Risk and Safety

in

Civil, Surveying and Environmental

Engineering

Prof. Dr. Michael Havbro Faber

Swiss Federal Institute of Technology

ETH Zurich, Switzerland

Contents of Today's Lecture

- The JCSS Framework for Risk Assessment
- Normative Procedure for Risk Assessment
- Techniques for System Identification
  - PHA
  - FMEA
  - FMECA
  - HAZOP
  - Risk screening
- Tools for Risk Analysis
  - Fault trees
  - Event trees

The JCSS Framework for Risk Assessment

- Decisions and decision maker

  A decision is:

  a committed allocation of resources

  the decision maker thus has responsibility for the committed resources – but also responsibility to any third party which may be affected by the decision

  the benefit of the decision should at least be in balance with the committed resources – this depends on the preferences of the decision maker – measured in terms of attributes

The JCSS Framework for Risk Assessment

- **Decisions and decision maker**

  Society – and decision making for society

- **Oxford: society - can be defined as:**

  a particular community of people living in a country or region, and having shared customs, laws, and organizations

  + sharing resources
  + sharing stakes
  + sharing values and moral settings – e.g. UN charter

The JCSS Framework for Risk Assessment

- Decisions and decision maker

  Society – and decision making for society

- For the purpose of decision making it is important to establish

  - preferences/values of decision maker
  - available resources, e.g. budget limitations
  - exogenously given boundary conditions
  - rights and responsibilities

The JCSS Framework for Risk Assessment

- Decisions and decision maker

  Society – and decision making for society

- It is in principle to define societies at different scale
  - Supranational authority
  - National authority and/or regulatory agencies
  - Local authority
  - Private owner
  - Private operator
  - Specific stakeholders

The differences are given by boundary conditions, resources preferences, responsibilities and rights

The JCSS Framework for Risk Assessment

- **Attributes of decision outcomes**

  Decisions aim to achieve an objective

  The degree of achievement is measured by attributes

  - natural attributes (measurable, e.g. costs and loss of lives)
  - constructed attributes (a function of natural attributes e.g. GDP)
  - proxy attributes (indicator which measures the perceived degree of fulfilment of an objective)

The JCSS Framework for Risk Assessment

- Preferences among attributes - utility

  The attributes associated with a decision outcome may be translated into a degree of achievement of the objective by means of a utility function

  different attributes are brought together on one or several scales

  multi attribute decision making implies a weighing of different attributes

The JCSS Framework for Risk Assessment

- Constraints on decision making

  In principle – any society may define what they consider to be acceptable decisions

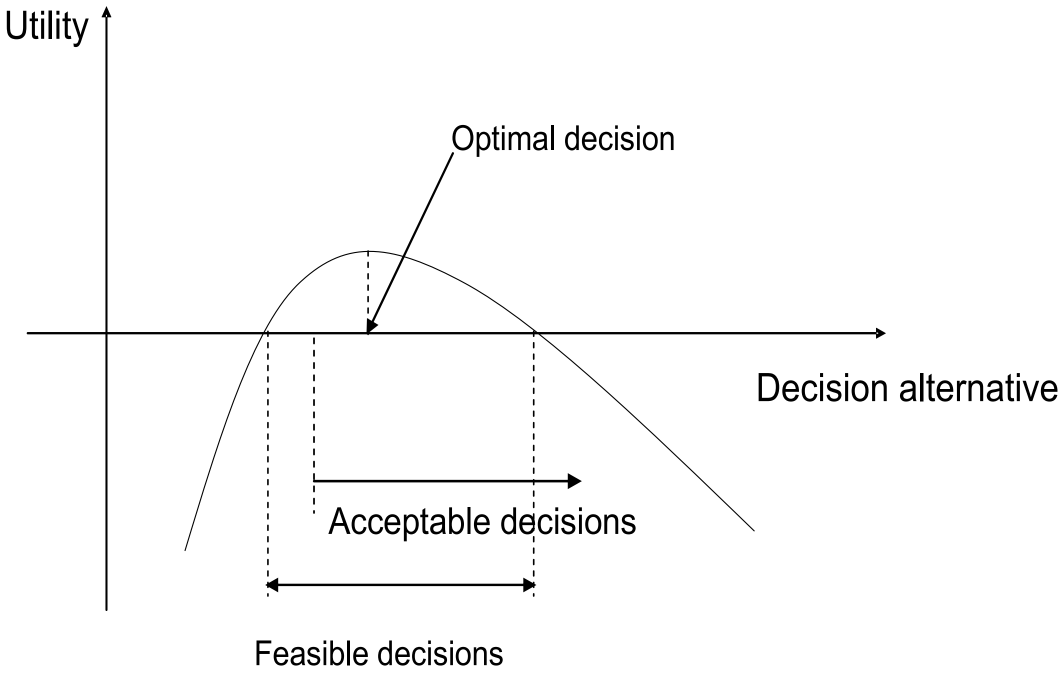
  Typically decisions are constrained – e.g. in terms of maximum acceptable risks to

