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

Grundlagen der technischen Risikoanalytik

Weitere Methoden und wichtige Trends in der Risikoanalytik

- Petri Netze, Kritische Infrastrukturen, Netzwerk Theorie und Objekt-orientierte Modellierungsansätze

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

Petri Netze

Petri Netze (PN)[1]

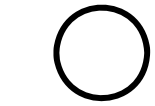
- Dienen zur Beschreibung verteilter diskreter Systeme
  - mit einzelnen wohlunterschiedenen (d.h. diskreten) Ereignissen oder Aktivitäten, bei denen Objekte (Bauteile, Ressourcen u.a.) benötigt, verbraucht oder erzeugt und
  - Bedingungen (Vorliegen eines Gegenstandes an einem bestimmten Ort, u.a.) benötigt, aufgeführt oder herbeigeführt werden.

2.1. Methodischer Ansatz

- PN zeigen den Fluss (abstrakter) Objekte, ihre Entstehung und Vernichtung.
- Verzögerungen im Fluss werden über Parameter, sog. Transitionen, eingebracht.
- Die Objekte werden im PN als Marken dargestellt, die in Stellen gespeichert sind.
- Transitionen und Stellen sind die Knotenarten eines PN und werden über Kanten verbunden.

1) Petri C., Fundamentals of a Theory of Asynchronous Information Flow, in Proc. 1st IFIP Congress. München: 1962, p.166-168

Basiselemente



Zustand
(Stelle, Platz)

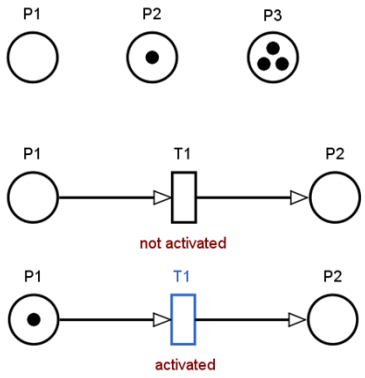
Ereignis (Transition)

Kante (Link)

Markierung (Token)

- Zustände beschreiben die momentane Lage eines Systems (z.B. aktueller Zustand einer Maschine
- Ereignisse stehen für Aktionen, welche ein bzw. mehrere Systemzustände beeinflussen können
- Kanten verbinden Zustände und Ereignisse (gerichtete Graphen)
- Mit Markierungen wird der aktuelle Sytemzustand gekennzeichnet

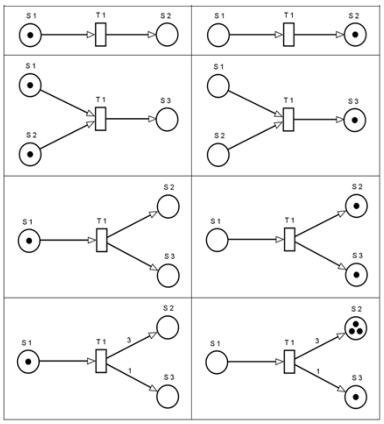
Schaltregeln I



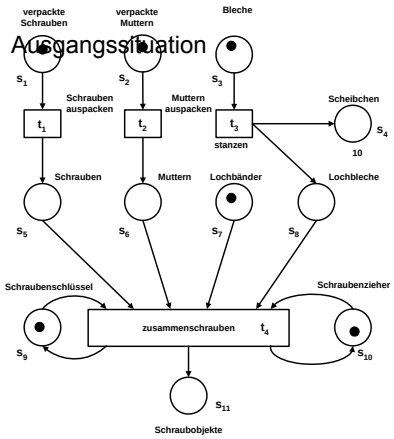
- Zustände können 0 bis ∞ Markierungen haben (limitiert durch definierte Kapazität)
- Transitionen sind aktiv, wenn alle Eingangs-Zustände mit mindestens einer Marke gekennzeichnet sind und die Ausgangs-Zustände markenfrei sind
- Einmal aktiviert, werden Transitionen zufällig oder mit definierter Verzögerung gefeuert
- Kanten verbinden Transitionen mit Zuständen und nicht zwei Zustände bzw. Ereignisse miteinander

