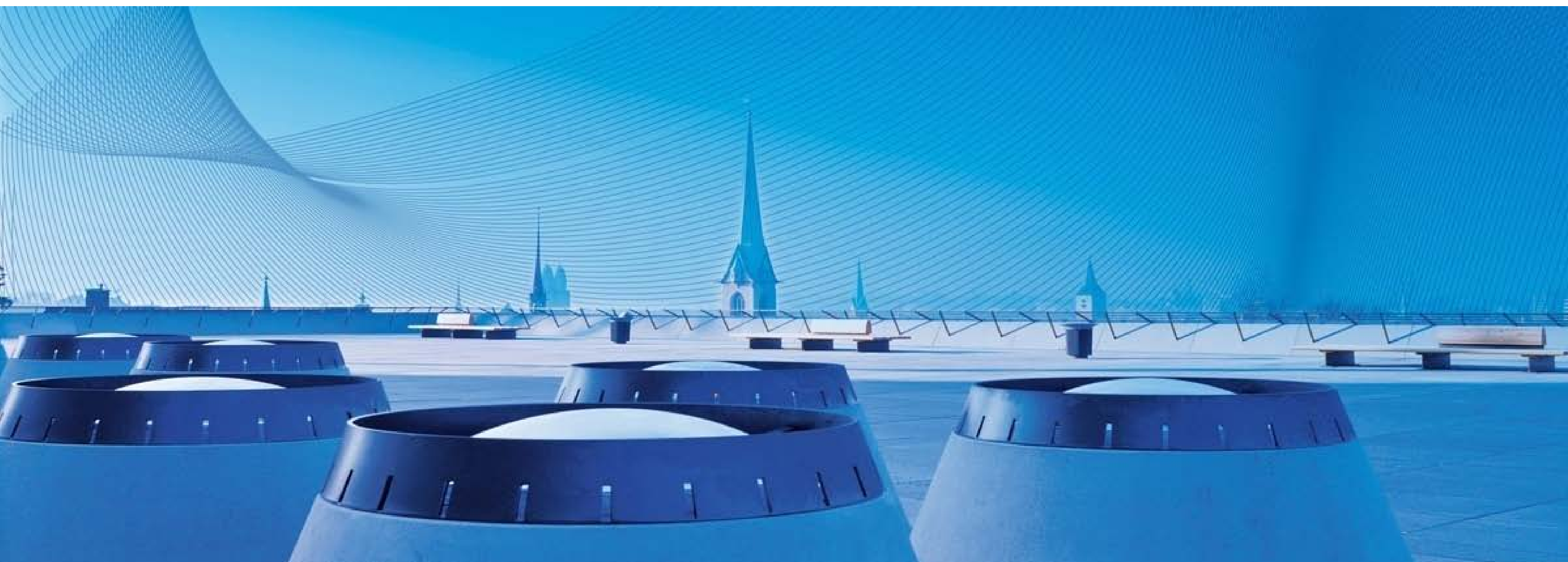
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Methods of Technical Risk Assessment in a Regional Context

- Wolfgang Kröger, Professor and Head of former Laboratory for Safety Analysis (www.lsa.ethz.ch)
  - Founding Rector of International Risk Governance Council Geneva (www.irgc.org)
    - Executive Director, ETH Risk Center (www.riskcenter.ethz.ch)

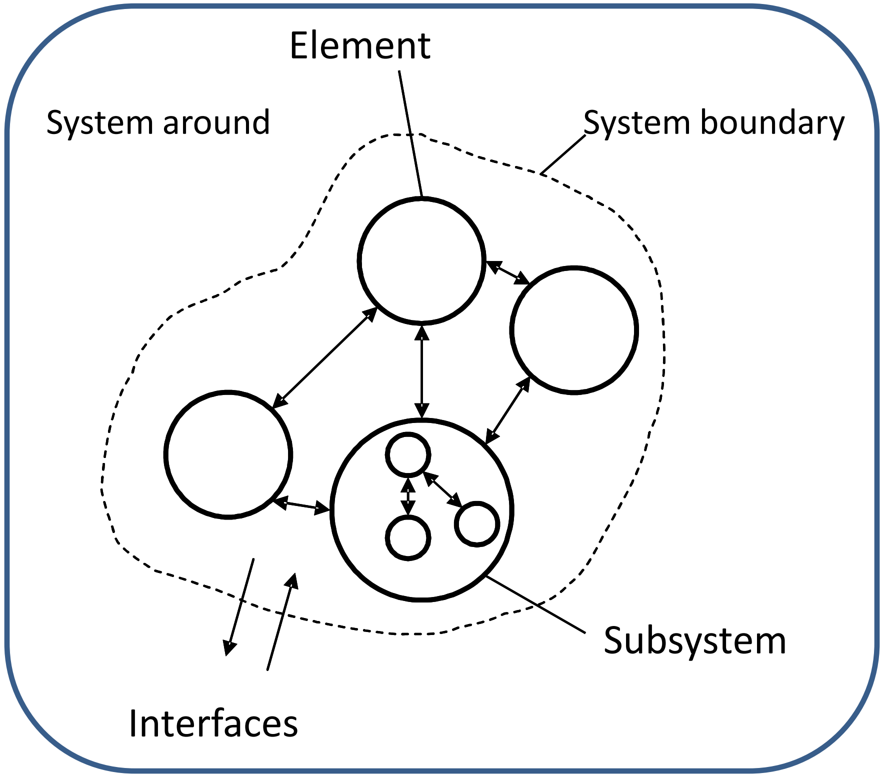


Challenges to Regional Assessment, Defining a Region and Systems within Conceptual and Methodical Frameworks

Contents:

Definition of a System

Definition: A system is a deterministic entity comprising an interacting collection of discrete elements.



