk (Grenzrisiko)

- Highest degree of justifiable risk regarding a specific action or state.

### Residual or remaining risk (Restrisiko)

- Descriptive: risk which remains after implementation of all planned safety measures, arising from
  - consciously accepted risks,
  - mis-assessed risks, and
  - unrecognized risks.
- Normative: Admissible risks following risk acceptability assessments.

## Elements of Risk: Damage

- General: negative effects of an undesirable event or procedure or an undesirable impairment of an object to be protected as a consequence of harmful events.
- In a narrow sense: degradation or impairment of the integrity of an object of concern resulting in a reduction of reliability, safety or capability.
- Damage quantification is not always well defined: depending on context, we may obtain different results.
- Example: counting the severely injured people after an accident.

## Common Damage Measurements with [Measuring Units]

- Impact of undesired event affects following:

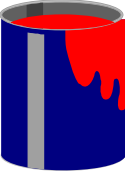
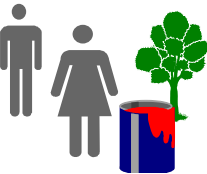
Inside installation	Outside installation
Employees, Persons [number] <ul style="list-style-type: none"> <li>• Death: immediate, possible</li> <li>• Injuries: light, heavy</li> <li>• Health damage: temporary, permanent</li> </ul>	The public [number] <ul style="list-style-type: none"> <li>• Death: immediate, possible</li> <li>• Injuries: light, heavy</li> <li>• Health damage: temporary, permanent</li> <li>• Evacuations: temporary, permanent</li> </ul>
Installation [quantity of released substances, energy] <ul style="list-style-type: none"> <li>• Undesired dangerous state of installation (nuclear meltdown, "runaway" reaction)</li> </ul>	Environment [quantity of released substances, energy, etc.] <ul style="list-style-type: none"> <li>• Released substances [quantity, toxicity, energy units]</li> <li>• Concentration [mass and volume units]</li> <li>• Contamination [area and mass units]</li> </ul>
Cost/Investment [monetary units] <ul style="list-style-type: none"> <li>• microeconomic</li> <li>• management</li> </ul>	Cost [monetary units] <ul style="list-style-type: none"> <li>• macroeconomic</li> </ul>
Loss of production [time, currency units]	Loss of area utilization [area and time units]

## Elements of Risk: Frequency

**Frequency of an event:** frequency is often used wrongly instead of other terms, although there are clear definitions:

- **Frequency (Häufigkeit):** a frequency denotes a number.
- **Relative frequency (relative Häufigkeit):** number of cases in which an event happened, divided by the number of cases in which the event could have happened (dimensionless)
- **Rate:** mathematical construct, which measures the actual change of a number in units of change of another number (usually time). Empirically, it can be done by estimating an average (relative frequency) over a long time interval.
- **Frequency (Frequenz):** can also be time related.
- **Probability (Wahrscheinlichkeit):** “a real number in the scale 0 to 1 attached to a random event.”(ISO 3534:1993). Defined by the axiom system of Kolmogorov.

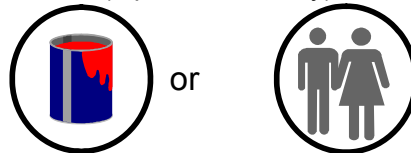
## More Precise Definition of Terms

<b>Danger (Gefahr)</b>	<b>Hazard (Gefährdung)</b>
<p>A danger is a state, factor [circumstance], or action which may cause damage to persons, the environment and/or goods. <b>Examples:</b> tank filled with gasoline, a knife</p>	<p>A hazard is a tangible, concrete danger to persons or goods, specified in its nature, extent and course – a “specified potential”.</p>
	



## Security

Control or isolation of a specified hazard (= active security) and/or the defence of a hazard (= passive security)



### Reliability (DIN 40042, 12/90)

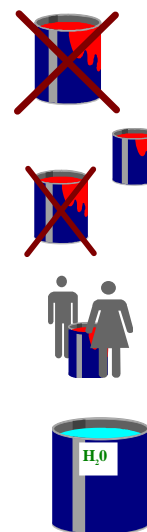
The ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90] (mission without maintenance). Reliability is expressed as probability.