Schaltregeln II

- Kanten können gewichtet werden:
  - Ein Eingang mit dem Gewicht drei verlangt drei Markierungen im entsprechenden Eingangsplatz um die Transition zu aktivieren
  - Ein Ausgang mit dem Gewicht drei verlangt drei Markierungen im entsprechenden Platz
- Wenn die Transition gefeuert wird, wird die Zahl von Markierungen entsprechend dem Gewicht des Eingangs entfernt und die Zahl entsprechend dem Gewicht des Ausgangs erzeugt



Beispiel: Stanzen von Blechen und Zusammenschrauben mit Lochblättern



- **Transitionen *t*** (Vierecke)**:** **Ereignisse**, Aktivitäten
- **Stellen *s*** (Kreise) und **Marken** (Punkte):

  Objekte, "Verbrauchsgüter"; für ein Ereignis benötigt, jedoch nicht veränderbar
- **Kantengewichte:** bei einem Ereignis werden entsprechend viele Objekte **produziert** oder **konsumiert** (hier: 1)
- **Kapazität**: **Obergrenze** der Markenanzahlen (hier: 1).

[Quelle: Baumgarten B., Petri-Netze (2. Auflage). Heidelberg etc.: Spektrum, Akad. Verlag, 1996]

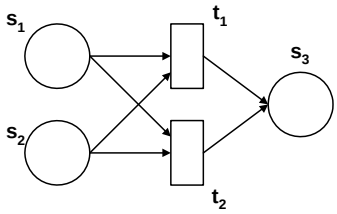
2.2. Übergang zu einer formalen Schreibweise

Definition: Ein Netz ist ein Tripel N = (S, T, F) mit

$$S \cap T = \varnothing$$
$$F \subseteq (S \times T) \cup (T \times S)$$

- S: Stellen
- T: Transitionen
- F: Kanten (Flussrelation)

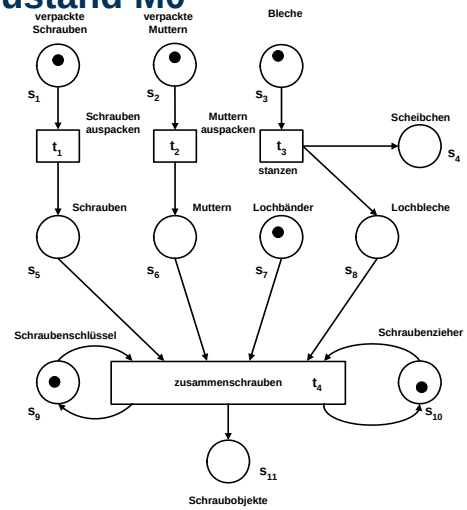
Beispiel



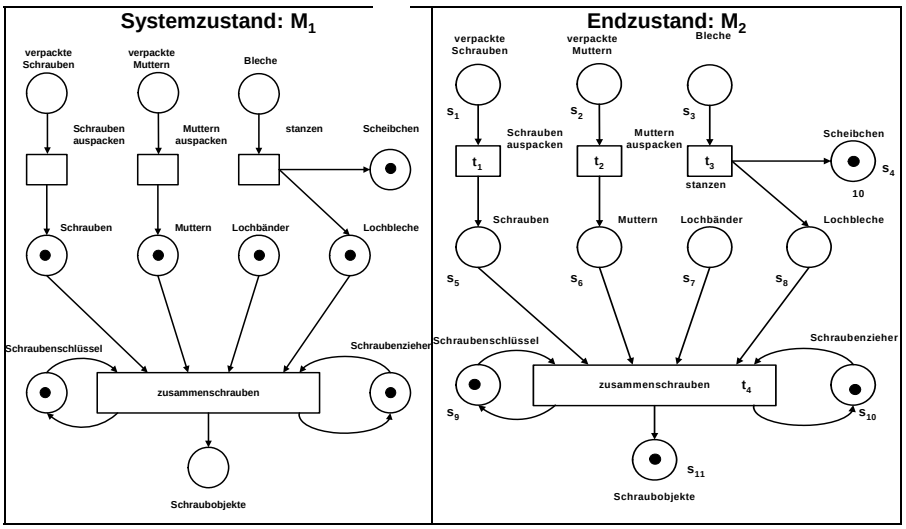
Netz *N = (S, T, F)* mit

- $S = \{s_1, s_2, s_3\}$
- $T = \{t_1, t_2\}$
- $F = \{(s_1, t_1), (s_1, t_2), (s_2, t_1), (s_2, t_2), (t_1, s_3), (t_2, s_3)\}$.