A System consists of:

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

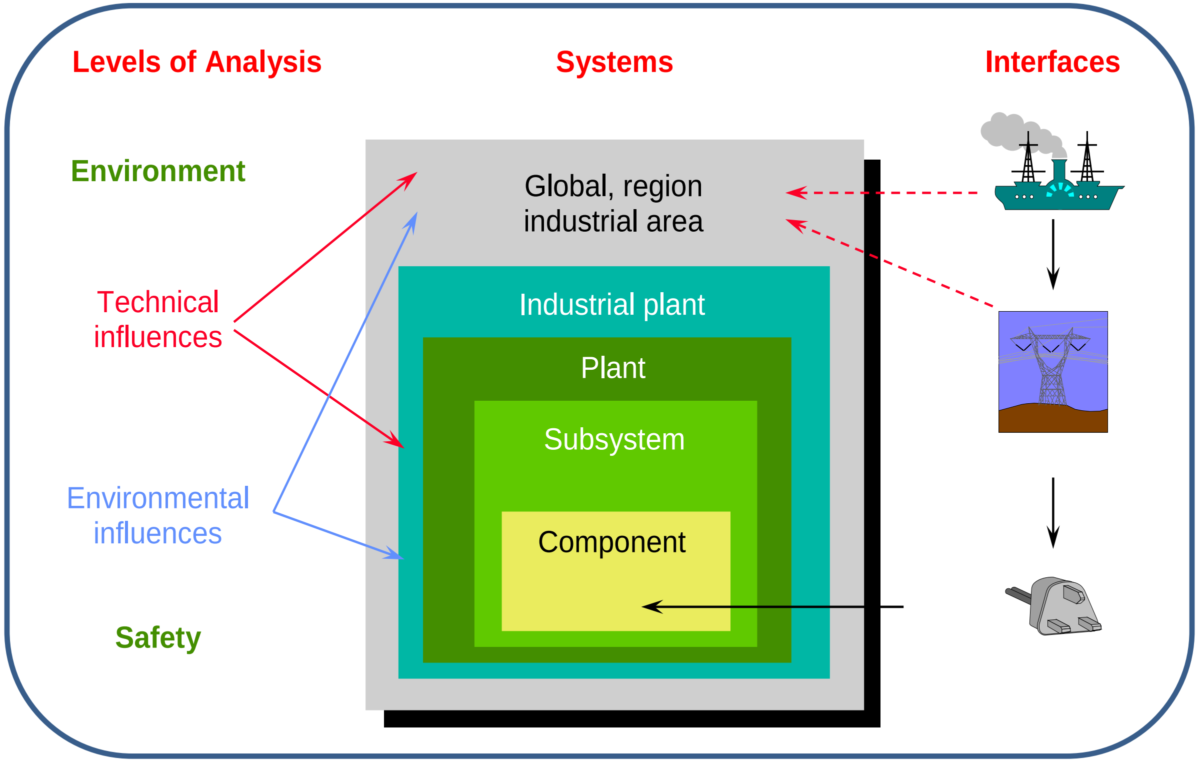
One can distinguish between open and closed systems.

System Boundaries

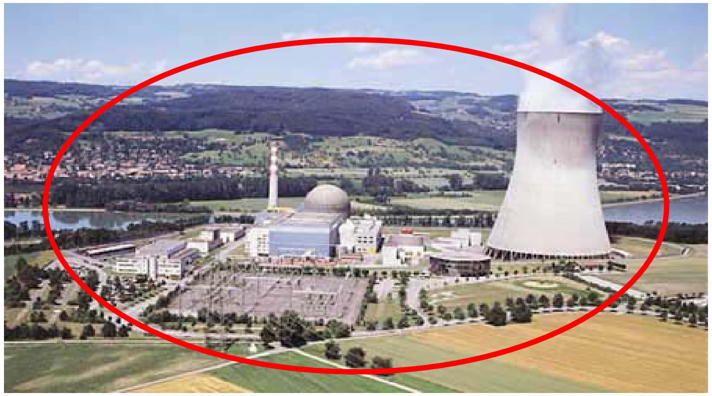
The boundaries of a system are not always obvious and per se given.

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.