  - persons
  - qualities of the environment

The JCSS Framework for Risk Assessment

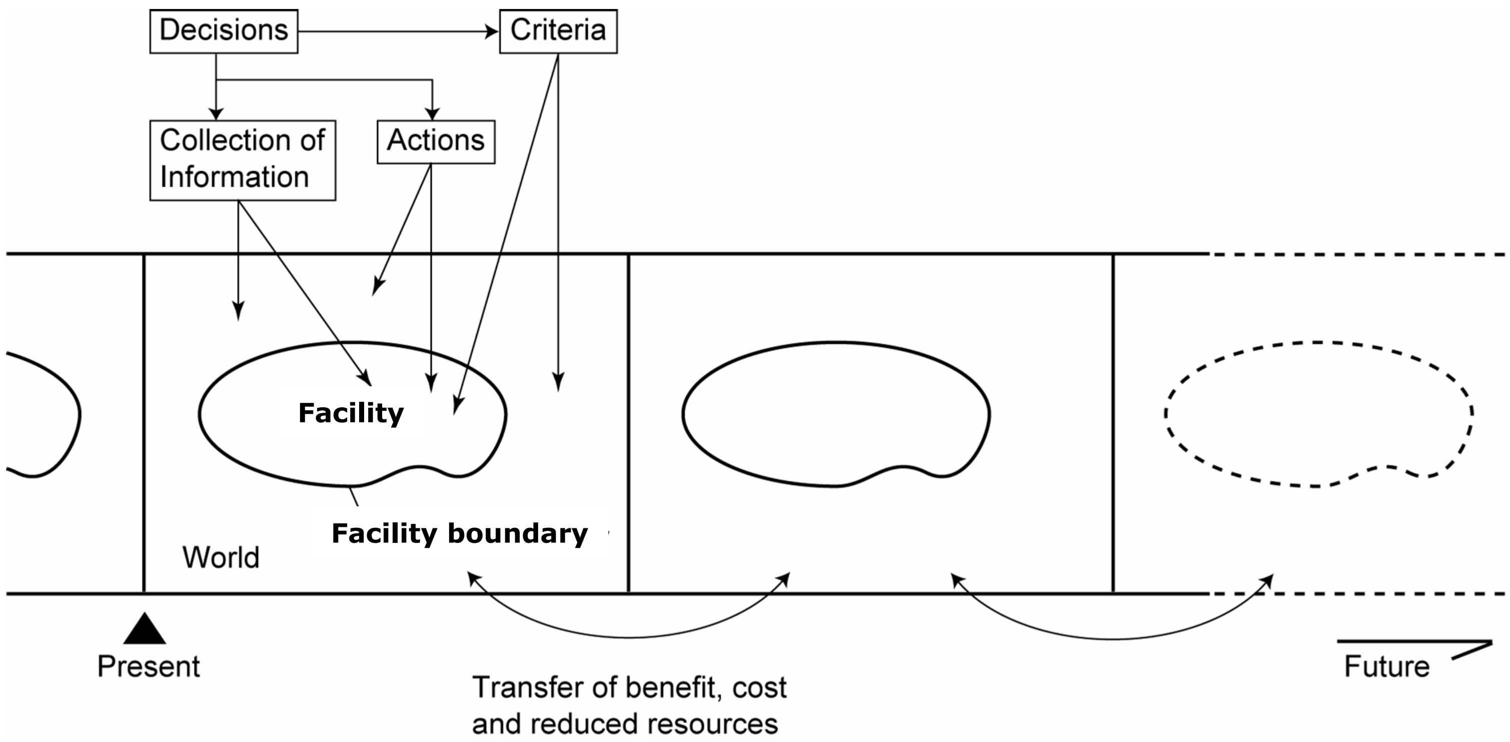
- **Feasibility and optimality**

  Feasible, optimal and acceptable decisions may be identified from



The JCSS Framework for Risk Assessment

- System modelling



The JCSS Framework for Risk Assessment

- **Knowledge and uncertainty**

  Remember that all uncertainties must be considered when the expected value of the utility is assessed

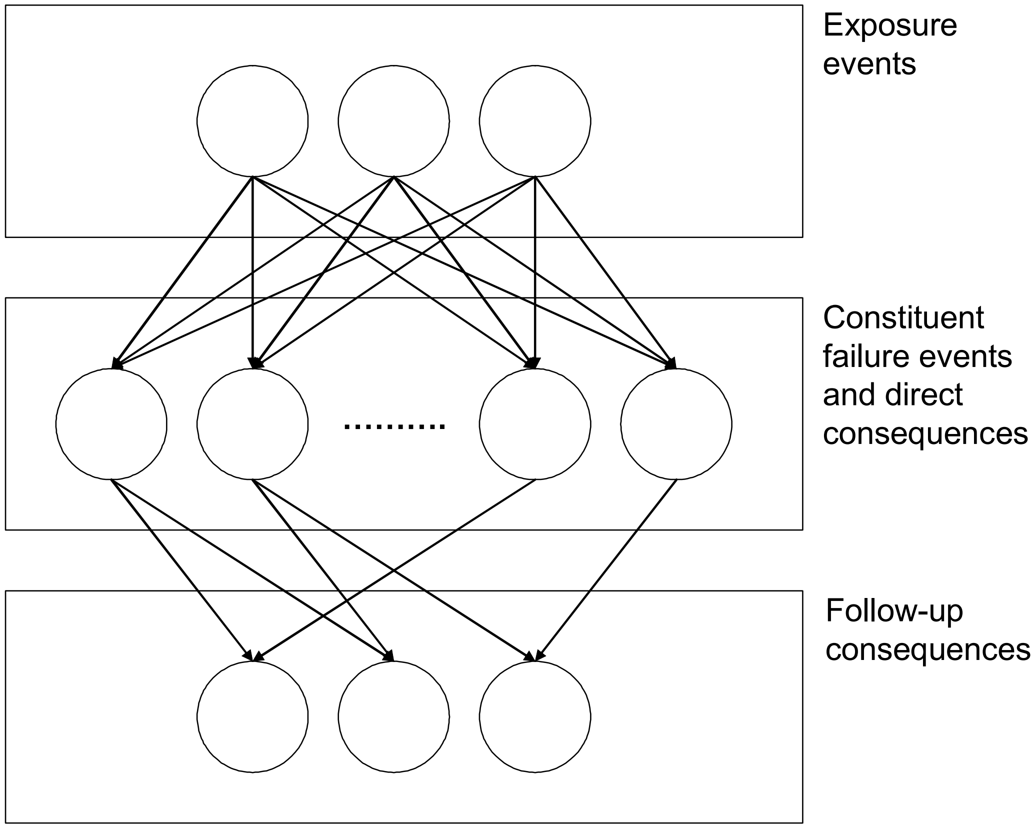
  - aleatory

  - epistemic

  It is important to address the possibility of the existence of different system hypotheses – and take this into account in the decision problem

