CHEN/SENG 460/660

Quantitative Risk Analysis in Safety Engineering

Spring 2016

Risk Management:
Ins and outs, and conditional factors

Hans Pasman

hjpasman@gmail.com

Mary Kay O'Connor Process Safety Center

Texas A&M University System, College Station, Texas, USA

MARY KAY O'CONNOR PROCESS SAFETY CENTER

TEXAS A&M ENGINEERING EXPERIMENT STATION

Overview

- Risk : types (business, safety, security etc.); ISO 31000; Prof. Aven
- Risk assessment; risk management; decisions on defenses and barriers; budgets on investment, inspection and maintenance.
- Risk assessment formal: process, abstraction/objectivation. *Identification; quadrant; consequence analysis; uncertainty analysis*
- Risk assessment informal: *perception; interpretation; appreciation.* Thinking process - System 1 and 2; - left and right brain halves; judgment - heuristics/intuition (Prof. Kahneman)
- Economics of risk and safety
- Decision making tools – Scorecard, MAUT, Tree, Knapsack, Game, Deep uncertainty
- Decision making process: IRGC; Risk acceptance: ALARP
- Conclusions

What types of risk? And for whom a risk?

- Large variety of risks:
  - Economic risks, political risks
  - Financial/trade risks,
  - Insurance risks,
  - Cyber risks,
  - Project risks (delivery time – money – quality),
  - Environmental risks,
  - Safety risks: personal and process safety risks.
- *Systemic risks*: Risk of collapse of entire, *e.g.*, financial system, as opposed to an entity; also due to component interactions.
- Risk for society, for the company, and for you personally.
- Risk can be subjective: '*What I feel as a risk, doesn't bother you*'.
- Most significant contribution RA is relative (= comparing) risk.

Hazards, danger, safety and risk

- **Hazard** is a capability/potential for harm or other damage.
- **Danger** is a hazardous situation prone to result in harm or damage consequence.
- **Safety** is the state of being protected against harm and other consequence of failure.
- **Risk** is the combination of possible consequence and its likelihood (and uncertainty), presenting a lack of safety.

To maintain acceptable safety level, we must identify and quantify risks and where necessary reduce risks

What is risk? ……..Many definitions!

- Elements of risk: - *Future event,*
  - Consequence/harm/damage/*loss*,
  - *Uncertainty*
- ISO 31000 Risk definition:
  Effect of uncertainty on objectives
- Risk = Combination of *consequence* and its *likelihood*, presenting a lack of safety –
- In engineering: Risk = Severity consequence × Probability

But is a large consequence and low probability perceived the same as a small consequence and high probability?

Risk and Resilience

R. Steen, T. Aven / Safety Science 49 (2011) 292–297

Descriptions:

Risk = (A,C,U) C is (B,C)

Risk = (A,B,C,U)

Risk = (A,B,C,P) in engineering, but it is incomplete

Risk = (A,B,C,P,U,K)

Vulnerability = (B,C,$U \mid A$) = (1 – Robustness)

Vulnerability = (B,C,P,U,$K \mid A$)

Resilience = (B,C,$U \mid$ any A), incl. new types of A

Or more complete:

Resilience = (B,C,P,U,$K \mid$ any A), incl. new types of A

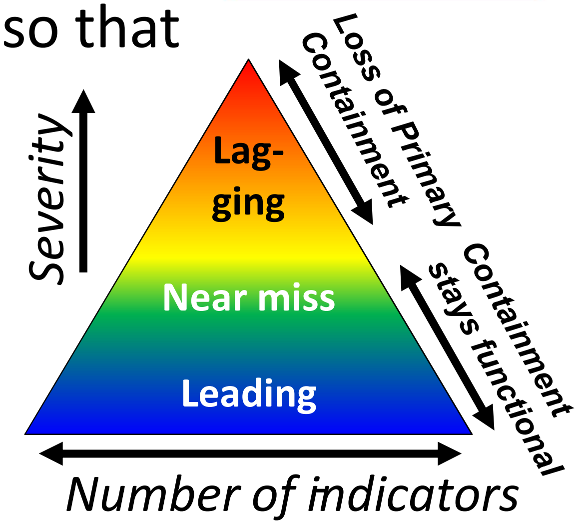
Risk elements:

A = Threat event, attack
C = Consequence
P = Probability
U = Uncertainty
K = Background knowledge
B = Barriers

What is management? What is risk management?

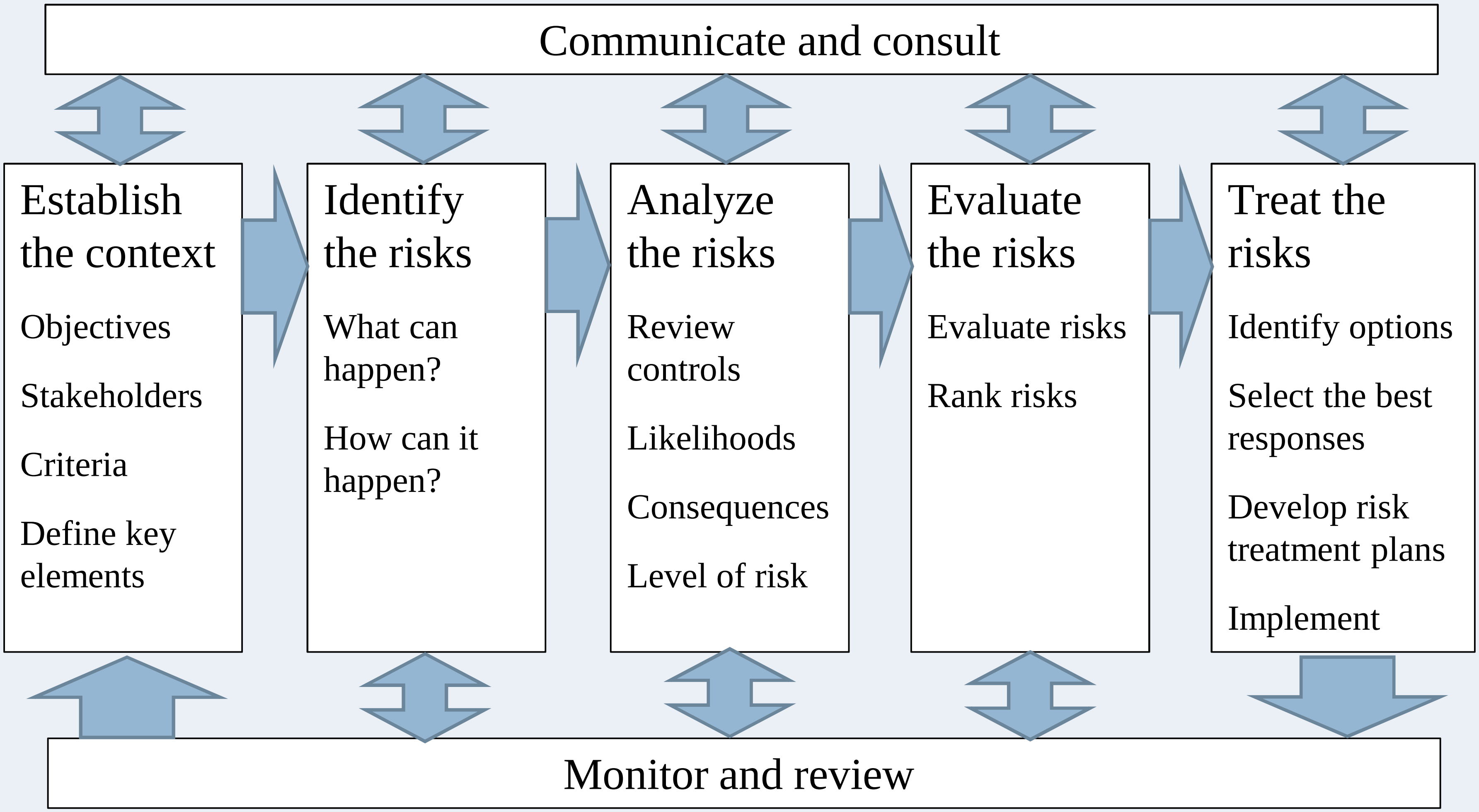
- *Management* (Wikipedia) = the act of getting people together to accomplish desired goals and objectives, using available resources efficiently and effectively.
- Plan – Do – Check – Act (correct) : *Indicator* based.
- *Manager* = Person responsible for the management in a functional area.
- *Leader* = Person who can inspire and is trusted so that people follow and support to accomplish tasks. *(It is therefore desirable that a manager is also leader).*
- *Risk Management* (ISO Guide 73-2009) = coordinated activities to direct and control an organization with regard to risk. *(It means performing risk assessment, and distributing scarce - resources to build and maintain defenses to reduce risk).*