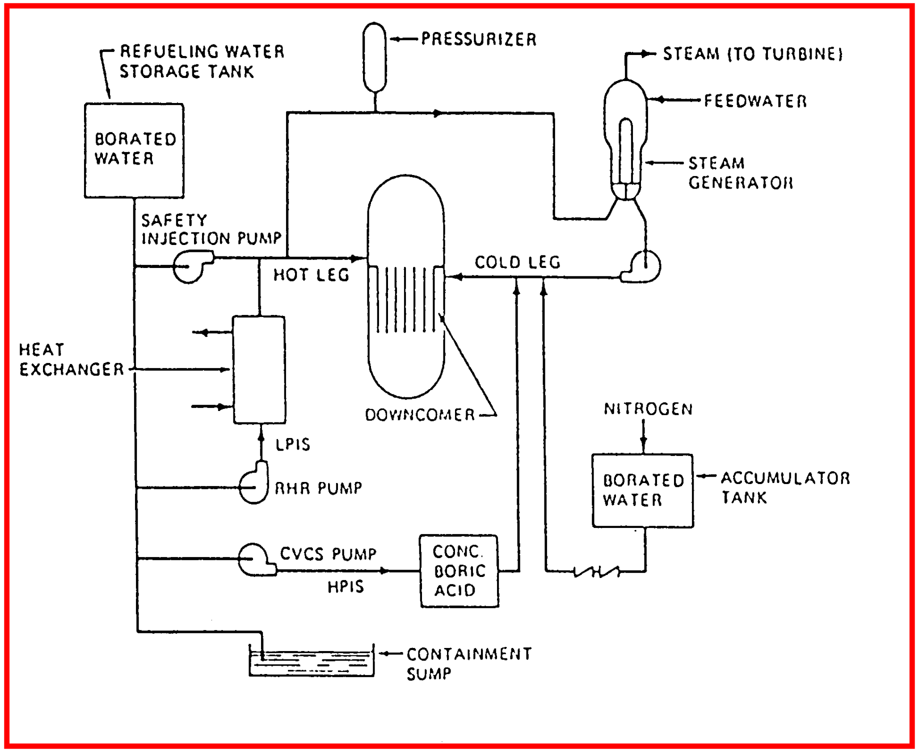


System Boundaries by Example



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

- Large number of highly connected components.
- Components have well-defined roles and are governed by prescribed interactions.
- Structure remains stable over the time.
- Low dynamical behavior.
- No adaptation. One key defect may bring the 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

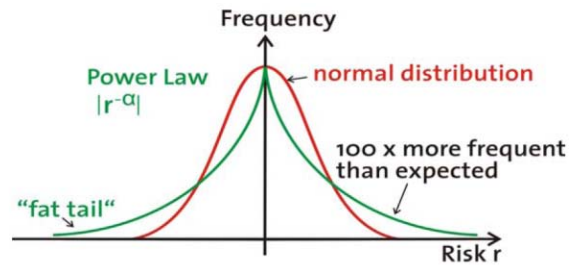
- Large number of highly connected components.
- Rules of interaction between the components may change over time and not be well-understood.
- Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not obvious.
- System responds to external conditions and evolves.
- 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.
- Tend to create surprise with their behavior.
- The overall behavior cannot be described simply in terms of their building blocks. The whole is much more than the sum of its parts.

*In general usage, complexity tends to be used to characterize something with many parts in intricate arrangement. The study of complex linkages is the main goal of complex system theory (Wikipedia).

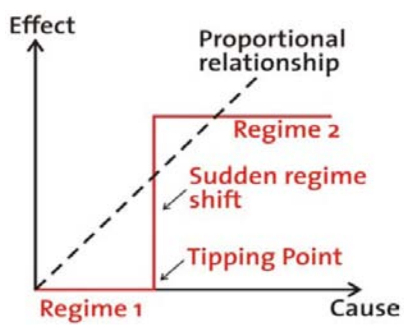
Understanding complex systems

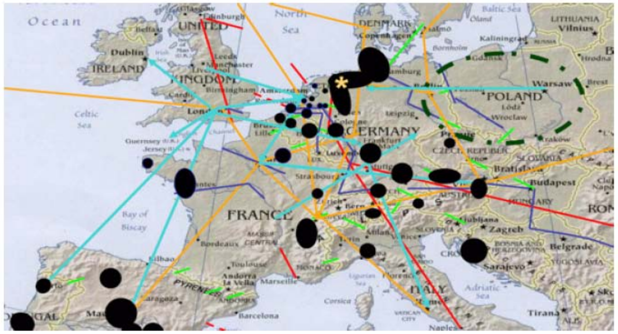
Examples: Power Grids, Traffic Flows, Financial Markets, Large Supply Chains, etc.

1. Large number of interacting (mutually coupled) system elements.



2. Element interactions are usually non-linear.





Causes & effects are not proportional to each other.

Network interactions inducing cascading effects.

3. Dynamic rather than static & probabilistic rather than deterministic behavior.

IRGC – Emerging Risks, 2010

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 o

Any redesign or upgrade affects how the engineering system is used and this, in turn, affects the requirements.

Principle of Reductionism and Holism

Holism and reductionism can be seen as complementary viewpoints, in which case they both would be needed to get a proper account of a given system.