The JCSS Framework for Risk Assessment

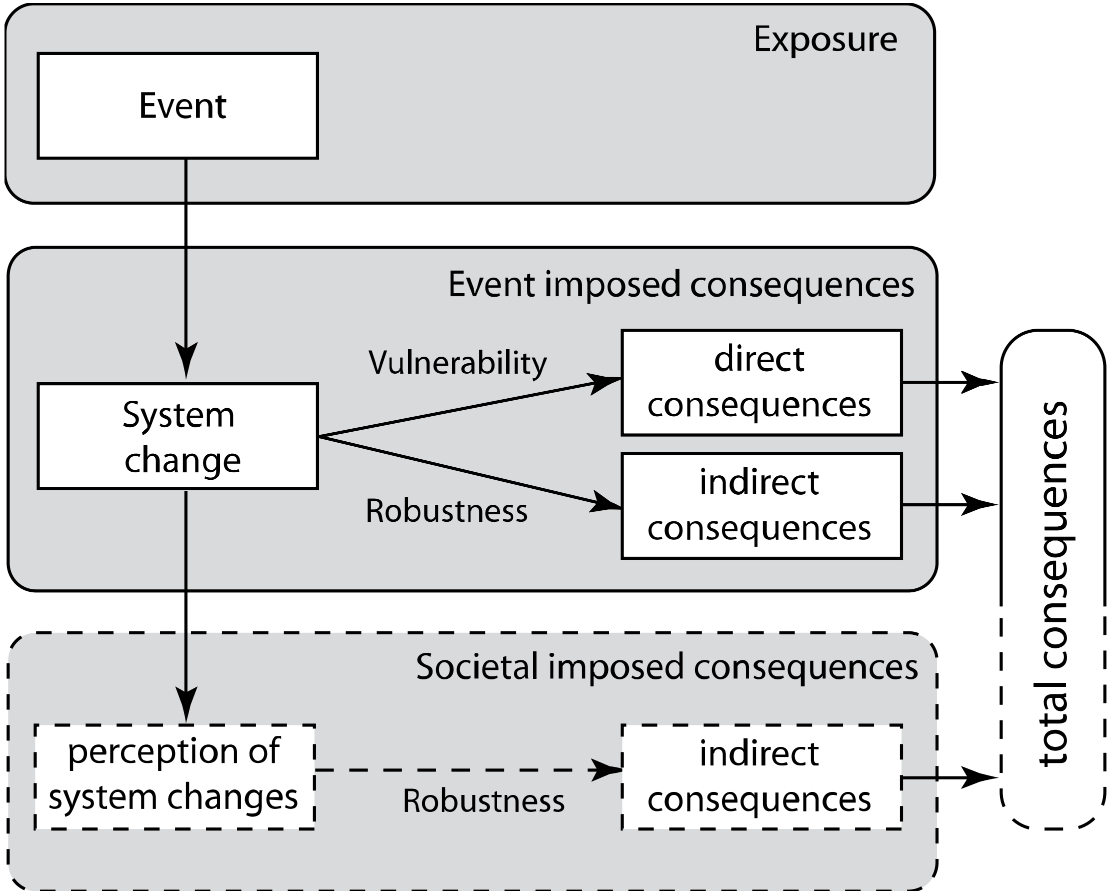
- System representation – scenarios of events



System representation must be refined enough to enable a comparison of the risks or benefits of different decision alternatives

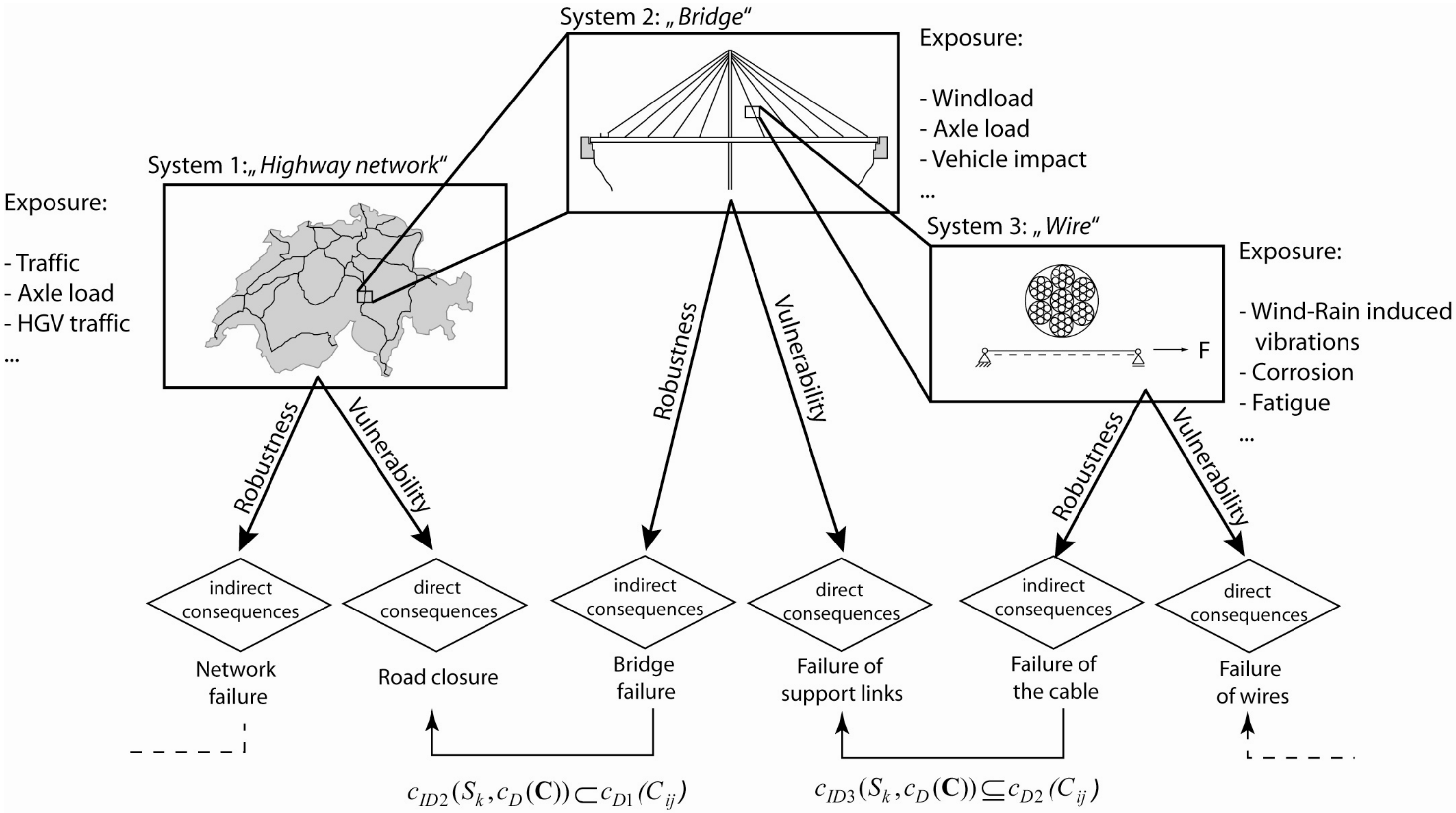
The JCSS Framework for Risk Assessment

- System representation – evolution of consequences



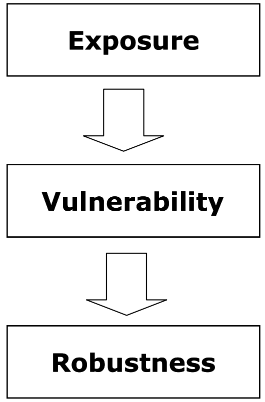
The JCSS Framework for Risk Assessment

- **System representation – multiple scales**



The JCSS Framework for Risk Assessment

- Assessment of risks



$p(EX_k)$

$p(C_{ij} | EX_k) c_D(C_{ij})$

$p(S_l | EX_k) c_{ID}(S_l, c_D(\mathbf{C}))$

Direct risks:

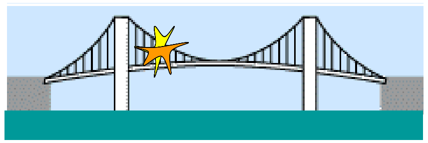
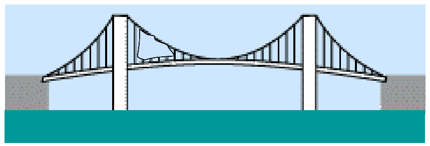
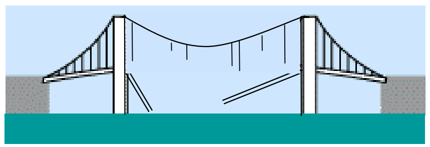
$$R_D = \sum_{k=1}^{n_{EXP}} p(C_{ij} | EX_k) c_D(C_{ij}) p(EX_k)$$

Indirect risks:

$$R_{ID} = \sum_{k=1}^{n_{EXP}} \sum_{l=1}^{n_{STA}} p(S_l | EX_k) c_{ID}(S_l, c_D(\mathbf{C})) p(EX_k)$$

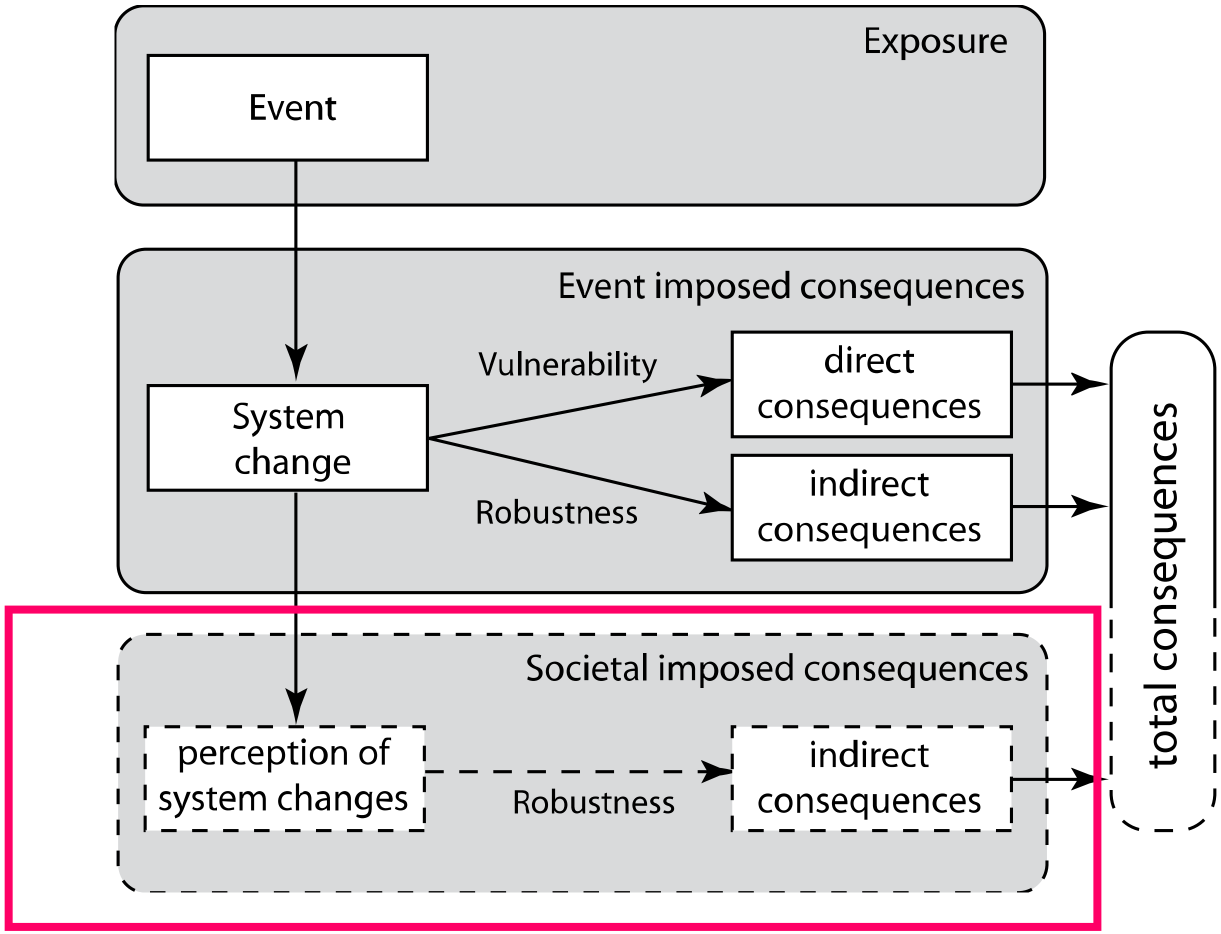
The JCSS Framework for Risk Assessment

- ## Indicators of risks

Scenario representation	Physical characteristics	Indicators	Potential consequences
Exposure 	Flood Ship impact Explosion/Fire Earthquake Vehicle impact Wind loads Traffic loads Deicing salt Water Carbon dioxide	Use/functionality Location Environment Design life Societal importance	
Vulnerability 	Yielding Rupture Cracking Fatigue Wear Spalling Erosion Corrosion	Design codes Design target reliability Age Materials Quality of workmanship Condition Protective measures	**Direct consequences** Repair costs Temporary loss or reduced functionality Small number of injuries/fatalities Minor socio-economic losses Minor damages to environment
Robustness 	Loss of functionality partial collapse full collapse	Ductility Joint characteristics Redundancy Segmentation Condition control/monitoring Emergency preparedness	**Indirect consequences** Repair costs Temporary loss or reduced functionality Mid to large number of injuries/fatalities Moderate to major socio-economic losses Moderate to major damages to environment

The JCSS Framework for Risk Assessment

- Risk perception



Due to perception of possible events

The JCSS Framework for Risk Assessment

- **Comparison of decision alternatives**

Optimal decision alternatives are selected by comparing expected total utility

$$E\left[U(a_j)\right] =$$

$$\sum_{k=1}^{n_{EXP}} p(C_{ij} \left| EX_k, a_j \right.) c_D(C_{ij}, a_j) p(EX_k, a_j) + \sum_{k=1}^{n_{EXP}} \sum_{l=1}^{n_{STA}} p(S_l \left| EX_k, a_j \right.) c_{ID}(S_l, c_D(\mathbf{C}), a_j) p(EX_k, a_j)$$

