Risk Analysis
An Introduction

Marvin Rausand
Department of Production and Quality Engineering
Norwegian University of Science and Technology
marvin.rausand@ntnu.no

Introduction

What is risk analysis?

A risk analysis is:

- "Systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment"

  – IEC 60300-3-9

- "A systematic approach for describing and/or calculating risk. Risk analysis involves the identification of undesired (accidental) event, and the causes and consequences of these events"

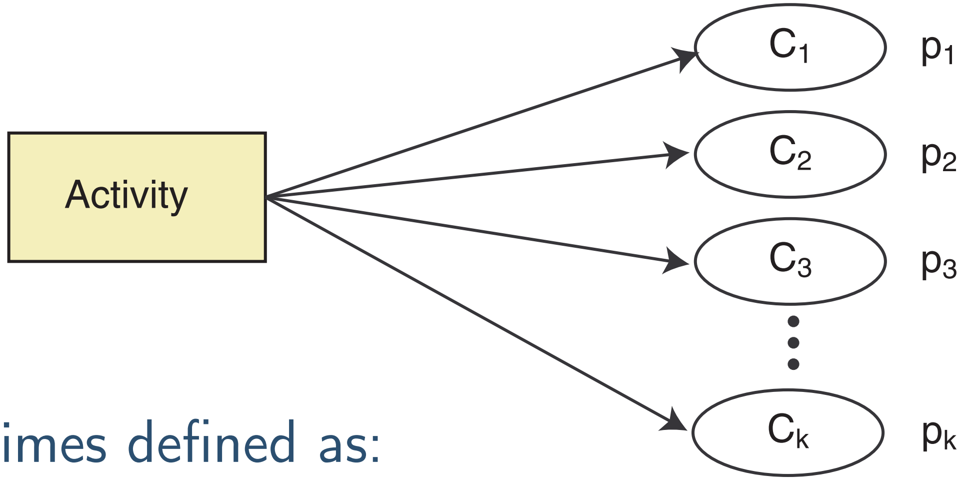
  – NS 5814

Brief history

- Nuclear industry from the 60s: Probabilistic Risk Assessment (PRA)
- Chemical industries from the 70s: quantitative risk assessment (QRA), Seveso directive (I and II)
- Offshore industry from the 80s: QRA, Industrial Self Regulation in Norway, Safety Case Regime in UK
- Shipping industry from 90s: Formal safety assessment (FSA)

Consequence spectrum

A *consequence spectrum* (or, *risk picture*) of an activity is a listing of its potential consequences and the associated probabilities (e.g., per year). Usually, only unwanted consequences are considered.

