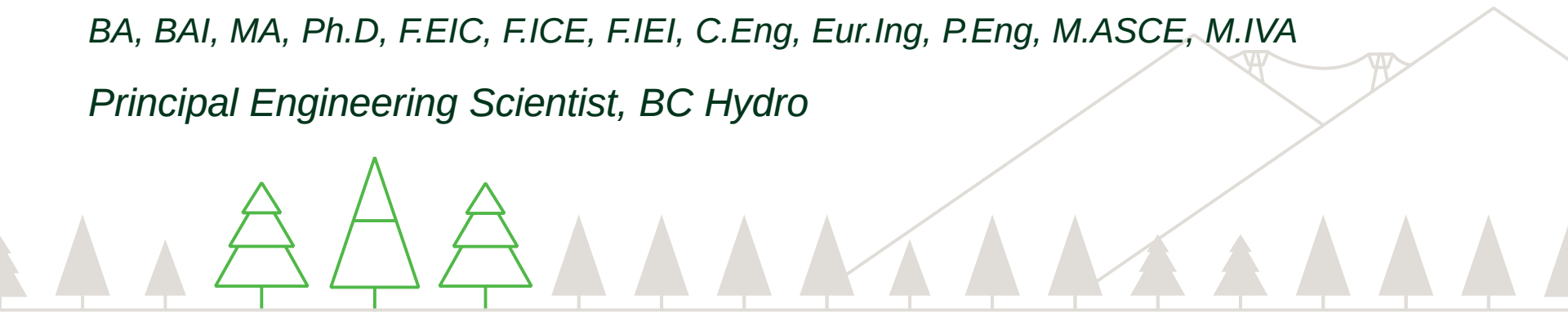
RISK: Engineering at the boundary between Science, Policy and Politics

Dr. D.N.D. Hartford

BA, BAI, MA, Ph.D, F.EIC, F.ICE, F.IEI, C.Eng, Eur.Ing, P.Eng, M.ASCE, M.IVA

Principal Engineering Scientist, BC Hydro

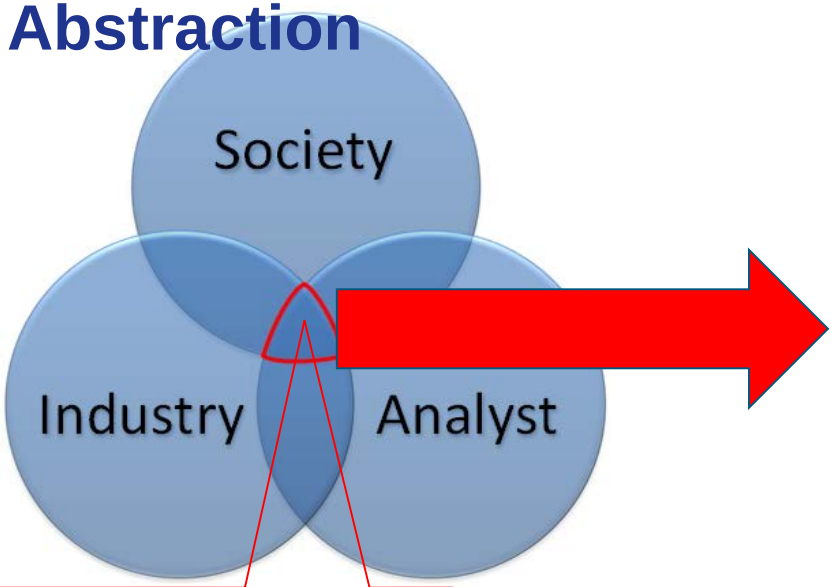


BC Hydro
Power smart

Some BC Hydro dams

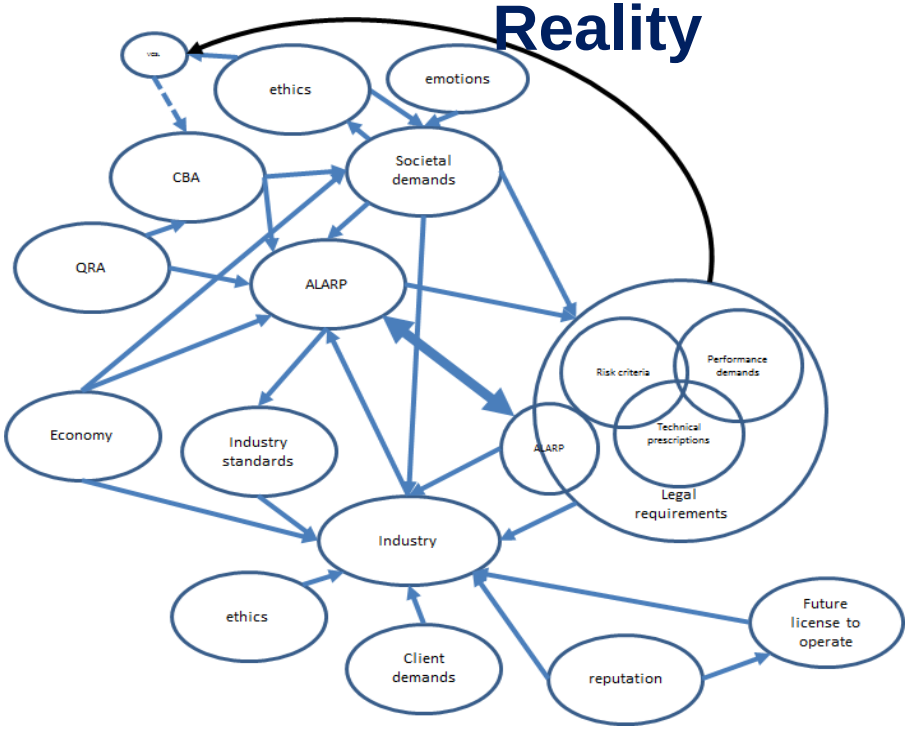
Risk decisions and the “infinite risk fence”

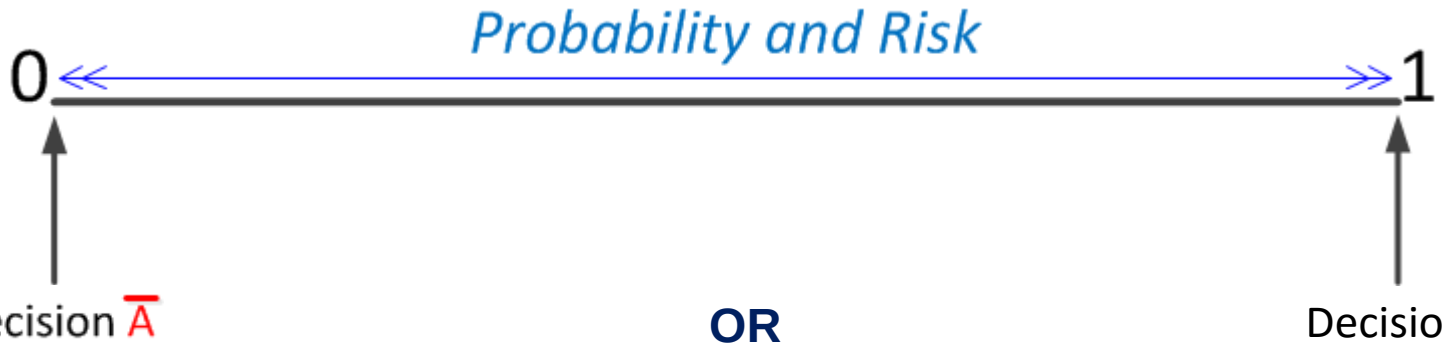
Abstraction



Societal risk criteria?

