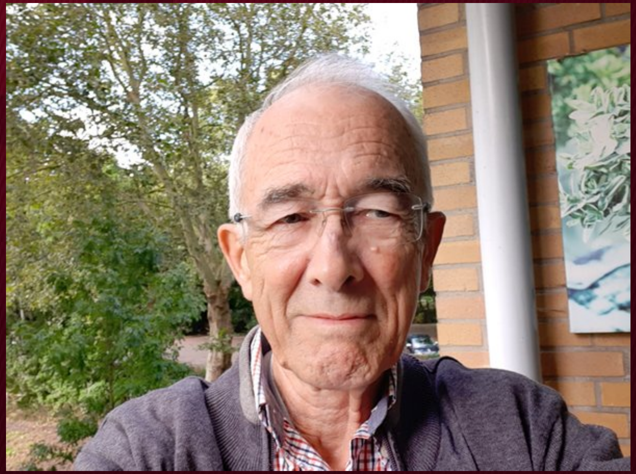
MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

Why is prediction of risks unreliable? Human limitations, dummy!

15 December 2021

Prof. Dr. Ir. Hans J. Pasman

TEES Research Professor,
College Station, Texas 77843, USA
Emeritus Professor Chemical Risk Management
Delft University of Technology, the Netherlands



Overview

1. Why risk analysis and assessment?
2. Can we trust the outcome of analyses?
3. What are sources of uncertainty?
4. Why is scenario identification problematic?
5. How to beat complexities and uncertainties?
6. How to express/account for uncertainty in the results?
7. Future outlook!
8. Conclusions

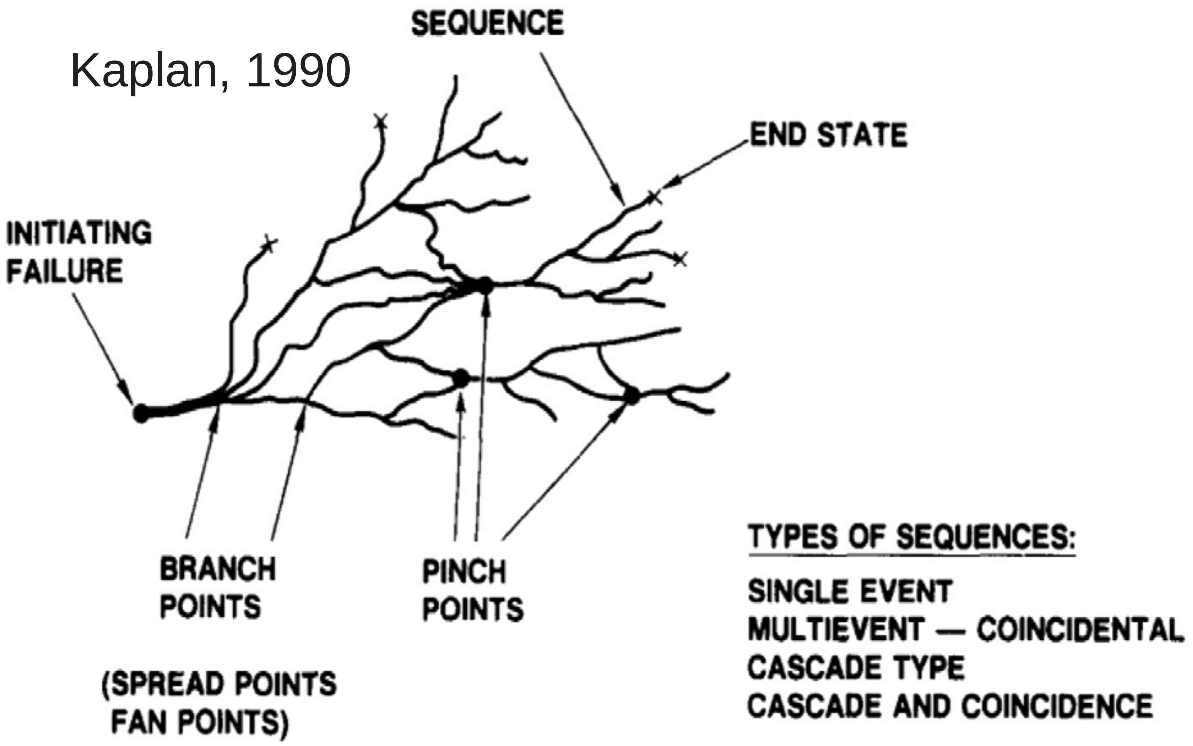
Why risk analysis and assessment?