The JCSS Framework for Risk Assessment

- Discounting

  In evaluating the benefit and risk – the time of consequences as well as investments must be taken into account – by discounting

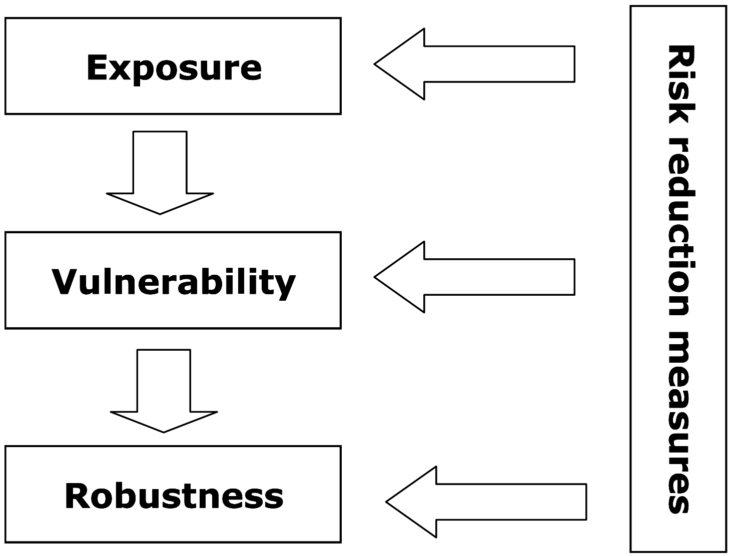
  - private discounting should consider long term investment return

  - public sector should consider only long term rate of economic growth – presently around 2 percent per annum

The JCSS Framework for Risk Assessment

- **Risk treatment – communication and transfer**

  - In principle risk may be treated at any level in the systems representation



Collecting more information

Changing the physical characteristics

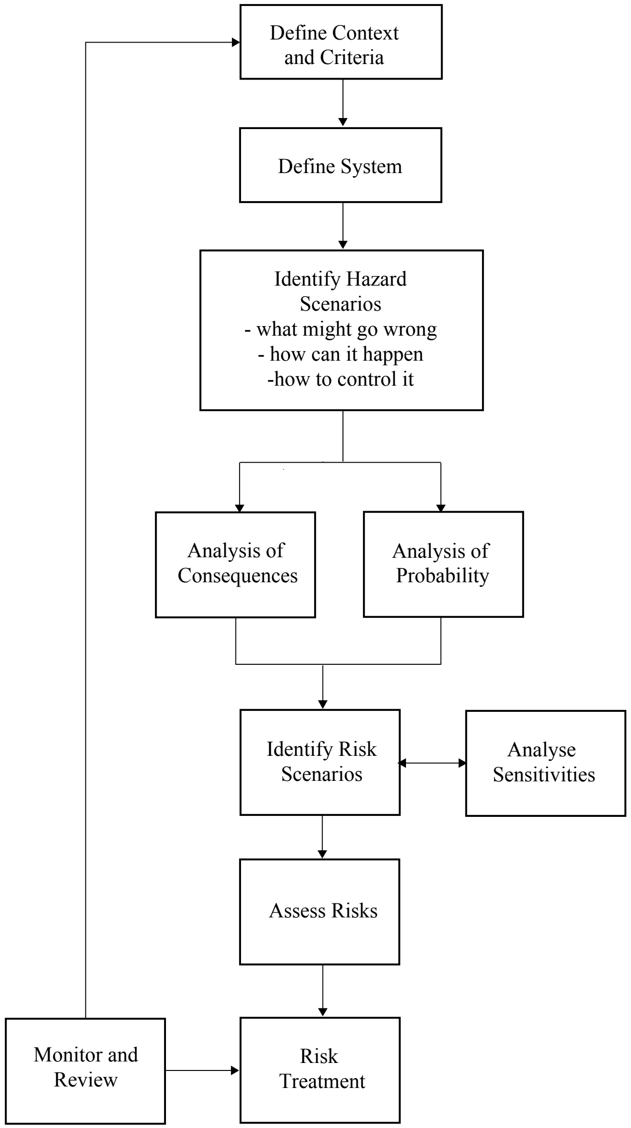
Risk information/communication

Transfer of risks - insurance

The Procedure of Risk Assessment

- Basically the same steps should be performed for any type of facility/application area

  Risk assessment procedures are generic



Techniques of System Identification

- Different techniques are available for the purpose of standardizing procedures of systems identification

  - PHA (preliminary hazard analysis)
  - FMEA (failure mode and effect analysis)
  - FMECA (failure mode effect and consequence analysis)
  - HAZOP (hazard and operability analysis)
  - Risk Screening (HAZID meetings)

  self study – for further details ☺

Risk Analysis Tools

- Different classical tools are available for the quantitative analysis of risks

  - Fault tree analysis

  - Even tree analysis

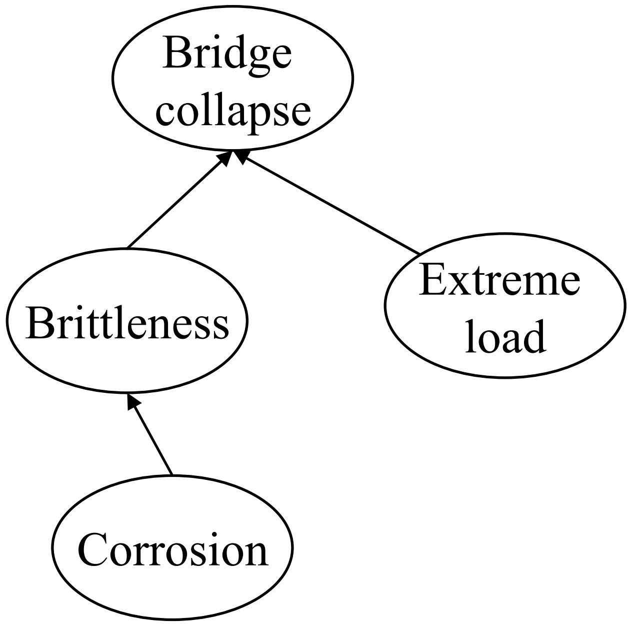
  - Cause/Consequence charts (a mix of the two above)

  Later we will look into an even stronger tool – which is also far more general – namely Bayesian Probabilistic Nets