Deming cycle Management



General risk assessment scheme

Cooper, D., Grey, S., Raymond, G., Walker, Ph., Project Risk Management Guidelines, Managing Risks in Large Projects and Complex Procurements, John Wiley & Sons, 2005, ISBN 0-470-02281-7



System approach: *Cardinal rules*

Dr. Rogers

System approach to overcome complexity, non-linearity:

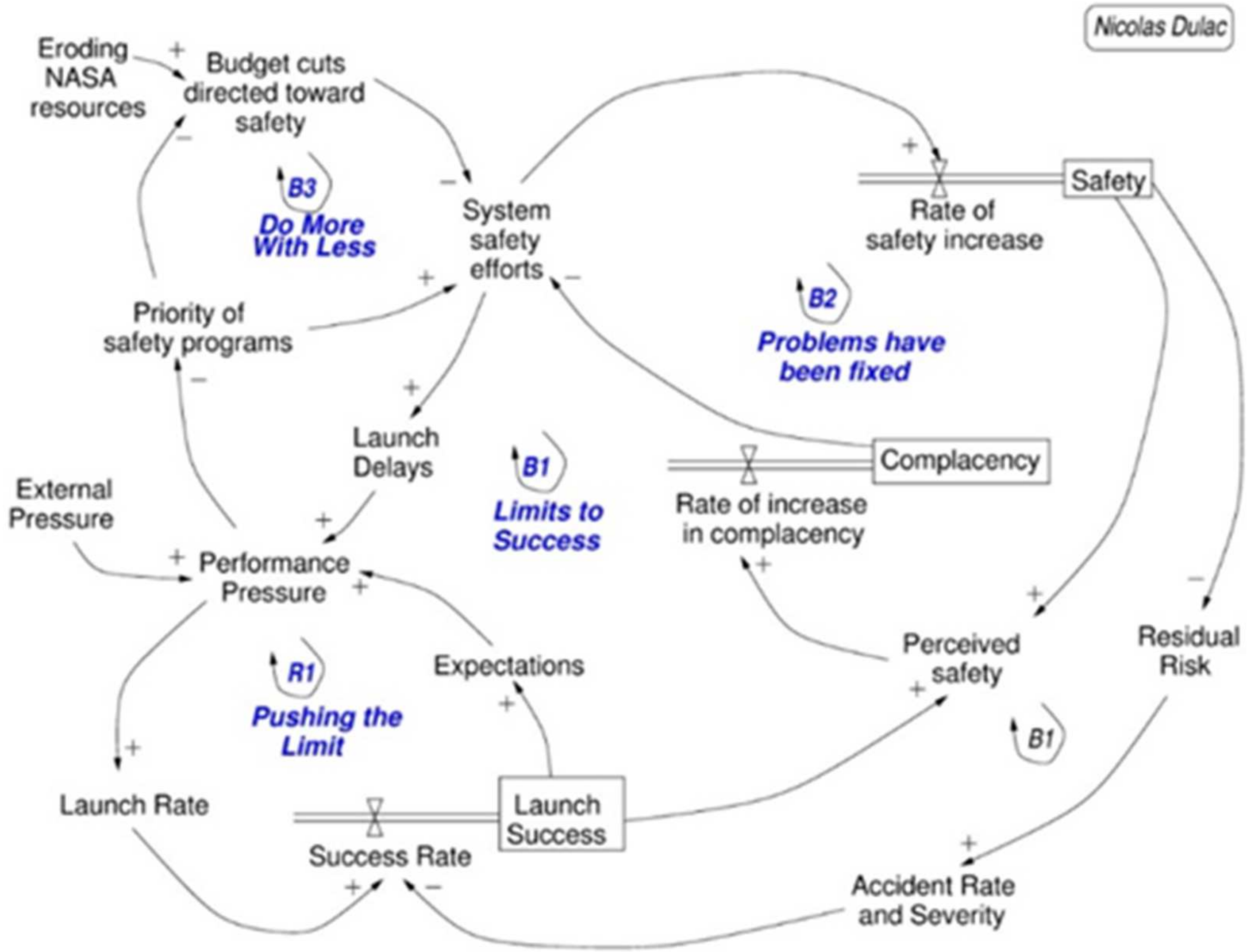
1. Define the system and its hierarchy of levels
2. Nothing in this world shall be taken certain
   (Avoid certainty delusion; avoid point value 'orphans')
3. Parameter values depend on conditions
4. Everything is dynamic, hence time dependent
5. Many variables are interdependent
6. Mind dysfunctional interactions and feedback loops
7. Use all evidence for analysis and conclusions

Effect of feed-back loops

System dynamics

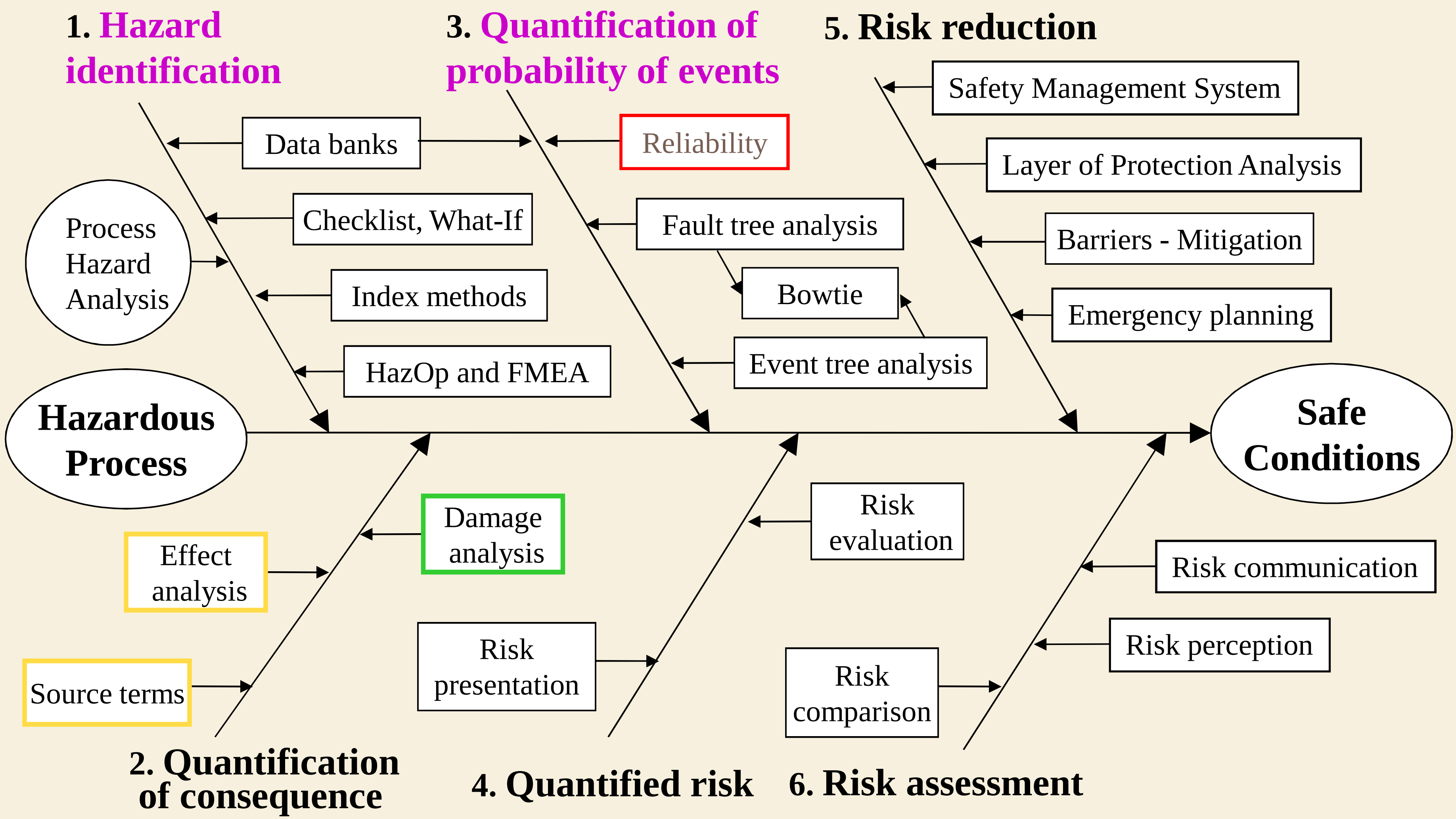
Drift to failure of NASA leading to Space Shuttle Columbia loss in 2003.