Reality





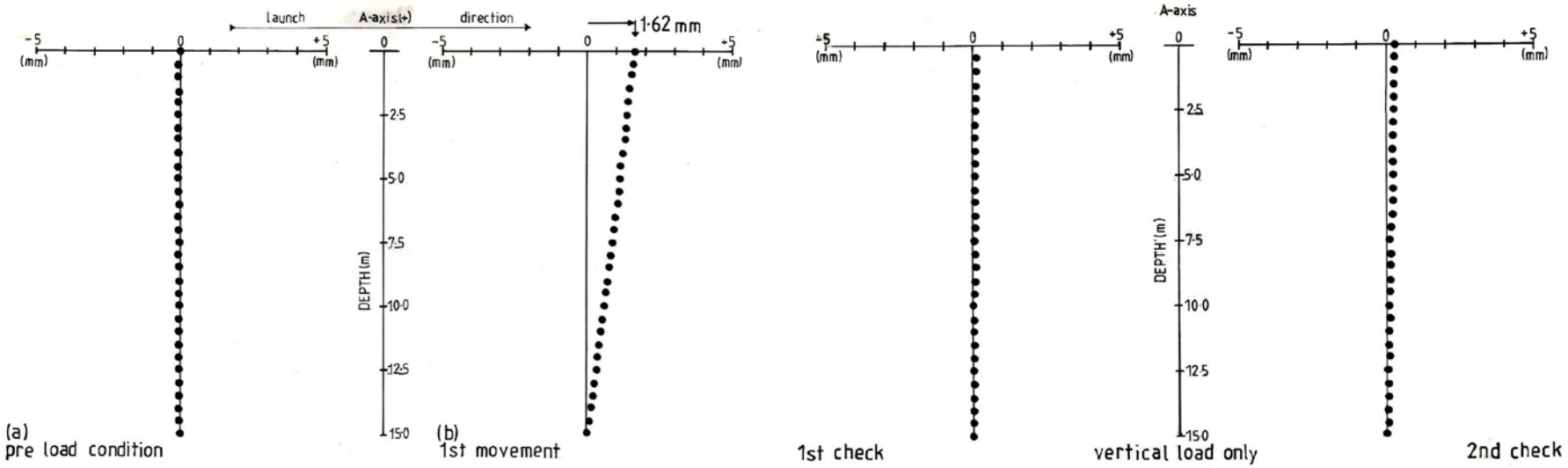
Launching the Malibamatso River bridge

Monte Carlo Simulation of rock joints

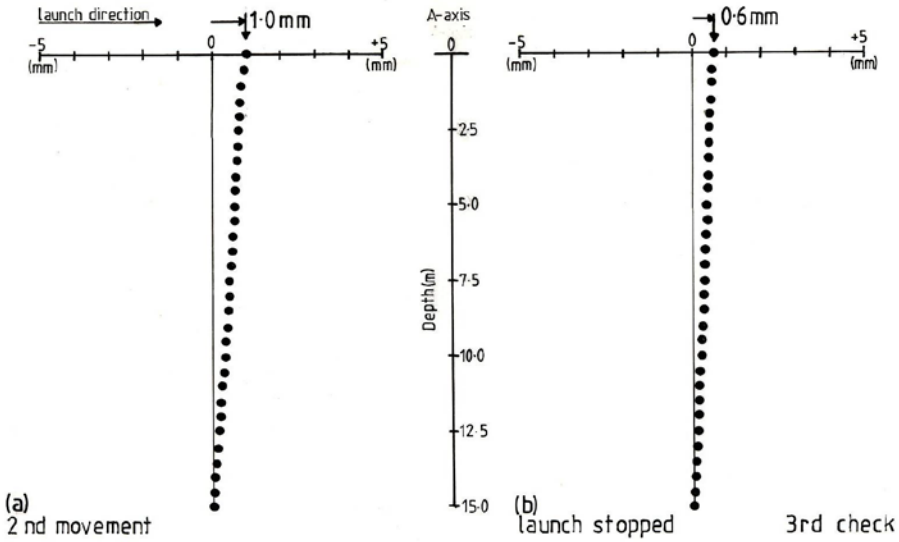
Probability of adversely orientated joints = 0.125

1st sign of trouble!

And stress relief!



And re-stress at 50% horizontal velocity!



Traditionally...

- Engineers took it upon themselves to be the guardians of the safety of engineered systems
  - The engineers gave an assurance that people could go about their daily lives in the knowledge that the engineered works did not pose a threat to their safety or to the many things that they value

But no more....*not in the societal risk context*

- In the modern context the “Engineer” no longer determines the safety of many engineered systems
  - Societal values and expectations have changed
    - Despite what professional “Codes of Ethics” might state
  - *The safety of people, property and the environment are highly political issues*

- Distribution of risk

- *It is the nature of risk that, frequently, those who create the risk do not bear its consequences nor its wider costs. So the market does not function properly as a distributive mechanism. The State must intervene to regulate risk.*

- *(J. Bacon, UK Health and Safety Executive, Forum Engelberg Lecture, 1997)*

Risk assessment promises...

- A rational basis for decisions
- But *rational* in whose paradigm?
  - The risk taker?
  - The target?
  - The adjudicator?
    - (a.k.a. the Regulator)

- Risk decisions often emerge through a different rationality than “decision-theoretic” rationality
  - Of the type that is the subject of so many scientific papers

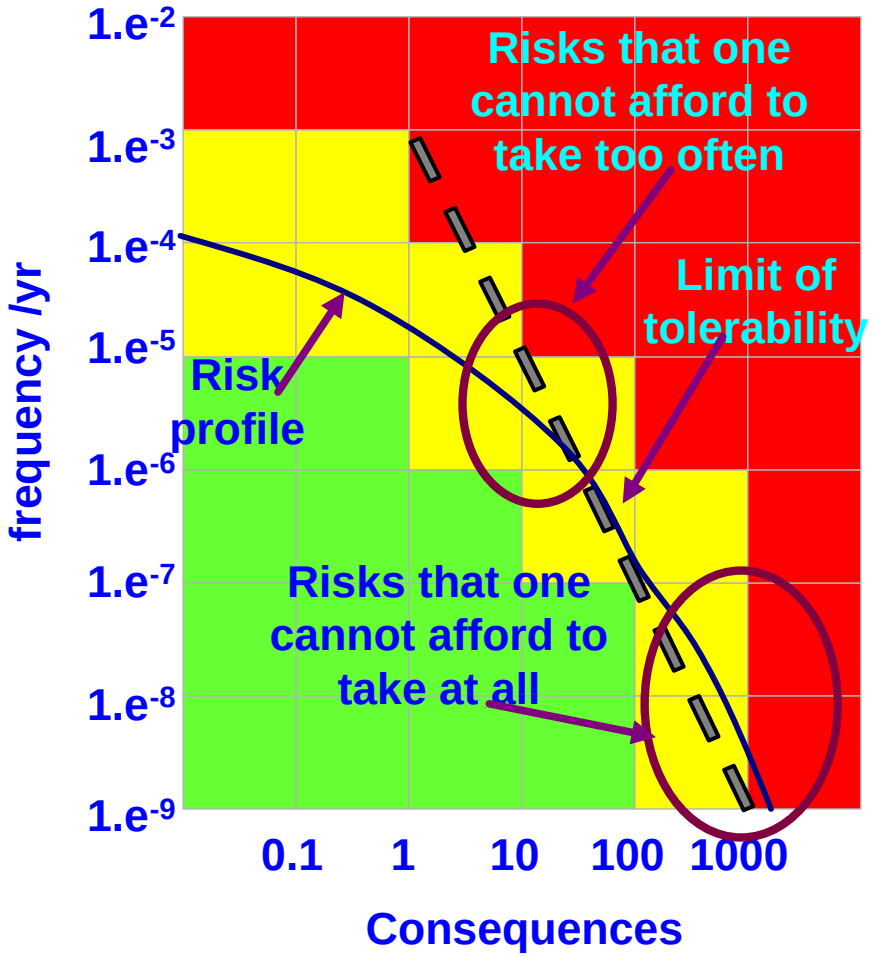
- Perhaps with the view to reducing risk “As Low as Reasonably Practicable”