Risk Analysis Tools

- **Fault tree analysis**

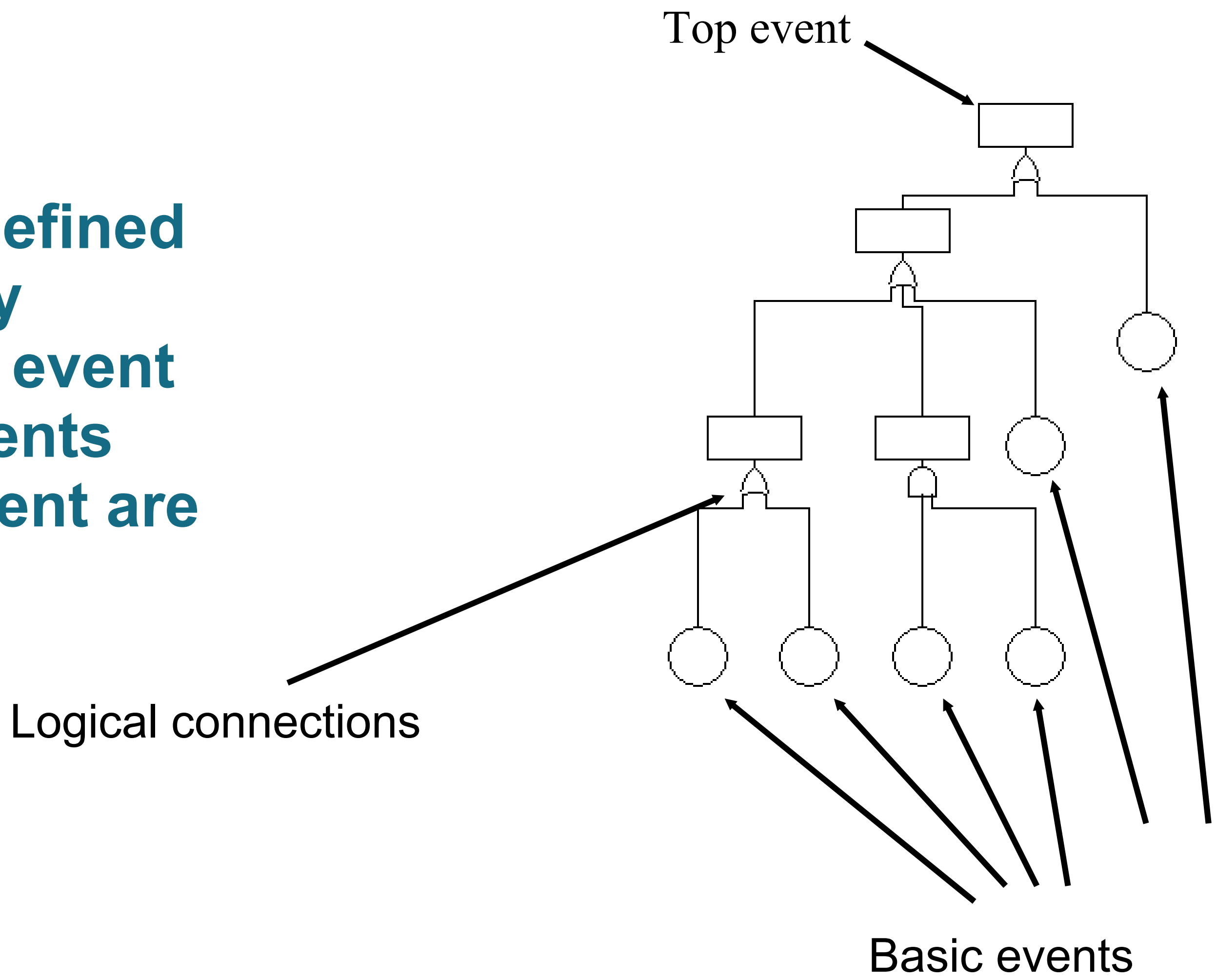
  A state of failure is defined as a top event and by logically interrelated event the sequences of events leading to the top event are modelled



Risk Analysis Tools

- **Fault tree analysis**

  A state of failure is defined as a top event and by logically interrelated event the sequences of events leading to the top event are modelled