- **For a given case to know how "*safe is safe enough*", one needs to know the risks.**
- **For the analysis, repeat the three classic 1980 Kaplan and Garrick questions:**
  - What can happen or go wrong (scenario)?
  - How likely is it (chance, probability)?
  - How large is the (expected) damage (consequence severity)?
- **Assessment means what risk (consequence-probability pair) is acceptable.**
- **It can be qualitative, semi-quantitative (risk matrix), quantitative (QRA).**
- **In the 1970-80s risk analysis was seen as panacea to beat major accidents.**
- **A host of effort followed in the 1980s and 90s:**
  - Introducing *HAZard and OPerability study*, *Failure Mode and Effect Analysis*,
  - *Gas dispersion* and *Vapor Cloud Explosion* field and laboratory tests, modeling,
  - 'Perpetual' discussions about reliability of equipment failure frequency data.

Can we trust the outcome of analyses?

- **Answer is NO!**
- Shocking: EU ASSURANCE benchmark project in 2000: *Seven experienced teams* performing QRA on same plant independently: **Orders of magnitude difference!**
- Uncertainties: **1) HAZID/Scenario**; 2) Lack of failure data, 3) Model limitations**.**

Kaplan, 1990



- **Another example: 12 teams on safety of a product** (max. required 1 in a million), e.g., pacemaker.
- **Safety argument + confidence argument** (RA + reasons why to trust the result)**.**
- **Graydon and Holloway (2017)** showed how each of the 12 results could be in doubt due to flaws in the reasoning or a counterexample.

What are sources of uncertainty?

An incomplete list of source examples:

- Scope and objective of analysis unclear
- Source material inaccurate, wrong assumptions
- Lack of human imagination of what can go wrong.
- *Lack of knowledge and experience of the analyst.*
  - This all occurs in HAZOP studies
- Model uncertainty due to simplicity
- *Lack of data, use of wrong data*
- Errors in the risk analysis; subjectivity in the risk acceptance level
- Unawareness that decision making depends too on information about magnitude of uncertainty. And: Risk is **not** always: Cons. × Prob.

Scenario knowledge of analyst

DefSecr Rumsfeld quadrant

K = Known; U = Unknown

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

Why is scenario identification problematic?

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

- **Kahneman: Thinking Fast (1)** ***and Slow (2)*****: WYSIATI and Laziness of the mind**
- When ’20’ you cannot imagine how you will function at ’80’. And ‘It will not happen to me’-thinking.
- **Complexity: socio-technical system, the “organism” dynamics.**
- In causation **Tight couplings, Non-linearity:** dysfunctional component interaction; organizational pressures → interacting control loops (time) **- STPA**
- **Domino effects** due to a primary event, **escalation** of disastrous effect
- Fallible **mental image** of physics and chemistry of the process.
- Large variability in **human operational performance (errors).**
- Viscosity of the organization **(bureaucracy)**
- **Miscommunication** between hierarchical levels, and within team/shifts
- **Hidden design errors, material problems**
- **Transient operations:** Start-up, turn-around, shut-down
- **Maintenance shortcomings:** too late, bad quality, no new parts 6

How to beat complexities and uncertainties?

- **Define scope and analysis objective with the stakeholders**
- **Set-up a list of assumptions. Use QRA to compare cases!**
- Use for HAZID a ***system approach***; follow Rasmussen, Leveson (STPA) and others (OntoCAPE/HAZOP, FMECA), and extract accident data bases (Dypasi)
- Try from the start to define the *accuracy* of models and data (confidence intervals).
- Models can be verified and analyzed on *sensitivity*, so that the most important parameters are identified and extra scrutinized
- Failure data are a problem. These should be derived from observations under identical conditions as in the case. Usually, impossible. *Expert estimates* may help.
- There are *data bases* available, and suggestions how to deal with *conditions*.
- **Observations can be derived from alarms, precursors and near-misses; event tree and hierarchical Bayesian analysis; solving with OpenBUGS or other MCMC.**

How to beat complexities and uncertainties? (2)

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

- Uncertainty is *aleatory* (**randomness**) or *epistemic* (**missing knowledge**), or mixed.
- Probability (1600s), subjective Probability (1950s), other forms (1990s).
- Helton & Johnson (2011) four different expressions of uncertainty:
  - (1) Probability theory (P statistics), **frequentist observations, Bayesian prior**
  - (2) Evidence theory (Dempster-Shafer), **pieces of evidence; belief and plausibility**
  - (3) Possibility theory and Fuzzy set approach, **membership function 0,1,0; logic/control**
  - (4) Interval analysis: **just the extremes, interval type 2 fuzzy set (Mendel & Wu, 2010) .**

Ad (1) *Bayesian*: prior × likelihood → posteriori distribution is tremendous progress.