Risk – an abstraction

- Risk arises because of uncertainty
  - It involves a set of uncertain circumstances
    - “Agents of change” (“hazards”, “threats”, “human whims”)
    - Pre-disposing conditions
      - “unusual combinations” of “usual conditions”
    - “Targets” which are real (“objects” – types and size of consequence)
- It does not exist in the “real world”
- But the losses will be real when they happen
- People, by nature are not good at thinking about and acting on risk
  - The same basic mistakes are made “over and over again”!

3 Types of risk

- Risks one can't afford to take
  - But you may be stuck with them
- Risks one can't afford to take too often
  - But will take more often than you think
- Risks that one can afford to take
  - But often won't
- And of course "who" is "one" ?
  - And what is the decision context"?



SOME THOUGHTS ON MODELS

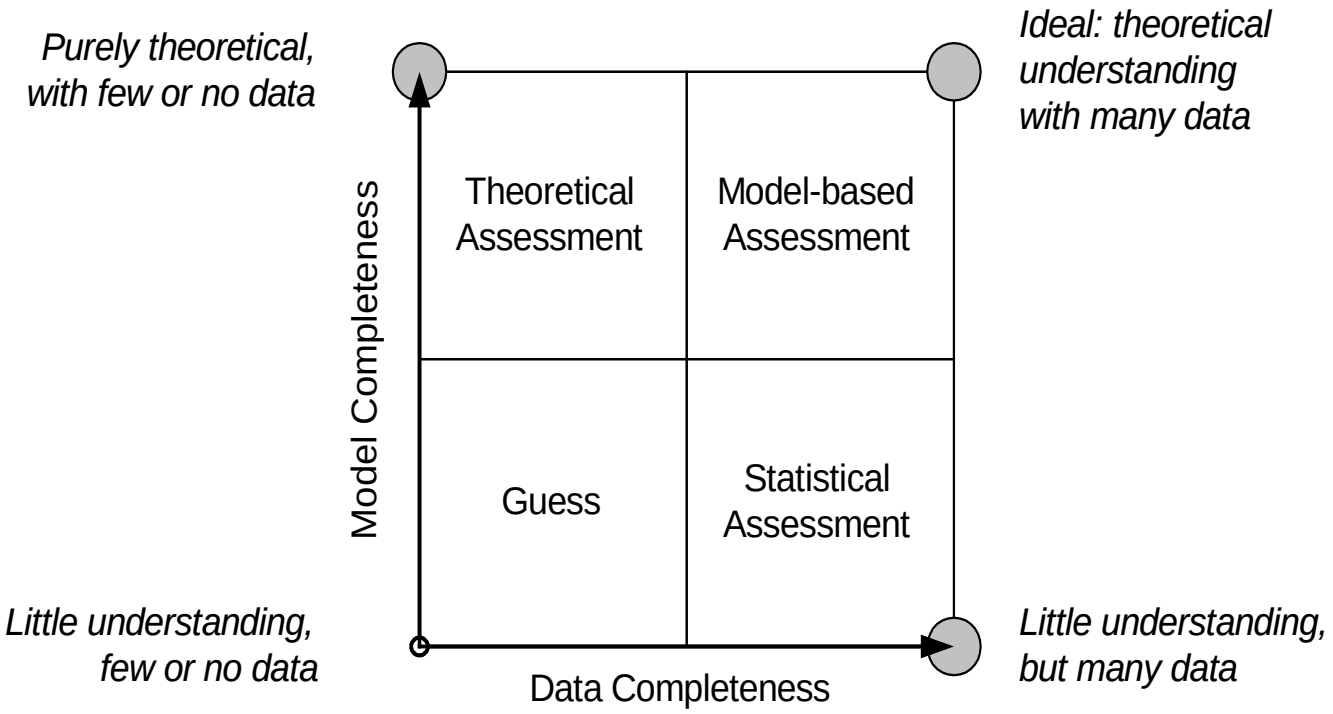
The probability that the model is right is zero!

Some models are useful

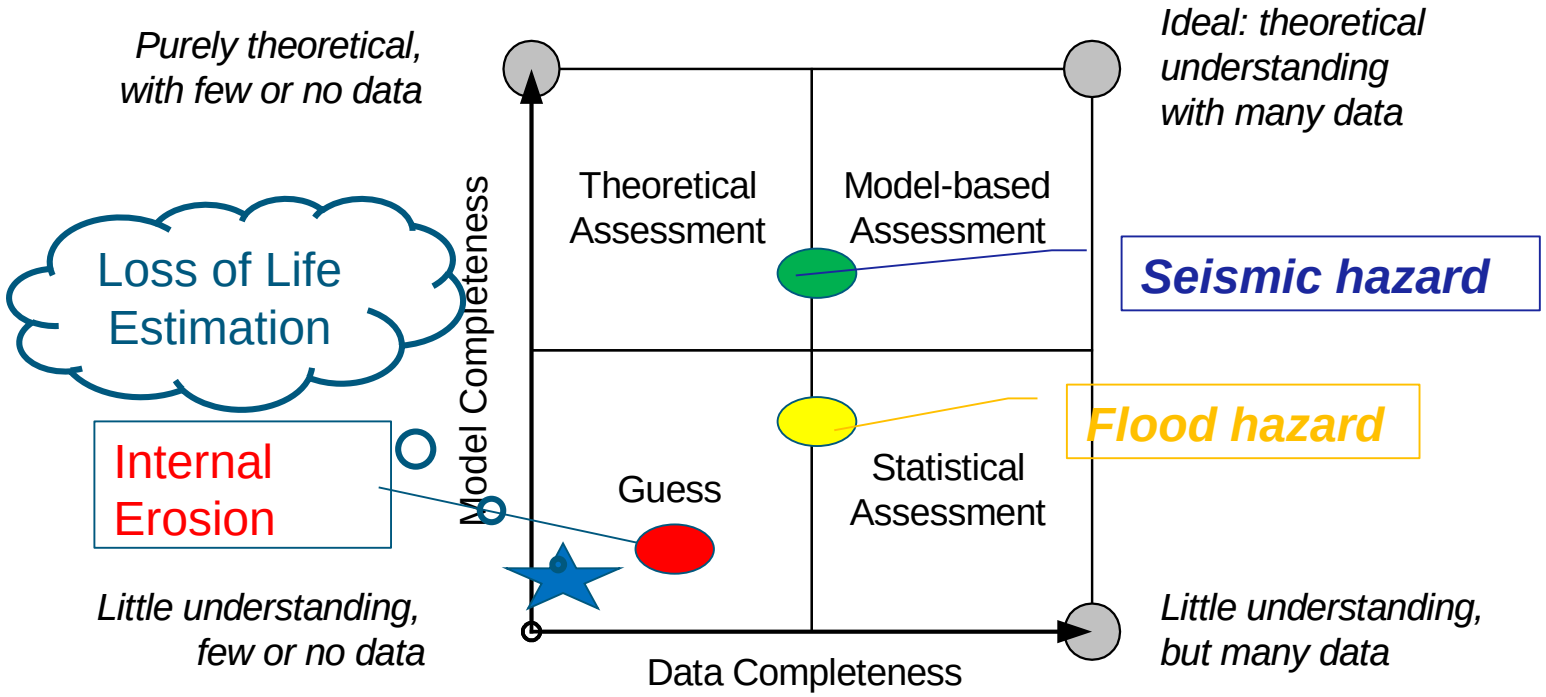
Many models are incredibly complicated - and sometimes without proper grounding in reality