2.3. Systeme mit anonymen Marken
Ausgangszustand M0



Simulationsablauf



Ansätze der Netzanalyse

Erreichbarkeitsmenge:

Nr.	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	Schaltung
M_0	1	1	1	0	0	0	1	0	1	1	0	$\{t_1, t_2, t_3\} \rightarrow M_1$
M_1	0	0	0	1	1	1	1	1	1	1	0	$t_4 \rightarrow M_2$
M_2	0	0	0	1	0	0	0	0	1	1	1	

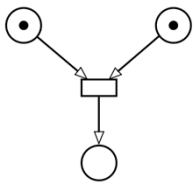
Erreichbarkeitsgraph:

$$M_0 \xrightarrow{\{t_1, t_2, t_3\}} M_1 \xrightarrow{\{t_4\}} M_2$$

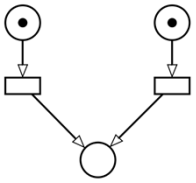
2.4. Petri Netze in der Risikoanalytik

- PN erlauben, komplizierte und dynamische Systeme zu analysieren. Zusätzlich hilft ihre graphische Natur, diese Systeme zu visualisieren.
- Reparatur- und Betriebszyklen lassen sich einfach darstellen.
- Keine Beschränkung auf linear ablaufende Szenarienketten, wie beim Ereignisbaum („Schleifen“).
- Die Ermittlung von Risiko- und Zuverlässigkeitskenngrössen ist mit bestimmten PN möglich (Generalized Stochastic Petri Nets, u.a.)
- **Ansatz**: Abschätzen der Systemausfallwahrscheinlichkeit SF
- $$S_F = \frac{n_z}{N_S}$$
- Ns: Anzahl aller Simulationsdurchgänge
- nz: Anzahl der unerwünschten Systemzustände („Ausfälle“)
- Der Einsatz von PN in der Risiko- und Zuverlässigkeitsanalyse ist eher selten.

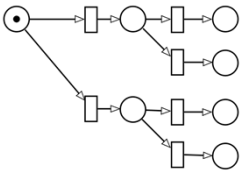
Petri Netze als Fehlerbaum oder Ereignisbaum



UND-Operator



OR-Operator



Ereignisbaum

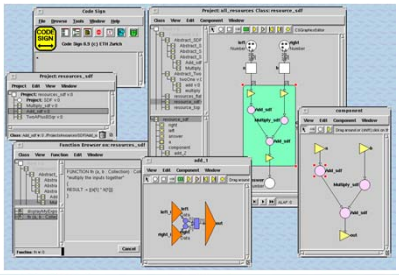
Merke: Jeder Fehler-/Ereignisbaum kann als Petri-Netz modelliert werden, nicht aber jedes Petri-Netz als Fehler-/Ereignisbaum.

2.5. Weitere Informationen

Einführung und Übersicht in Petri Netze

- http://www.informatik.uni-hamburg.de/TGI/PetriNets/

- CodeSign (entwickelt an der ETHZ)
  http://www.tik.ee.ethz.ch/~codesign/#Overview
- PACE
  http://www.ibepace.com/



