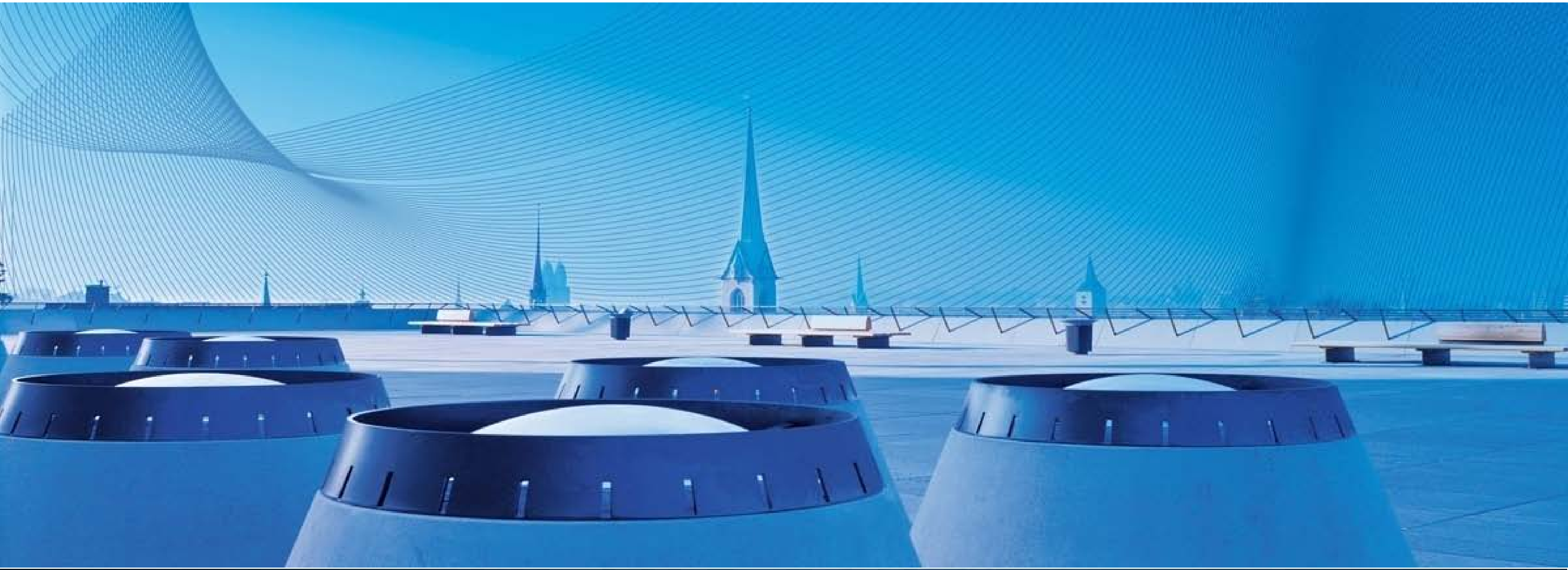
Methods of Technical Risk Assessment in a Regional Context

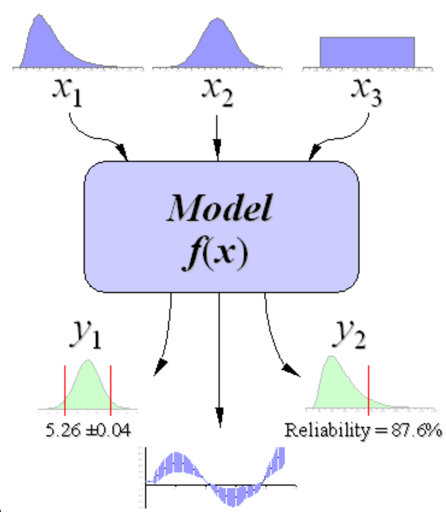
- Wolfgang Kröger, Professor and Head of former Laboratory for Safety Analysis (www.lsa.ethz.ch)
  - Founding Rector of International Risk Governance Council Geneva (www.irgc.org)
    - Executive Director, ETH Risk Center (www.riskcenter.ethz.ch)



Monte Carlo Simulation

Definition: The use of randomly generated data and computer simulations to obtain approximate solutions to complex mathematical and statistical problems.

Step 1: Create a parametric model, y = f(x1, x2, ..., xq).
Step 2: Generate a set of random inputs, xi1, xi2, ..., xiq.
Step 3: Evaluate the model and store the results as yi.
Step 4: Repeat steps 2 and 3 for i = 1 to n.
Step 5: Analyze the results using histograms,
summary statistics, confidence intervals, etc.



Monte Carlo is about invoking laws of large numbers to approximate expectations

Advanced Methods for Complex Systems Modeling (I) and Simulation

- Monte Carlo (MC) Simulation
- State Models, Markov Chains
- Petri Nets (PN)
- Graph and Complex Network Theory

State Model

Instead of subdividing a system into components it can also be subdivided into **global states** $Z_1, \ldots, Z_m$. Each state Z_i represents a combination of component states: $Z_i = (K_1, \ldots, K_n)$.

The **transition rates** $\alpha_{i,j}$ between states Z_i and Z_j define the mean number of transitions from Z_i to Z_j per time unit provided that the system is in state Z_i $(1 \le i \le m$ und $1 \le j \le m)$.

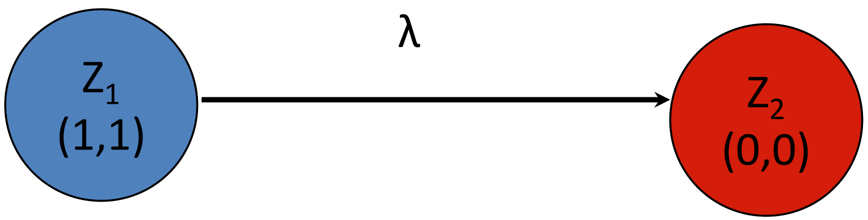
Advantages:

- Modeling in great detail: Any state transitions can be expressed, in particular: fault tolerance techniques (like reconfiguration) and **repair**.
- joint performance and reliability evaluation

Disadvantage: High computation overhead due to the large state space.

p_i is a probability of a state i.

Application of the State Model: Unrepairable System



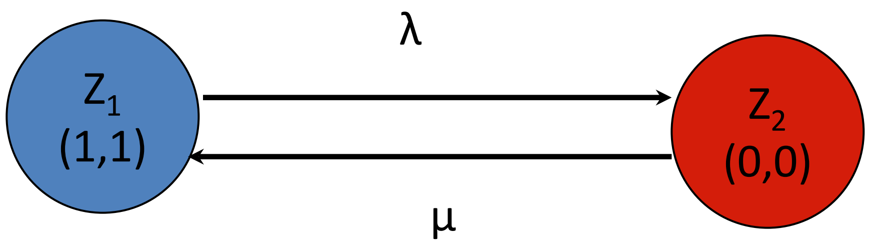
$Z_i(K_i,S)$, where K_i state of component, S - conditional state of system.
λ: failure rate

Homogenous system of equalities: $$\left(\dot{p}_1(t), \dot{p}_2(t)\right) = \left(p_1(t), p_2(t)\right) \cdot \begin{pmatrix} -\lambda & \lambda \\ 0 & 0 \end{pmatrix}$$

To be solved under conditions: $p_1(t)+p_2(t)=1$ and $p_1(0)=1$

Solution (via Laplace transformation): $$p_1(t) = e^{-\lambda \cdot t} \ and \ p_2(t) = 1 - e^{-\lambda \cdot t}$$

Application of the State Model: Repairable System



$Z_i(K_i,S)$, where K_i state of component, S- conditional state of system.
λ - failure rate, μ – repair rate

Homogenous system of equalities: $$\left(\dot{p}_1(t), \dot{p}_2(t)\right) = \left(p_1(t), p_2(t)\right) \cdot \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix}$$

To be solved unter conditions: $p_1(t)+p_2(t)=1$ and $p_1(0)=1$

Solution: $$p_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} \cdot e^{-(\lambda+\mu)\cdot t}$$

It is the time dependent Availability V(t)!