Risk Analysis Tools

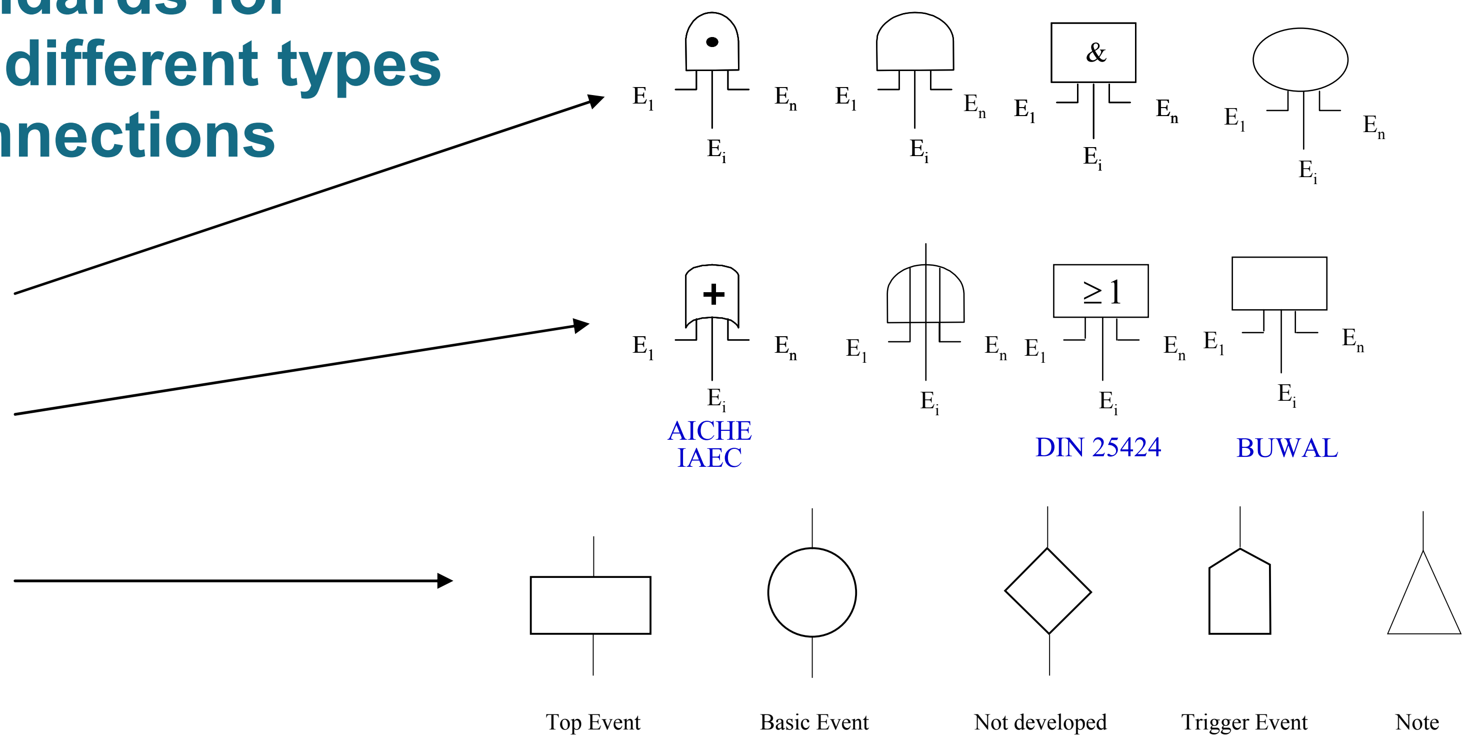
- **Fault tree analysis**

Different standards for denoting the different types of logical connections

“and” gates

“or” gates

event

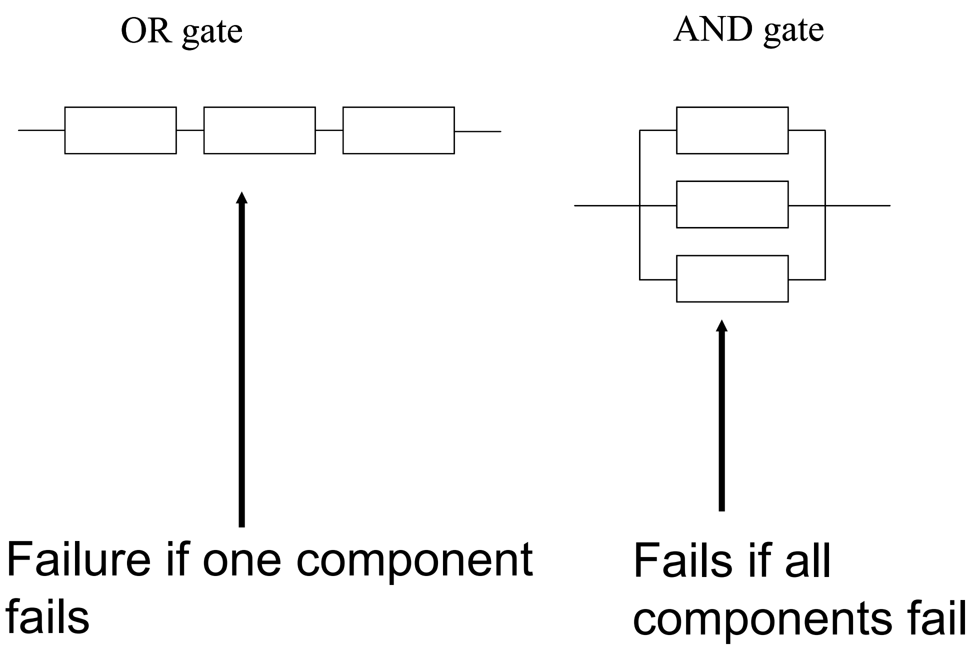


Risk Analysis Tools

- **Fault tree analysis**

  “and” gates will fail only if all components connected fail

  “or” gates will fail if any one of the components connected fail

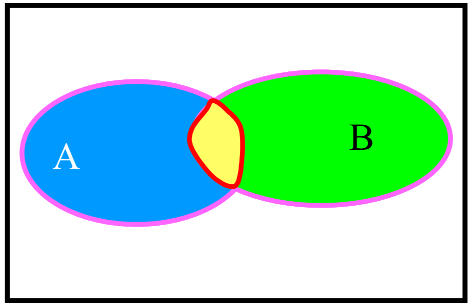


Risk Analysis Tools

- **Fault tree analysis**

  The probability of gate failure may be calculated easily from

  Assumption: component failures are independent



$$A \cap B = P(A)P(B)$$

$$P = \prod_{i=1}^{n} P_i$$

$$A \cup B = P(A) + P(B) - P(A)P(B)$$

$$P = 1 - \prod_{i=1}^{n} (1 - p_i)$$

Risk Analysis Tools

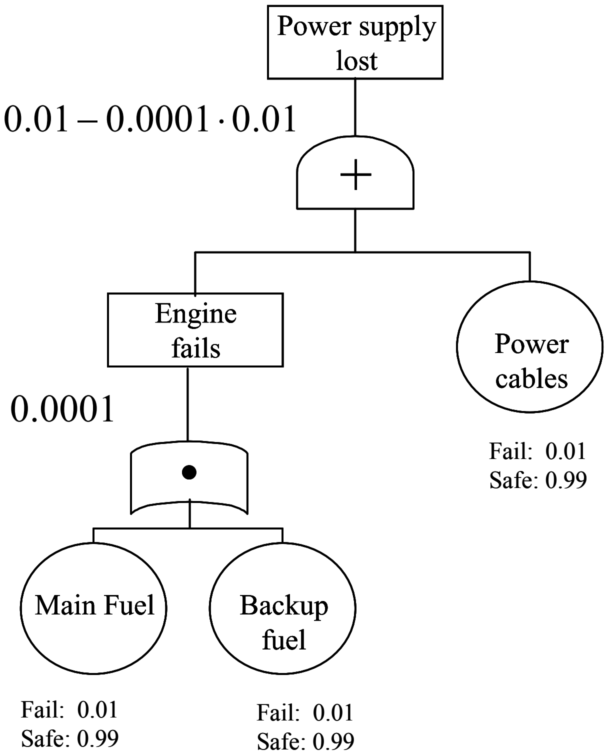
- **Fault tree analysis**

  Example: Power Supply System

  System failure of power supply is lost

$$P_{PF} = 0.0001 + 0.01 - 0.0001 \cdot 0.01$$
$$= 0.0101$$

$$P_{EF} = 0.01 \cdot 0.01 = 0.0001$$