Knowledge

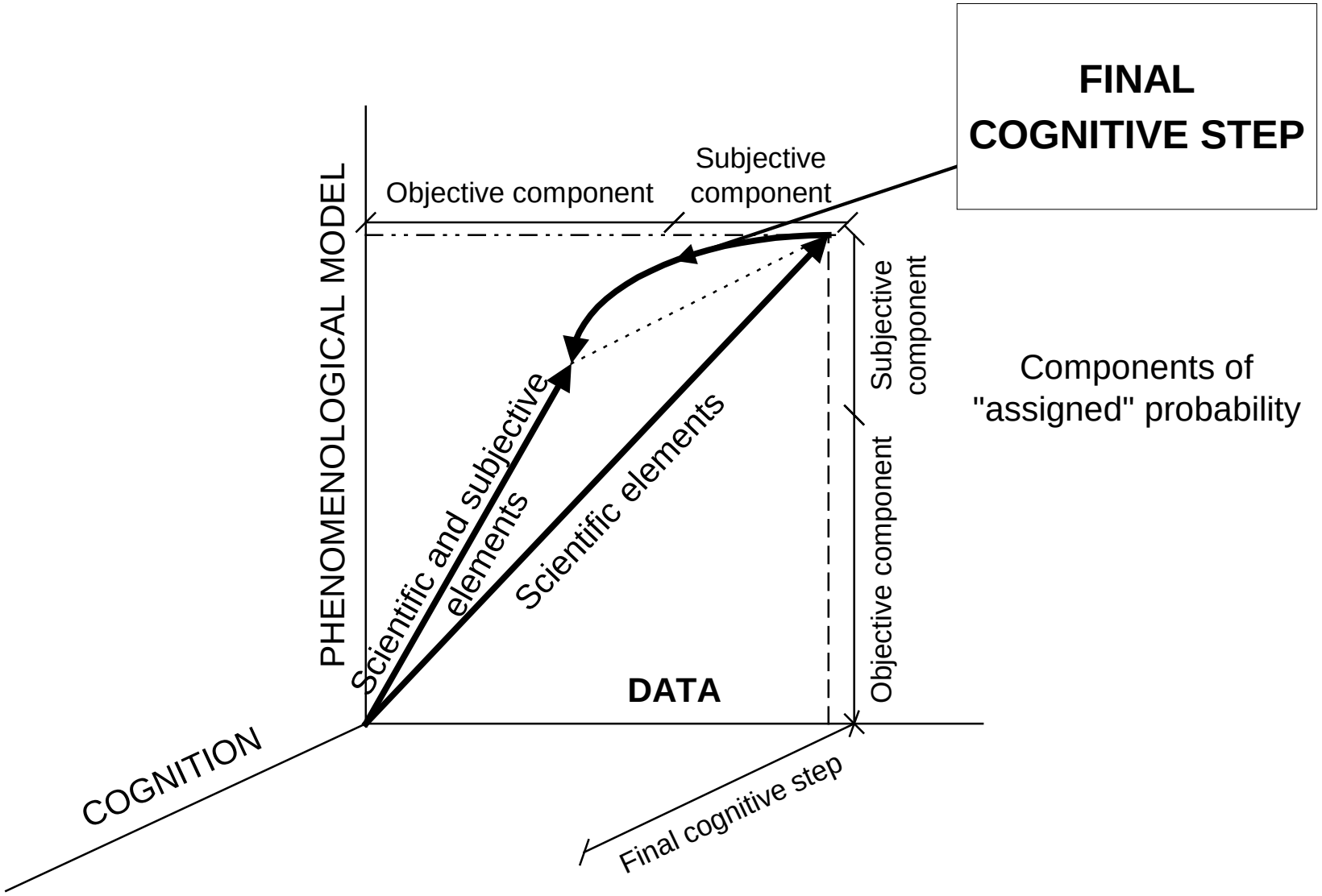
- In dealing with risk, the first thing that we must accept is:
- We don’t actually know!
  - We sort of know with some probability of being right
  - We need to know where we are in "knowledge space”
  - Judgement is interwoven across the knowledge space