Leveson & Dulac, Safety and Risk-Driven Design in Complex Systems -of-Systems, 1st Space Exploration Conference: Continuing the Voyage of Discovery; Orlando, FL USA 30. 2005. 1-25



Process/Plant Risk Assessment Tools: QRA

Six step Quantified Risk Analysis Sequence



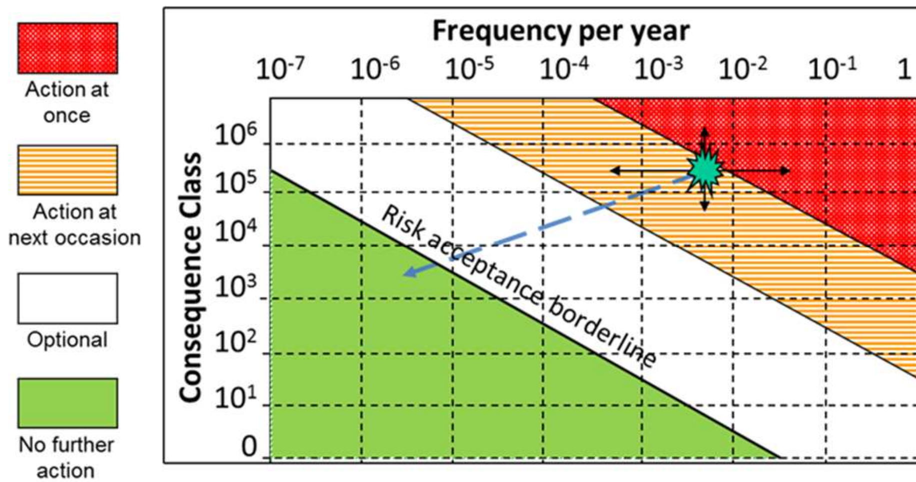
General problems with QRA

Rumsfeld quadrants

UK	**UU** **Black swan**
KK	**KU** **Perfect storm**

1. *Identification:* Methods are fallible:
   - Lack of imagination; overlooking
   - Complex causation: domino effects
   - Overconfidence: “doesn’t happen to me” attitude.
   - Dynamics, changing conditions
2. *Consequences*: Model deficiencies (> factor 2).
3. *Failure frequencies*: Lack of suitable data (>factor 10).
4. Not making *uncertaint*y explicit: No error bars, or confidence intervals, numbers with 4-5 decimals!

Risk Matrix for overview of results

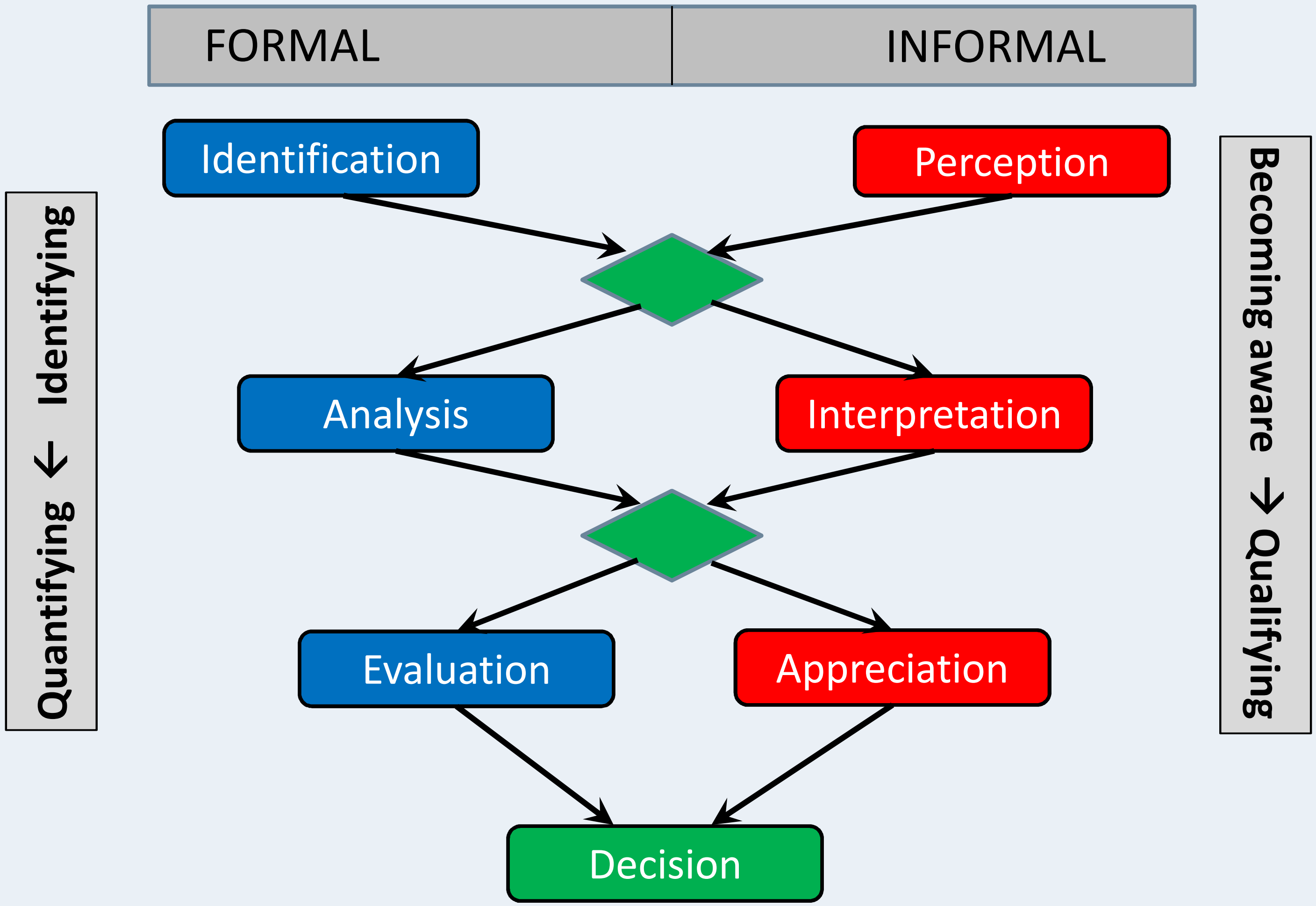


Consequence Class	Own employees	Community effects/ media coverage	Environment	Financial loss, $1000
10^6	Catastrophe	Multiple fatalities	Disastrous effects, long term	>1,000,000
10^5	Multiple fatalities	Fatality; International news	Disastrous effects	>100,000
10^4	Fatality	Injuries (severe); Regional news	Severe short term effects	>10,000
10^3	> 1 Injury	Injuries; local news	Serious impact	> 1000
10^2	Single injury	Noise/smoke/odor	Permit violation	> 100
10^1	No lost time	No hazard externally	No notification	< 100
0	No lost time	Normal operation	No notification	0