### Availability (DIN 40042, 12/90)

The probability of a unit to be in working order at the time  $t$  (including maintenance work).

## Definition of Vague Terms: Safety

- **absolute sense:** attribute defined by the absence of any danger (ultimately unobtainable).
- **relative sense:** attribute defined by (a) the absence of a specific danger, (b) involving a comparatively low and thus acceptable risk or (c) complying with normative requirements.
- **subjective:** perceived certainty of danger protection.
- **intrinsic:** attribute which mandatorily limits to a predetermined or acceptable extent or excludes a danger to a state, process or product.



## Conclusion

In risk analysis we find standardized, but also „vague“ terms that can be defined or understood in different ways, depending on the context. The interdisciplinary approach in risk analysis requires Definitions. Without an agreement on terminology “expensive” misunderstandings can occur.

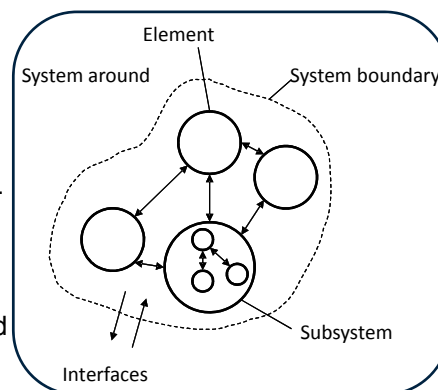
## Definition of a System

**Definition:** „A system is a deterministic entity comprising an interacting collection of discrete elements“ [1].

A System consists of:

- Boundaries.
- Elements: notional or real units which can be a system themselves.
- Interactions: establish a structure between the elements.

One can distinguish between open and closed systems.



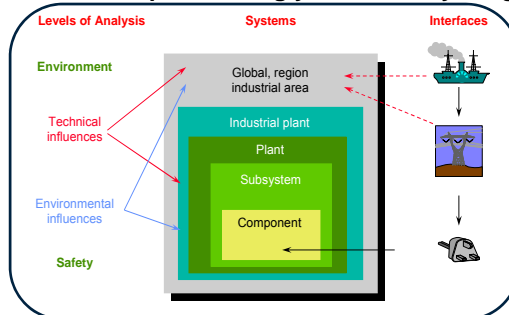
[1] Roberts, N.H., et al., *Fault Tree Handbook (NUREG-0492)*. 1981, Washington, D.C.: U.S. Nuclear Regulatory Commission. 1-209.

## System Boundaries

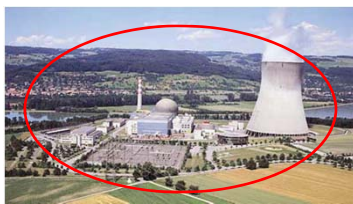
The boundaries of a system are not always obvious and per se given.

**Example:** In a technical system like an industrial plant the boundaries are not clearly definable. Moreover they are interconnected with other systems like transport infrastructure and the environment and may differ depending on the goals of the analysis.

→ **System boundaries depend strongly on the analysis' goals.**

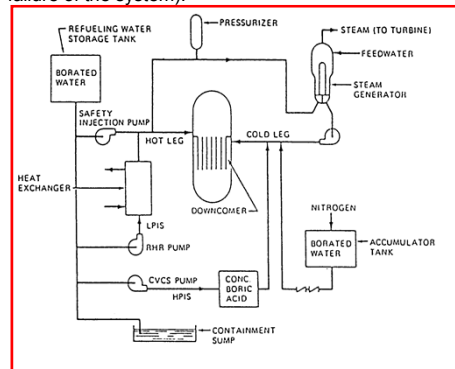


## System Boundaries by Example



Risk due to operation of a nuclear power plant.