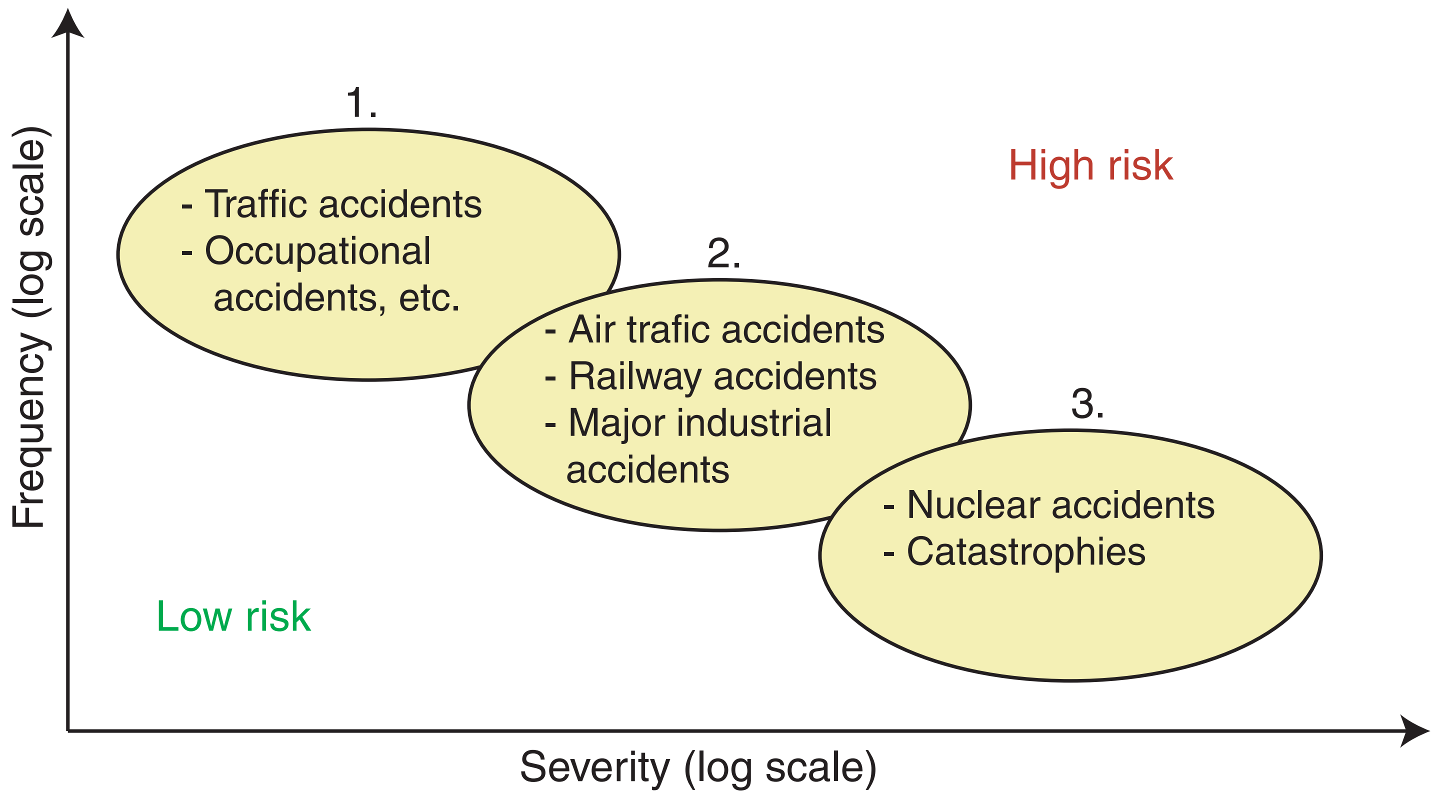


Risk is sometimes defined as:

$$\text{Risk} = C_1 p_1 + C_2 p_2 + \cdots + C_k p_k = \sum_{i=1}^{k} C_i p_i$$

This requires that all consequences may be measured with a common measure (e.g., as monetary value)

Categories of accidents



– Based on Rasmussen (1994)