- *Demarcation lines are arbitrary; risk tolerance/acceptance will be explained later. First, human thinking and judging.*
- *Mentioned examples in consequence class category slots are based on experience, and appear to be rather time-independent*

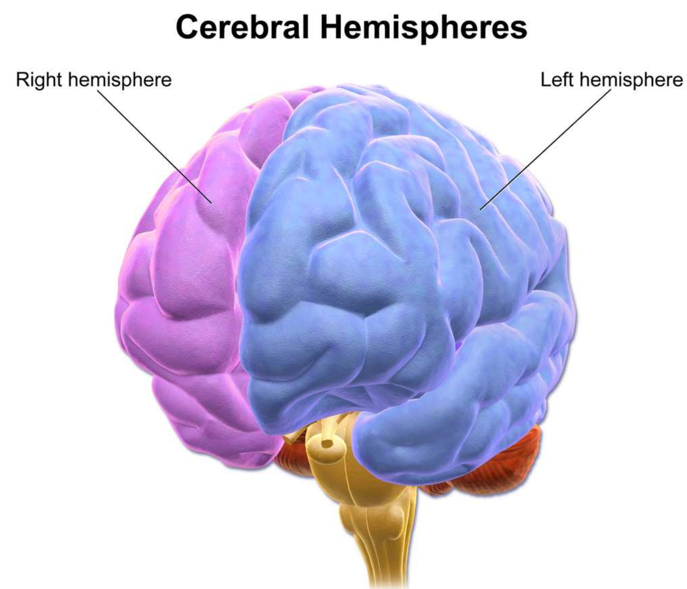
Now, let's look at it from a general human point of view!

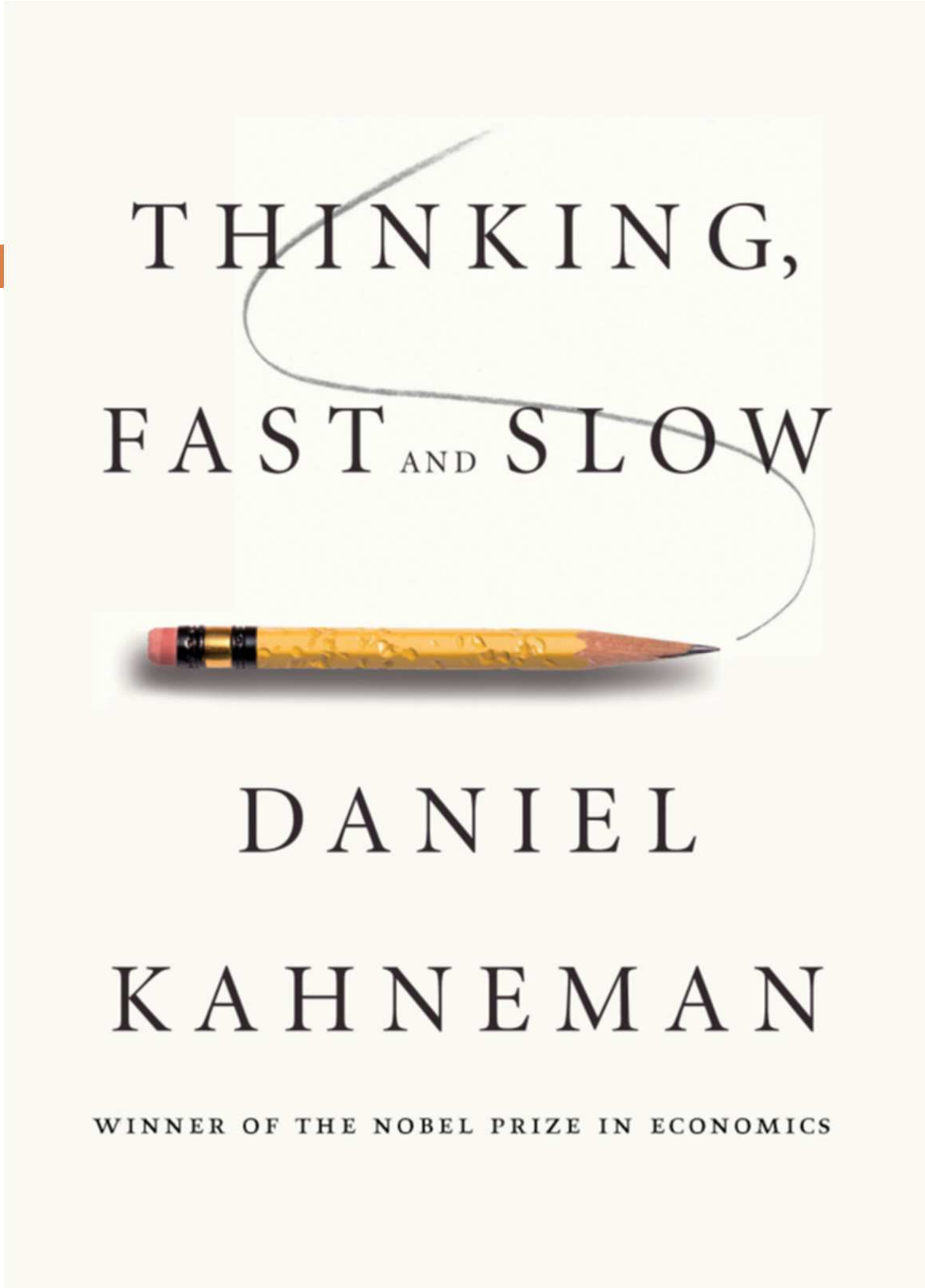
Dutch Royal Institution of Engineers, Risk management division (KIvI RBT) discussions



Left and right brain halves

Right half	Informal	Left half	Formal
Creative		Analytical	
Imaginative	*Culture*	Logical	*Rules*
Associative		Precise	
Conceptual		Organized	
Intuitive	*Behavior*	Repetitive	*Process*
Ad-hoc		Sequential	
Grand picture		Details	*Quanti-*
Heuristic	*Qualitative*	Scientific	*tative*
Accepting		Verifying	
Pictorial		Specific	
Involving	*Implicit*	Excluding	*Explicit*
Empathic		Uninvolved	





Psychologist – economist (Kahneman and Tversky)

http://vk.com/doc23267904_175119602?hash=8e08bedff908264985&dl=28aabb49a7217e1962

or

https://ia802504.us.archive.org/17/items/pdfy-XdUn_Gp9fEO3IuY6/Daniel%20Kahneman-Thinking,%20Fast%20and%20Slow%20%20.pdf

Daniël Kahneman: Thinking Fast and Slow

Farrar, Straus and Giroux, FSG Books,18 West 18th Street, New York 10011, Copyright © 2011 by Daniel Kahneman, ISBN: 978-0-3742-7563-1 - **Psychologist and economist; NOBEL prize winner 2002**

- Mental life regarding judgment and choice: System 1 and 2.
- System 1: Fast, intuitive, causal, heuristic, automatic, (no checks).
- System 2: Slow, also causal, but controlled, puzzling, disciplined.
- He presents many examples of failures of intuitive judgment.
- Many types of biases; WYSIATI, jumping to conclusions; availability heuristic, anchoring, planning fallacy, effect of luck, et cetera.
- Equations/Algorithms are better than Expert opinions.
- Statistics are difficult for the human brain, even for system 2.
- Statistics requires thinking about many things at once.
- You may draw once blindly from an urn with 9 iron balls and 1 gold one, or from another with 90 iron balls and 10 gold ones. Which urn do you prefer?
- How do you explain: “10^{-6} per year”?