Reliability/availability of an emergency core cooling system (core damage frequency contribution due to failure of the system).



## Complicated vs. Complex

**Complicated Systems** (mechanical watches, aircraft, **power plants, etc.**) **Complex Systems** (stock market, **www**, power grid, 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.
- 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.

## Examples of Complicated and Complex Systems

**Complicated Systems:** Mechanical watches, Boeing 747, ...



**Complex Systems:** Stock market, Power grids, Highways, World Wide Web, Natural ecosystems, Social networks, ...



**The nation's Power Grid is an example of a complex system that evolves continually.**

It must respond to the challenges such as

- incorporating new, intermittent sources at new locations such as wind and solar,
- supporting a market in bulk electricity.
- accommodating new loads such as electric cars,
- exploiting the ongoing advances in communications, computer power, materials and devices.



Scrapping the Power Grid and redesigning it from scratch is not an option: advances must build on and coexist with components and technologies that are up to 50 years old.

Any redesign or upgrade affects how the engineering system is used and this, in turn, affects the requirements. **This interaction with and adaptation to the changing environment makes the evolving system more complex.**

## Questions in risk analysis

- What can go wrong? (accident sequences, scenarios)
- What is the probability of these scenarios?
- What are the consequences?

## Set of multiple threats disclosing vulnerabilities

- **Natural events** such as earthquakes, hurricanes, tornados, severe flooding, or other (increasing) extreme weather conditions
- **Accidents or technical factors** leading to the debilitation of plants, networks and operations
- **Human factors** such as unintended failures, malicious physical or cyber-attacks
- **Market factors** e.g. economic pressure trading-off security factors
- **Policy factors** such as misusing “energy” for political purposes

## Risk management

- Coordinated activities to direct and control an organization with regard to risk (ISO/IEC Guide 73, 2002)
- A systematic approach for identification, quantification, assessment, optimization, monitoring and communication of risks, which can affect the health or security of people or the environment and are related to an activity, a function or a process. It is a stepwise process that allows a continuous enhancement in the context of decision making. It can be applied at any stage of an activity to minimize losses and take advantage of possibilities:
  - R & D
  - Design, planning and site selection
  - Construction
  - Operation
  - Emergency preparedness and planning
  - Accident management and emergency measures
  - Decommissioning, removal.
- Risk management has to be highly integrated in the continuous operation of any organisation.

## Relationship between terms: “Risk Analysis” and “Risk Management“ (ISO/IEC Guide 73, 2002)

Risk Management ... <i>coordinated activity to direct and control</i>	
Risk Assessment	
Risk Analysis	
Source Identification... <i>potential for a consequence (= hazard)</i>	
Risk Estimation ... <i>events, prob., consequences</i>	
Risk Evaluation ... <i>against given risk criteria</i>	
Risk Treatment ... <i>selection and implementation of measures to modify risks</i>	
Risk Avoidance ... <i>decision not to become involved, or action to withdraw</i>	
Risk Optimization ... <i>process</i>	
Risk Transfer ... <i>burden sharing</i>	
Risk Retention ... <i>acceptance of burden/benefit ... unidentified risks</i>	
Risk Acceptance ... <i>decision (by whom?)</i>	
Risk Communication ... <i>sharing info between decision maker and other stakeholders</i>	

## Risk management approaches for technical systems

- **Trial-and-error** with organized feedback of experience; Design and adherence to a body of rules and regulations
  - Can only be applied, if a failure does not lead to extreme high damage
- **Risk-based approach (analysis and minimization of Risks)**  
Systematic identification of hazards and scenario analysis.  
Identification of weak spots and optimization possibilities using experience / know-how  
⇒ requires detailed description and knowledge of the system
- **Precautionary principle**  
Extrapolatory analysis of negative and positive implications and the comparison to alternatives
  - Useful when the degree of uncertainty is high; protects against “unpleasant surprises”

## Safety oriented approach as basis for Risk Management