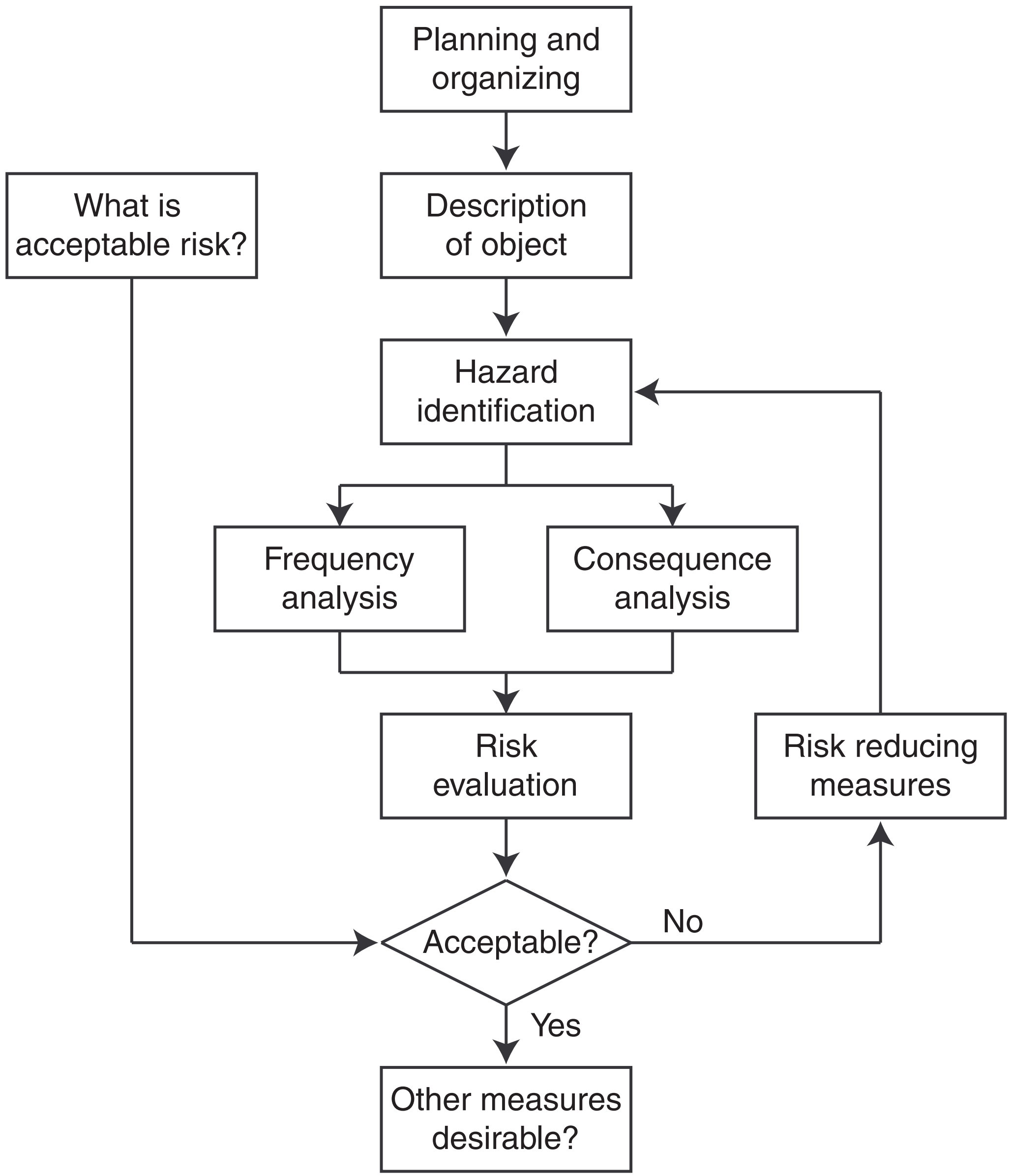
Standards for risk analysis

- IEC 60300-3-9: "Risk analysis of technological systems"
- EN 1050: "Safety of machinery – Risk assessment"
- EN 50126: "Railway applications – The specification and demonstration of reliability , availability, maintainability amd safety (RAMS)"
- ISO 17776: "Petroleum and natural gas industries – Offshore production installations – Guidelines and tools for hazard identification and risk assessment"
- NORSOK Z-013: "Risk and emergency preparedness analysis"

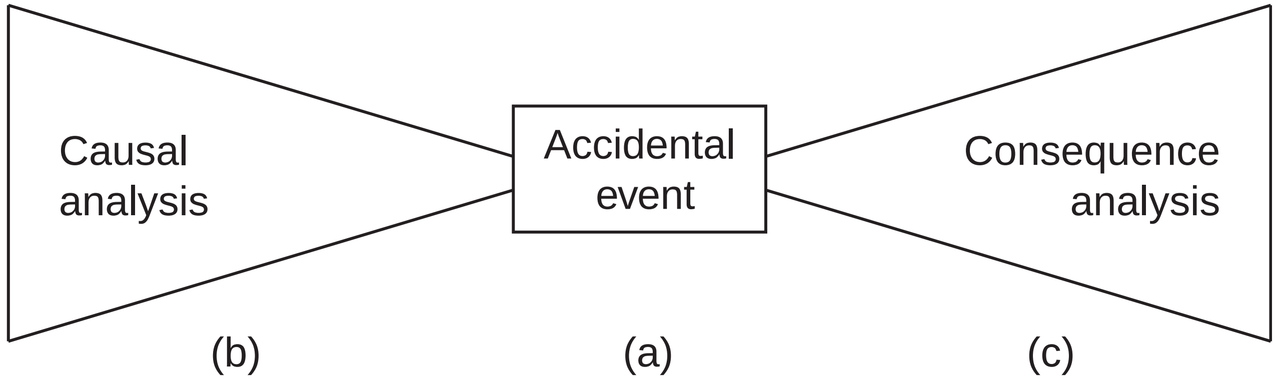
- EN 1441: "Medical Devices - Risk Analysis"