Example of statistical appraisal

under the circumstances that existed on the night of the

Kahneman: A cab was involved in a hit-and-run accident at night.

- Two cab companies, the Green and the Blue, operate in the city.

Case 1:

- 85% of the cabs in the city are Green and 15% are Blue.
- A witness identified the cab as Blue.
- The court tested the reliability of the witness under the circumstances that existed on the night of the accident and concluded that the witness correctly identified each one of the two colors 80% of the time and failed 20%.
- *What is the probability that the cab involved in the accident was Blue rather than Green?*

Case 2:

The two companies operate the same number of cabs, but Green cabs are involved in 85% of accidents.

The information about the witness is as in the previous version.

- *Again, what is now the probability that the cab was Blue rather than Green?*

Solution

- *Case 1*: Apply Bayes theorem to calculate Pr(Blue|Witness conf):
- Prior A = fraction Blue cabs = 0.15; likelihood based on witness confidence $B \mid A$ = 0.8,

hence $P(A|B) = \frac{P(A|B)\times P(A)}{P(B|A)\times P(A)+P(B|\bar{A})\times P(\bar{A})} = \frac{0.8\times 0.15}{0.8\times 0.15+0.2\times 0.85} = 0.41$

- *Case 2:*
- Prior A = probability a Blue cab is involved in accident = 0.15; likelihood again 0.8,

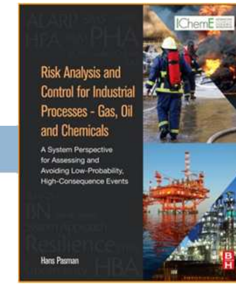
hence $P(A|B) = 0.41$

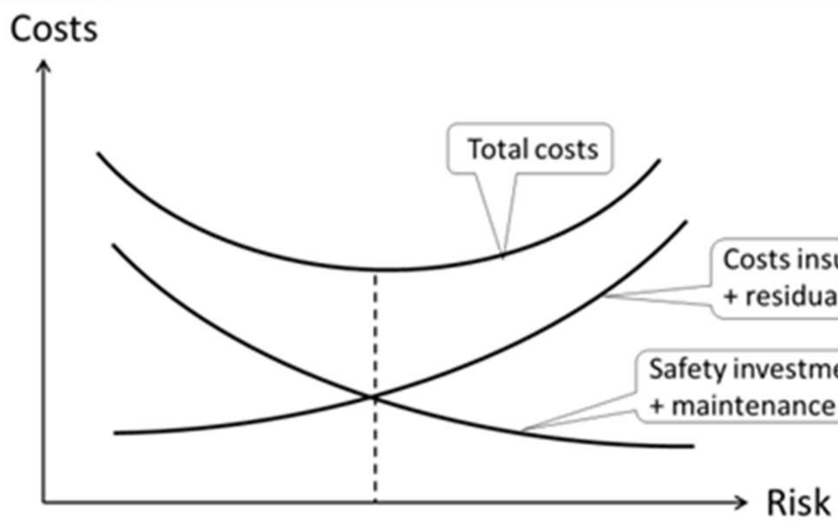
Economics: *after a disastrous accident goes the stock value down; sometimes with no recovery (e.g., BP after Macondo)*

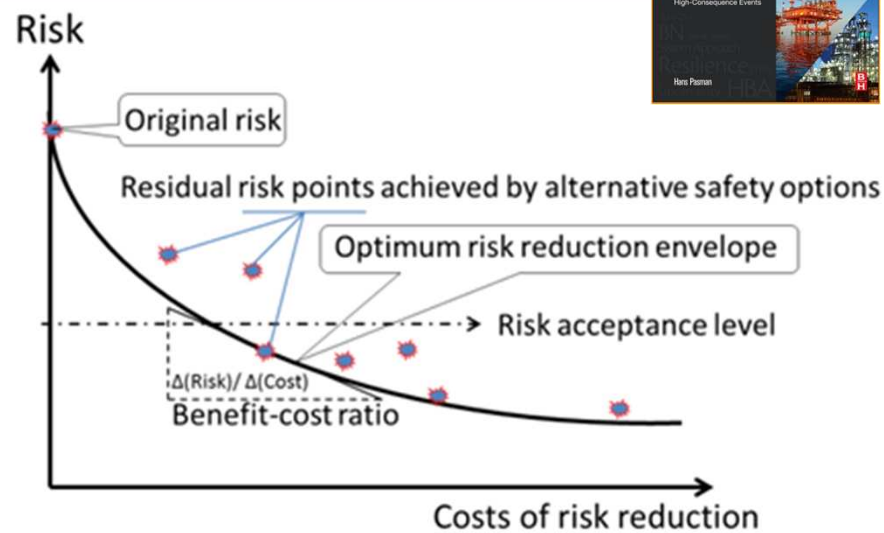
Concept	Meaning	Equation
Annual **cash flow**, here defined as:	Annual sales income, minus various types of annual expense, minus annual tax, minus expenditures on investment capital.	A_{CF}
Investment profita-bility: **Pay-Back Period**	Project life cycle number of years, n required to accumulate a total cash flow equal to the amount of fixed capital cost, C_{FC}.	$n = C_{\mathrm{FC}}/(\sum_{i=1}^{n} A_{\mathrm{CF},i})$
Net Present Value, NPV	Present worth of money, P is related to value, F of that money, j years in the future through the discount factor, being the reciprocal of annually compounded interest, i over j years.	$P = F \times f_{\mathrm{d},j}$ $f_{\mathrm{d},j} = 1/(1+i)^{j}$
Investment profita-bility, A over n years	NPV of the discounted annual cash flows, $A_{\mathrm{DCF},j}$ from the year of investment ($j = 0$) until and including year n.	$A_{\mathrm{DCF},j} = A_{\mathrm{CF},j} \cdot f_{\mathrm{d},j}\,;\ NPV_{\Sigma\mathrm{CF}} = \sum_{j=0}^{n} A_{\mathrm{DCF},j}$
Even more realistic is a **discounted** measure of profitability	Discounted Cash Flow Rate of Return, DCFRR is the accumulated cash flow the project generates over n years after covering all expenses, interests and taxes, which repays the original investment capital, C_{FC}.	$NPV_{\mathrm{DCFRR}} = C_{\mathrm{FC}}$
Expected Annual Loss cost, **EAL**, and event risk reduction measure	EAL cost is risk expressed as the product of expected event frequency per year, p, and the damage consequences (impact) of the event in monetary units, D.	$EAL = p \cdot D$ A risk reduction measure results in: $\Delta EAL = p_0 \cdot D_0 - p_1 \cdot D_1 = \Delta(p \cdot D)$
NPV of EAL amount	In analogy with investment NPV, a discounted loss cost can be calculated.	$\Delta EAL_{\mathrm{D},j} = \Delta EAL_j \cdot f_{\mathrm{d},j} = \Delta EAL \cdot f_{\mathrm{d},j}$; as ΔEAL is constant over the years.
Pay-off of risk reduction	Over the life cycle of the project of n years the discounted 'savings' by lower risk shall be larger than the investment cost of the safety measures, $C_{\mathrm{FC,S}}$ (although this does not need to be true in case the measure is due to regulation). The annuity present-worth factor, f_{AP} represents the interest expression.	$\sum_{j=0}^{n} \Delta EAL_{\mathrm{D},j} \geq C_{\mathrm{FC,S}}$ As ΔEAL is constant, this simplifies to: $\Delta EAL \times (\frac{(1+i)^n - 1}{i \cdot (1+i)^n} \geq C_{\mathrm{FC,S}}$ Or with the annuity present-worth factor: $\Delta EAL/f_{\mathrm{AP}} \geq C_{\mathrm{FC,S}}$