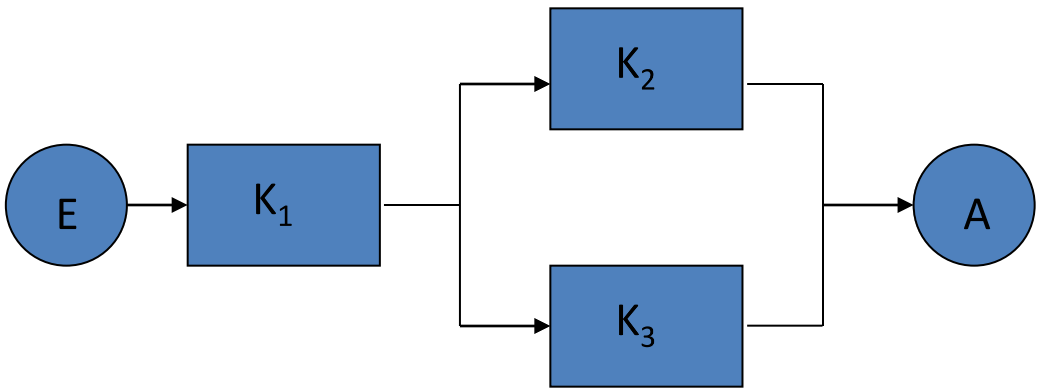
State models express each combination of component states by a separate global state.

In a system from two components K_1 and K_2 we have the global states:

- Both K_1 and K_2 are faultless, expressed by the global state $Z_1 = (1, 1)$.
- K_1 is faultless and K_2 is faulty, expressed by the global state $Z_2 = (1, 0)$.
- K_1 is faulty and K_2 is faultless, expressed by the global state $Z_3 = (0, 1)$.
- Both K_1 and K_2 are faulty, expressed by the global state $Z_4 = (0, 0)$.

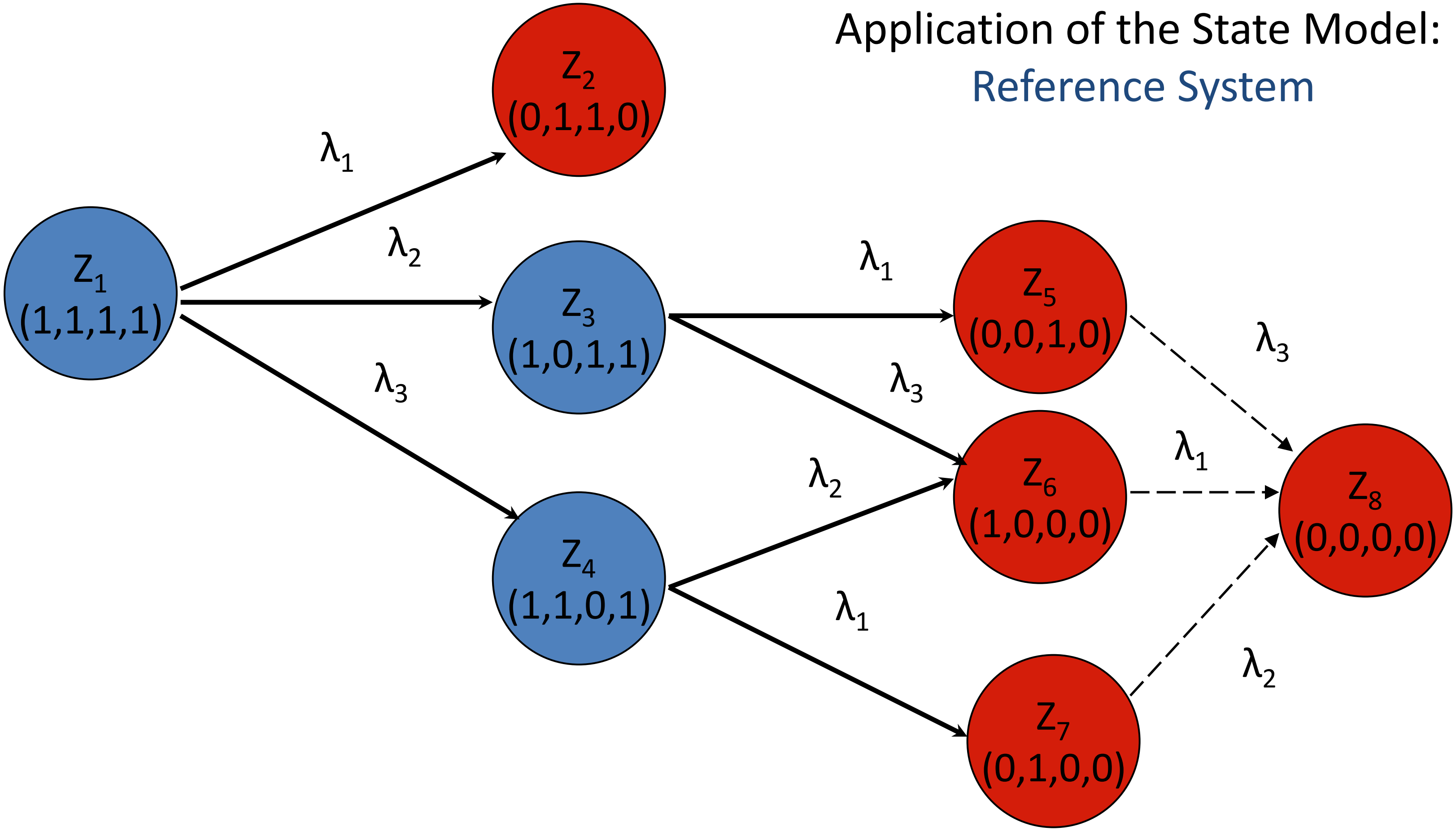
The transition rate $\alpha_{i,j}$ can also be seen as the reciprocal of the mean duration between the entering of state Z_i and the transition from Z_i to Z_j. However, it must be taken into account, that from Z_i also other states could be reached.

Application of the State Model: Reference System



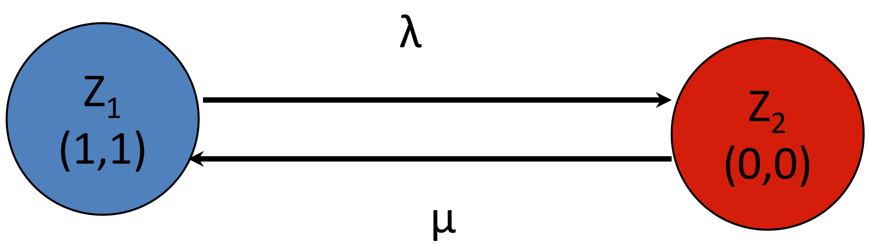
Number of states $2^3=8$

Application of the State Model:
Reference System



Stationary availability is calculated by $V=p_1+p_3+p_4$

Application of the State Model: Repairable System



Z_1: $\lambda * p_1 = \mu * p_2$

Z_2: $\lambda * p_1 = \mu * p_2$

$p_1 + p_2 = 1$

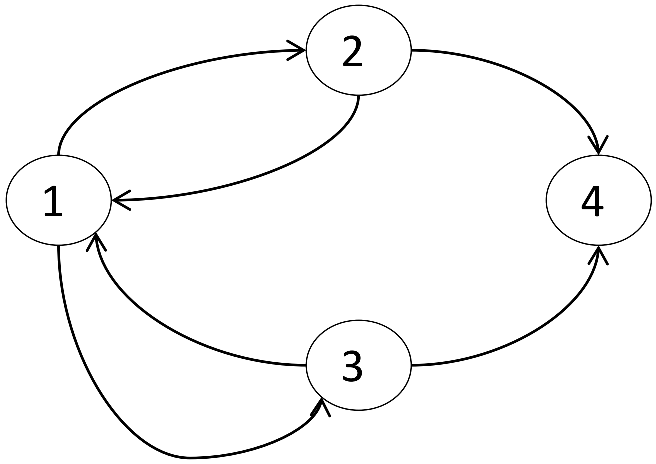
Stationary availability (steady-state availability)

V is calculated by:

$$p_1 = \frac{\mu}{\lambda + \mu}, \text{ the complementis } p_2 = \frac{\lambda}{\lambda + \mu}$$

Finite state machines

A model consisting of a set of states *S*, a start state, possible transitions and a transition function that maps states to a next state. It changes to new states depending on the transition function.



