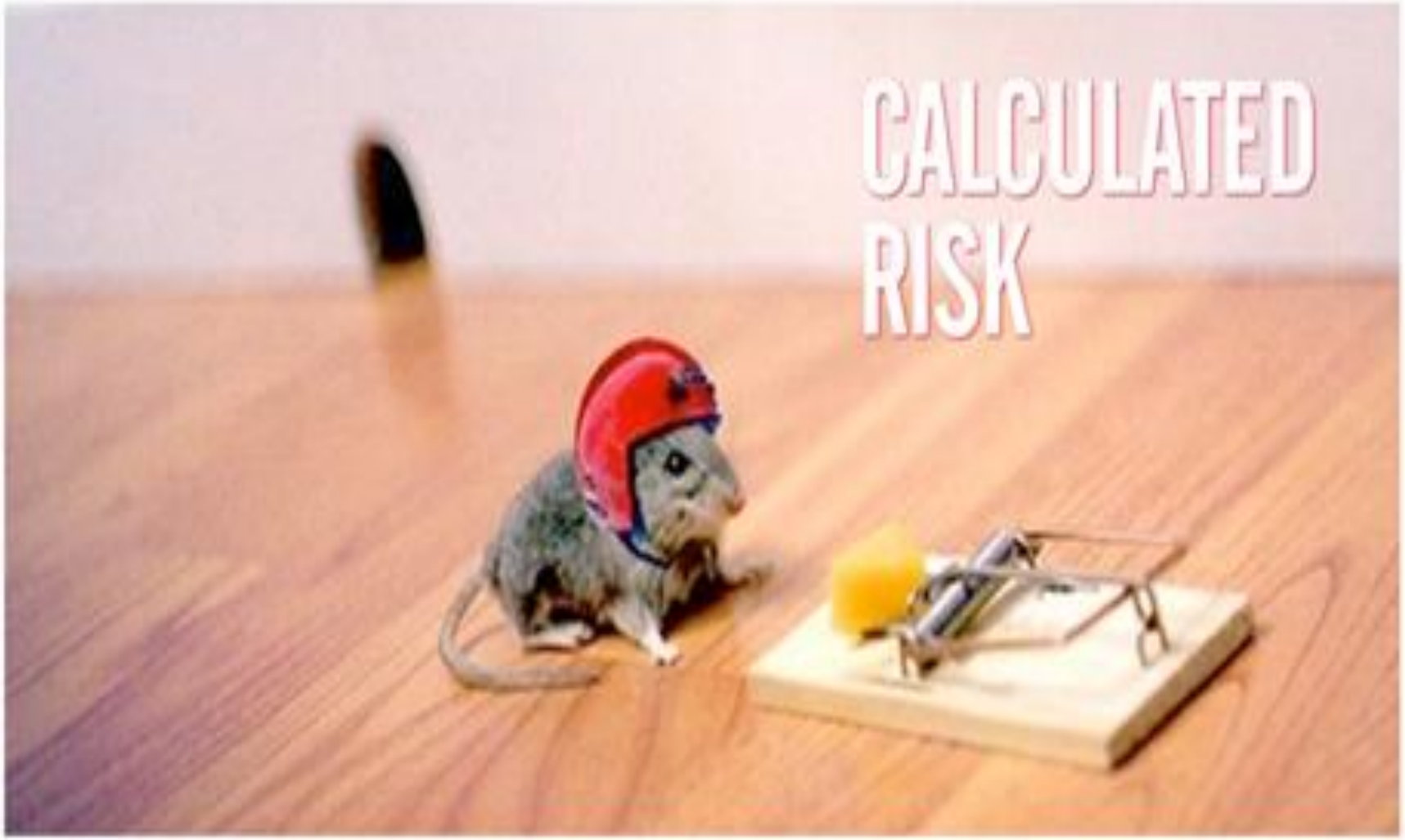
Engineering Risk Management
Lecture 6

Risk assessment techniques, Part 1

Prof. dr. ir. Genserik Reniers
Safety and Security Science Group (TU Delft)
KULeuven (Campus Brussel, CEDON)
UAntwerpen (ARGoSS)

g.l.l.m.e.reniers@tudelft.nl
Genserik.reniers@kuleuven.be
Genserik.reniers@uantwerpen.be

Calculating the risk



Risk assessment techniques, introduction

- Multi-disciplinary by nature
- Uncertainty!
- Specialistic ánd generalistic
- Public debate / public concern; many different opinions → controversial
- Risk analysis = rocket science??

Risk assessment techniques, background (i)

- Many critiques have been formulated on the concept of 'risk assessment' (O'Brien, 2000):
  - "risk assessment gives the industry the aura of being scientific"
  - "risk assessment processes allow governments to hide behind 'rationality' and 'objectivity' as they permit and allow hazardous activities that may harm people and government"
  - "risk analysts know that the assessments are often based on selective information, arbitrary assumptions, and enormous uncertainties. Nonetheless they accept that the assessments are used to conclude on risk acceptability."

