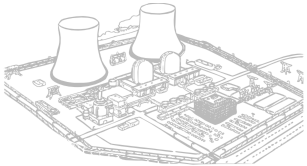
RISK ENGINEERING



Risk acceptability and tolerability

Eric Marsden

<eric.marsden@risk-engineering.org>

How safe is safe enough?

Warmup. Before reading this material, we suggest you look through:

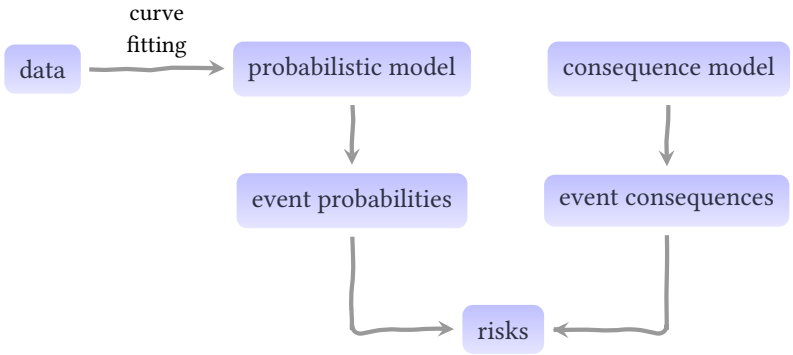
- slides on risk metrics (how to measure risk levels?)
- slides on risk perception

Available from `risk-engineering.org` & `slideshare.net`

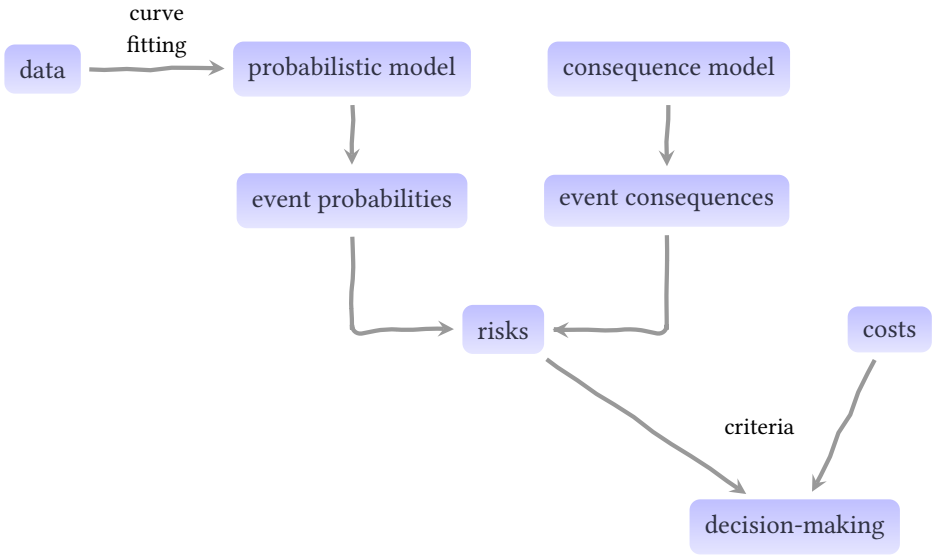
What is risk acceptance?

- Risk acceptance issues affecting **individual decisions**:
  - *Should I buy airplane tickets on Tinkertown Airlines, which are 300€ cheaper than Air Reliable?*
  - *Do I go skiing hors piste?*
- Risk acceptance issues affecting **societal decisions**:
  - *Encourage nuclear power plants, or coal-fired plants, or increased electricity pricing?*
  - *Should we allow genetically modified foods?*
- Note: risk acceptance is often controversial both in theory and in practice…