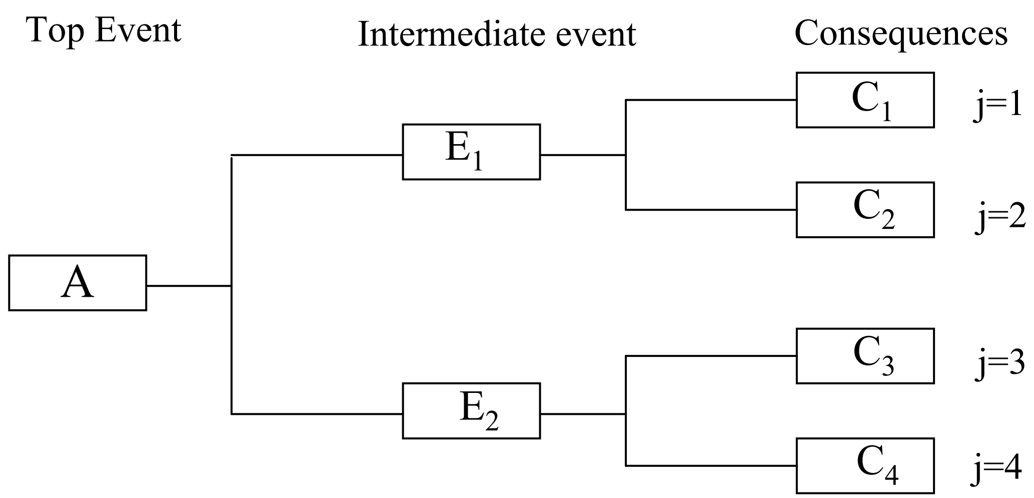


Risk Analysis Tools

- **Event tree analysis**

  An event tree typically starts from a top event – and attempts to model the consequences of such an event

  propagating the effect of e.g. an exposure or failure event



Risk Analysis Tools

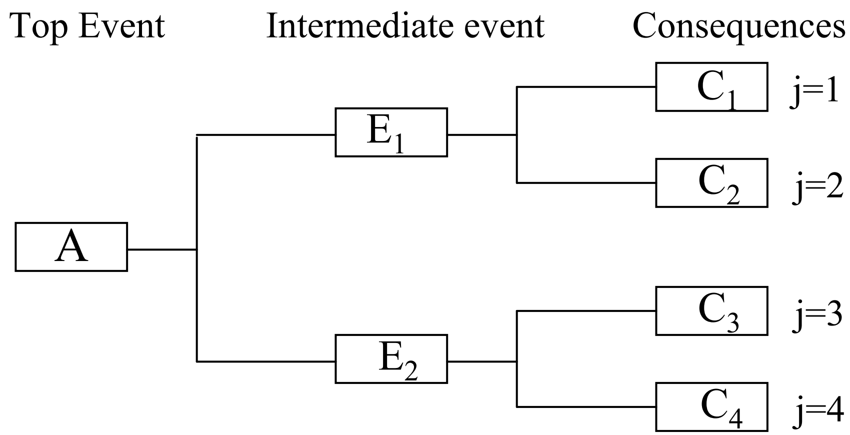
- Event tree analysis

  Assuming that the events are independent eases analysis – but dependencies must be taken into account !

$$P(C_j | A) = \prod_{i=1}^{n_j} P_{ij}$$

$$P(C_j) = P(A)P(C_j | A) = P(A)\prod_{i=1}^{n_j} P_{ij}$$

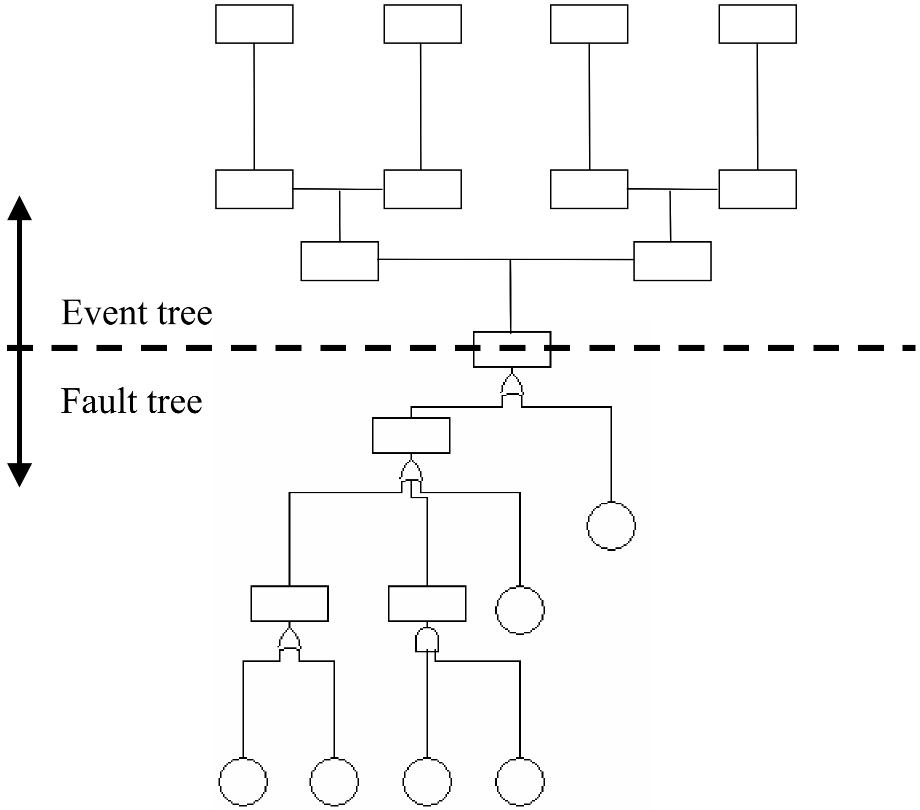
$$\text{Risiko} = R = \sum_{i=1}^{n} C_i P(C_i)$$

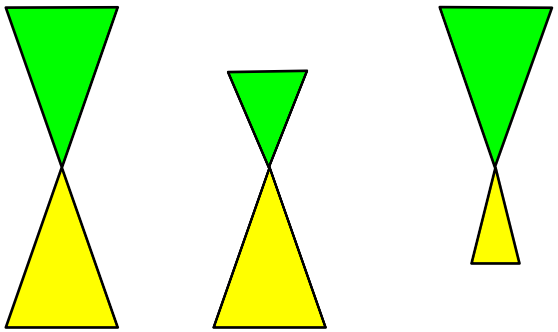


Risk Analysis Tools

- **Event tree analysis**

  Event trees are often used together with fault trees





Balanced | **Large fault tree** | **Large event tree**

Risk Analysis Tools

- Event tree analysis

  Example

  How is the event of power supply failure propagated to further consequences depending on whether the failure takes place during day or night