Analytical uncertainty in risk analysis of dams



Subjectivity cannot be eliminated

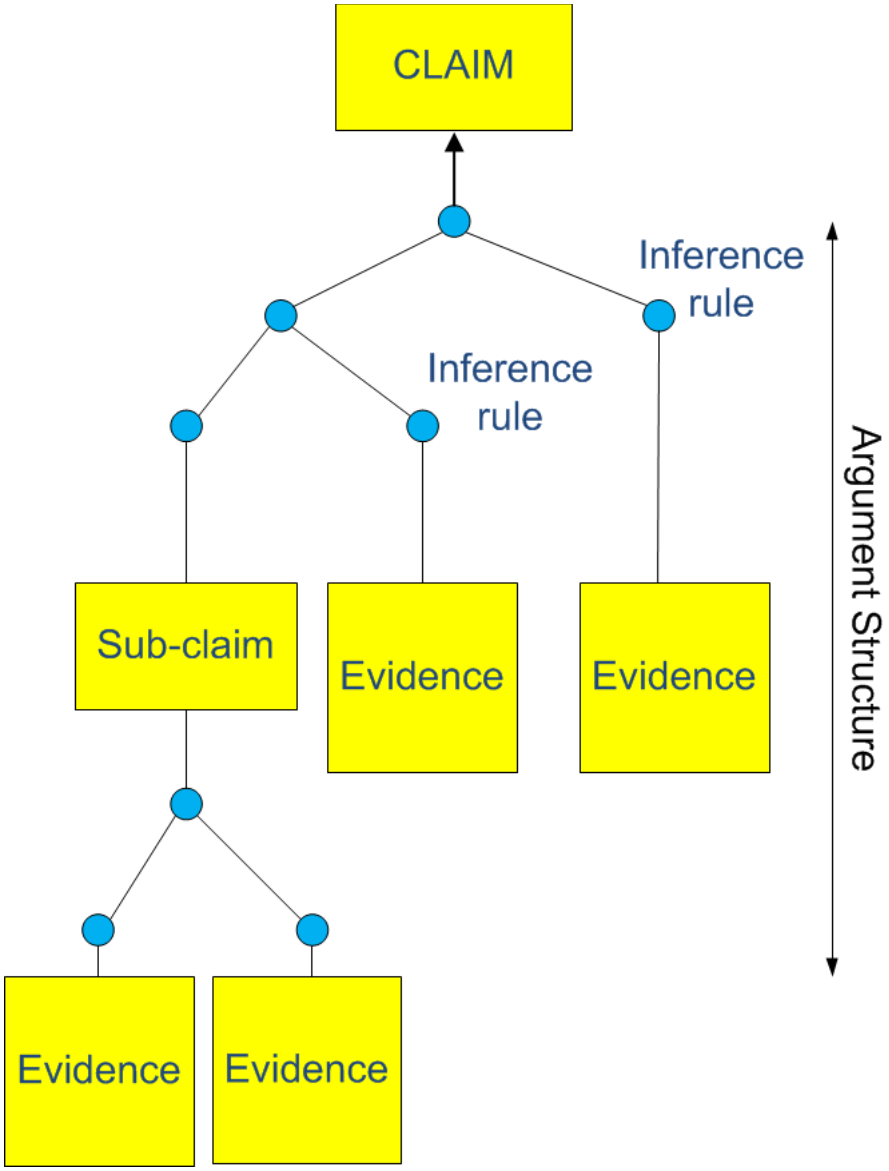


Role of judgement

- Judgement has an important role to play in performance assessment of engineered systems to varying degrees
  - But it must be used appropriately
    - To control the effects of uncertainty

- Essence of ***risk-informed*** performance assessments are:
  - Predictive analysis models that reflect the physics of the failure mechanisms
  - Quality, scientifically qualified data
  - Experts selected on the basis of qualities and expertise
  - Systems analysis methods

Justifying the “judgements”?



Reductionism (classical science) is not always up to the challenge

- Analysis is the process of breaking a complex topic or substance into smaller parts to gain a better understanding of it. “The whole” is constituted, and re-constituted, from the parts put together

- 2 fundamental assumptions
  - The interaction between parts is non-existent, or so weak that it can be neglected
    - This is the essential condition such that the parts can be “worked out” actually, logically and mathematically and then “put back together”
  - The relations describing the behaviour of parts is linear
    - Only then is the condition of summation given
      - An equation describing the behaviour of the total is of the same form as the equations describing the behaviour of the parts
      - Partial processes can be superimposed to obtain the total process.
        - The Principle of Superposition

Need systems thinking to get at risk in systems

- Systems:- Parts in interaction
- A “System” (or “organised complexity”) may be characterised in part by the existence of:
  - “strong interactions between parts”, or,
  - interactions that are “non-trivial”
    - i.e. non-linear
      - The methodological concern of systems theory is to provide approaches to problems which, compared to the “analytical-summative” problems of classical science, are of a more general nature
- Thus our starting point is “a general solution to a general class of problem” in the safety of engineered systems
  - That can be adapted to suit any specific problem within the general class

Engineering Replacement of Factor of Safety?

A silver bullet?

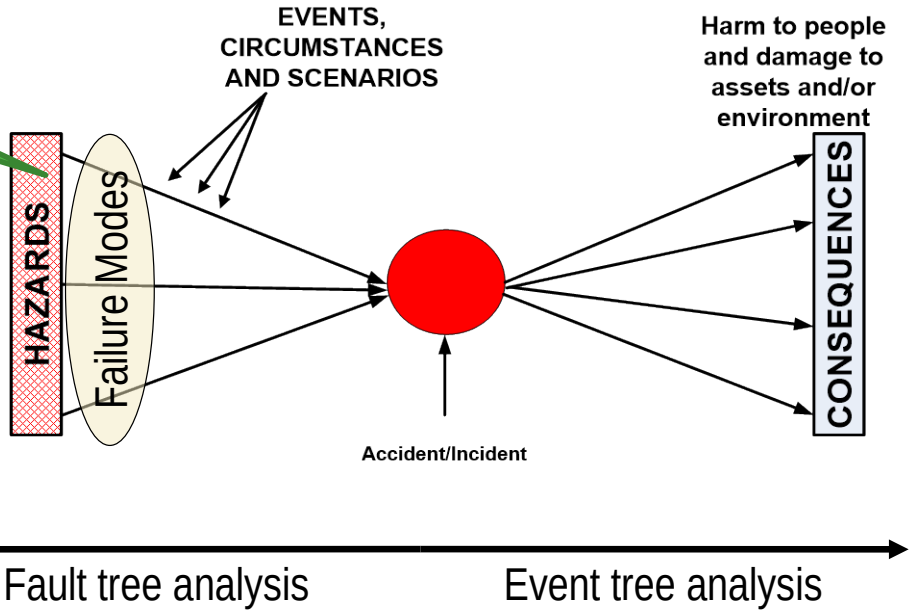
A “pipe dream”?

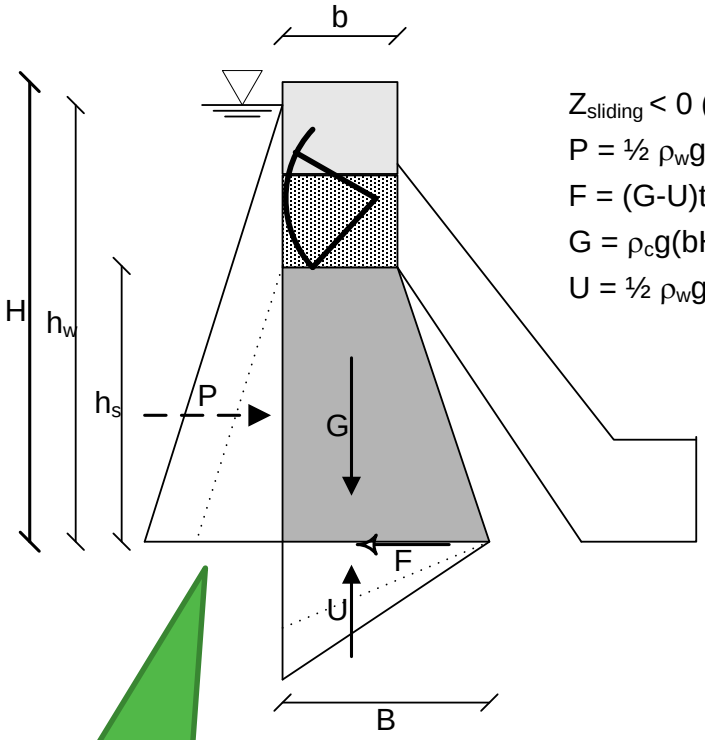
Not as straightforward as portrayed in the engineering literature!