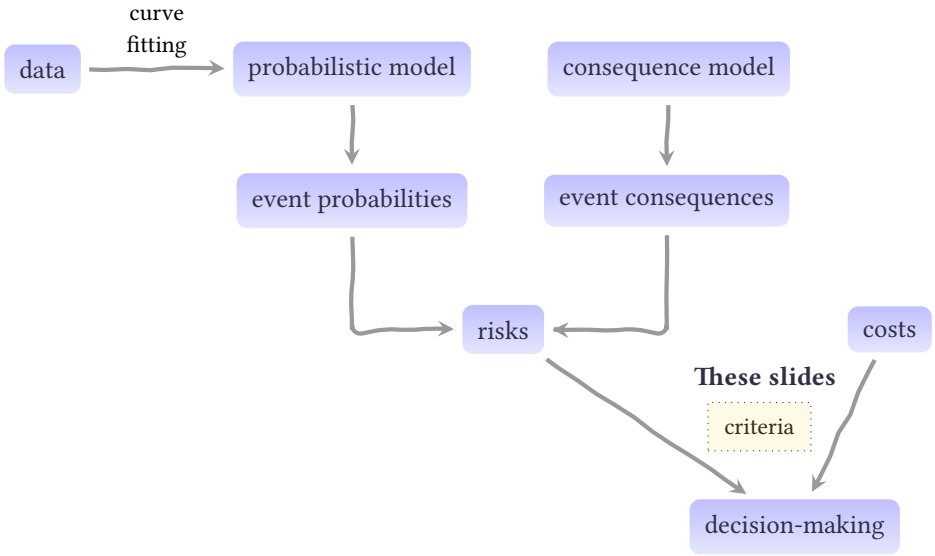
Where does this fit into risk engineering?



Where does this fit into risk engineering?

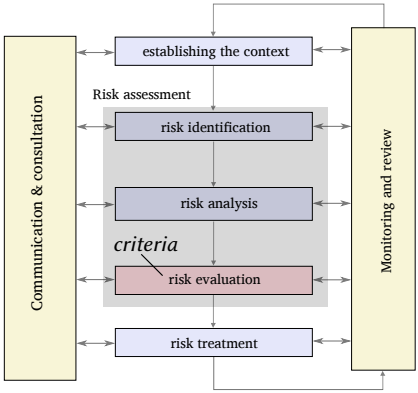


Where does this fit into risk engineering?



Risk acceptance criterion

- Criterion: a standard of judging; any established law, rule, principle or fact by which a correct judgment may be formed
- Risk acceptance criteria: criteria used as basis for decisions about acceptable risk, during the **risk evaluation** phase of risk analysis
- **Risk evaluation**: comparison of risk analysis results with risk criteria in order to determine whether a specified level of risk is acceptable or tolerable



The risk management process, according to the ISO 31000 standard

Risk acceptance criteria: examples

▷ Some examples of qualitative risk acceptance criteria:

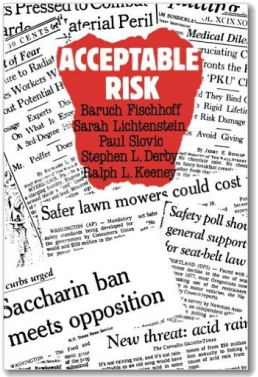
- *"All avoidable risks shall be avoided"*
- *"Risks shall be reduced wherever practicable"*
- *"The effects of events shall be contained within the site boundary"*
- *"Further development shall not pose any incremental risk"*

Risk acceptance criterion

- Risk acceptability is inherently **contingent** on time and situations, and is hence never absolute, nor universal:

> *The act of adopting an option does not in and of itself mean that its attendant risk is acceptable in any absolute sense. Strictly speaking, one does not accept risks. One accepts options that entail some level of risk among their consequences.*

- An extensive social sciences literature develops these concepts and relationships with risk perception, trust, communication and governance

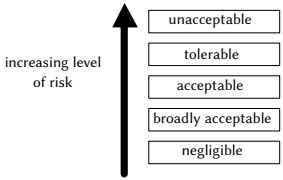


Source: *Acceptable Risk*, Fischhoff et al. 1981

“Tolerable” risk

- UK *Health and Safety Executive* distinguishes between *tolerable* and *acceptable* risks:

> *“Tolerability” does not mean “acceptability”. It refers to a willingness to live with a risk so as to secure certain benefits and in the confidence that it is being properly controlled. […]*
>
> *For a risk to be “acceptable” on the other hand means that for purposes of life or work, we are prepared to take it pretty well as it is.*



- ISO 31 000 standard:
  - *risk appetite*: the amount and type of risk that an organization is prepared to pursue, retain or take
  - *risk tolerance*: organization/stakeholder’s readiness to bear risk after risk treatment in order to achieve its objectives

Source: *The tolerability of risk from nuclear power stations*, UK HSE, 1992

Factors influencing risk acceptance

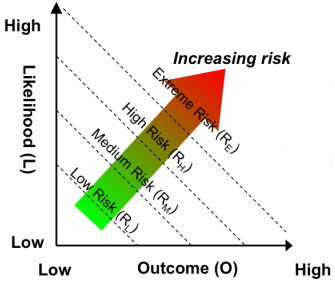
- Objective level of risk generated by a project
- Is the origin of the risk natural or industrial/technological?
- Is the nature of the hazard familiar or unfamiliar?
- Are the possible effects memorable or easily forgotten, dreaded or not?
- Is the hazard of a catastrophic or a chronic nature?
- Is exposure to the risk perceived to be fair or unfair?
- Is the activity perceived to be morally relevant?
- Are sources of information concerning the risk and the activity perceived to be trustworthy?
- Is the governance of the industrial activity and the risk management process perceived to be open and responsive?

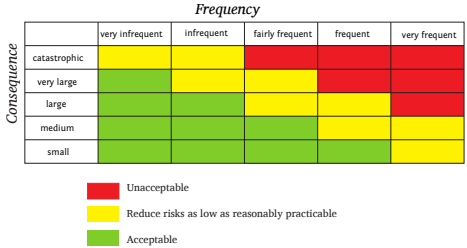
Decision rules

Absolute risk targets

- **Aviation** safety: probability of catastrophic failure should be less than 10^{-9} per flight hour
  - other targets for Hazardous, Major and Minor severity effects
  - accompanied by a design principle: *In any system or subsystem, the failure of any single element, component, or connection during any one flight should [...] regardless of its probability [...] not be Catastrophic.*
- **Air traffic management**:
  - maximum tolerable probability of ATM directly contributing to an accident of a commercial air transport aircraft of $1.55 \cdot 10^{-8}$ accidents per flight hour
- **Maritime** safety, for new ships:
  - maximum tolerable probability of fatality for crew members: 10^{-4} per ship-year
  - maximum tolerable probability of fatality for passengers or public: 10^{-5} per ship-year

Risk matrix



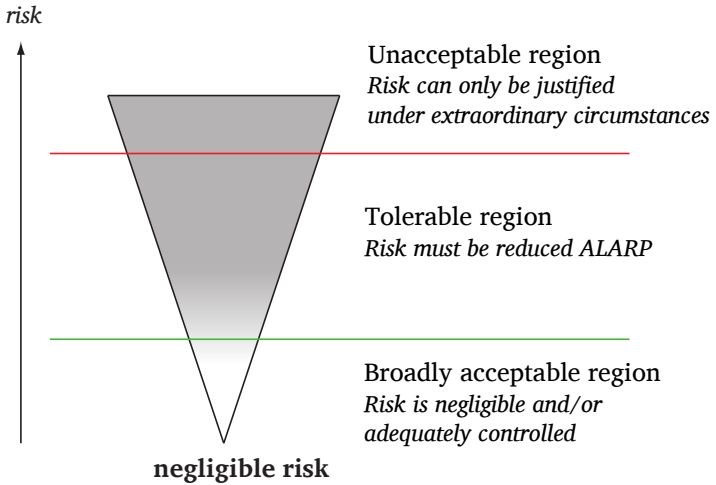


- Risk matrices are widely used in the process industry
- Companies and regulators use specific frequency and consequence thresholds
  - *where is the cutoff between "infrequent" and "fairly frequent" for our activity?*