CBA: Cost-Benefit Analysis and Optimization

Hans Pasman, Risk Analysis and Control for Industrial Processes – Gas, Oil and Chemicals, Butterworth-Heinemann, 2015, ISBN: 978-0-12-800057-1







Overall operational life cycle safety cost optimization:

$$C_{\mathrm{tot}} = C_{\mathrm{FC,S}} + (C_{\mathrm{M}} + C_{\mathrm{Ins}} + EAL_{\mathrm{ResR}})/f_{\mathrm{AP}}$$

FC, S = Fixed capital cost – Capex – Safety

f_{AP} = Annuity present-worth factor

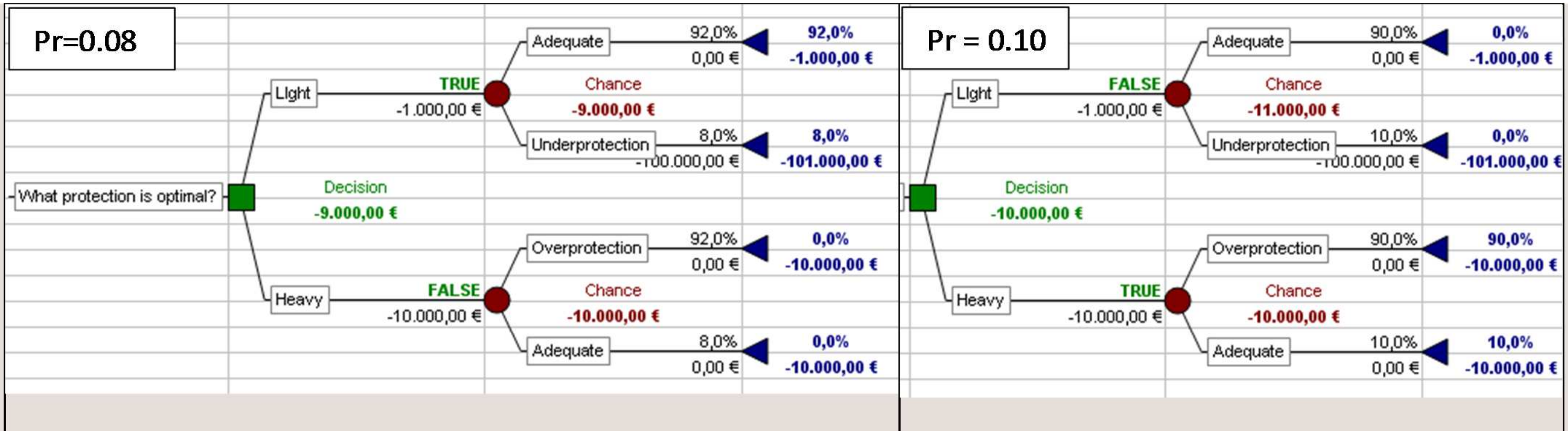
Optimum envelope line drawn such that tangent is at a residual risk point on the line, with no other points below the line. This represents the best B-C ratio.

Value of statistical life, VSL, or investment to avert the possibility of fatality, or willingness to pay: 3-10 M$

Other decision methods

- *Balanced scorecard*: scores based on performance indicators.
- *Analytic Hierarchy Process*: group, pairwise comparisons, rating.
- *Multi-Attribute Utility Theory*: Utility , functions [0,1], weights; simplest linear combining : $u(Q,C) = w_Q u_Q(Q) + w_C u_C(C)$.
  $\mathrm{E.g.}, Q$ is product quality, C is energy consumption
- *Optimal budget allocation*: Determine risk reduction measures and their cost, budget, optimize distribution: Knapsack – MILP.
  (Mixed Integer Linear Progrmming).
- *Economic utility of risky investments*: economics, risk appetite.
- *Game theory*: In case of opposing interests optimizing pay-offs.
- *Decision analysis and decision trees*: Dr Rogers; next slide.
- *Decision making under deep uncertainty*: AgenaRisk KUUUB and bootstrapping methods.

Example of Palisade's software decision trees, and the equivalent GeNIe Bayesian net



Decision about choice of a **protection system**: *light* costing €1000 - only adequate for normal situation, or *heavy* €10,000. At *under-protection* damage is €100,000.

Left: Coincidental hazardous process condition is estimated to occur 8% of time, light protection is best in cost-effectiveness. *Right*: at occurrence probability of 10% or higher, heavy protection makes sense.

<u>KU.UU.B factor:</u> Key risk indicators (KRI) plants A, B and C.

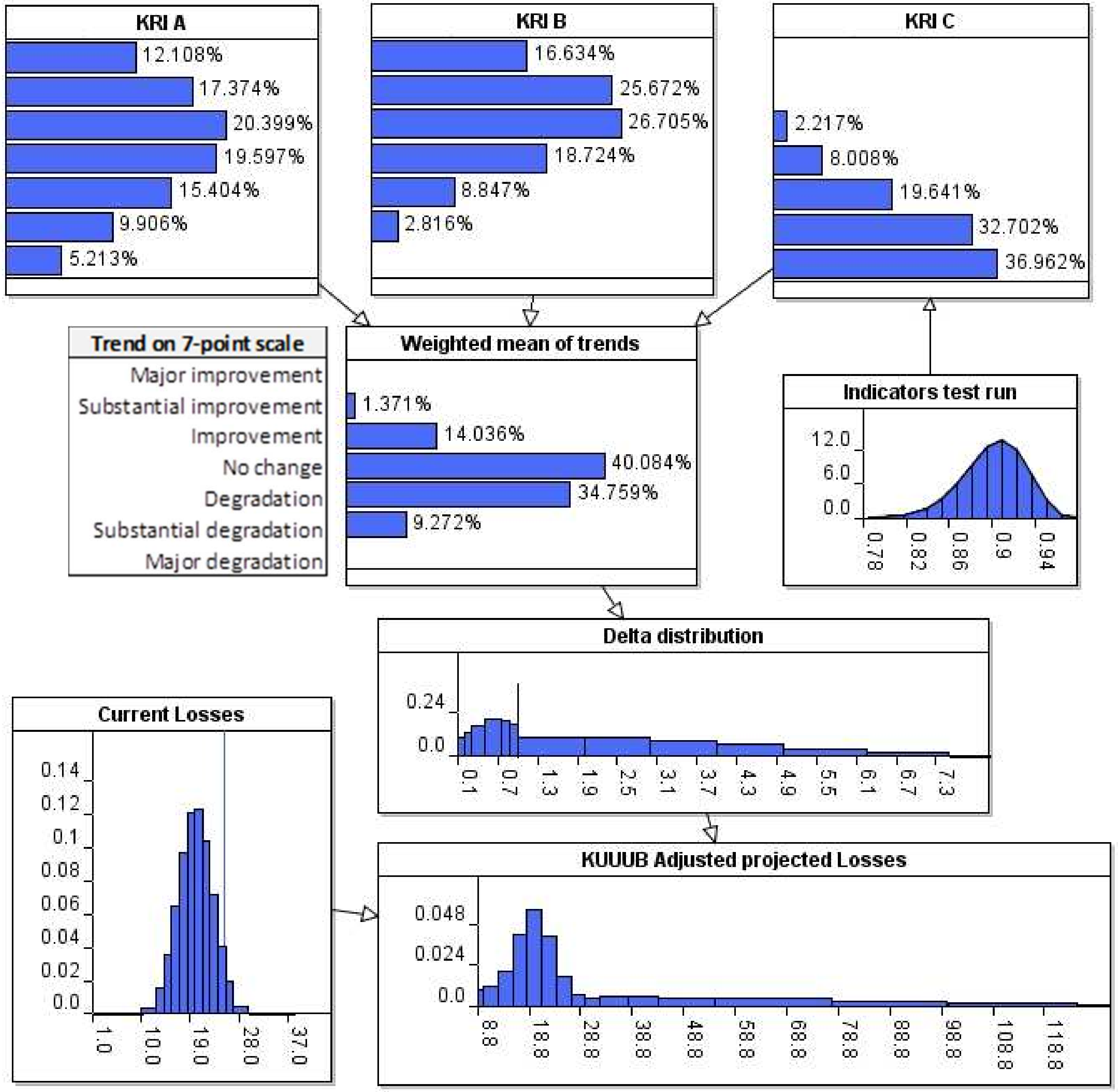
7-point scale depending on stress and maintenance.