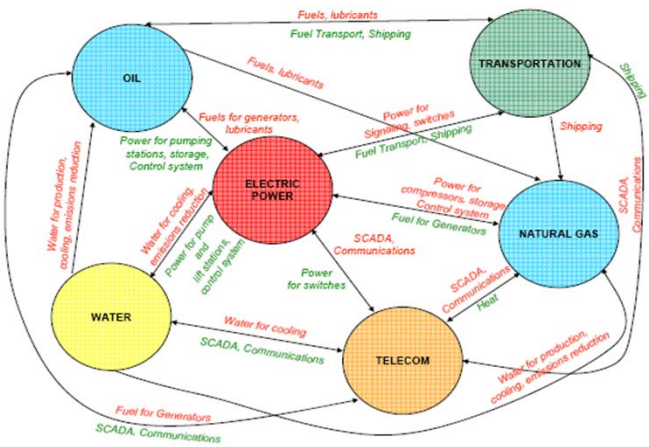
Critical Infrastructures (1/2)

- A network of large-scale human-made systems that function synergistically to produce a continuous flow of essential services
- Subject to multiple threats (technical-human, physical, natural, cyber, contextual; unintended or malicious); may pose risks themselves
- Highly, inter-dependent, both physically and through a host of industrial ICT (“system of systems”); subject to rapid changes

Critical Infrastructures (2/2)

- Disruptions may cascade (recall “blackouts”), even “normal” service interruptions cost industrialized countries a few percent of GDP
- No single owner / operator / regulator; based on different goals / logics
- Infrastructures are considered as critical when they are „so vital that their incapacitation or destruction would have a debilitating impact on defence or economic security“ (US PCCIP, 97) of any state (EC COM (2004)702)

Interdependencies



Source: *Rinaldi, Peerenboom, Kelly, 2001*

Kritische Infrastrukturen: Zur Erinnerung

Italian Blackout, September 28, 2003 – Mechanismus

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

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

- Risk refers – in general terms – to the possibility (frequency) of loss, damage or injury and their extent (impact indicators). These variables and associated uncertainties are regarded as being quantifiable.
- With regard to critical infrastructures the level of risk depends on the value placed on the asset by its owner / operator and the impact of loss or change (1) to the asset and (2) the likelihood that specific vulnerability will be exploited by a particular threat.

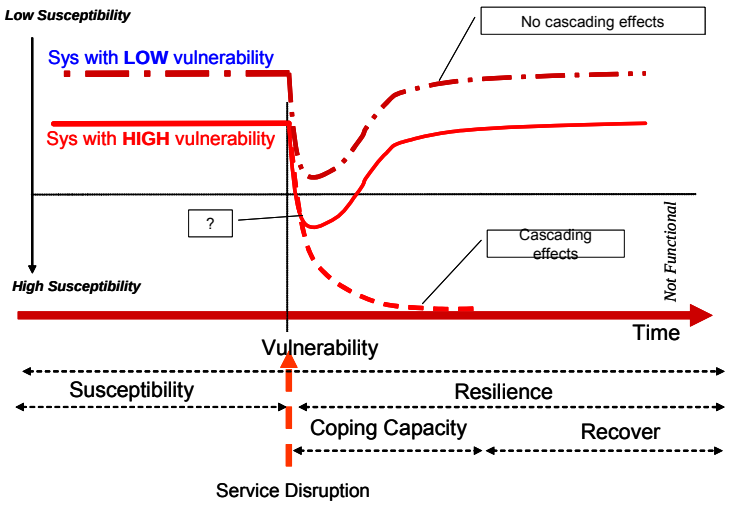
Concept of vulnerability – definition of terms

We define vulnerability as a flaw or weakness (inherent characteristic including resilience capacity) in the design, implementation, operation and/or manage-ment of an infrastructure system or its elements that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat.

The concept of vulnerability develops in three main steps and finally focuses on three elements:

- degree of loss and damages due to the impact of a hazard;
- degree of exposure to the hazard, i.e., likelihood of being exposed to hazards of a certain degree and the susceptibility of an element at risk to suffer loss and damages;
- degree of capacity of resilience, i.e., the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a hazard or disaster (social).

Vulnerability scenarios



Verletzbarkeitsanalyse für vernetzte Systeme (Infrastrukturen): Einführung in fortgeschrittene Methoden

How can we quantify the reliability of infrastructures and **assess the risk** of such large-area breakdowns?

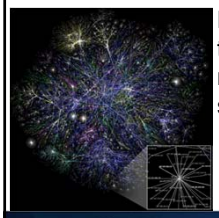
Basic problem: Infrastructures are **highly complex** and interdependent systems, consisting of an enormous number of technical and non-technical, interacting components; classic reliability analysis methods become limited due to the state space explosion.