Example: 4 States

2 Components in Parallel

State 1: Both components working (start state)

State 2: Component 1 failed

State 3: Component 2 failed

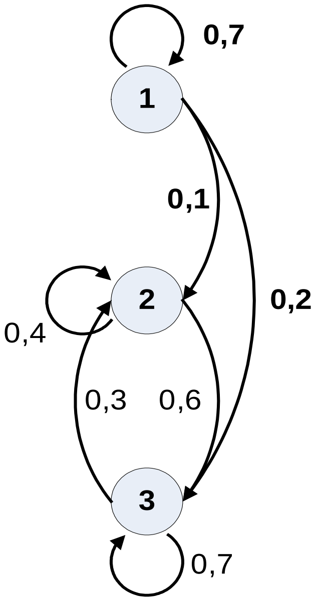
State 4: Component 1 and 2 failed Final state (no transitions out)

Markov Chains

A Markov chain consists of a state space *S={1,...,n}* and a transition Matrix *T* that defines the probabilities of each transition.

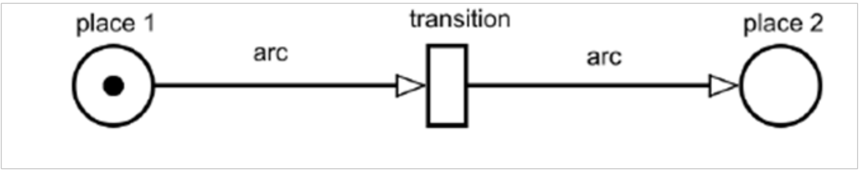
Transition Matrix

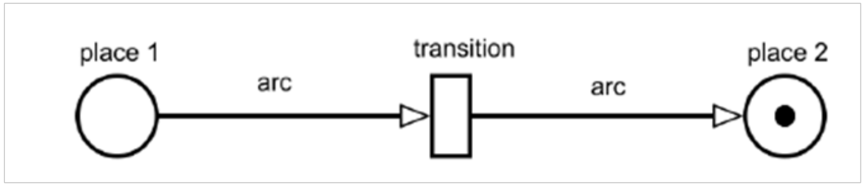
$$\begin{pmatrix} 0{,}7 & 0{,}1 & 0{,}2 \\ 0 & 0{,}4 & 0{,}6 \\ 0 & 0{,}3 & 0{,}7 \end{pmatrix}$$



Markov chains are directed graphs that have a weight (numeric value) associated with each edge

Basics of Petri Nets (PN)





- Three elements
  - Place describes systems state
  - Transition stands for an event which influences the system state
  - *Directed* arcs defines relation between states an events

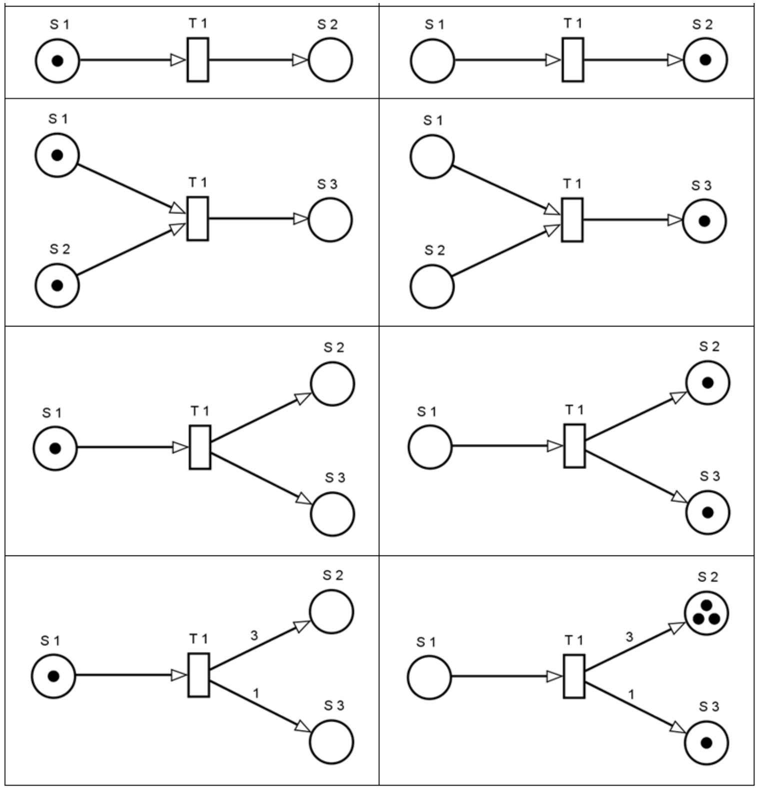
- Black points, named tokens, mark the actual system state

- If event occurs and system state changes, tokens will be removed from place 1 and insert in place 2

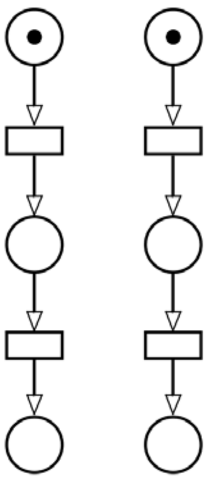
Rules

- Transistions are only *activated*, if all input places are marked with at least one token
- If the transition fires, in all output places will be inserted a token

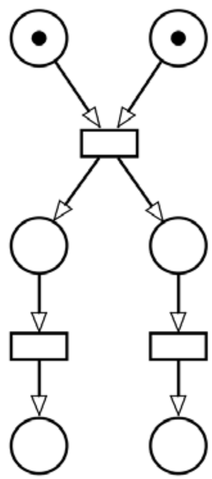
- Arcs can be weighted:
  - An input arc with weight three requires three tokens in the adequate input place to activate the transition
  - An output arc with weight three insert three tokens in the adequate place