A existing plant
B new product
C new hi-hazard.

Weighted mean trend estimates.

Δ distribution depending on trend, estimated by experts.

F&N Fig. 11.15



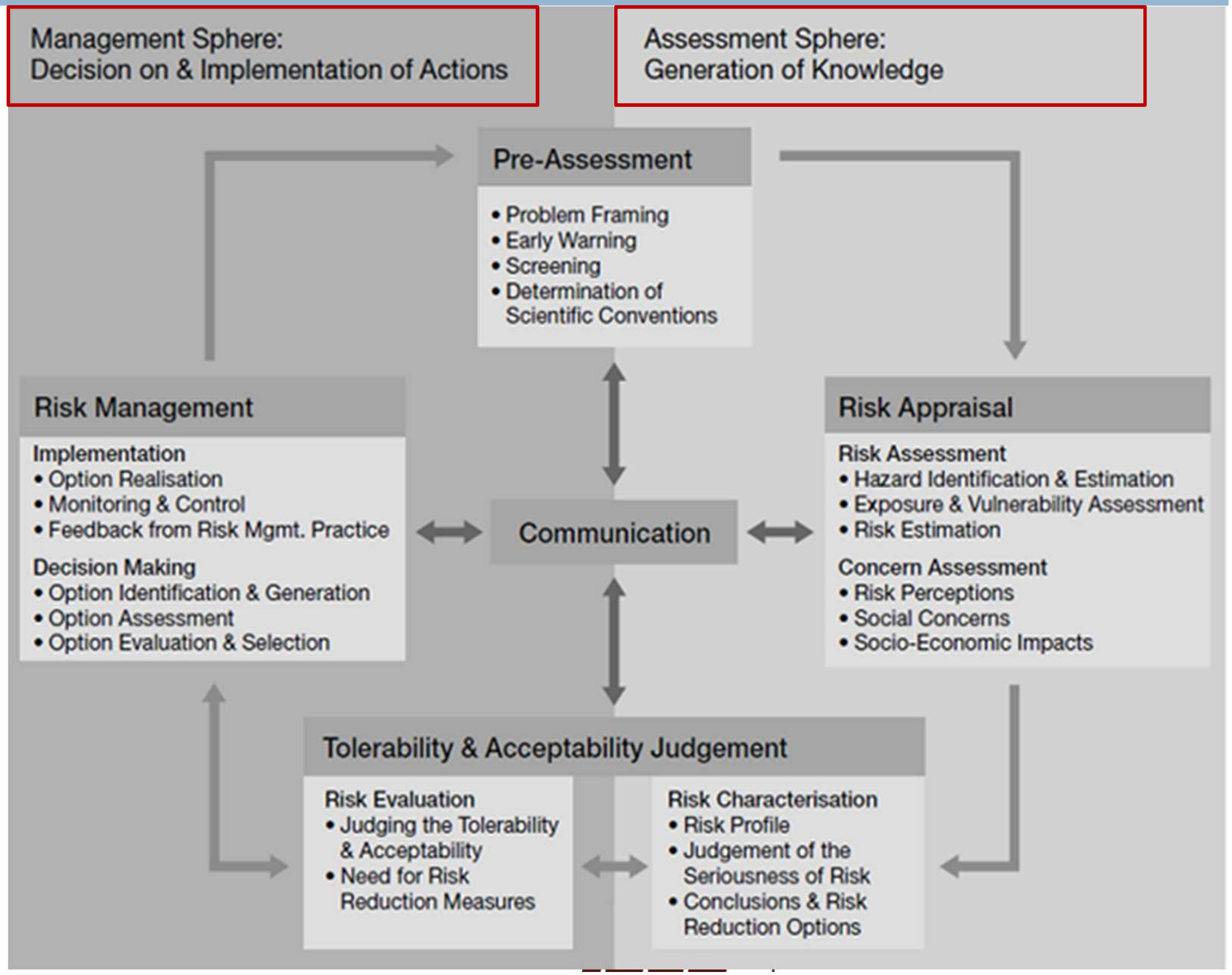
Int'l Risk Governance Council, Geneva

White paper on risk governance towards an Integrative approach: September 2005. www.irgc.org

IRGC's framework of risk governance.

Risk appraisal encompasses scientific assessment of risk: *first* in a physical sense, then in a *second* stage socially and economically.

Appraisal and risk management are strictly separated. *Communication* is central.



Risk communication: EPA's 7 rules

1. Accept and involve the public as a legitimate partner.
2. Plan carefully and evaluate your efforts.
3. Listen to the public's specific concerns.
4. Be honest, frank, and open.
5. Coordinate and collaborate with other credible sources.
6. Meet the needs of the media.
7. Speak clearly and with compassion.

Covello, V.T., and Allen, F.H., Seven Cardinal Rules of Risk Communication. Pamphlet drafted by U.S. Environmental Protection Agency, Washington, DC, April 1988, OPA-87-020.

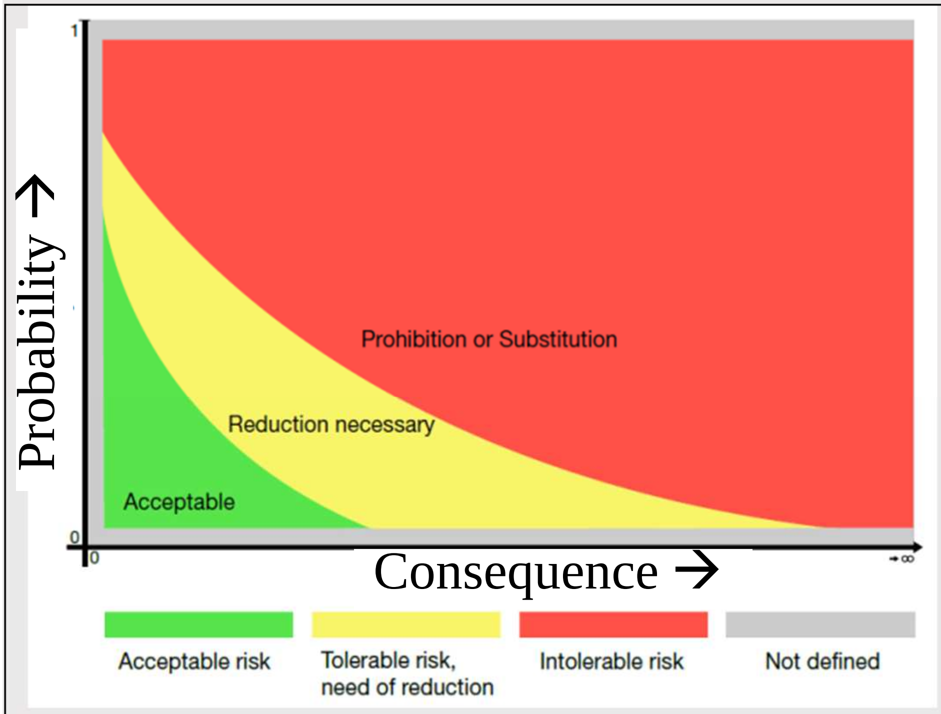
Risk communication according to Baruch Fischhoff