RISK CRITERIA

Abstract view of “safe”

Risk Analysis





$Z_{sliding} < 0$ (F-P < 0)

$P = ½\ \rho_w g(h_w)^2$

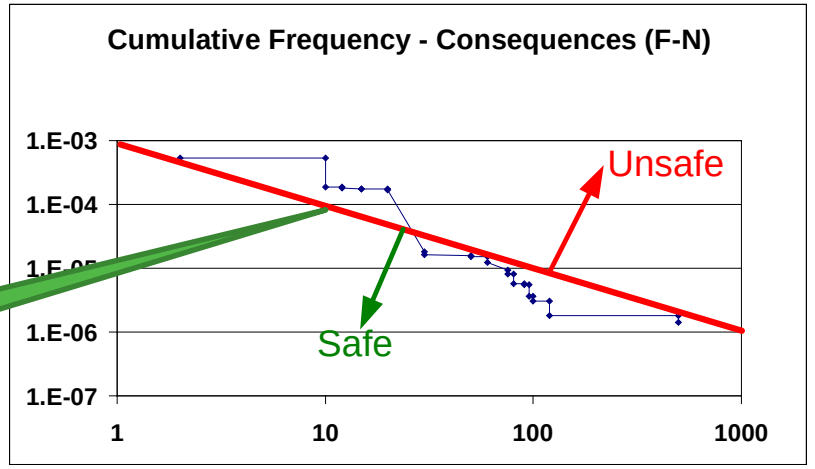
$F = (G-U)\tan\ \delta$

$G = \rho_c g(bH + ½(B-b)h_s)$

$U = ½\ \rho_w g h_w B$

Models

Safety Criterion



The "Risk Information" Problem

- The information you have is not the information you want
- The information you want is not the information you need
- The information you need is not the information that you can obtain
- The information you can obtain costs more than you want to pay
  - *Against the Gods, the remarkable story of risk, Peter Bernstein, 1996, Wiley*

- Uncertainty
  - Cannot be eliminated – may be reduced
  - Cannot be avoided!

“Forces” around a hazardous activity

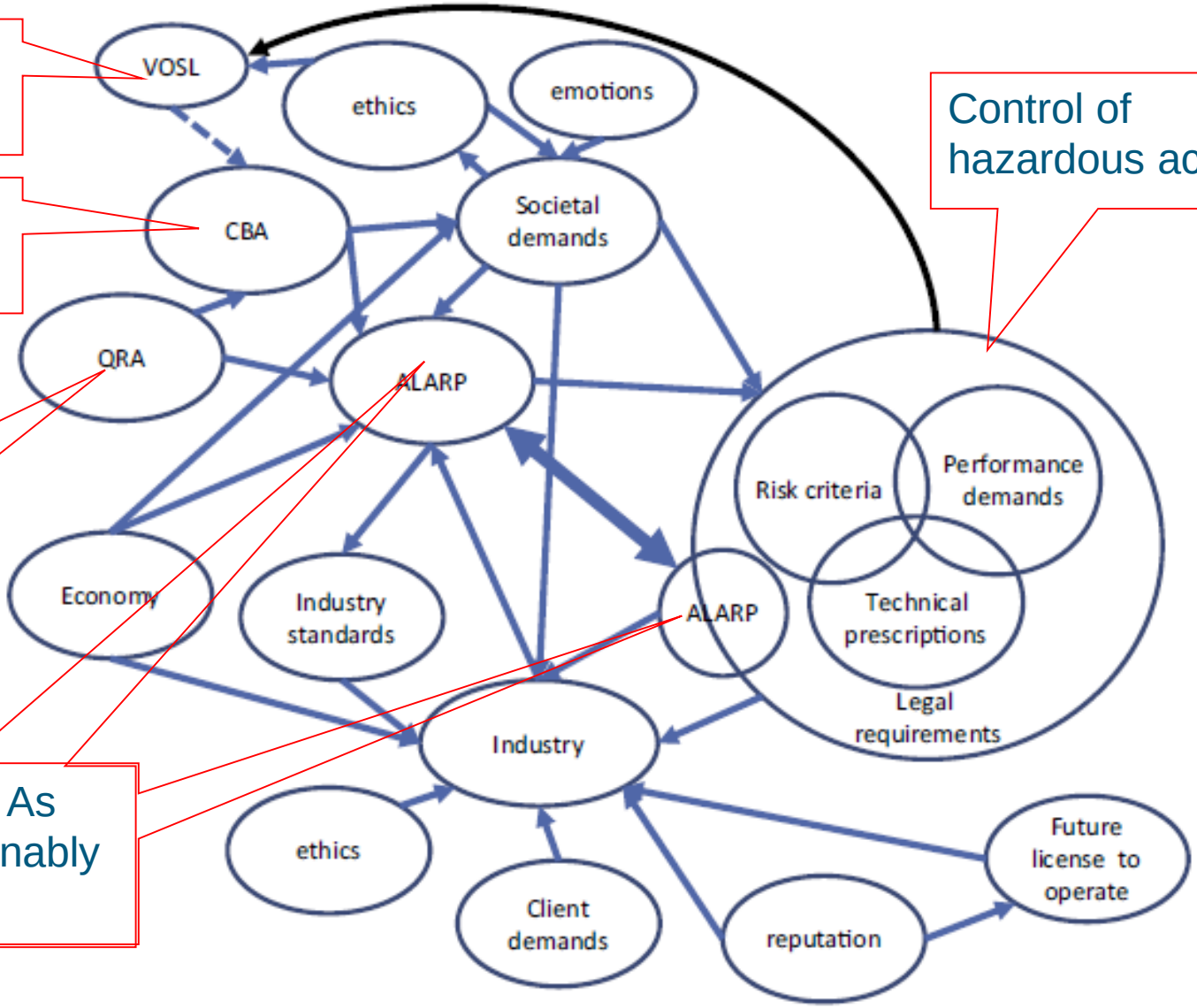
Value of a “Statistical Life”

Cost-Benefit Analysis

Quantitative Risk Assessment

Risks reduced As Low As Reasonably Practicable

Control of hazardous activity



ALAP and ALARA

- As Low as Practicable
- Radiation Protection in the 1950's in the USA
  - In 1970 title 10 of the Code of Federal Regulation Parts 20 and 50 specified that exposure to radiation should be kept as far below the limits as was reasonably practicable
- ALARA
- Radiation Limits
  - By 1970 the notion of limits, to be used also as reference, was part of the protection construct. In 1979 ALAP changed in to As Low As Reasonably Achievable
  - In radiation protection the ALARA principle is used as a ratchet mechanism to update – i.e. lower – the radiation exposure limits as a function of the developments in science and technology. When the limit technically can be set lower it will.

ALARP and SFAIRP

- As Low as Reasonably Practicable

- So Far as is Reasonably Practicable

Have different origins (the UK)

- The principle that measures should be reasonable and practicable was already used earlier in the United Kingdom in the Electricity Regulations 1908, in the Spinning by Self-acting Mules Regulations of 1905 reg 3 and in Section 5 of the Salmon Fishery Act 1861. Another early use was found in the Chaffing Machines Act 1897, the Threshing Machines Act 1878 and the Alkali Act Amendment Act 1874.