Ad (2) Example: 2 experts and interviewer: will that accident happen this year?

Ad (3) Possibility degree distribution – can be treated as fuzzy set. Quite popular in RA nowadays:

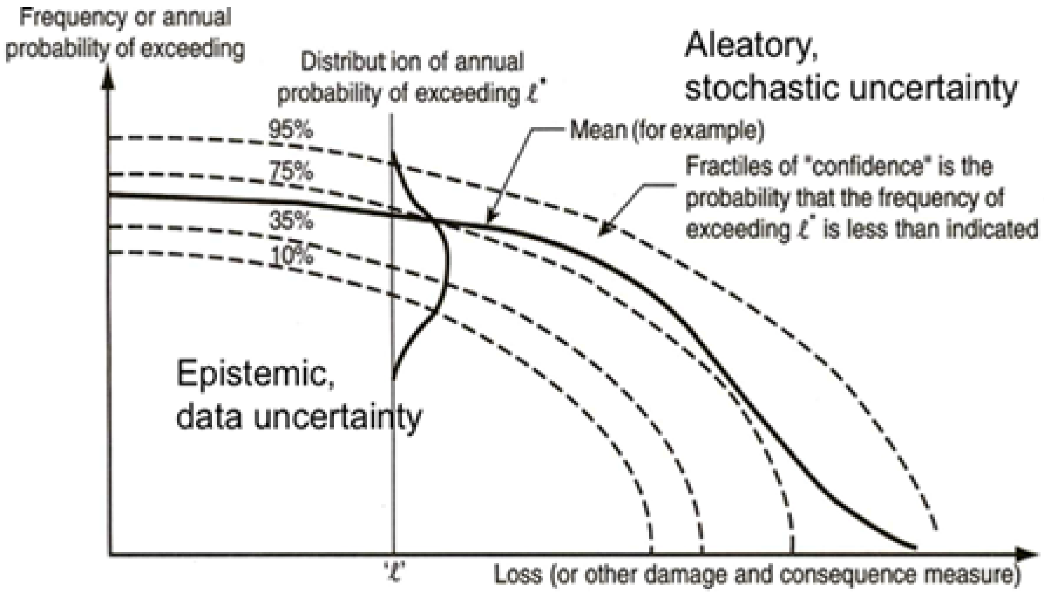
Expert estimates: Linguistic or numerical; importance weighting with AHP or another of the many **decision methods** to obtain the best compromise!

Given causal structure, **Bayesian (belief) network** can tie all event probability distributions together.

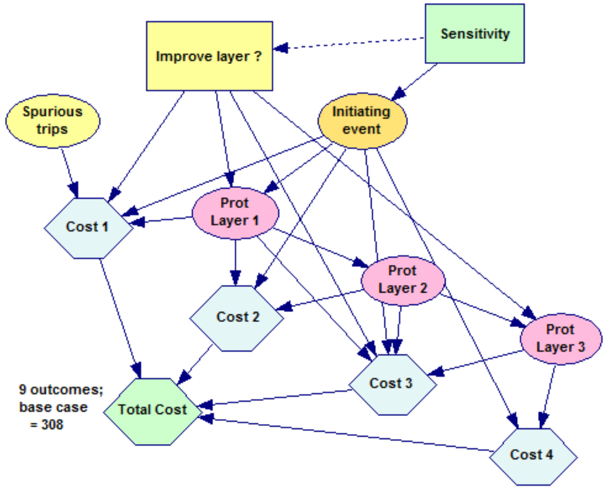
How to express/account for uncertainty in the results

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

- **Paté-Cornell (1996): Multiple risk curves**
- **Bayesian network (after 2000) produces a result probability distribution.**
- **Johansen & Rausand (2014): Complexity indicator** (28 complexity indicators), since:
  - A system can be complex to one analyst, but not to another.
  - A system be complex today, but not tomorrow.
  - A system be complex in one assessment context, but not another.
- Avoid **ambiguity** in result wording.
- **Flage & Aven (2017): analyst Strength of Knowledge,** strong, medium, low



BN LOPA Pasman & Rogers, 20



Future outlook: improvements are arriving!