Reduction

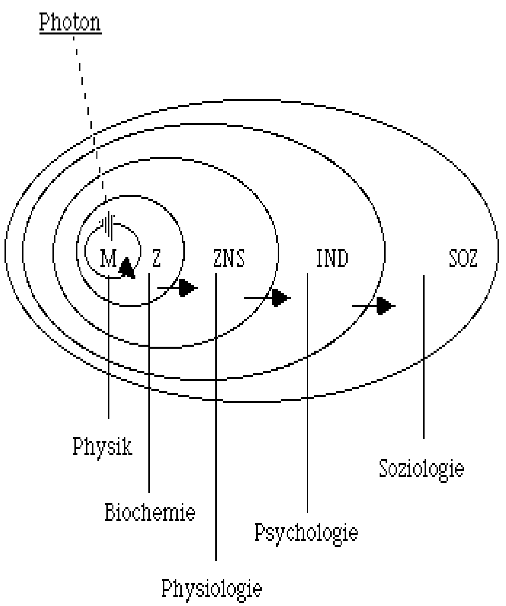
Problems are divided into distinct parts and the parts are examined separately.

- The division into parts will not distort the phenomena being studied.
- The components are the same when examined singly as when they are playing their part in the whole.
- The principles governing the assembling of the components into the whole are straightforward.
- In general for solving "complicated" problems.

Holism

Problems cannot be meaningfully solved by examining component parts in isolation.

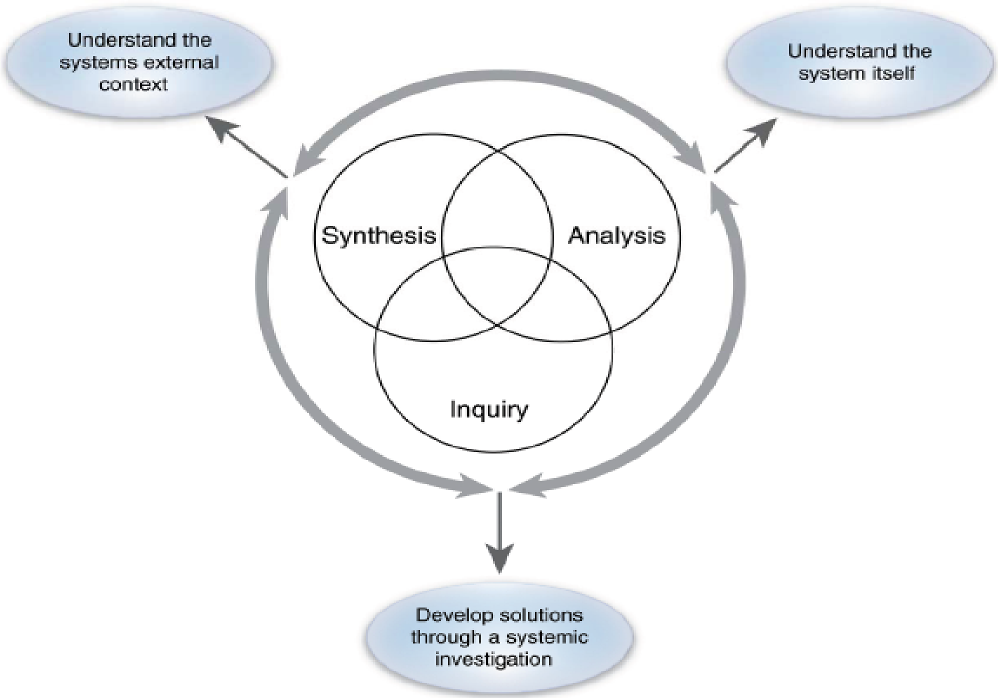
- *"The whole is more than the sum of its parts." (Aristotele)*
- Emergence
- Integration
- In the latter half of the 20th century, holism led to system thinking and its derivatives, like the sciences of chaos and complexity.



M...molekulare Ebene
Z...zelluläre Ebene
ZNS...zentralnervöse Ebene
IND...Ebene des individuellen Bewußtseins
SOZ...Ebene des gesellschaftlichen Bewußtseins