More standards on: http://www.ntnu.no/ross/srt

Risk analysis procedure



Risk analysis procedures - (2)



Methods		
- Fault tree analysis* - Reliability block diagrams* - Influence diagrams* - FMECA* - Reliability data sources*	- Checklists - Preliminary hazard analysis - FMECA* - HAZOP - Event data sources	- Event tree analysis* - Consequence models - Reliability assessment* - Evacuation models - Simulation

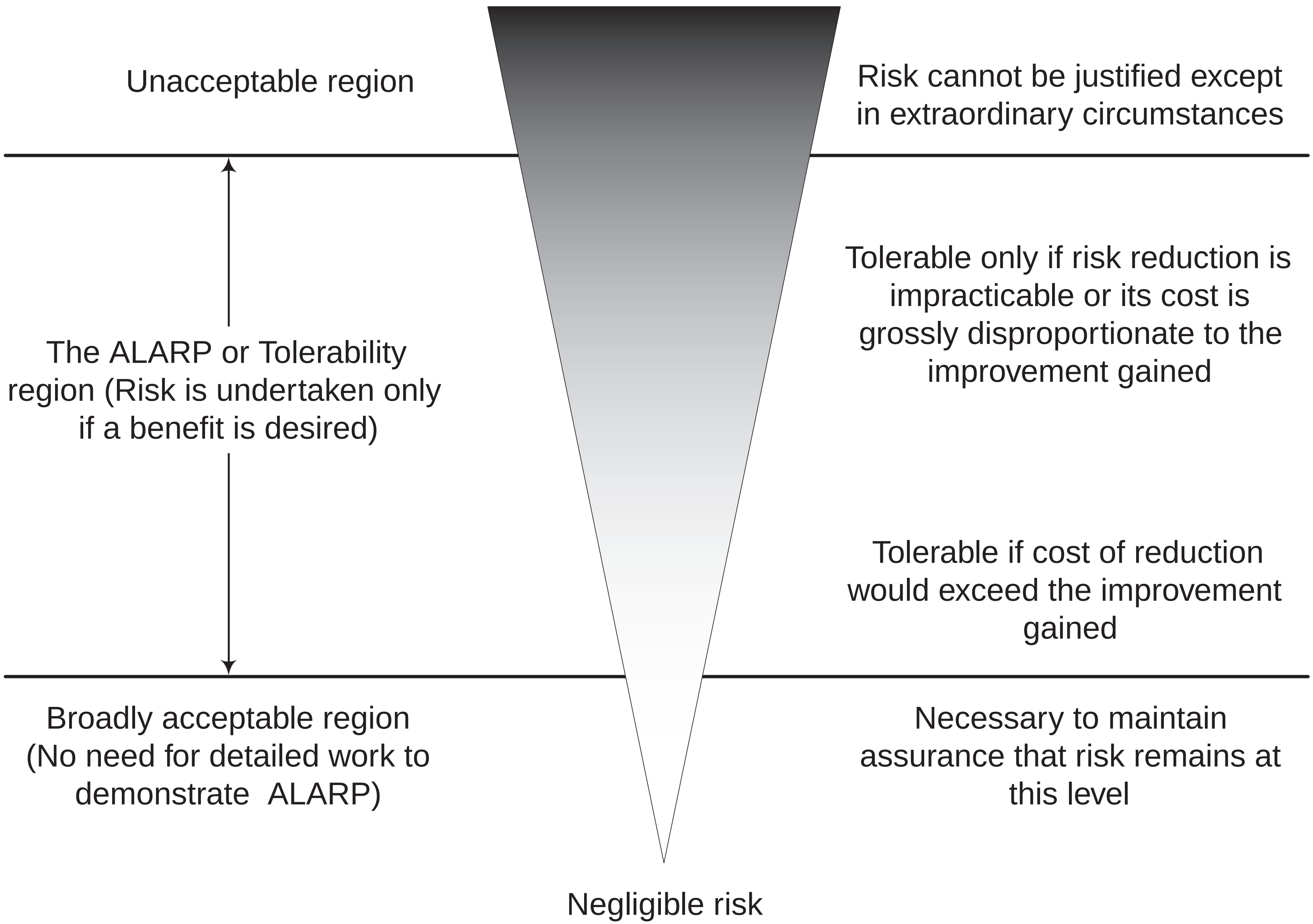
Acceptable risk

Several principles can be used to determine the acceptable risk:

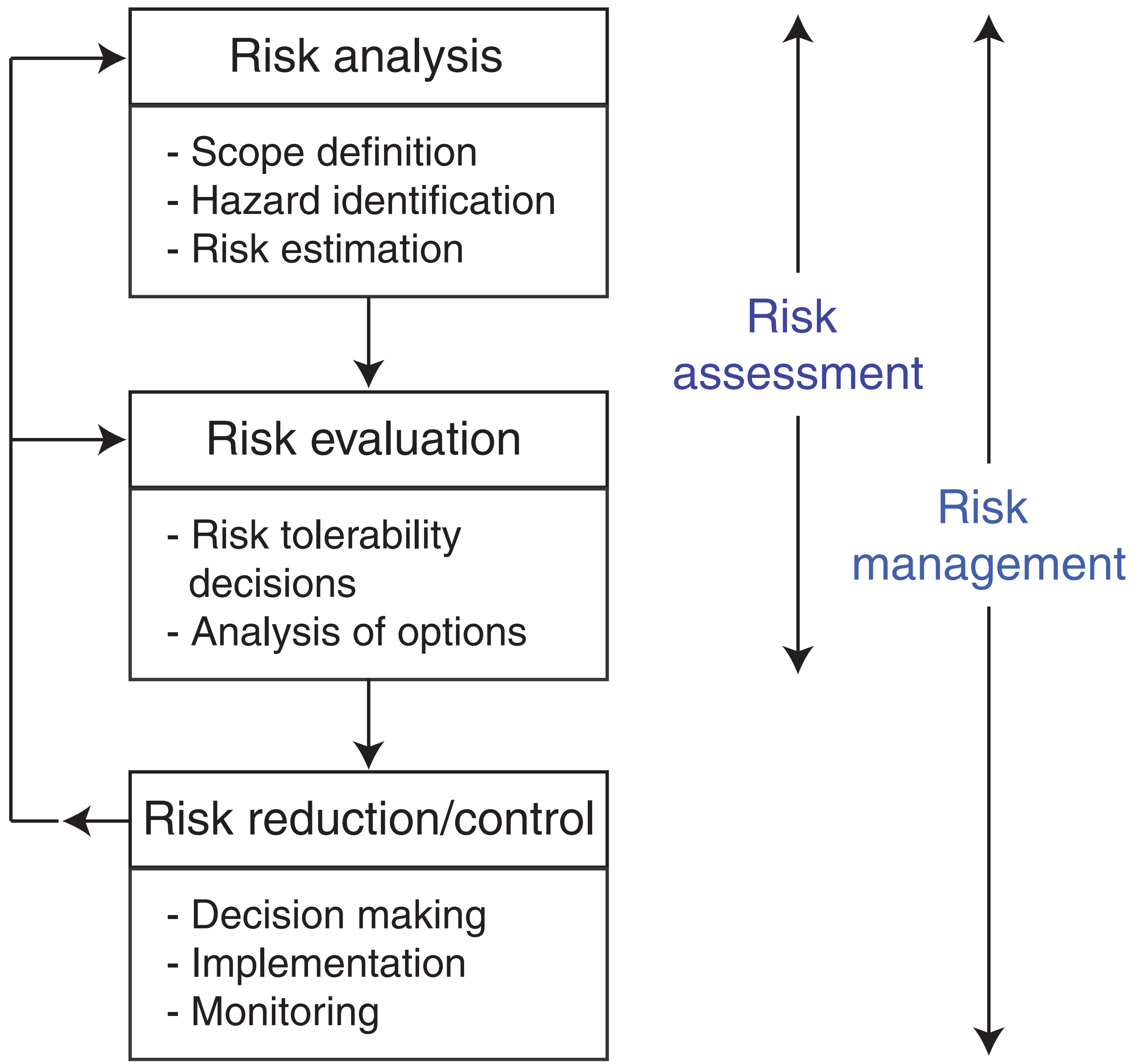
- The ALARP principle (“As low as reasonably practicable”)
- The precautionary principle
- Risk acceptance as defined in NORSOK Z-013
- Minimum endogeneous mortality (MEM)
- Globalement au moins aussi bon (GAMAB)