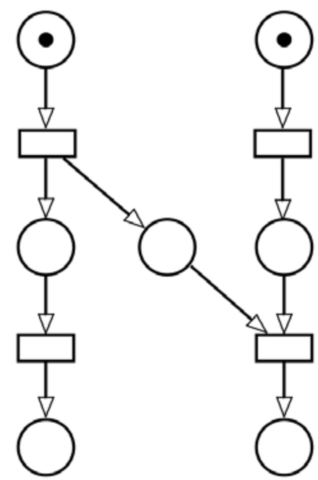
Special nets



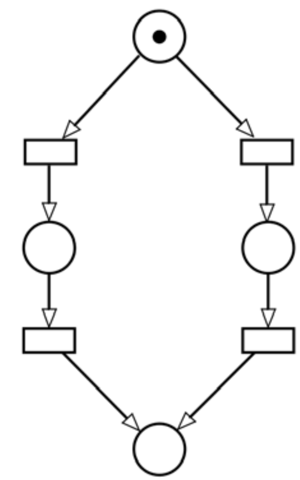
Concurrency



Synchronization

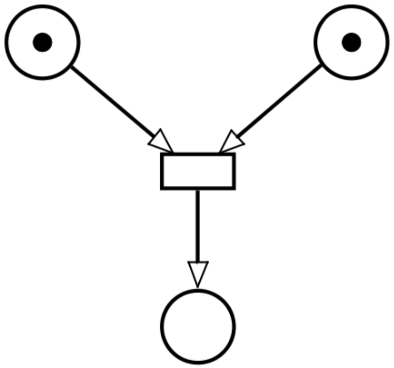


Communication

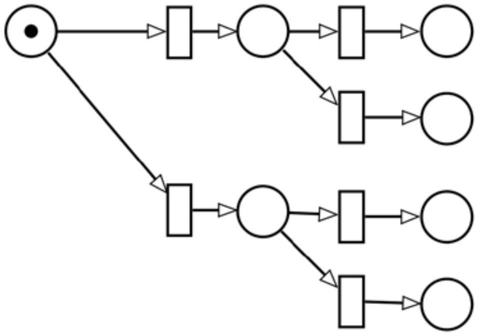


Conflict

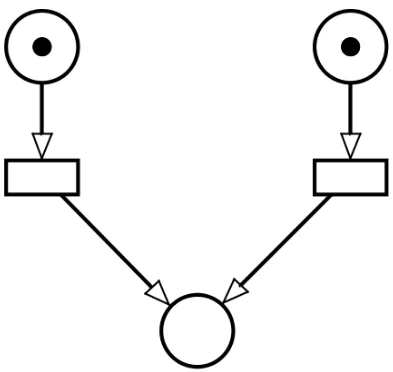
Petri nets as fault tree or event tree



And-Operator



Event tree



Or-Operator

Characteristics

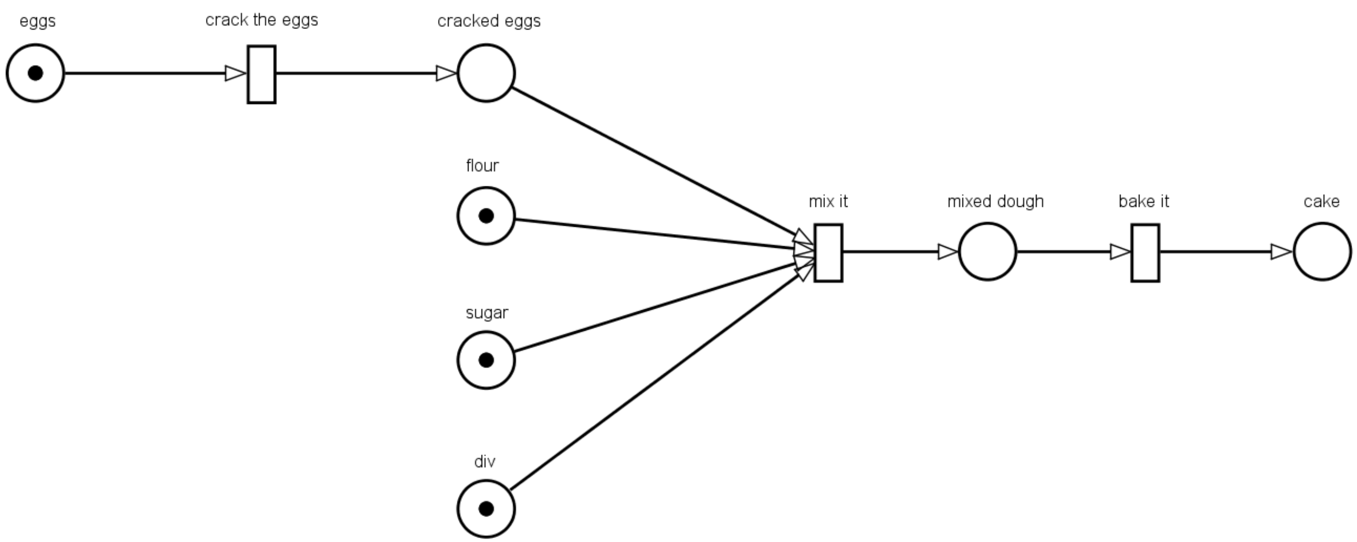
Pros

- Simple **Design** – easy to understand
- Graphical illustration
- Lot of tools available, in which changes of firing rates are easy to implement

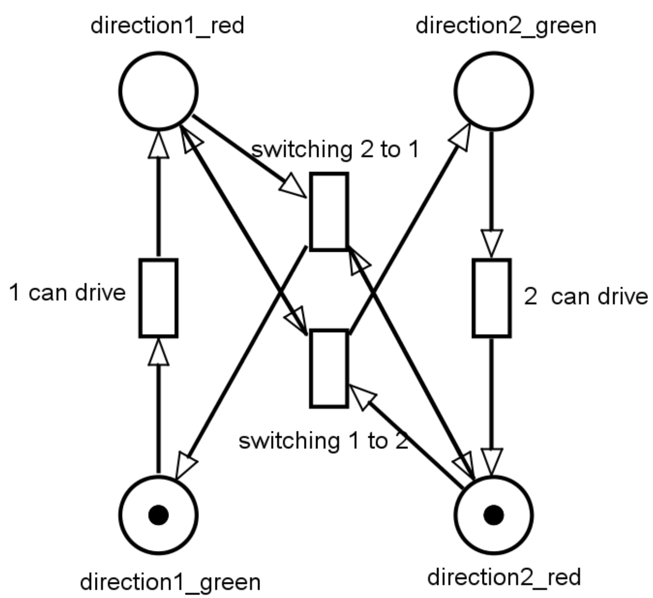
Cons

- Nets grow very fast
- No guidelines for correct build up of a net – every net looks induvidual
- Big nets are difficult to understand

Example I – bake a cake



Example II – traffic signal



- Starting with one signal green, the other red
- X minutes one direction is allowed to drive
- After changing to red, there is some time to switch
- When switching is completed, direction 2 can drive

Bibliography

Books

- C. A. Petri. “Kommunikation mit Automaten“, Schriften des Rheinisch-Westfälischen Institutes für instrumentelle Mathematik an der Universität Bonn, (1962) – “Invention“ of Petri Nets
- W.G. Schneeweiss. Petri Nets for Reliability Modeling, LiLoLe Verlag (1999), ISBN 3-934447-00-7
- L. Priese, H. Wimmel. Petri-Netze, Springer Verlag (2008), ISBN 978-3-540-76970-5

Websites

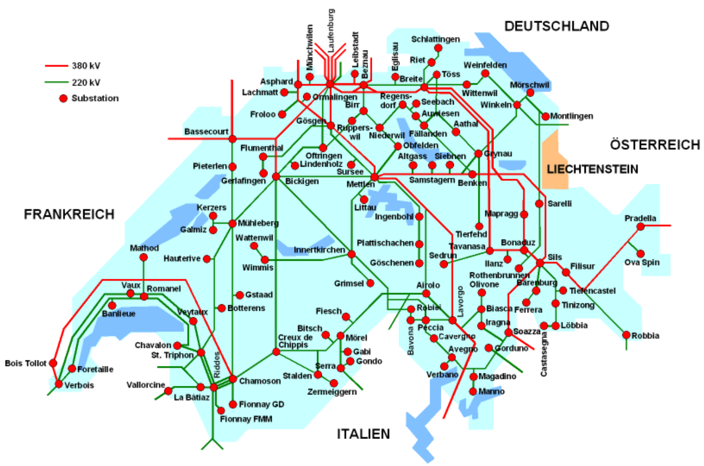
- http://www.informatik.uni-hamburg.de/TGI/PetriNets/ - everything about Petri Nets
- http://www.informatik.uni-hamburg.de/TGI/PetriNets/tools/java/Braunl/ - simple Petri Net simulator