- Industry *digitalization* will provide data-driven solutions: **Industry 4.0 → Safety 4.0**
- Data from sensors, safety management and admin systems feed models.
- The academic literature is *exploding*: machine learning and AI algorithms to make sense of data are being developed and improved continuously.
- Process *fault detection and diagnosis* “takes the cake”. The number of different solutions for both continuous and batch processes overwhelms.
- Maintenance data (via Central MMS) enables failure/*availability* prediction.
- *Similarity algorithms* enable extraction data from incident data bases.
- *Digital twins* enable process scenario research and operator training.
- Weak *warning signals* will enable correction before an incident occurs.
- Alarm management becomes much easier. Start-up and other *transients* can be tackled.
- Altogether, *dynamic risk assessment* and *resilience management* is in reach.

Conclusions

- 50 Years of risk assessments produced many papers, worldwide.
- A long time progress was only *moderate*: only consequence analysis improved due to field tests and CFD developments.
- Human and organizational factors were largely *ignored*.
- Public was often *non-believer* due to uncertainty and different interpretations.
- Since 2000, the *socio-technical system* concept enabled a holistic approach.
- Since 2000, *Bayesian approach* and *Bayesian network* opened new possibilities.
- During the last decade, *digital solutions* produce a strong renewal impulse.
- So, *computerization* compensates human limitation.
- Because of the energy transition, we shall need improved risk assessment badly.
- **So, why not to participate in the CISAP and Loss Prevention symposia?**

References

- Kaplan S, Garrick B.J. (1980) On the quantitative definition of risk. Risk Analysis 1(1), 11-27.
- Lauridsen K, Kozine I, Markert F, Amendola A, Christou M, Fiori M., (2002). Assessment of uncertainties in risk analysis of chemical establishments. The ASSURANCE project Final summary report. Roskilde, Denmark: Risø National Laboratory; May 2002. 52p, http:// www.risoe.dk/rispubl/sys/syspdf/ris-r-1344.pdf.
- Kaplan S. (1990) On the inclusion of precursor and near miss events in quantitative risk assessments: a Bayesian point of view and a space shuttle example. Reliability Engineering and System Safety 27, 103-115.
- Graydon, P.J., Holloway, C.M., (2017). An investigation of proposed techniques for quantifying confidence in assurance arguments. Safety Science 92, 53–65.
- Kahneman, D., (2011). Thinking Fast and Slow, Farrar, Strauss & Giroux, New York.
- Rasmussen J., (1997). Risk management in a dynamic society: a modelling problem. Safety Science 27, 183-213.
- Leveson N.G., (2011). Engineering a safer world, systems thinking applied to safety. The MIT Press; 608 pp., ISBN-10:0-262-01662-1, ISBN-13:978-0-262-01662-9.
- Single J,I., Schmidt J., Denecke J., Ontology-based computer aid for the automation of HAZOP studies. J Loss Prevention in the Process Industries 68, 104321.
- Paltrinieri N., Tugnoli A., Buston J., Wardman M., Cozzani V., (2013). Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool. J Loss Prevention in the Process Industries 26, 683-695.

References (2)

- Yu H., Khan F., Veitch Br., (2017). A Flexible Hierarchical Bayesian Modeling Technique for Risk Analysis of Major Accidents. Risk Analysis 37 (9). 1668-1682.
- Paté-Cornell M.E., (1996). Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety 54, 95-111.
- Paté-Cornell M.E., (2012). On “Black swans” and “Perfect storms”: risk analysis and management when statistics are not enough. Risk Analysis 32, 1823-1833.
- Helton, J.C., Johnson, J.D., (2011). Quantification of margins and uncertainties: alternative representations of epistemic uncertainty. Reliability Engineering and System Safety 96, 1034–1052.
- Mendel, J.M., Wu, D., (2010). Perceptual Computing: Aiding People in Making Subjective Judgments. IEEE Press, Wiley, ISBN 978-0-470-47876-9.
- Pasman H.J., Rogers W.J., (2013). Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable! J Loss Prevention Process Industry 26, 434-442.
- Johansen I.L., Rausand M., (2014). Defining complexity for risk assessment of sociotechnical systems: a conceptual framework. J Risk & Reliability 228 (3), 272-290.
- Johansen I.L., Rausand M., (2015). Ambiguity in risk assessment. Safety Science 80, 243–251.