Risk acceptable is generally a complicated and multifaceted issue.

ALARP principle



Risk assessment and management



– IEC 60300-3-9

Main Steps

Planning and organization

- Identify relevant laws and regulations
- Clarify internal policies and risk acceptance criteria
- Define the purpose and objectives of the risk analysis
  - What type of risks should be studied? (Major accidents vs. occupational accidents; random hazards, deliberate actions, and/or environmental loads)
  - Which life phases should be included? (Normal operation, start-up, end-of-life, major overhaul, etc.)
- Organize the work, multidisciplinary team where selected experts provide the required expertice

Description of the analysis object

Description encompassing everything that can incluence the analysis results

Main questions:

- What is the system dependent upon? (inputs)
- What activities are performed by the system? (functions)
- What services does the system provide? (outputs)

Description of the analysis object - (2)

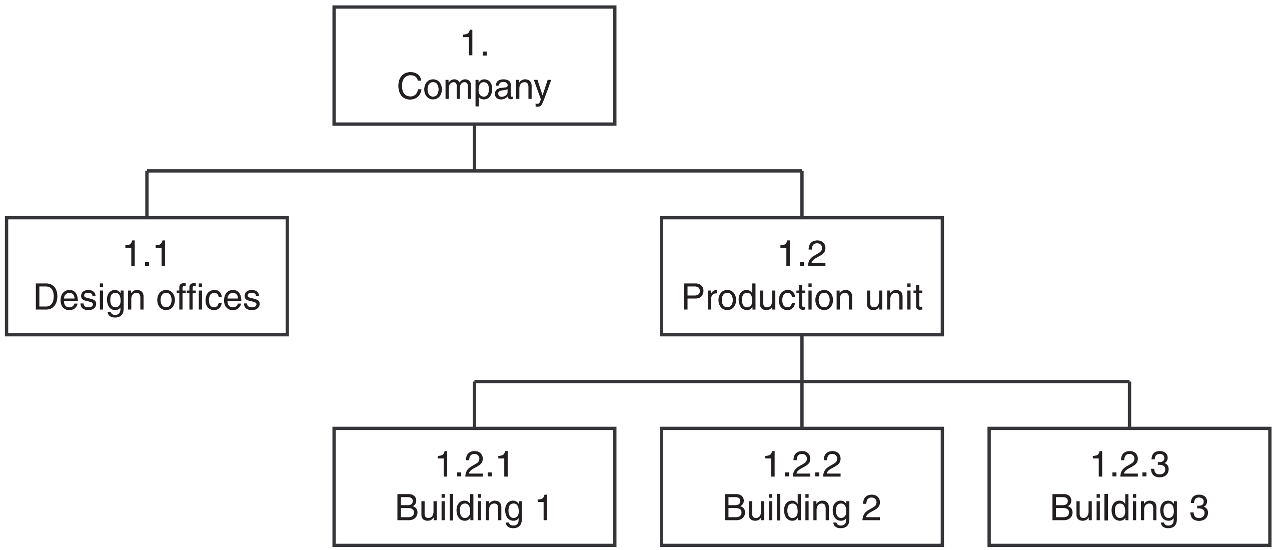
- Technical, personnel, and organizational relationships
- Significant political, social, and economic relationships
- Association with and dependency on the wider world
- External support if an accidental should occur

