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 Analysis of Highly-integrated Systems

RB II: Principles and Methods for Risk Evaluation
(Target Lines, Cost-Benefit-Analysis)

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

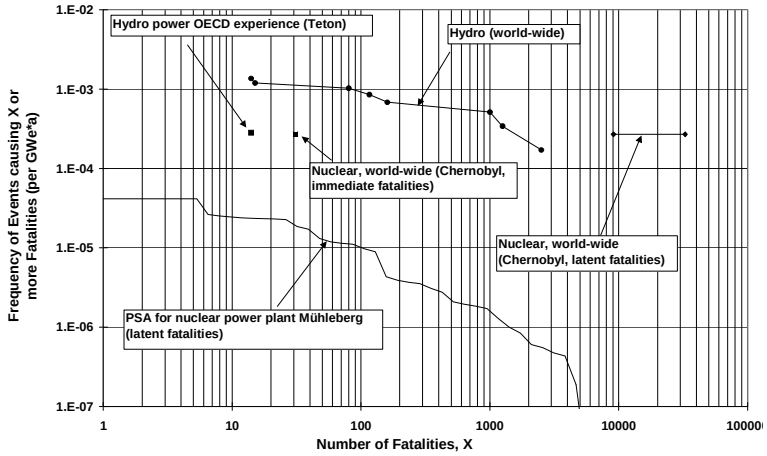
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT Departement Maschinenbau & Verfahrenstechnik: Department of Mechanical & Process Engineering

"How Safe is Safe Enough?"

- Answers given by internal or official requirements
  - Undesired event frequencies (e.g. IAEA: Total frequency of core melt down accidents 10-4/10-5 per reactor and year for old / new plants)
  - Risks smaller than the risk of alternatives (e.g. 1%) or regarded as unavoidable (natural) or accepted risks (threshold values/curves – individual or societal; e.g. traffic accidents)
  - Exclusion criteria (e.g. max. damage)
- Necessity of reasoning:
  - Comparison of risk information (F/C-diagrams)
  - ALARP-principle ("as low as reasonably practicable"), cost-benefit comparison of risk reducing measures
  - Cross comparison of the effectiveness of investments made ("life saving costs")

Assessing risks by using F/C-Diagrams - here comparative assessment of energy systems



GWe: Gigawatt electric

Risk assessment and comparison

To compare risk assessment results (e.g. F/C-diagrams), the different damage indicators must be aggregated, e.g. by

- Expected value of risk (one or more damage types)
- Risk-value trade-off-models (variance as a measure of risk)
- Damage indicators or index

These aggregations include basic ethical concepts and aren't therefore equally accepted.

Rating criteria of the Swiss Major Accidents Ordinance

Representation of possible damage dimensions:

- Hazardous incidents can cause various damages to the population or the environment:
- Life and health of people
- Destruction of living environment
- Property values

Different damages are measured by a set of damage indicators:

- n_1, Fatalities [number]
- n_2, Injured [number]
- n_3, Polluted surface water [volume in m^3 or area in km^2]
- n_4, Polluted ground water [loss in man-month]
- n_5, Soil with derogated soil fertility [area-years in $km^2 \cdot a$]
- n_6, Property damage [Mio. Fr.]

Rating of damage dimensions

The possible damage dimension of a failure is estimated by the use of damage indicators:

- Damage values between 0 and 1 are allocated to the damage dimension.
- Combinations of damage values are generally not necessary.
- Damage values ≥ 0.3 correspond to a severe damage (Major Accidents Ordinance is only valid for these damage values).
- Damage values > 1 are not to be expected in Switzerland.

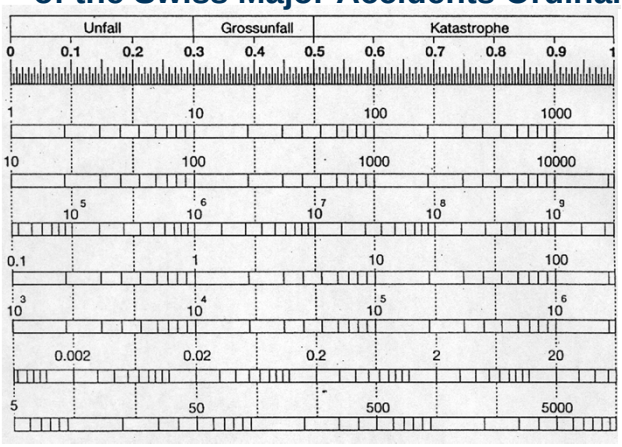
Uncertainties:

- In the process of risk assessments the uncertainties of damage dimensions and/or event frequencies must be discussed but need not be laid open.