Not the same

- ALARP and SFAIRP are not the same
- even if an authoritative source suggests that they are
  - The important point here, that is generally not made, is that the two qualifications are applied to quite different properties. ALARP is applied to the level of ‘risk’ whereas SFAIRP is applied to being ‘safe’.
  - The key question is whether being ‘safe’ is determined solely by the level of ‘risk’. Safety is relative and influenced by values whereas risk is quasi-objective and held to be value-free. The numbers mean the same to everyone, which of course is why risk became the parameter or property of choice. In practice, the difference means that the requirement ‘safe SFAIRP’ focuses on reducing the hazard. This is what the law requires and on which the courts pass judgement.
    - But do the numbers really mean the same to everybody?

ALARP and ALARA

- ALARA seems to imply that achievable includes that it could be theoretically possible to go lower even if it has not been demonstrated in any way to be feasible in practice.
  - ALARA then demands to do work, research, engineering to make it work.

- Practicable seems to indicate that the technical feasibility needs to have been demonstrated.
  - Whether this also means that the technical implementation of the possibility should have been realised in practice and that practicable means the same as available technology is unclear.

What constitutes Reasonable?

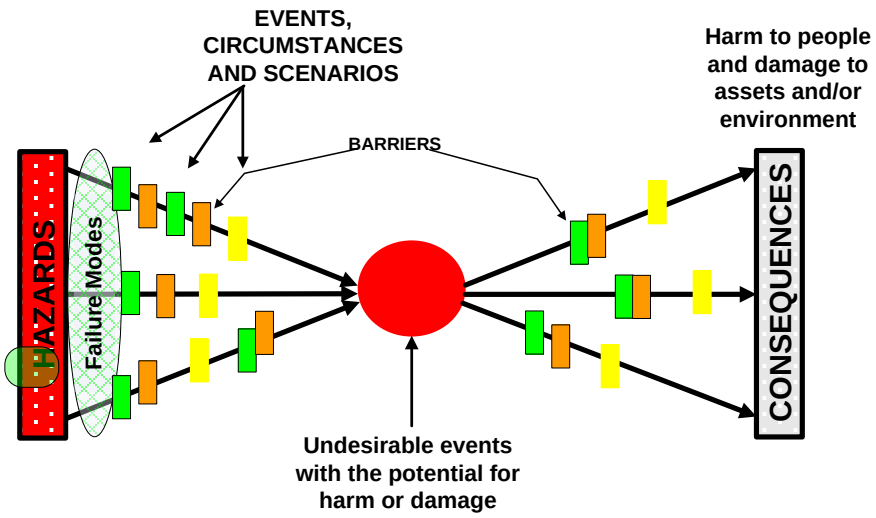
- Is central to the whole endeavour.
  - The use of the term reasonable suggests that it is not sufficient to just adhere to some limit, if it exists, and that the reasonability of performing or refraining from an action is not just a matter of money.
  - The term expresses that besides aspects that can be expressed in terms of money or have a monetary or market value, there are aspects that do not have such a monetary value, or such a value cannot be established with reasonable accuracy.
    - The aspects may comprise such things as equity, sociality and even maybe beauty – even if it is only in the eye of the beholder.
  - Reasonability comprises much more than money and it is only loosely defined.
    - It is what those who happen to make a decision consider reasonable.

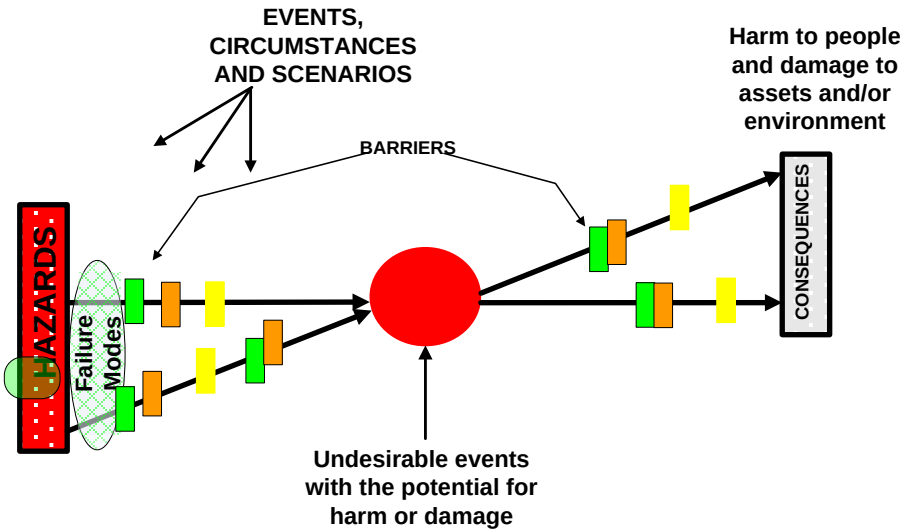
Somewhere between BAT and CATNIP

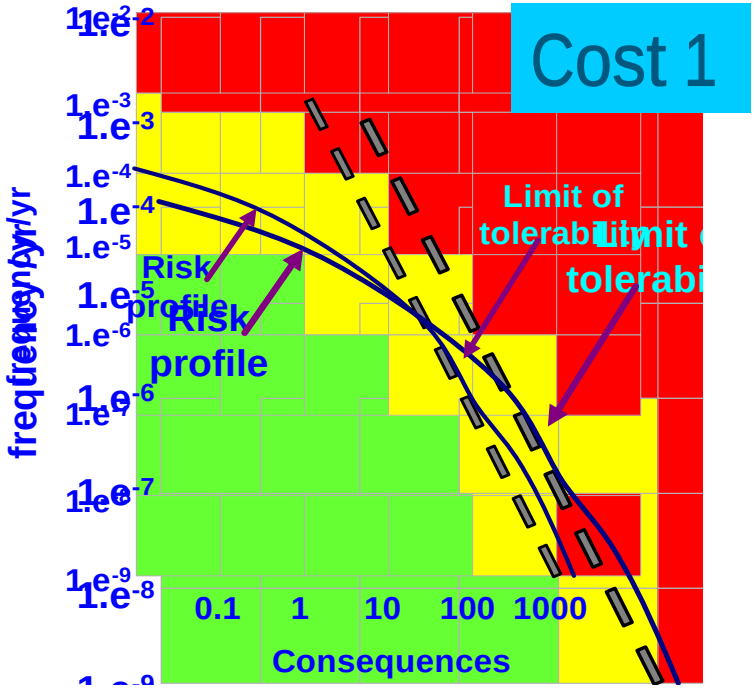
- BAT
  - Best Available Technology
- BATNEC
  - Best Available Technology Not involving Excessive Cost
    - But the “NEC” is values driven and subjective and may be anywhere within the spectrum of choices
- CATNIP
  - Cheapest Available Technology Not Inviting Prosecution