- Indicate special relationships that are significant to safety

Description of the analysis object - (3)

- Large enterprises can be broken down into smaller elements (i.e., objects and/or functions)
- A breakdown that constitutes too many too small elements will demand much resources, whereas insufficient breakdown of the enterprise can lead to unintentional omissions of rare but significant events
- A possible technique for breaking down a system is hierarchical breakdown

Hierarchical breakdown



Identification of hazards

- Potential hazards related to the activity must be identified (e.g., mechanical hazards, fire, explosion, toxix materials, radiation)
- In which part(s) of the system are the hazards relevant (e.g., pressure vessels, cranes, storage)

Methods and tools

- Checklists
- Preliminary hazard analysis (PHA), also known as:
  - Hazard identification (HAZID)
  - Rapid risk ranking (RRR)
- Failure modes, effects, and criticality analysis (FMECA)
- Hazard and operability analysis (HAZOP)
- Brainstorming
- Experience data - data bases

Accidental events

Some questions to consider when defining accidental events:

- What type of event is it?
  - Describe the type of event (e.g., fire, gas leak, falling object)
- Where does the event take place?
  - Describe where the event occurs (e.g., in process area A)
- When does the event occur?
  - Describe the conditions under which the event occurs (e.g., normal operation, start-up, during maintenance)

Example: "Contamination of water supply by bacteria during flood conditions"

Accidental events - (2)

- The list of accidental events arising from the PHA or brainstorming should be sorted and filtered (i.e., events may be disregarded due to insignificant consequences or likelihood of occurrence are closed out without unnecessary delay)
- The different accidental events are considered for each of the elements to be analyzed. Where are the events relevant? In this relation one can use a simple event/element matrix.

Event-element matrix

Area (System element)	Accidental event: Collision	Fire	Explosion	Toxic exposure	Dropped object					
Admin. building		X								
Production unit	X	X		X	X					
Laboratory		X		X						
Storage		X	X							
Loading area	X	X			X					

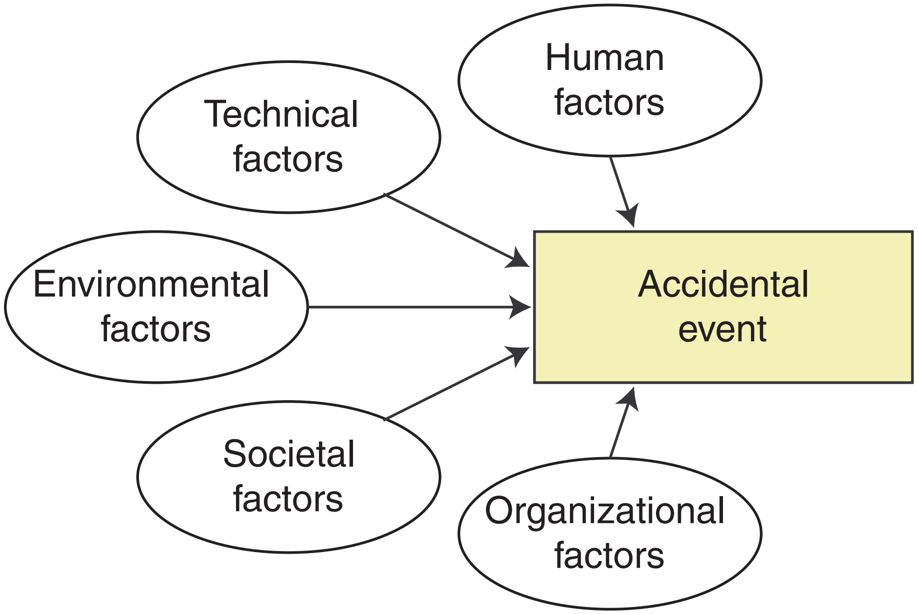
Accidental events - (3)