Risk matrix

- The risk matrix (also called a "heat map") can be used for three main purposes:
  - determine how significant each risk is
  - prioritize or rank risks relative to one another to help allocate safety spending
  - highlight areas for further more detailed risk assessment (*e.g.* fully quantitative rather than qualitative for higher level risks)
- When used for decisions related to acceptability of a hazardous activity, the **aggregate risk level** should be used
  - all risks from the facility added together then positioned in the matrix
  - it's not sufficient for each accident scenario from the facility to be in an "acceptable" location of the matrix, considered in isolation!

ALARP principle



ALARP: As Low As Reasonably Practicable

ALARP principle

- The ALARP principle is fairly widely used
  - for example by UK HSE
  - similar concepts: ALARA ("as low as reasonably acheivable") used concerning radiation protection, SFAIRP ("so far as is reasonably practicable")
- Much discussion revolves around interpretation of the term "**reasonably**"
  - companion principle ASSIB ("And Still Stay In Business") is also important
- To determine "**reasonably practicable**", either:
  - refer to industry standards and good practice
  - use **benefit-cost analysis** with a "gross disproportion factor"

→ *Benefit-cost analysis slides at* `risk-engineering.org`

Compromise on safety? Never!

- Implicit in ALARP approaches is the idea of balancing safety benefits with their costs
- Some observers/critics refuse this type of compromise out of principle
- Certain safety authorities and regulators seem quite embarrassed by the issue and avoid mentioning it in public communications
- Others acknowledge the issue in a transparent manner, see commitments from UK Office of Nuclear Regulation in its Strategy 2020-25 document (point 3 below)

To our licensees and dutyholders:

- be open to innovation in both how and what we regulate;
- systematically seek and use inspection and intervention feedback to improve our impact;
- provide greater clarity about the costs of our regulatory decisions;
- seek more learning from UK and international organisations to improve the outcomes we influence and ensure no unnecessary regulatory burden;
- act as an enabling regulator consistently across industry;
- be more efficient and effective.

MEM decision rule

- MEM: Minimum Endogenous Mortality
- Basis:
  - there are different mortality rates in society, depending on age and gender
  - these deaths are partly caused by hazardous industrial systems
- Decision rule: new system should not lead to a significant increase in risk estimated for a population with the lowest endogenous mortality
  - number of natural deaths is the reference point for acceptability
- Mostly used in Germany, for railways

Endogenous mortality: deaths due to internal causes (disease, aging)

RISK ENGINEERING

GAME decision rule

- GAME: *Globalement au Moins Equivalent*, or Globally at least equivalent
- Mainly used in French railways
- The EN 50126 standard:
  - *"All new guided transport systems must offer a level of risk globally at least as good as the one offered by any equivalent system"*
- Example: Channel Tunnel Safety Authority imposed a requirement that the safety performance of the Tunnel should be no worse than that of a surface railway of similar length
- Note: requires an existing system which acts as the reference

“Best available technology” rule

- BAT: Best available technology
  - a regulatory principle which is widely used to control environmental risks
  - emissions limit values and the equivalent parameters and technical measures in permits shall be based on the best available techniques, without prescribing the use of any specific technique or technology
  - “available” means developed on a scale which allows implementation in the relevant industrial sector, under economically and technically viable conditions, taking into consideration the costs and advantages
- BATNEEC (Best available techniques not entailing excessive costs): applied to air pollution emissions from large industrial installations (EU directive 84/360/EEC)