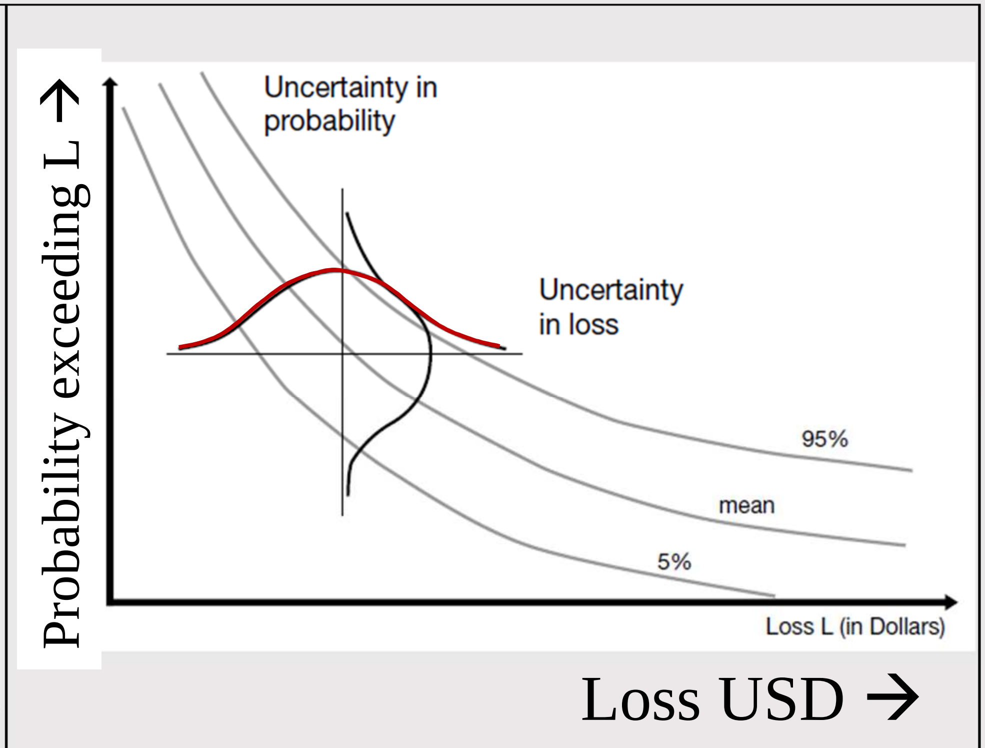
Fischhoff, B., Risk Perception and Communication Unplugged: Twenty Years of Process, Risk Analysis, 15 (1995), 137-145

Fischoff's Impression of Risk Analysts trying to convince the Public:

- All we have to do is get the numbers right (*that will not be ready tomorrow!)*
- All we have to do is tell them the numbers (*which will raise more questions)*
- All we have to do is explain what we mean by the numbers (*but the public may want other type of information on the project, e.g., how the reactor works)*
- All we have to do is show them that they've accepted similar risks (*risk comparisons can worsen the situation!)*
- All we have to do is show them that it's a good deal for them (*telling them their benefits of the project may help)*
- All we have to do is treat them nice (*they want their concerns taken seriously)*
- All we have to do is make them partners (*the public may want more influence)*
- All of the above (*there is no escape of going through the whole process!)*

IRGC: Risk acceptance and uncertainty

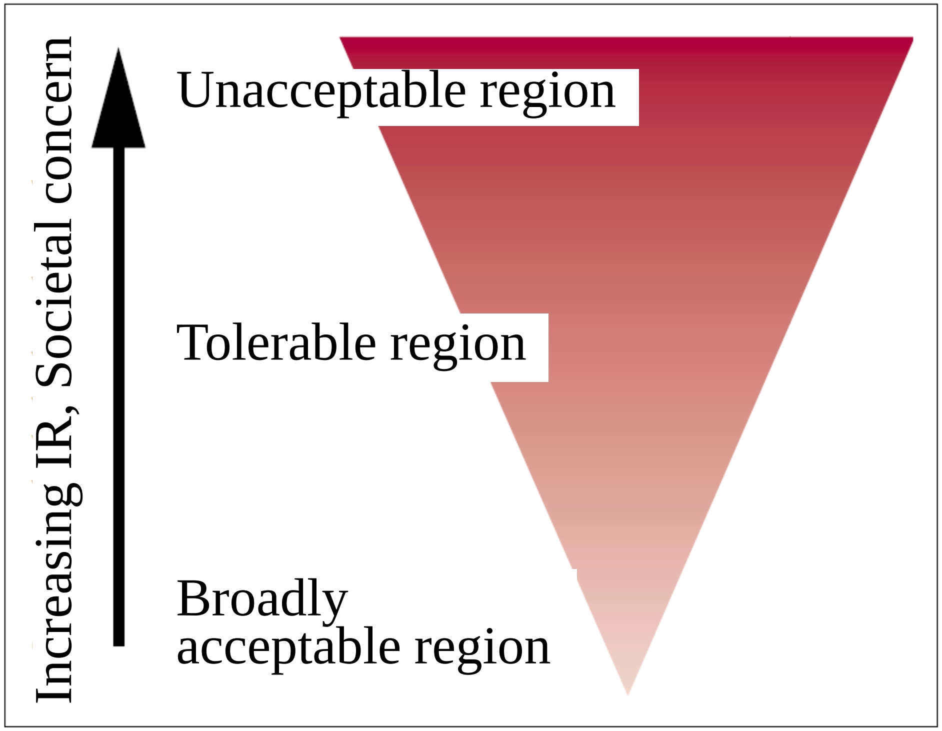




Left: Qualitatively, **acceptable** risk area, **tolerab**le, and **unacceptable**. In the tolerable part (middle) **reduction** is needed. At large consequence, probability of event occurrence shall be nil. *Right*: Dealing with uncertainty by **distributions**. Also, **sensitivity analysis** is necessary.

ALARP, As Low As Reasonably Practicable, HSE UK Risk criterion gaining popularity around the world

- ALARP must be applied as a ***holistic*** approach during all project phases of design, construction, commissioning, and operation.
- BAST: Best Available/Safe Technology
- Apply HSE's recognized good practice, standards, and codes (US: RAGAGEP = Recognized and Generally Accepted Engineering Practice).
- Inherently safer tech where possible.
- Risk reduction until costs become *disproportionately* (grossly) higher than the benefits, or acceptable limit
- Unacceptable/tolerable limit: fatality workers 10^{-3} ; public 10^{-4} per annum; Tolerable/acceptable limit: 10^{-6} p.a.



Health & Safety Executive UK. *Reducing risk, protecting people: HSE's decision makings process*. HSE Books; 2001, ISBN 0-7176-2151-0. http://www.hse.gov.uk/risk/theory/alarpglance.htm.

Conclusions

- Risk is relative and subjective. Probability of a rare event does not tell us much in absolute sense: It may be never, it may occur today.
- Although there is much improvement numerical risk assessment results are still highly uncertain. Order of magnitude errors exist.
- Nevertheless RA enables risk management, and with that improved decision making about distributing resources on risk reduction. Intuition can be erroneous. RA makes risks explicit. RA enables communication about risks between opposing parties.
- Business decision making will be highly cost/benefit based.
- Societal decision making has to be an open process. Human's 'system 1' may suffer from biases. Playing fears down does not help. Communication and an atmosphere of trust are crucial.