Criteria for the rating of severe damage

Damage indicator	Criteria for severe damage (damage value ≥ 0.3)
Fatalities	10 fatalities
Injured	100 injured
Polluted surface water	Pollution of about $10^6 m^3$ of water or 1 km^2 of water surface.
Polluted ground water	Stoppage of a groundwater well of about 10'000 man-month
Soil	Derogated soil fertility of about 0.02 km^2 for at least one year
Property	Property damage of about 50 million Fr.

Damage indicators and corresponding damage values of the Swiss Major Accidents Ordinance



Damage indicator

n_1, Fatalities [number]

n_2, Injured [number]

n_3, Polluted surface water [volume in m^3]

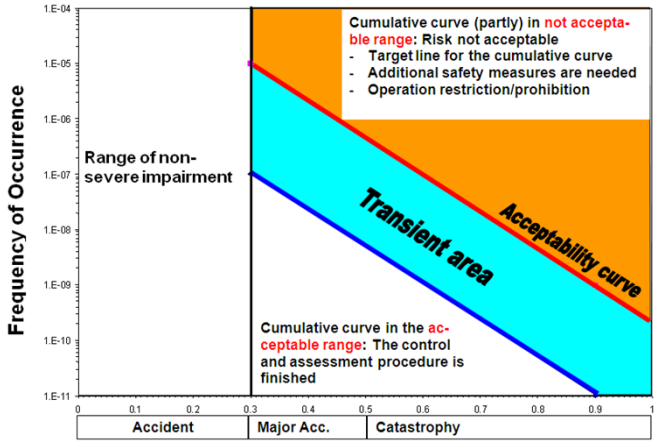
n_3, Polluted surface water [area in km^2]

n_4, Polluted ground water [loss in man-month]

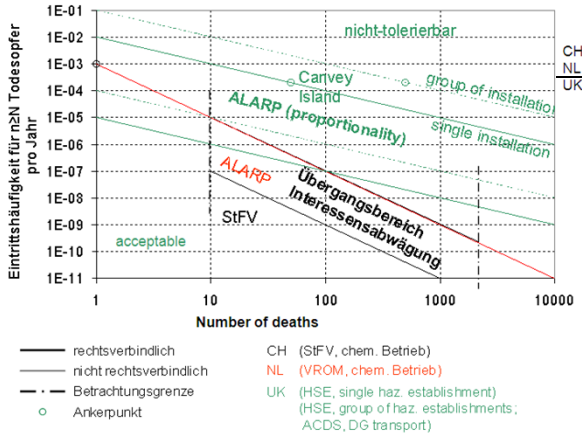
n_5, Soil with derogated soil fertility [area-years in $km^2 \cdot a$]

n_6, Property damage [Mio. Fr. index of 1996]

Tolerability assessment of risk (on risk analysis level)



Comparison of acceptability curves



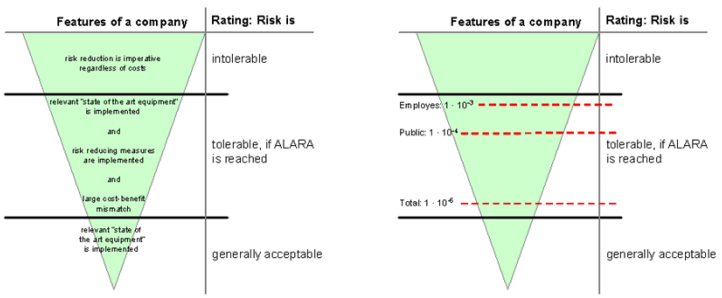
	Reference	Indication of acceptability curves
CH	Based on everyday life risks	Risk aversion (Exponent 2)
NL		
UK	Based on the accepted risk of the Canvey Island chemical facility	No risk aversion (Exponent 1)

Tolerability of risk

- A band between the point of maximum tolerability (above which a project must be abandoned altogether) and the point of minimum tolerability (below which a risk is so small that the project can proceed without formal assessment).
- A “tolerable risk” is one that society is prepared to live with in order to have certain benefits and in the confidence that the risk is being properly controlled.
- An “acceptable risk”, which implies that the risk, although present, is generally regarded by those exposed to it as not worth worrying about.
- These different perceptions mean that there is scope for confusion in communicating with the public and non-specialists on risk issues, and great care needs to be taken.