RISK ENGINEERING

Criteria used by US federal regulatory agencies

	Individual risk considered	Population risk considered	Usual acceptable residual risk (lifetime risk for lifetime exposure)
Toxics	Yes " reasonable worst case for occupational exposure	Yes, indirectly	Unstated, but usually 10^{-5} to 10^{-6} for public, 10^{-4} to 10^{-5} for occupational exp.
Pesticides	No for carcinogenic additives; yes for residue tolerance	Yes for residue tolerance	Zero for additives (Delaney clause) 10^{-6} for assumed max residues in average diet, 10^{-6} for non-dietary exposure
drinking water	Yes, a standard exposure scenario in middle range	No	10^{-4} to 10^{-6} range considered to be adequate
water quality	Yes, a standard exposure scenario in middle range	No	10^{-5} to 10^{-7}
hazardous waste handling, active disposal	Yes	No	listing : 10^{-5} corrective actions : 10^{-4} to 10^{-6} incinerators : 10^{-5}
Superfund sites	Yes, " reasonable maximum exposure " using mix of midrange and conservative assumptions	Yes	10^{-4} to 10^{-6}, depending partly on anticipated future use of site
hazardous air pollutants	Yes	Yes	10^{-4} to 10^{-6}
food additives, colours and contaminants; cosmetics	No for carcinogenic additives; yes for additives, contaminants	No	Zero for additives; 10^{-6} for assumed max residues in " high use " diet
occupational exposure	Yes, for full working life at possible exposure limit	No	Feasible controls (in practice 10^{-3})

Note absence of homogeneity for different risk categories...

Source: *A survey of methods for chemical health risk assessment among federal regulatory agencies*, L. Rhomberg, 1996

RISK ENGINEERING

The precautionary principle

- The purpose of the precautionary principle is to create an impetus to take a decision notwithstanding scientific uncertainty about the nature and extent of the risk

> *Where there are threats of serious or irreversible environmental damage, lack of full scientific certainty shall not be used as a reason for postponing cost effective measures to prevent environmental degradation.*
>
> — *1992 Rio Declaration on Environment and Development*

- Simpler definition: incomplete scientific knowledge is not a valid excuse for regulatory inertia

"Better safe than sorry"

The precautionary principle

- UK guidance: precautionary principle should be invoked when:
  - there is good reason, based on empirical evidence or plausible causal hypothesis, to believe that harmful effects might occur, even if the likelihood of harm is remote
  - a scientific evaluation of the consequences and likelihoods reveals such uncertainty that it is impossible to assess the risk with sufficient confidence to inform decision-making

Source: hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm

RISK ENGINEERING

The Imperative of Responsibility [Jonas]

- Hans Jonas (1903–1993), German philosopher

> *[…] the frivolous joyous human holiday of several industrial centuries will perhaps be paid for by thousands of years of transformed terrestrial life.*

- *The Imperative of Responsibility: in Search of an Ethics for the Technological Age* (1979)
  - human survival depends on our efforts to care for our planet and its future
  - we have a responsibility to future generations
  - Jonas' supreme principle of morality: "Act so that the effects of your action are compatible with the permanence of genuine human life"
  - inspired the environmental movement in Germany in the 1970s

RISK ENGINEERING

Image credits

- Cat stretching (slide 2): norsez via `flic.kr/p/e8q1GE`, CC BY-NC-ND licence
- Railway tracks on slide 10, Martin Fisch via `flic.kr/p/o4Hice`, CC BY-SA licence
- Ducks on slide 21, `flic.kr/p/6jFbTs`, CC BY-SA licence

For more free content on risk engineering, visit `risk-engineering.org`

RISK ENGINEERING

Further reading

- *Reducing risk, protecting people: HSE's decision-making process*, UK Health and Safety Executive, 2001, `hse.gov.uk/risk/theory/r2p2.pdf`

For more free content on risk engineering, visit `risk-engineering.org`

Feedback welcome!

Was some of the content unclear? Which parts were most useful to you? Your comments to `feedback@risk-engineering.org` (email) or `@LearnRiskEng` (Twitter) will help us to improve these materials. Thanks!

`@LearnRiskEng`

`fb.me/RiskEngineering`

For more free content on risk engineering, visit `risk-engineering.org`