Software

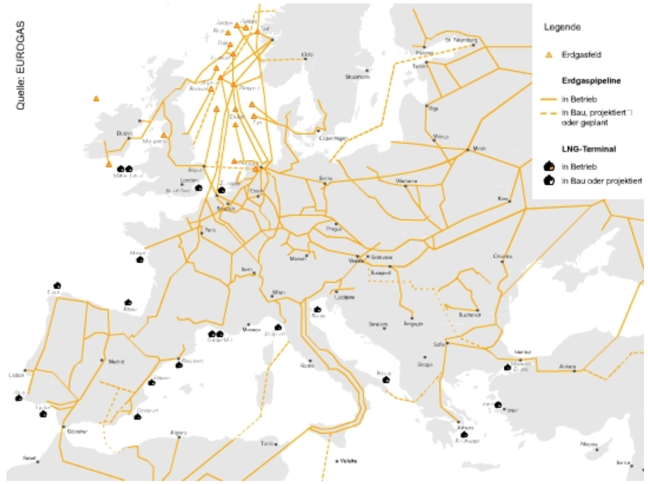
- CPN-Tools – freeware, from Aarhus University
- TimeNet – free for academic use, TU Ilmenau

Examples of Technical Networks

Swiss Power System



Natural Gas Pipelines

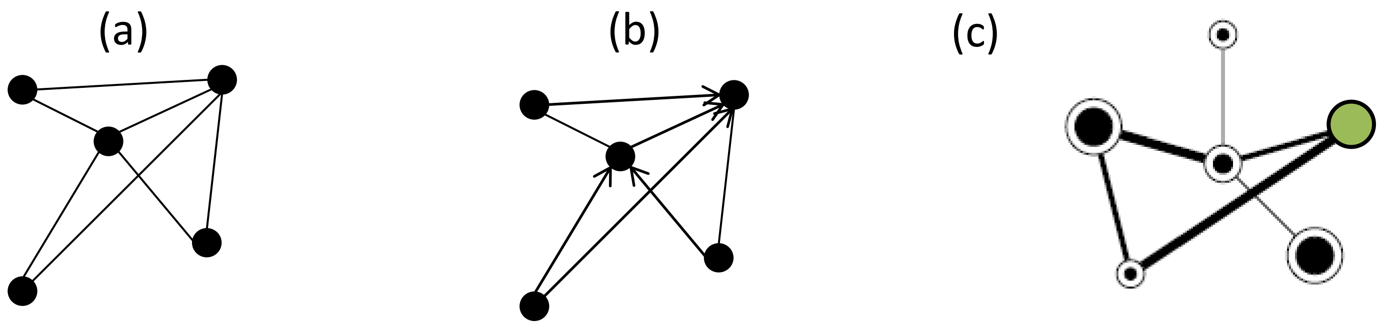


- Internet
- World Wide Web
- Railway
- Motorway
- …

Basics of complex network theory for structural investigations

- Network (or **graph** G**(***N,L*): set of *N* **nodes** (vertices) connected by *L* **links** (edges)

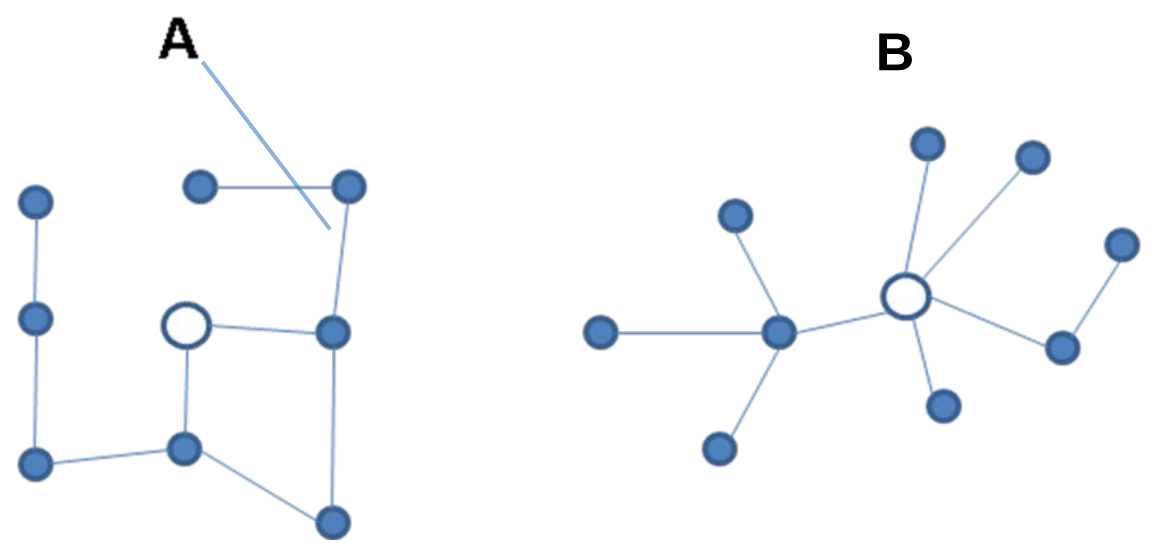
- Networks with undirected links (a), directed links (b), weighted nodes and links (c); the **adjacency matrix** provides a complete description of a network



- The total number of connections of a node is called its **degree** *k;* the **degree distribution** P(k) is the probability that any randomly chosen node has a certain degree, either Poisson, exponentially or Power Law shaped.
- G is connected if there is a path u between to nodes

Assignment: Complex Network Theory (CNT)

Consider the following two simple network topologies:



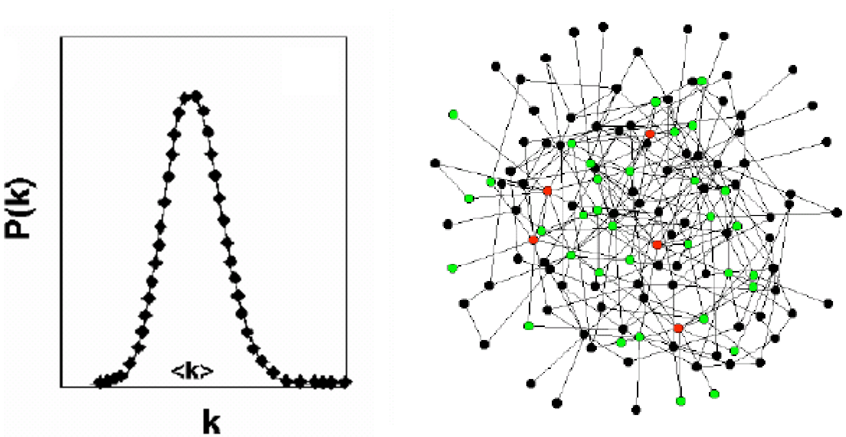
Exercises:

1. Calculate the clustering coefficients C of the white nodes.
2. Find the adjacency matrix for network A.
3. Determine the empirical degree distribution $\hat{P}(k)$ of both networks. What is the average degree $\bar{k}$?
4. Which network is more vulnerable to random failures (with respect to system splitting)? Why?