Example: Consider a system of N=20 components with two states (e.g. up state and down state). A "state enumeration approach", such as a complete markovian chain would have to consider $2^N = 2^{20} \sim 10^6$ *system states!*

Introduction and Problem Description

Approach 1: *Simulate the systems realistically by means of extensive modeling methods, including the physical laws and operational dynamics, e.g., by applying the object-oriented modeling approach combined with MC simulation.*

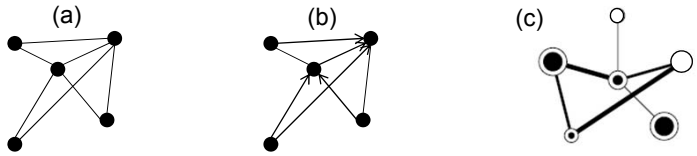
Approach 2: *Use highly simplified models in order to understand the* ***basic mechanisms*** *leading to infrastructure breakdowns. In this respect* ***network theory*** *allows for gaining valuable knowledge about the basic functioning of infrastructure systems, being networks in nature.*



However, due to its highly simplifying approach, network theory cannot replace more detailled reliability analysis methods. It rather serves as a first „screening" of the systems.

Network characteristics: Some basic notations

- Network (or **graph**): set of *N* **nodes** (or **vertices)** connected by *L* **links** (or **edges)**
- **G***(N,L)*: arbitrary graph of **order** *N* and **size** *L*
- Networks with undirected links (a), with directed links (b), with weighted nodes and links (c)



- The total number of connections of a node is called its **degree** *k*

Network characteristics: Adjacency matrix

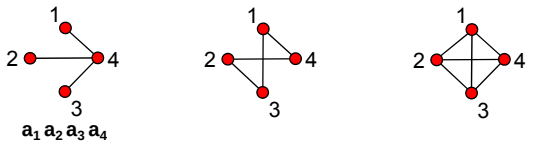
- The adjacency matrix provides a complete description of a network
- Consider a network with *N* nodes labelled by their index *i* (*i*=1,…,*N*); the adjacency matrix is a *N x N* matrix with elements a_{ij} while,

if the network is undirected:

$a_{ij} = a_{ji}$, $a_{ij} = 1$ *if there exists a link between node i and j*

$a_{ij} = 0$ *otherwise*

- Examples for undirected graphs:



$$\begin{array}{c} \\ \mathbf{a_1} \\ \mathbf{a_2} \\ \mathbf{a_3} \\ \mathbf{a_4} \end{array} \begin{array}{c} \begin{array}{cccc} \mathbf{a_1} & \mathbf{a_2} & \mathbf{a_3} & \mathbf{a_4} \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{array} \qquad \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$k_i = \sum_j a_{ij}$$

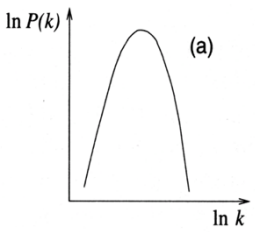
$k_4 : 3...2...3$

Network characteristics: Degree distribution

The **degree distribution** *P(k)* is the probability that any randomly chosen vertex has degree *k*; the **total degree** distribution is given by:

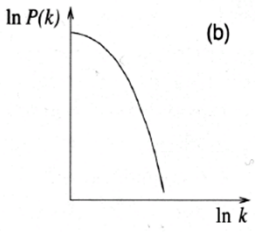
Poisson

$$P(k) = \frac{e^{-\alpha}\alpha^k}{k!}, \text{ where } \alpha = \overline{k}$$



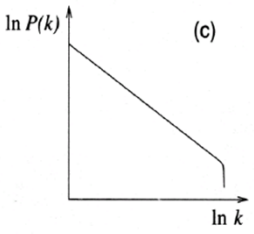
Exponential

$$P(k) \propto e^{-k/\alpha}, \text{ where } \alpha = \overline{k}$$



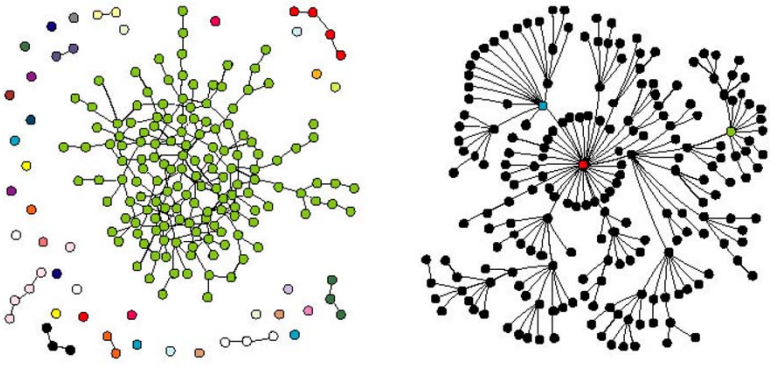
Power law

$$P(k) \propto k^{-\gamma}, \; k \neq 0$$



Source: Dorogovtsev, S. N. and Mendes (2003)

Network architectures for typical degree distributions

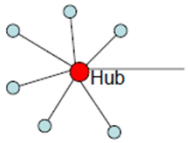


Left: random graph (Poisson), right: scale-free network (power law).
Source: Strogatz, S. H. (2001)

Random Failure and Attack Tolerance

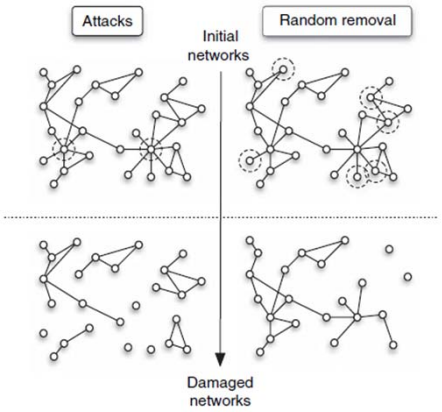
type of impact	exponential network	scale-free network
random	robust	extreme robust
malicious attack	robust	extreme vulnerable

scale-free network:



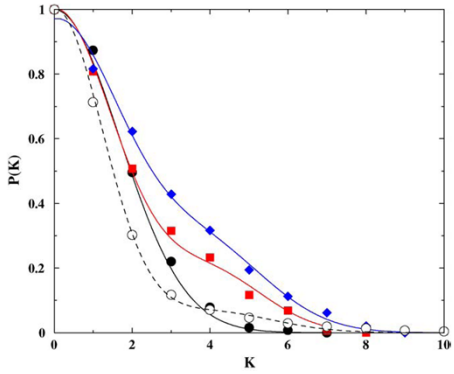
the chance to destroy the hub with a random attack is 1:7

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



Schematic comparison of random and targeted removal. On the left, we show the effects of targeted attacks on the two nodes with largest degrees. The resulting network is made of small disconnected components. In the case of random removal of six nodes (right column), the damage is much less significant as there is still a path between most of the nodes of the initial network.

Degree distributions – Electric power systems

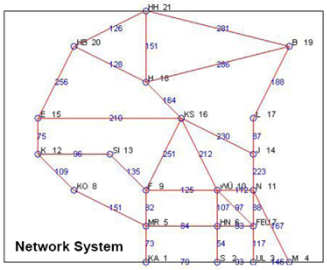


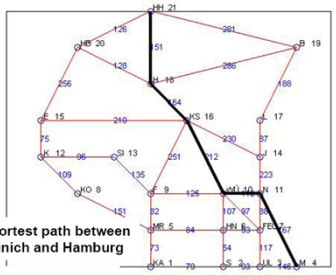
Cumulative distribution of the node degrees for the high-voltage transmission networks in Italy (full circles), Spain (diamonds) and France (squares). The empty circles represent the Italian „fine-grain“ network (from 380kV down to the distribution level).