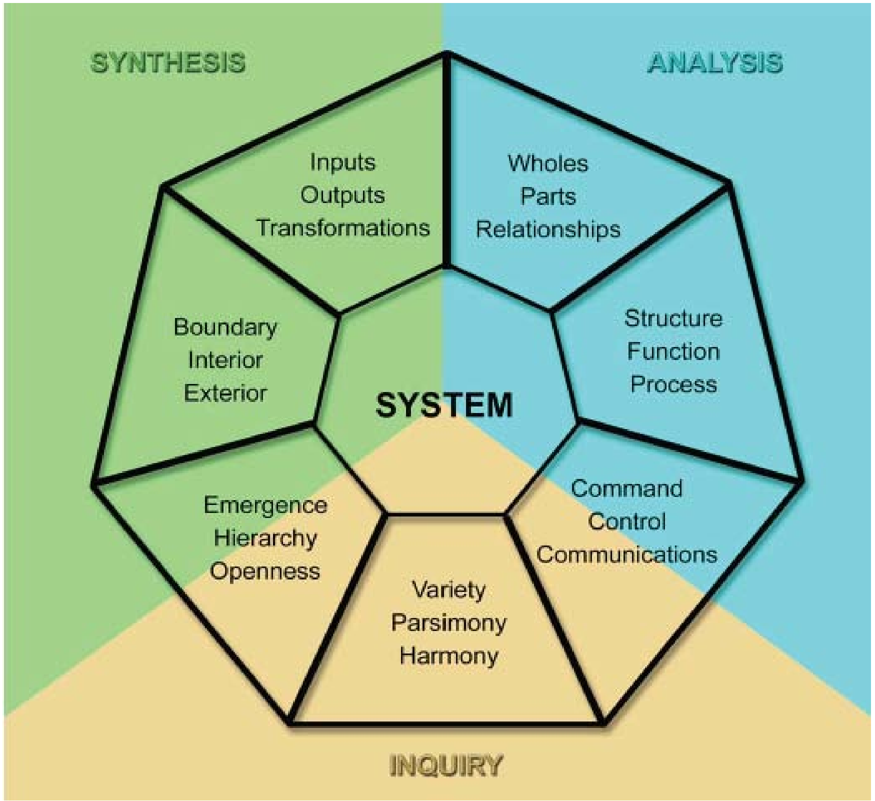
Systems Thinking

Think about Complexity in a new way.



Development of resilient systems requires systems thinking.

The Conceptagon



Framework of Application of Systems Thinking Principles

Explanations on the Framework of Systems Thinking Principles

Boundary Depiction

- *Interior*
- *Exterior*

Purpose of the System

- *Inputs*
- *Outputs*
- *Transformations*

How do the Parts Create the Whole ?

- *Wholes*
- *Parts*
- *Relationships*

How does the System Work ?

- *Structure*
- *Function*
- *Process*

What is the Governance Model ?

- *Command*
- *Control*
- *Communications*

How Flexible/Robust is the System?

- *Variety*
- *Parsimony*
- *Harmony*

How Permeable is the System Boundary ?

- *Emergency*
- *Hierarchy*
- *Openness*

Definition of a Region

Questions:

- What is a region?
- How to define a region?
- Where are the boundaries of a region?
- What resolution/scale is necessary/makes sense?

Suggested factors for the definition of a region:

- The goal/aim of the analysis must be clearly defined
- The area should be selected for physical, industrial and economic characteristics and defined on the basis of facilities and systems of concerns
- Potential areas that can be directly affected
- Hard boundaries should not be drawn before an initial hazard analysis and prioritization has been made.

The scope of regional risk assessment studies are:

- Sources of continuous emissions and accidental releases
- Scenario for accidental states
- Risk assessment for environment and public
- Safety/risk management actions

(see [2])

Visualisation of hazardous potential in the canton Basel-Landschaft

- Based on the Swiss Ordinance of February 1991 on Protection Against Major Accidents (Störfallverordnung, StFV).

- Evaluation of production units (like loading infrastructure, production plant, etc.).

- Only the most dangerous substance is taken into account, with regard to the amount, state of aggregation and the specific characterisations.

- The considered aspects of danger are:
  - What happens when gaseous substances are set free by a leakage?
  - What is the impact of heat and fire?
  - What effect has a fire or heat on toxic substances and products?
  - How explosive is the substance?
  - What effect has a leakage of fluid substances to soil, ground and surface water?
  - Can the water for fire-fighting lead to flooding?

- The index value (acceptable <2, intersection ≥ 2 and < 4, unacceptable ≥ 4) is represented on a logarithmic scale.

Source: http://www.geo.bl.ch/parzis/SIT_Erlaeuterungen_Gefahrenquellen.PDF

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

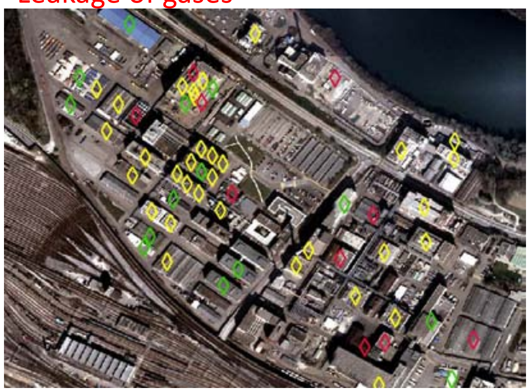
DMAVT
Departement Maschinenbau & Verfahrenstechnik
Department of Mechanical & Process Engineering

Analysed Scenarios based on Companies handling Hazardous Substances

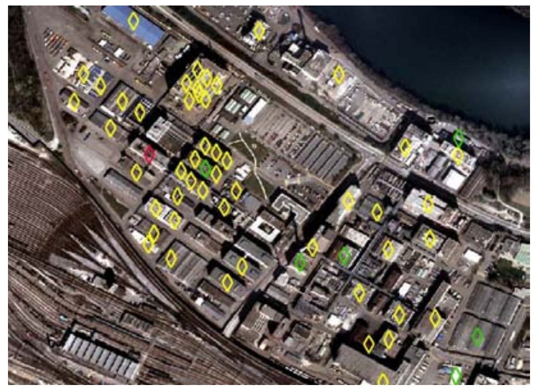
Störfallbetriebe pro Gefahrenpotential

- Gefahrenpotential-Index < 2
- Gefahrenpotential-Index >=2 und < 4
- Gefahrenpotential-Index >= 4