Types of Networks

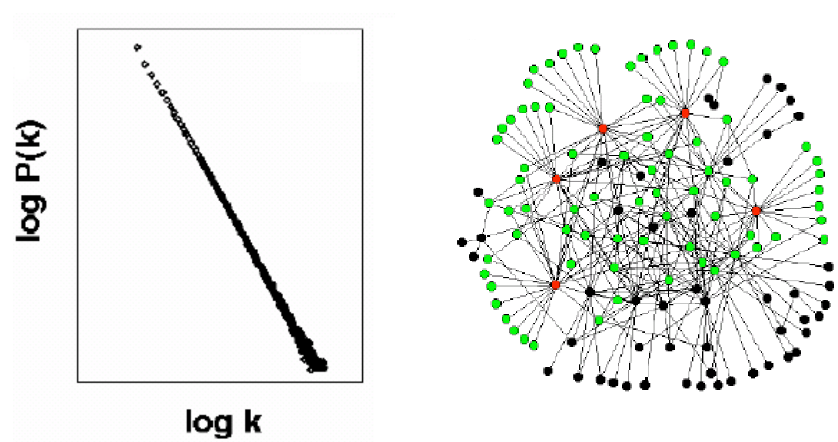
Random network

Poisson distribution of the number k of edges between nodes



Scale-free network

Exponential distribution of the number of edges k between nodes



Examples: Internet, Power System

Figures: Bornholdt, Schuster: Handbook of Graphs and Networks

Vulnerability Assessment of Real Networks

Most of the technical networks are scale-free, e.g., Power System, Internet

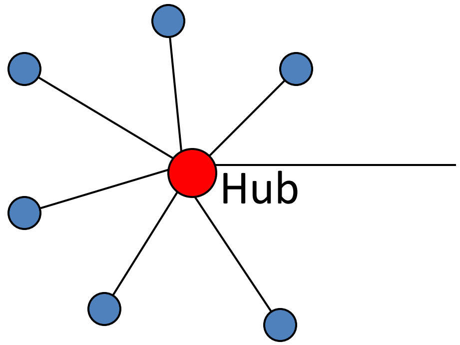
Reasons:

- less expensive, fewer edges necessary (end user needs only one connection)
- efficient
- natural growth

Vulnerability of Network Types

type of impact	exponential network	scale-free network
random	robust	extremely robust
malicious attack	robust	extremely vulnerable

scale-free network:



the chance to destroy the hub with a random attack is 1:7

a malicious attack to the hub destroys the connection to six nodes

Vulnerability Assessment of Networks: Network Parameters

Measures to characterize and analyze the vulnerability of a network with N vertices and M edges

Size of the graph: number of edges in the graph

Degree of distribution k_i: number of edges connecting vertex i; the average degree is given by k=2M/N

Clustering coefficient: ratio of existing and maximum possible number of edges between the neighboring vertices k_i of a vertex i; neighboring vertices are the vertices actually connected to node i

Shortest path: shortest path between two vertices

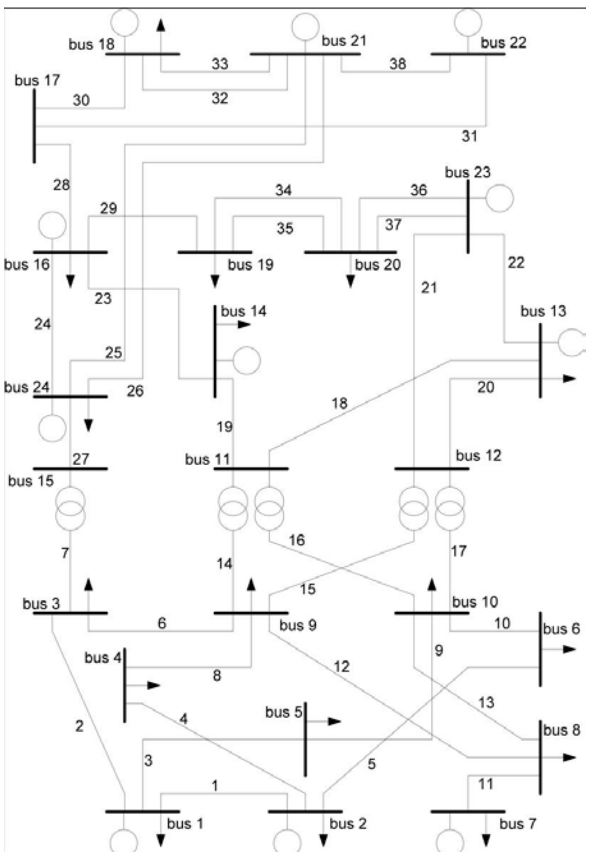
Average path length: average of all shortest paths in the network

Most stressed edge: most utilized edge in all shortest paths

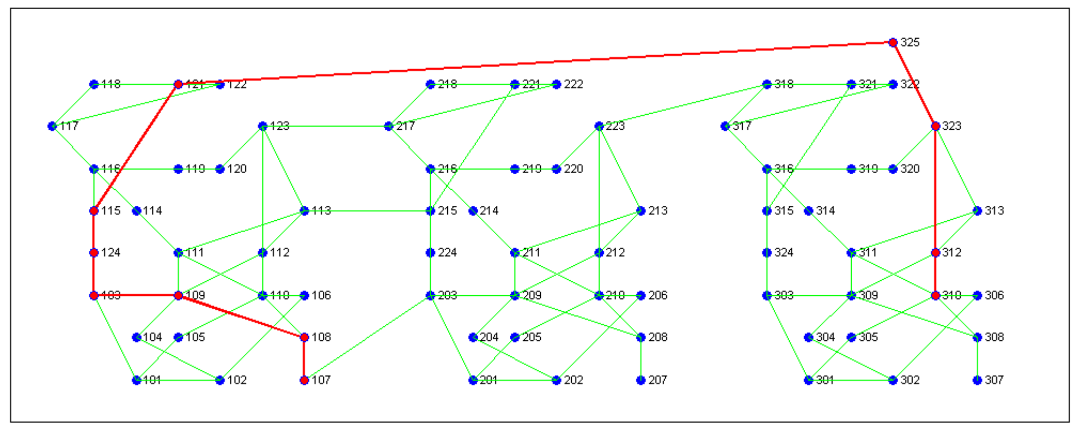
Vulnerability Assessment of Networks – Shortest Path

Dijkstra-Algorithm – one method to calculate the shortest path between two nodes:

IEEE-Test-System

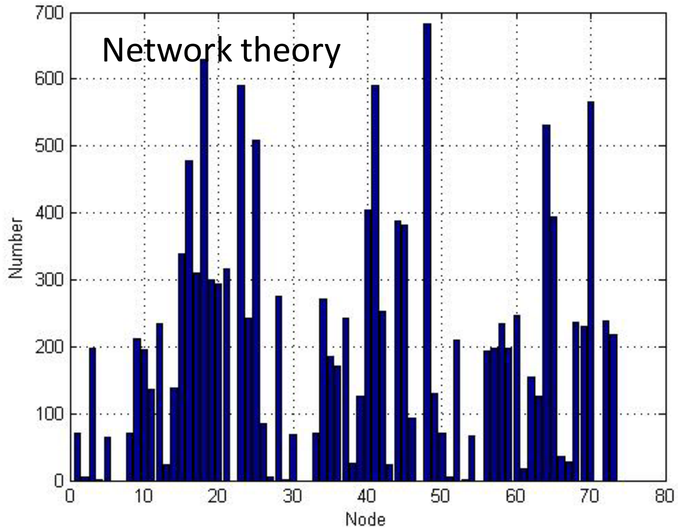


Shortest Path between node 107 and 310

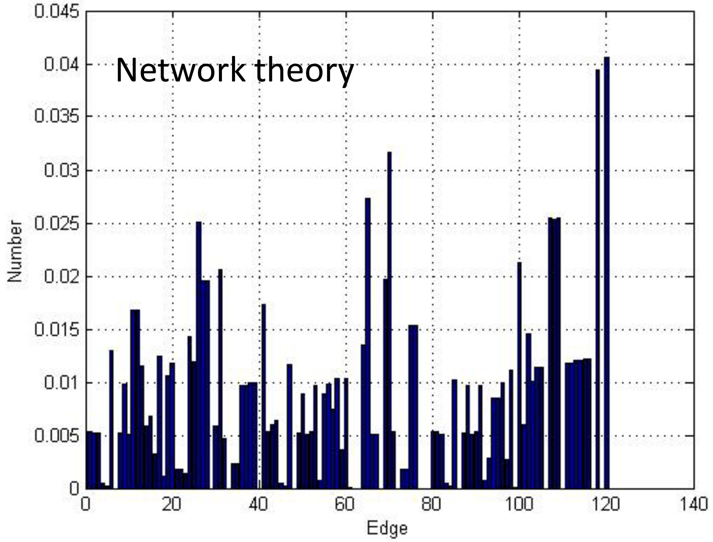


Vulnerability Assessment of Networks – Most stressed edges and nodes

Most stressed node

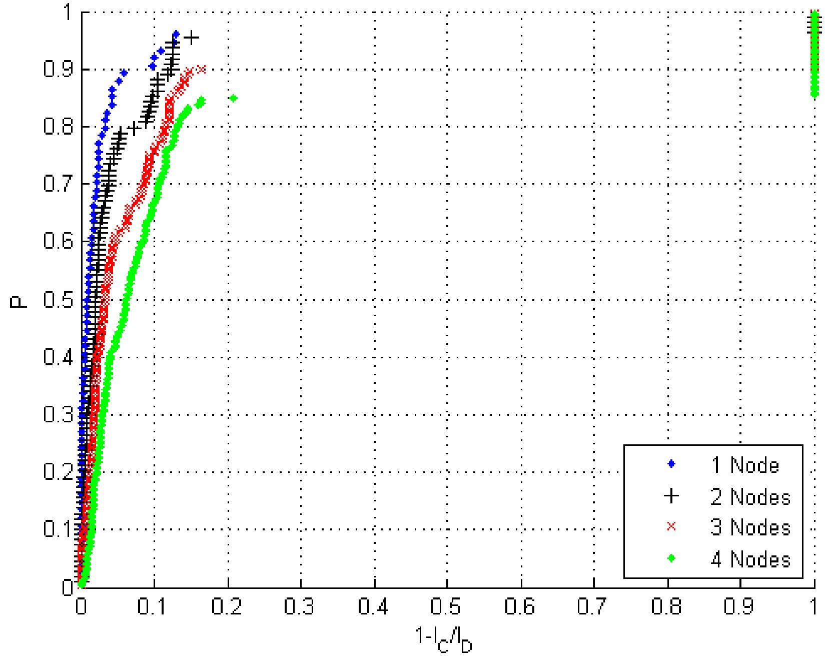


Most stressed line

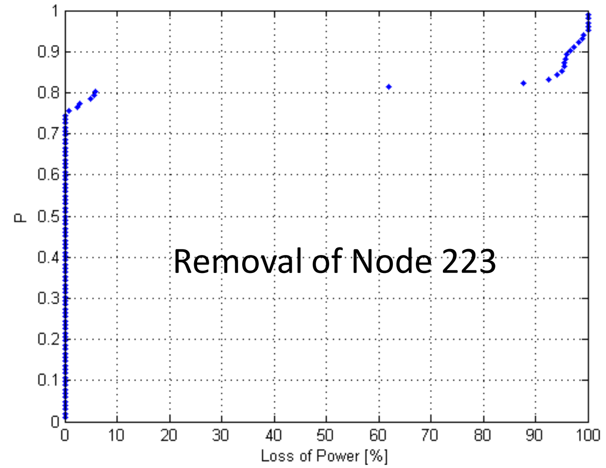


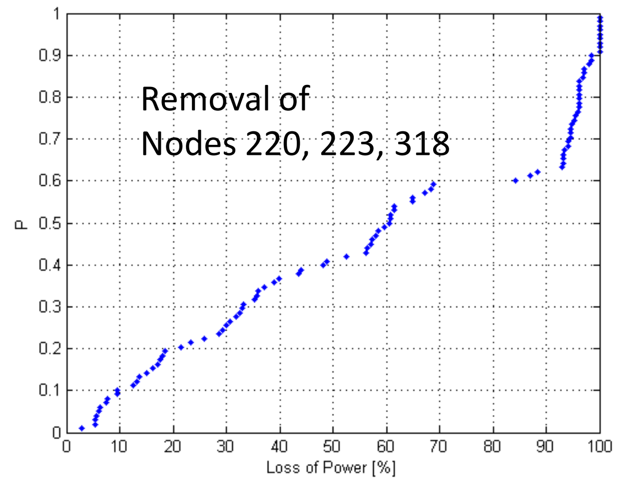
Vulnerability Assessment of Networks – Removal of nodes