Source: V. Rosato, *S. Bologna, F. Tiriticco*: Topological properties of high-voltage electrical transmission networks, Electric Power Systems Research, Vol. 77, 2007

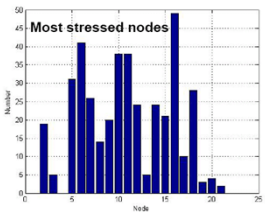
Network Characteristics: Shortest Path

Example: Highway Network





Most stressed nodes (“betweenness”): most utilized nodes in all shortest paths



Network characteristics: Clustering coefficient C

How interlinked are my friends?

C measures the density of connections around a particular node.
Suppose you have *z* close friends.

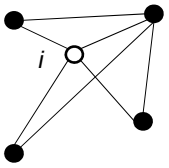
If they all are again friends among themselves there will be:

$$C_{max} = \frac{z(z-1)}{2}$$

links between them. Suppose that there are only *y* connections between them*C* will be

$$C = \frac{2y}{z(z-1)} = \frac{y}{C_{max}}$$

Example:



C_i=0.5

Recommended literature on network theory

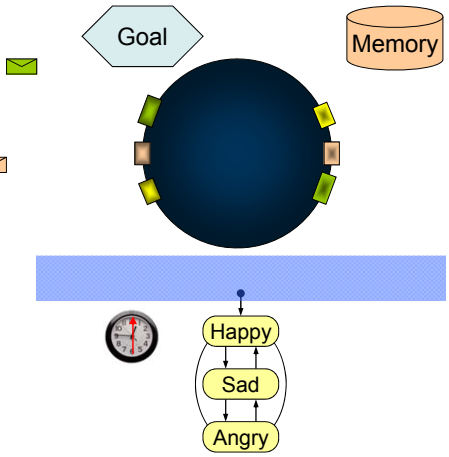
- Dorogovtsev, S.N. And Mendes, J.F.F., “Evolution of Networks – From Biological Nets to the Internet and WWW”, (Oxford University Press, Oxford, 2003)

Object-oriented modeling approach – framework

- Modeling the behaviour of the **components** (objects) and their interaction with the environment
- Stochastic simulation (Monte Carlo methods) of all components to investigate the **macro-behaviour** of the whole system
- In contrary to established methods for risk analysis (ETA, FTA) the observed scenarios and system states are not predefined, but they emerge during the simulation (**emergence**)
- Frequency and consequence of events are determined **"experimentally"**

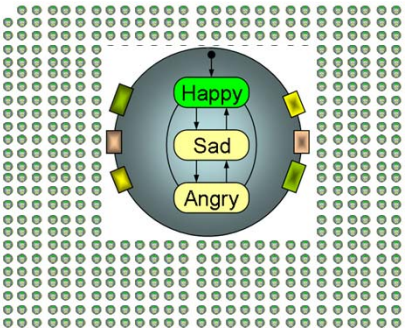
An object…

- Has different states (Finite State Machine, FSM)
- Is capable of interaction with its environment (e.g. other objects)
- Has „receptors" and „effectors" for specific („messages") and non-specific (environmental variables) signals
- Can act randomly
- May have a memory (learning)
- Can strive for a goal



Simulation of N objects

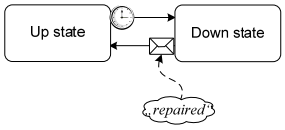
- One single object does not tell us much about the behaviour of its macro-system
- Therefore every component of a system has to be modelled separately by an object
- By the computational simulation of all objects, the global system behaviour and the system states s emerge



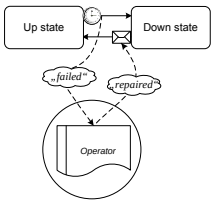
How to build a simplified object-oriented model for reliability analysis