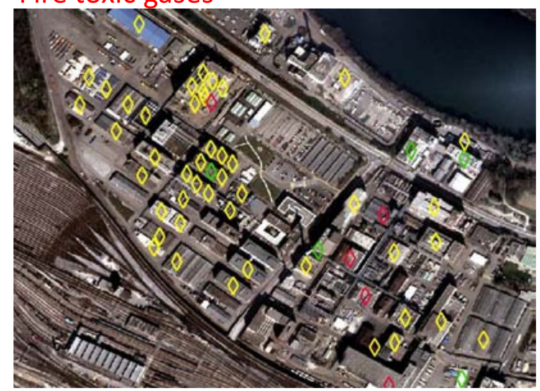
Leakage of gases



Heat fire



Fire toxic gases

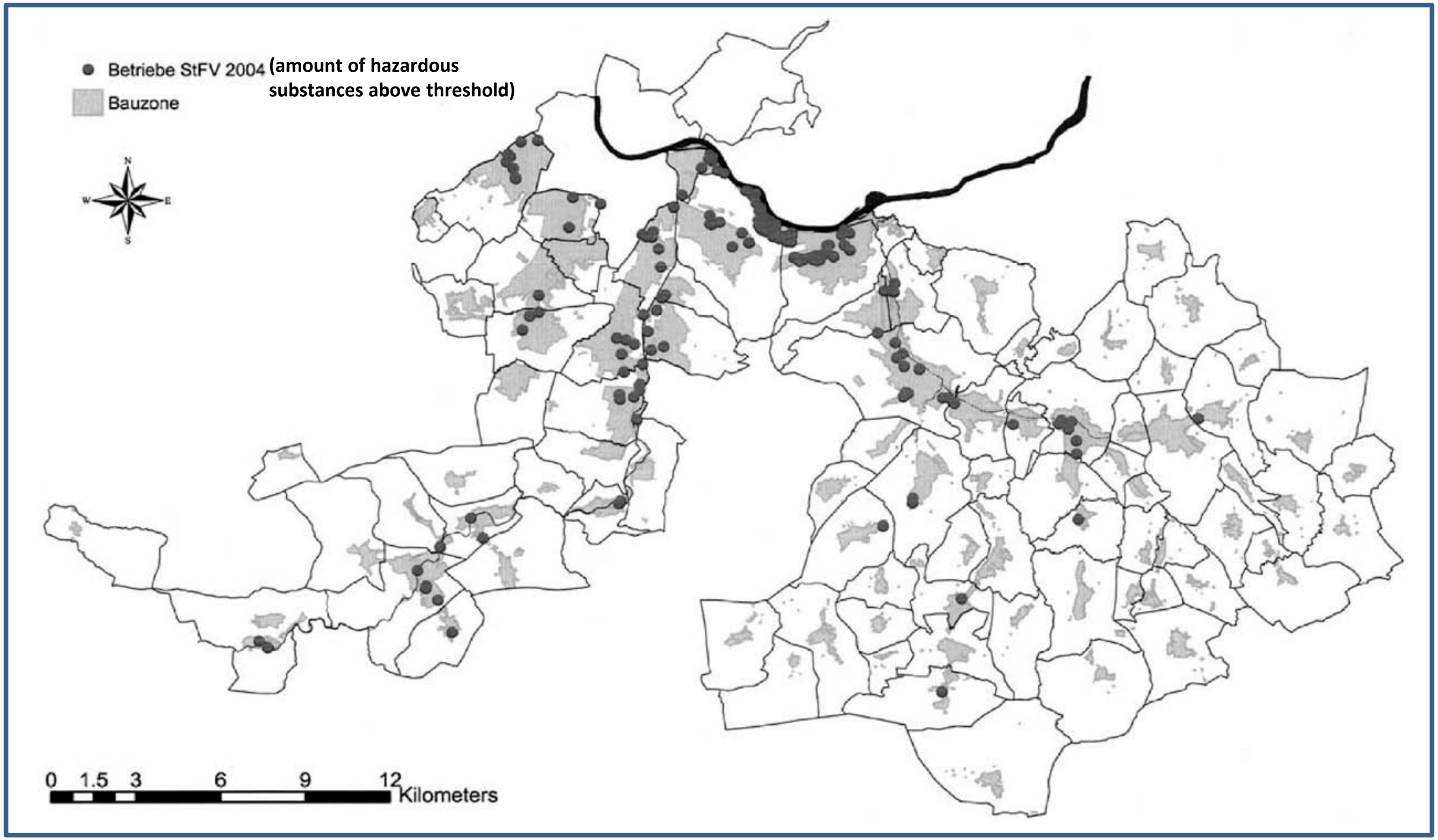


Explosion

Liquid leakage

Flooding by fight-firing water

Companies in Canton Basel-Landschaft, which are subject to the StFV

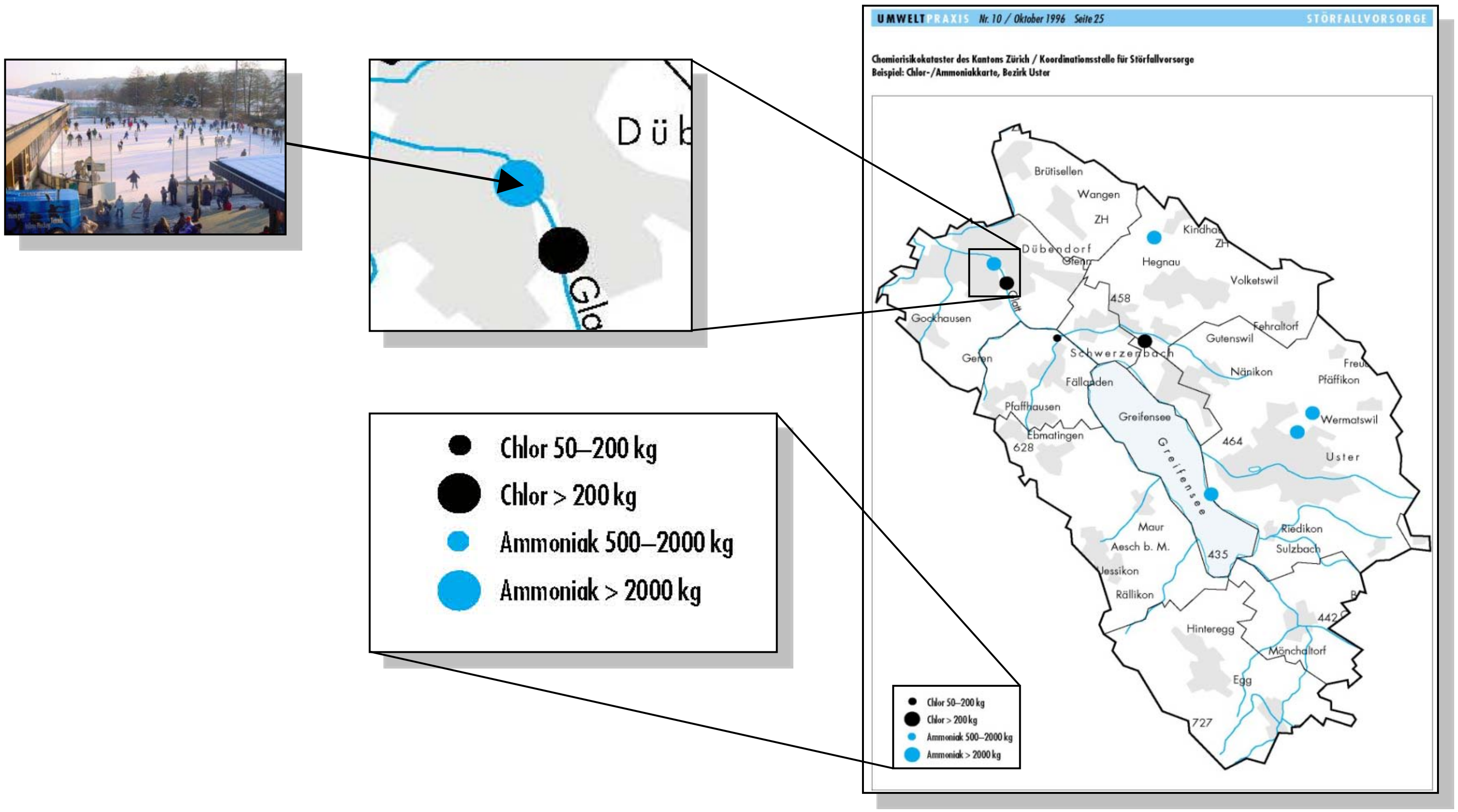


Source: http://www.baselland.ch/docs/bud/sit/karte-stoerfall.pdf

Chemical Hazard Cadastre

(Chemierisikokataster des Kantons Zürich)

Example: chlorine and ammonia map, district Uster.



Source: http://www.stoerfallvorsorge.zh.ch/internet/bd/awel/awb/sv/de/dokumente.html

Hurricane Katrina – Impacts on the New Orleans urban water system

- August 29, 2005: Landfall of Katrina; power provider Entergy fails due to the storm; the New Orleans Sewerage and Water Board (S&WB) can switch on their backup power plant and can keep the system running.

- August 31: Flooding of New Orleans due to the destroyed dams of lake Pontchartrain
  1. shut-down of the backup power plant
  2. purification facilities fail and water pressure is lost
  3. contaminants as from broken sewage pipes enter the system
  4. “boil water order” of the Department of Health and Hospitals

- Water purification plant rapidly restored (few days)

- The distribution system is heavily damaged due to debris such as houses, trees and cars; some hard hit areas are removed from the system

- October 6: the "boil water order” for the city of New Orleans was lifted by the Department of Health and Hospitals for all areas of the city west of the Industrial Canal.

- Restoration of the whole system for potable or drinking water is still in progress. Although the water, sewage and drainage services are available throughout the city.