Network theory - Increase of the average path length after the removal of nodes

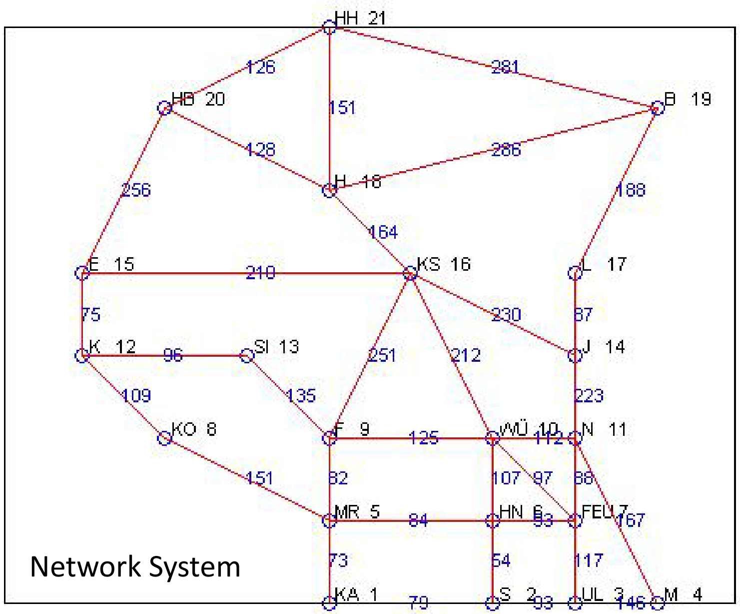


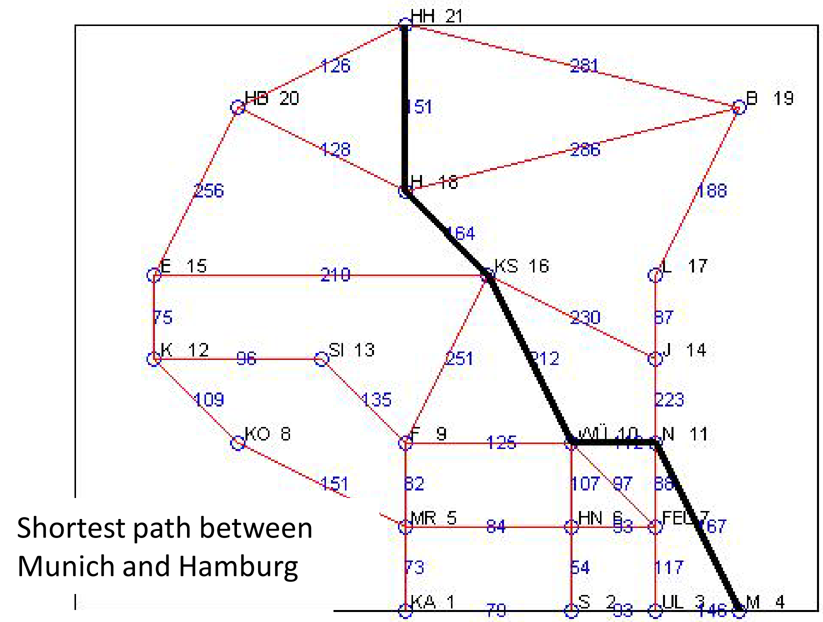
ABM – calculations
max loss of power

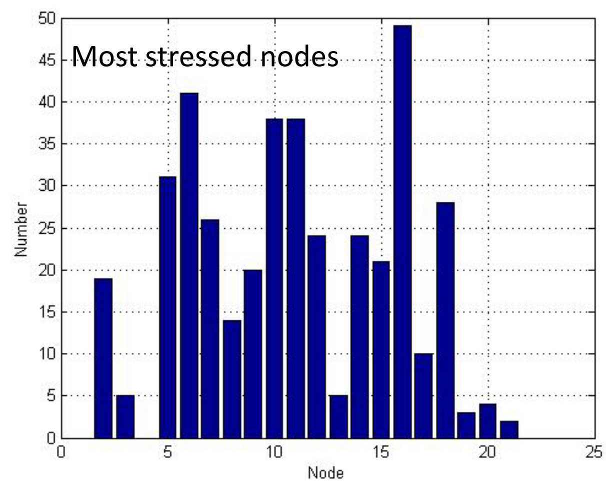




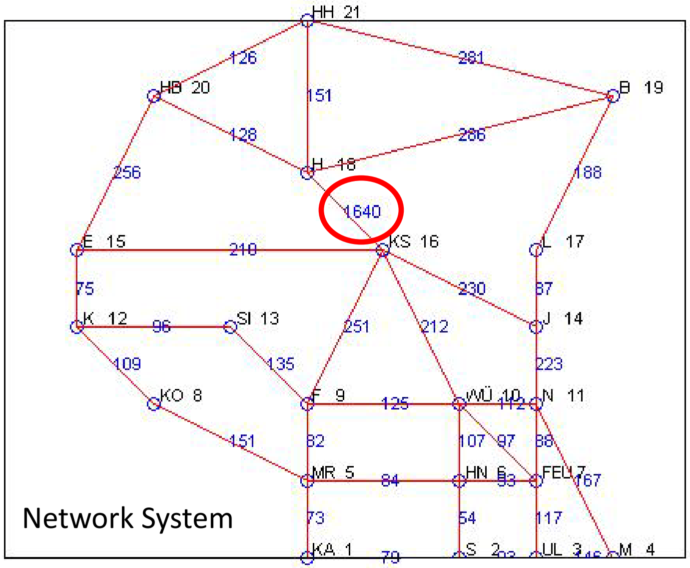
Vulnerability Assessment of Networks – Highway Network

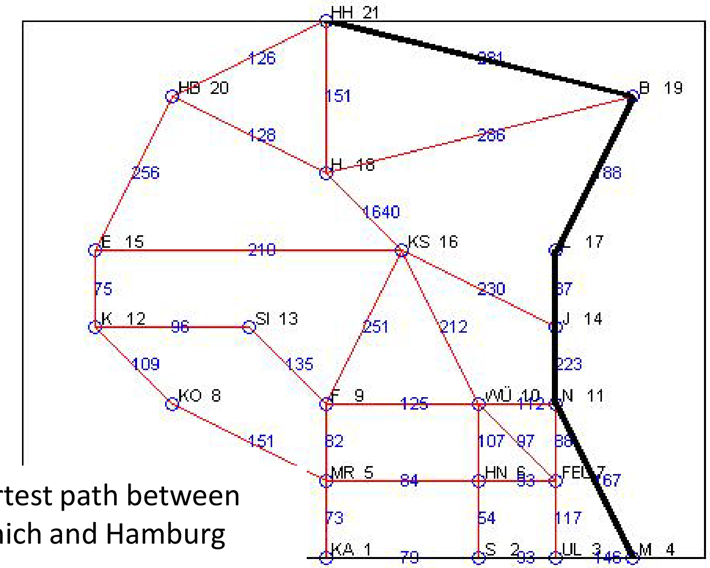




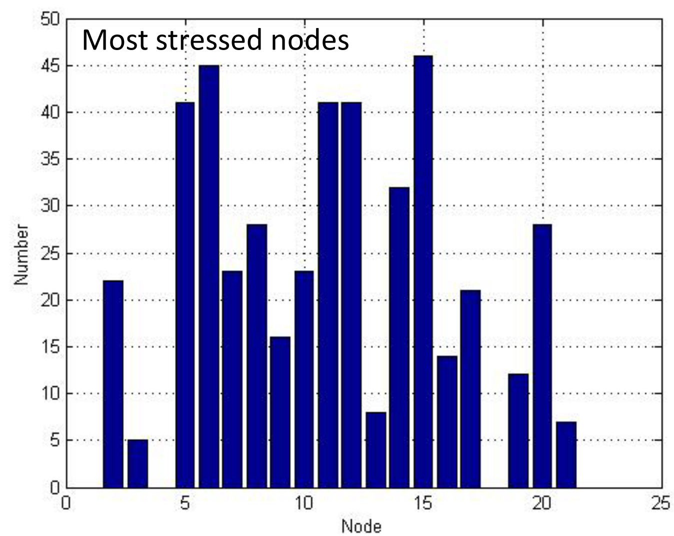


Vulnerability Assessment of Networks – Highway Network





Shortest path between Munich and Hamburg



Heuristic investigation of potential attacks based on CNT

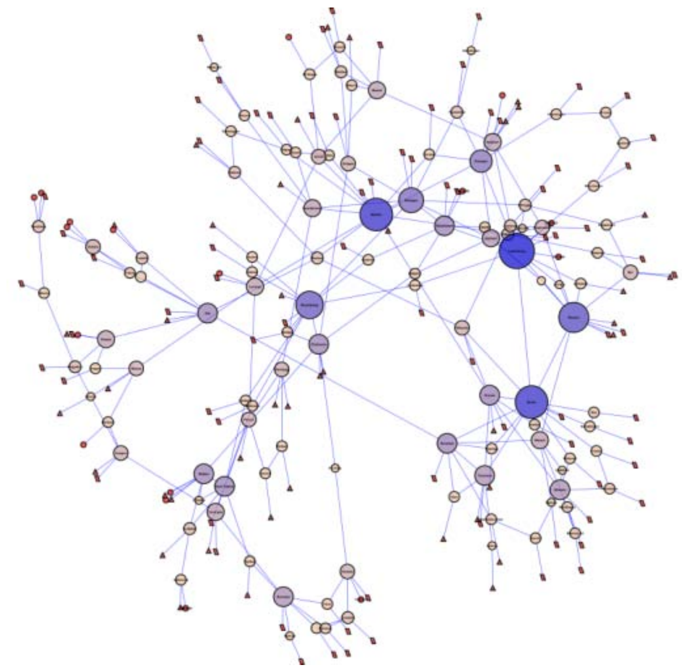
Important elements of the **Swiss transmission grid** are identified by centrality analysis for simulated

a) deterministic attacks, targeted on vital substations

b) stochastic attacks on lines (randomly removed)

Results based on response analysis:

- No highly unstable conditions emerged from the attack on the most critical substations (hubs)
- Although the load flow model is quasi-dynamic, the effect of cascading failures was very small
- Overloading of transmission lines in only a few scenarios shows good safety margins for the grid



Representation of the Swiss grid by 242 nodes for substations, loads, or power generating stations and 310 links for transmission lines. Node size is analog to node degree centrality.

Source: E. Bilis, ETH-LSA, 10