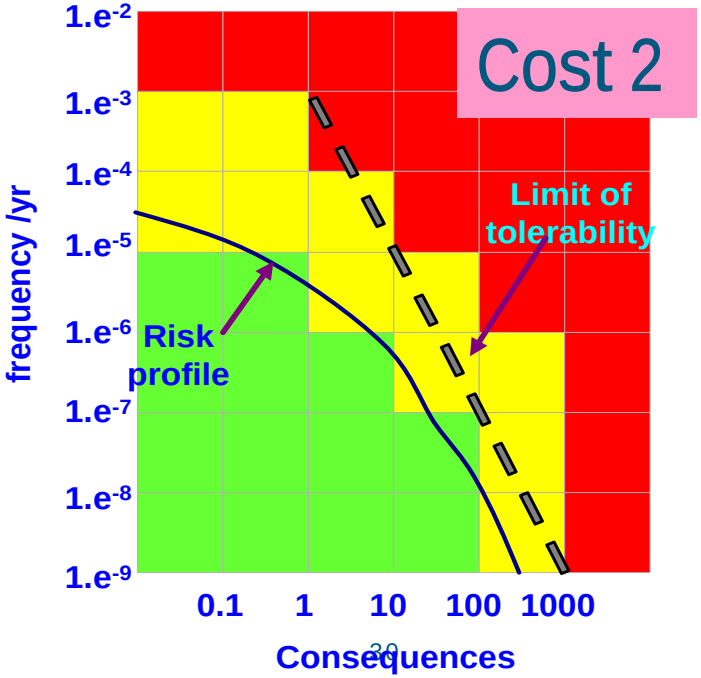
  - BAT implies that the costs are not considered. Then BAT means the same as ALAP.
  - ALARP apparently means that the technology not only should be available, but also that the costs should be reasonable.

Risk informed decisions









Decisions based on CBA

- Its primary merit is that it is precisely defined and the decision is predictable.
- Its disadvantage is that it does not take into account the imponderables that more often than not weigh into the decision.
  - Using CBA also suggests that the Value of Life is a known and universal constant while there is no scientific evidence other than that the VOSL varies over a large range and highly depends on the circumstances and on the method used to determine it.
  - What seems to have emerged is that decisions on statistical human lives and anonymous future victims are much easier than on real human beings.

Decisions based on ALARP

- The advantage of a qualitative somewhat vague concept, and decision-making that depends on a to a large extent subjective value judgement by a decision maker, lies in that it avoids questions that are difficult to answer.
- It also avoids questions that have ethical connotations.
  - The stinging problem of the monetary value of a human life is avoided.
  - By demanding substantial disproportionality or gross disproportionality of costs before refraining from a risk reducing measure, the problem of precisely setting a value on a human need not be addressed.

Suggested decision principles

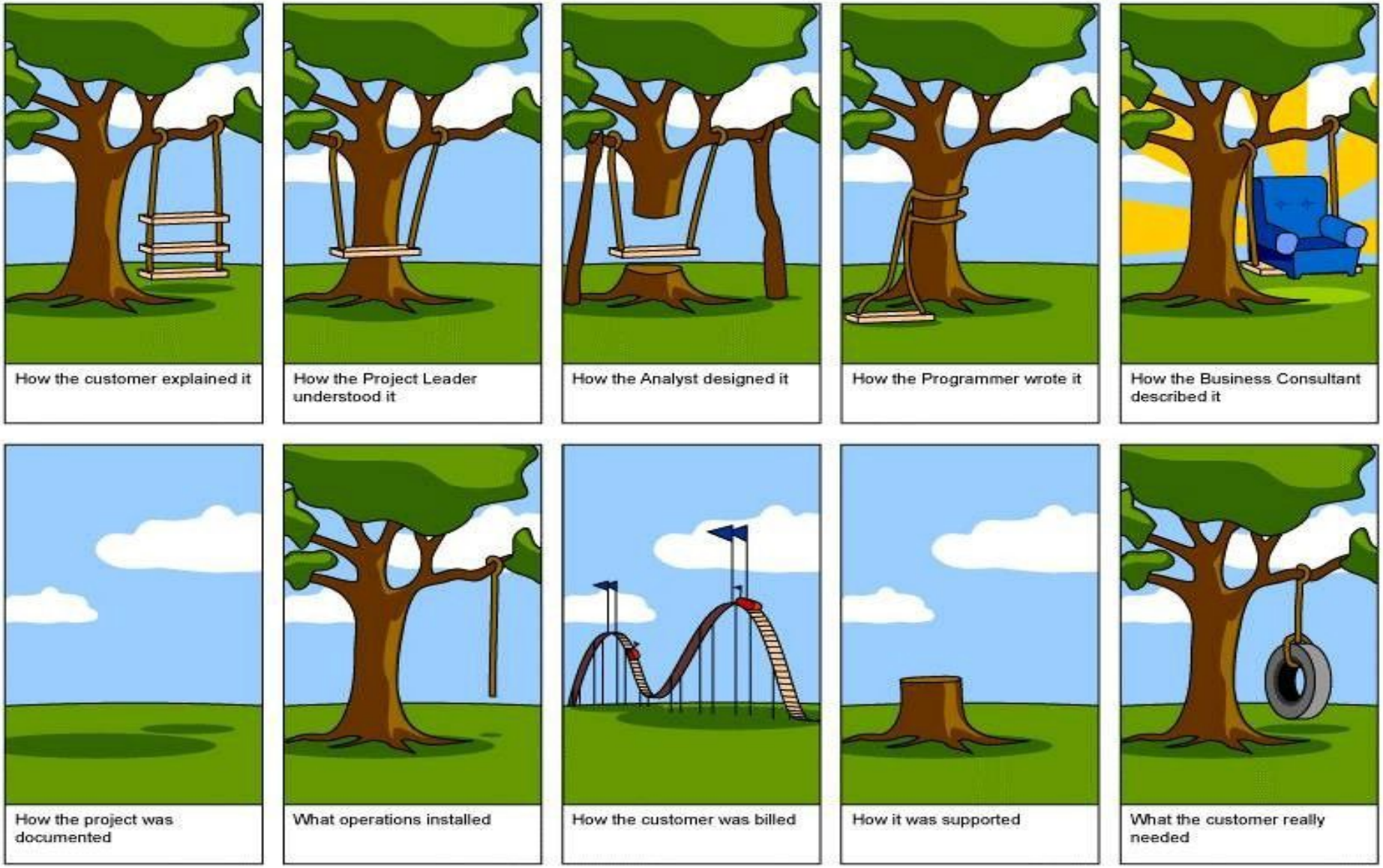
- Owners of hazardous installations should meet or exceed all:

1. General Legal Duties
2. General Duties of “Hazard” Ownership
3. Legal Duties associated with “Hazard” Operation and Safety
4. Regulatory requirements with respect to “Hazard” Operation and Safety
5. Conform to established engineering principles for safety of engineered systems
6. Established dam safety standards/criteria and norms
   - And if the safety issue remains unresolved:
7. Perform quantitative risk assessment
   - With specific consideration of Totality of the consequences of failure
   - It is not simply a matter of lives lost and damage costs
     - And Cost to Save a Statistical Life
8. Obtain societal consent through the political process

So what does happen...

- When a statistical life becomes a real person?
- Case from the Netherlands
  - In health care the Dutch Health Councils prefers a value of €80,000 per Quality Adjusted Life-year (QALY). However, when the costs of medicines decreases this may lead to the conclusion that it is worthwhile to treat half of the Dutch population against hypertension even when this risk of adverse consequences is marginal.
  - Recent decisions according the preference of the Health Council regarding the treatment of among other things Pompe's disease resulted in a parliamentary debate and in a revoking of the decision to no longer pay for this treatment under the basic health insurance system in the Netherlands.

Project risk!




BC Hydro
Power smart