Hurricane Katrina - Emergency measures and responsibilities

- The Louisiana plan: Evacuation is the responsibility of the local parish.
- The New Orleans evacuation plans: "The primary means of hurricane evacuation will be personal vehicles. School and municipal buses, government-owned vehicles … may be used to provide transportation for individuals who lack transportation and require assistance in evacuating." 27% of the New Orleans households were without privately-owned transportation (approximately 120'000 people).
- August 26: Governor Blanco activates the National Guard of Louisiana. Red Cross relief in New Orleans remains forbidden.
- August 27: Mandatory evacuation of New Orleans (by Mayor Nagin).
  White House authorizing Federal emergency assistance for Louisiana. It authorizes FEMA and DHS[1] to coordinate disaster relief and required emergency measures for all parishes except the coastal parishes (like New Orleans).
- August 28: City buses transport citizens to the Louisiana Superdome (about 20'000 to 25'000 people).
- Additional help from outside was asked for by Mayor Nagin, but the coordination of transportation outside the parish is the responsibility of Governor Blanco.
- The request for Federal troops to support the National Guard of Louisiana removes the Governor from the command chain and sets the President in charge. This request was handed in one day after Katrina hit the city and much of it was under water.
- The security situation in New Orleans prevented humanitarian aid workers from entering the city safely.