Costs versus benefit as rating scale

ALARP (As Low As Reasonably Practicable), HSE (UK):
Principle of cost-benefit optimization: The optimum is reached when the ratio between saved accident costs (increased security) and investment in security measures is “reasonable”. The acceptability of the ratio depends on the risk situation; maximum security is not reached.



Chain of action when applying the ALARP-principle

1. Identification of influencing factors and available options
2. Quantification of the relevant factors
3. Comparison and selection of options
4. Sensitivity analysis
5. Results

ALARA: As Low As Reasonably Achievable

1. Identification of influencing factors and available options

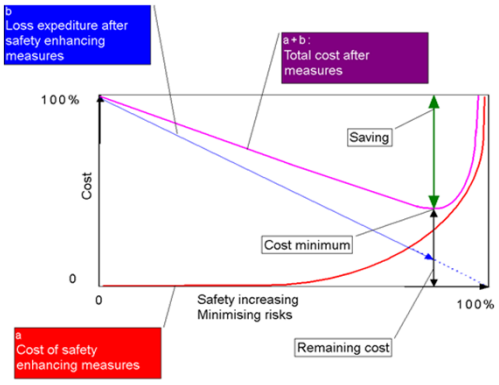
Distinguish between quantifiable (e.g. costs, radiation dose) and not quantifiable (e.g. political decision making process) factors

Cost as central factor for

- Safety measures:
  - Capital expenditure: from planning to operating stage of a facility, installations, equipment, training of personnel, etc.
  - Operational cost: salary, operation, administration, maintenance, reparation, etc.
- Loss expenditure
  - Health damaging effects (lethal or not lethal)
  - Non health damaging effects (e.g. loss of image)

Options are various technical and/or organisational measures for exposition minimization. They are often derived from the analysis of the influencing factors (e.g. protection walls, protective equipment, etc.).

2. Quantification of the relevant factors
   Based on models and simulations
3. Comparison and selection of options
   - Simple problems: Intuitive comparison - expert judgment, “best practice”
   - Complex problems: Quantitative, decision aids like Cost-Benefit Analysis

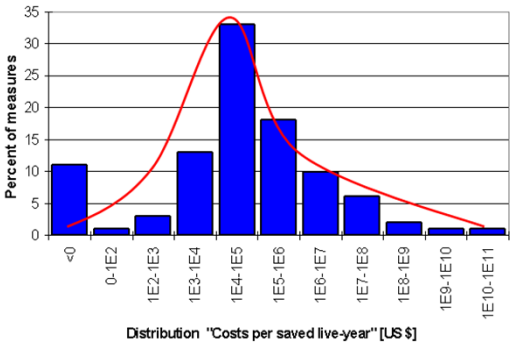


Costs for safety enhancing measures

To save lives means that we end up with additional life years. The cost of implementing safety measures can therefore be translated into cost of measures per life year.

Measure	Life saving costs (1000$ per saved life)
PAP - Test	25
Mobile treatment of heart attacks	15-30
Security belts on front seats ()	25-110
Flying ban for DC-10	30’000
New regulations for high-rise buildings ()	100’000
Asbestos abatement in schools	Up to 1’400’000
Hydrogen-recombinators in nuclear power plants	3’000’000

Distribution of the costs per saved life



- 587 measures from different fields (road safety, fire and radiation protection, etc)
- Value < 0: benefit of the measures is higher than its costs

Source: Risk Analysis, Tengs et al., "Cost-Effectiveness of Saving Lifes"

Criticality of Infrastructures: EU Document "COM (2004) 702 final" Critical Infrastructure Protection in the Fight against Terrorism"

The criteria for determining the factors that make a particular infrastructure or element of an infrastructure critical need to be studied. These selection criteria should also be based on a sectorial and collective expertise. Three factors might be suggested for identifying potential critical infrastructure:

- Scope - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, provincial/territorial or local.
- Magnitude - The degree of the impact or loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which could be used to assess potential magnitude are: public impact, economic, environmental, interdependency, political.
- Effects of time - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other)