1. Identify the components of the system
2. Determine the states of each component by making use of FSM, e.g.:

3. Determine the transitions between the states and their triggers (e.g. lapse of time or signal from outside)

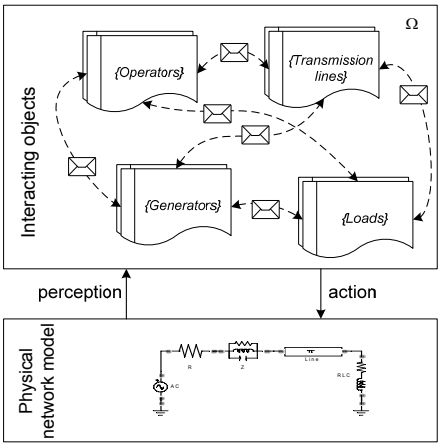


4. Establish the communication among the objects:

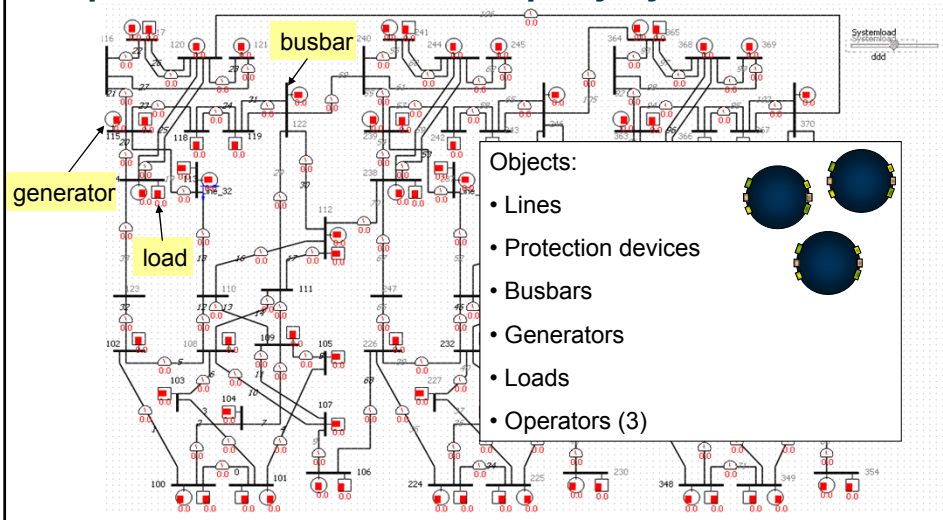


5. Simulate your model to generate the system states *s* and estimate failure probabilities $\bar{Q}$

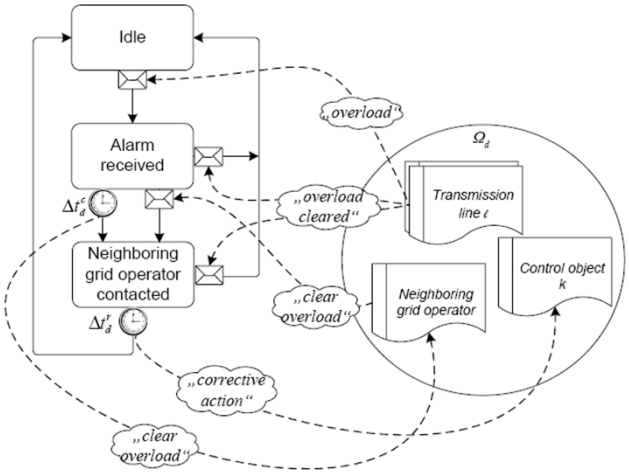
Modeling the Electric Power System – Two-layers approach



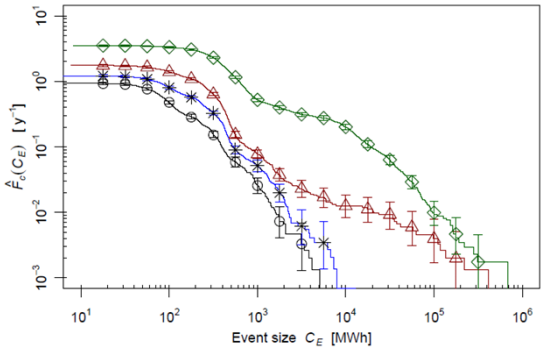
Implementation of an exemplary system



Objects: The Operator as an Example



Results: Expected Frequencies of Blackouts



Complementary cumulative blackout frequencies for four different system loading levels L=1.0, 1.1, 1.2 and 1.37 (circles, stars, triangles and diamonds, respectively) without operator intervention. The error bars indicate the 90% confidence interval.