Sources:
http://www.noaanews.noaa.gov/stories2005/s2495.htm
http://enr.construction.com/news/environment/archives/050902b.asp
http://www.nola.com/
http://en.wikipedia.org/wiki/Hurricane_Katrina
http://www.findarticles.com/p/articles/mi_qn4200/is_20060724/ai_n16640725

Lessons Learned from Hurricane Katrina *

- We live in a new "normal". Changed expectations, have to create a certain preparedness in our communities (e.g. by education, good public policy).

- Some supercritical infrastructures need emergency power supply, as main systems will fail; don't build buildings out of glass.

- 42% of the US population lives within 20 miles of oceans, and rich natural environments.
  Disasters have a worst impact on the "poor" : 70% of New Orleans' people comeback - the poor can no longer afford the city, e.g. due to tripling of insurance rates, causing a cultural shift

- 25% of the US gas comes out of the Gulf of Mexico which has the potential to disrupt the whole society/supply chain.

- Critical infrastructures are owned by the private sector - outsourcing means loss of impact, often redundancy.

- Need to integrate private industry (logistics) into national emergency planning and response.

- For very few $ invested in preparedness, we save 6 - 7$.

* according to LT General Russel L. Homore, commander of Federal emergency support

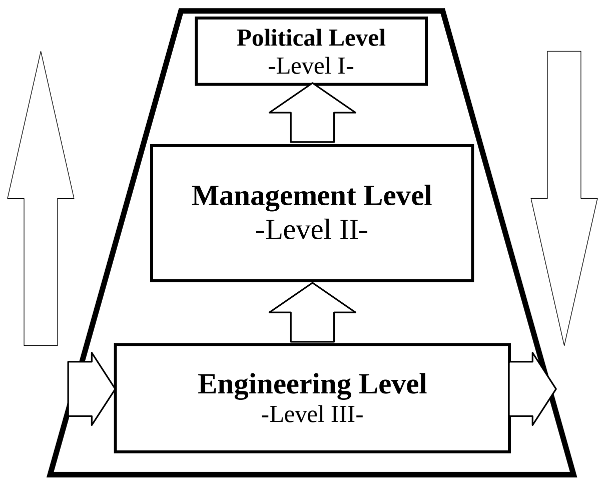
Regional Risk Assessment and Safety Planning

Regional risk assessment and safety planning is a co-ordinated strategy for risk reduction and safety management in a spatially defined region, across broad range of hazard sources.

It deals equally with normal operation of plants, as well as with accidental situations, including their synergetic effect.

Regional risk assessment differentiate in its respect from the risk assessment at plant level. It introduces more subjectivity and stakeholder interaction. As many as possible of the authorities within the risk management scope should become involved.

The hierarchical approach to problem solving in an integrated regional risk assessment and safety management:



(see [2])

Level I *(Political Level)*, specific use is addressed to multicriteria decision models, analytic hierarchical techniques, trade off analysis.

Level II *(Management Level)* models and instruments of work have to be adequately tailored to decisions regarding management decisions: cost benefit risk analysis, safety management.

Level III *(Engineering Level)* asks for models involving engineering-economic and simulation, consequence assessment, probability assessment, etc.

References

1. W. Kröger, E. Zio, Vulnerable Systems, Springer, ISBN 978-0-85729-654-2, 2011

2. A.V. Gheorghe, R. Mock, and W. Kröger, *Risk assessment of regional systems.* Reliability Engineering & System Safety, 2000. 70(2): p. 141-156.

3. L. Dueñas-Osorio , Srivishnu Mohan Vemuru, *Cascading failures in complex infrastructure systems*. Structural Safety 31 (2009) 157–167.

4. L.A.N Amaral and J. M. Ottino, *Complex Networks, augmenting the framework for the study of complex systems*. Eur. Phys. J. B 38, 147-162 (2004).

5. A. Barrat, M. Barthelemy, A. Vespignani, *Dynamical processes on complex networks*. Cambridge University Press, 2008.

6. Boccara, N., *Modeling complex systems*. New York Springer, 2004.

7. M. E. J. Newman, *The structure and function of complex networks*. SIAM Review, Vol. 45, No. 2, pp. 167 – 256, 2003.

8. S.N. Dorogovtsev and A. V. Goltsev, *Critical phenomena in complex networks*. Reviews of Modern Physics, Vol. 80, Oct-Dec 2008.

9. J. M. Ottino, *Speech: Engineering complex systems and complex systems engineering*. Video Library of www.researchchannel.org, 2007.

Laboratory for Safety Analysis

INSTITUTE FOR ENERGY TECHNOLOGY

Course material:

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