The results from this step are:

- A listing of all relevant hazards
- A listing and description of all potential (and relevant) accidental events
- Identification of where each accidental event may occur

Causal analysis

The causes of each accidental event must be identified and described



Methods and tools

- Fault tree analysis
- Bayesian belief networks (Influence diagrams)
- Cause-effect diagrams
- Reliability block diagrams
- Root cause analysis
- Experience data - data bases

Causal analysis results

- For each potential accidental event:

  All combinations of events (technical failures, human errors, environmental loads, etc.) that may lead to the accidental event (minimal cut set)
- The minimal cut sets may be used to reveal weaknesses in the system and form a basis for improvements

Frequency analysis

- After the causes of the accidental event have been identified, one is better placed to estimate the frequency (and how the accidental event may be avoided)
- The frequency of the accidental events may be estimated based on:
  1. Data from previous incidents (and data bases)
  2. Fault tree analysis
  3. Expert judgement

Consequence analysis

- What is the result?
- Identify consequences - bot immediate and delayed, given the accidental event

When analyzing consequences, do not forget:

- The whole chain of events triggered by the accidental event (can a relatively benign event ultimately end up in a disaster?)
- Both immediate consequences and those that are not apparent until some time after the event.

Consequence categories

It is often desirable to classify consequences into different categories:

- Personnel (i.e., health and safety)
- Environmental
- Economic
- Operational
- Company reputation

Consequence chains

- All potential event chains following an accidental event must be identified and described
- Most systems have one or more safety functions (barriers) that may stop or mitigate the effects of the accidental event. The event chains will depend on whether or not these safety functions are functioning or not.

Methods and tools

- Event tree analysis
- Cause consequence analysis
- Fire and explosion calculations
- Simulation
- Experience data - data bases

Risk evaluation

- Which risks are present in my enterprise?
- Risk classification matrices should be developed for each consequence category.

Risk evaluation - (2)

- Risk is a function of the frequency of the accidental events *and* the consequences of the accidental events
- Higher frequency of occurrence $\Rightarrow$ higher risk
- More severe consequences $\Rightarrow$ higher risk

- A useful tool for describing risk is a risk classification matrix

Risk classification matrix

Frequency/ consequence	1 Very unlikely	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic					
Critical					
Major					
Minor					

Acceptable - only ALARP actions considered

Acceptable - use ALARP principle and consider further investigations

Not acceptable - risk reducing measures required

Risk evaluation - (2)

- What do we do with accidental events once classified?
- Part of risk management: guidelines for what should be done with individual events dictated by the risk category to which they belong (Shouldn't this have been done during the planning phase?)

Risk elimination

- All accident causal factors (hazards) should be eliminated! We may, however, not have the resources to accomplish it
- We must therefore prioritize our corrective actions by addressing *high* risks before *low* risks

Risk analysis report

1. Summary and conclusions
2. Objectives and scope
3. Limitations, assumptions and justification of hypotheses
4. Description of relevant parts of the system
5. Analysis methodology
6. Hazard identification results
7. Models used, including assumptions and validation
8. Data and their sources
9. Risk estimation results
10. Sensitivity and uncertainty analysis
11. Discussion of results (including discussion of analytic difficulties)
12. References

– IEC 60300-3-9

Conclusions

Criticism

We sometimes hear that:

- A risk analysis takes too much time and resources
- The risk analysis is used to slow down decision processes
- Risk analysis can be a manipulative tool

Challenges

- Where data lacks, qualitative assessments through expert judgment is unaviodable
- Confidence in achieved results highly depends on:
  - the confidence in the experts (i.e., their qualification and competence)
  - the effectiveness of assessment procedures
- However, uncertainties will be revealed and documented, rather than suppressed
- When properly performed, a risk analysis is very transparent

– Adapted from IACS (2002)