- HOWEVER: THERE IS NO ALTERNATIVE (!): to support the decision-making, we need to assess risk. The right way forward is not to reject the risk assessment, but to improve the tool and its use!

Risk assessment techniques, background (ii)

- **Two fundamental scientific requirements** should be met:

  1. **<u>Reliability</u> requirements of the Risk Assessment:**

     - The degree to which the risk analysis methods produce the same results at reruns of these methods

     - The degree to which the risk analysis produces identical results when conducted by different analysis teams, but using the same methods and data

     - The degree to which the risk analysis produces identical results when conducted by different analysis teams with the same analysis scope and objectives, but no restrictions on methods and data

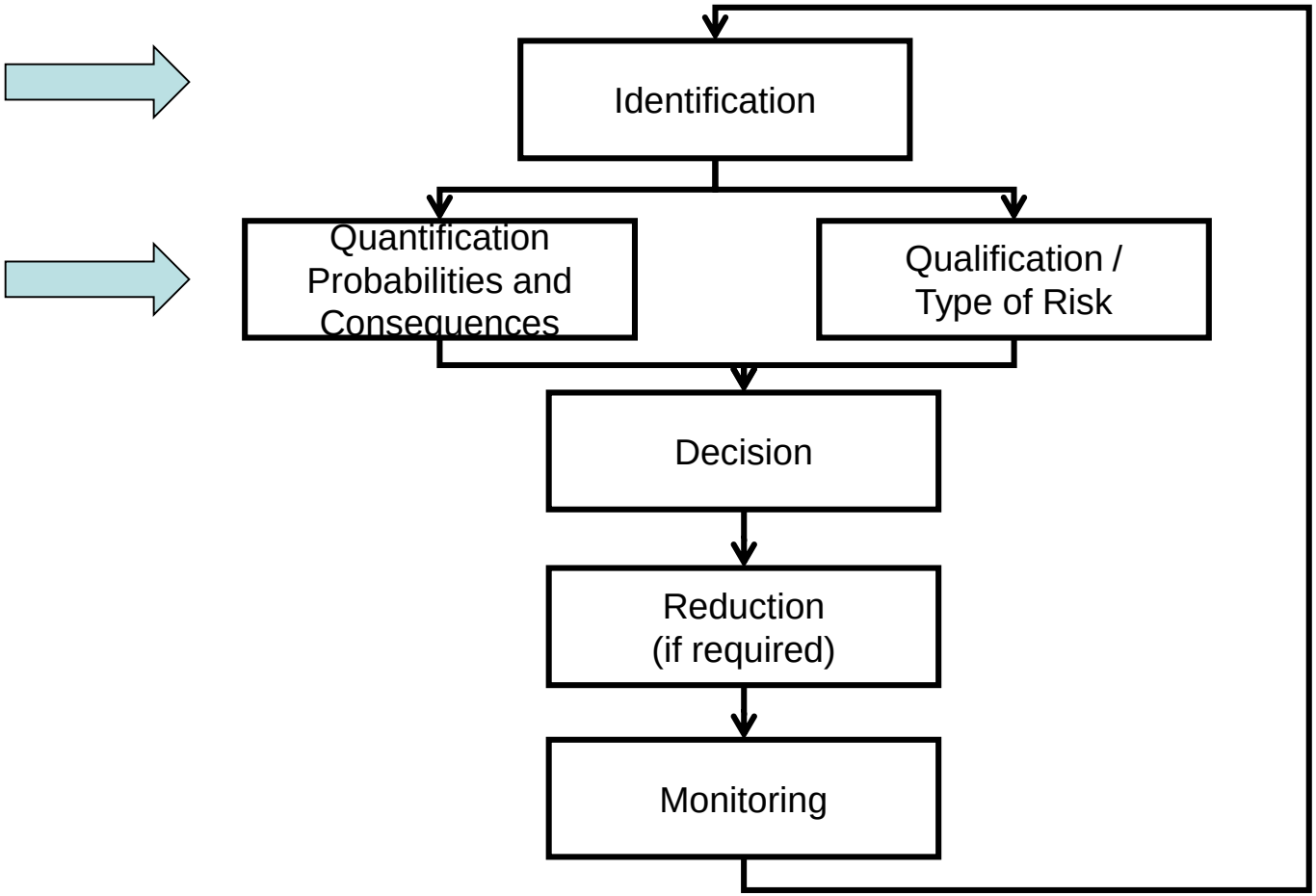
Risk assessment techniques, background (iii)

- **Two fundamental scientific requirements** should be met:

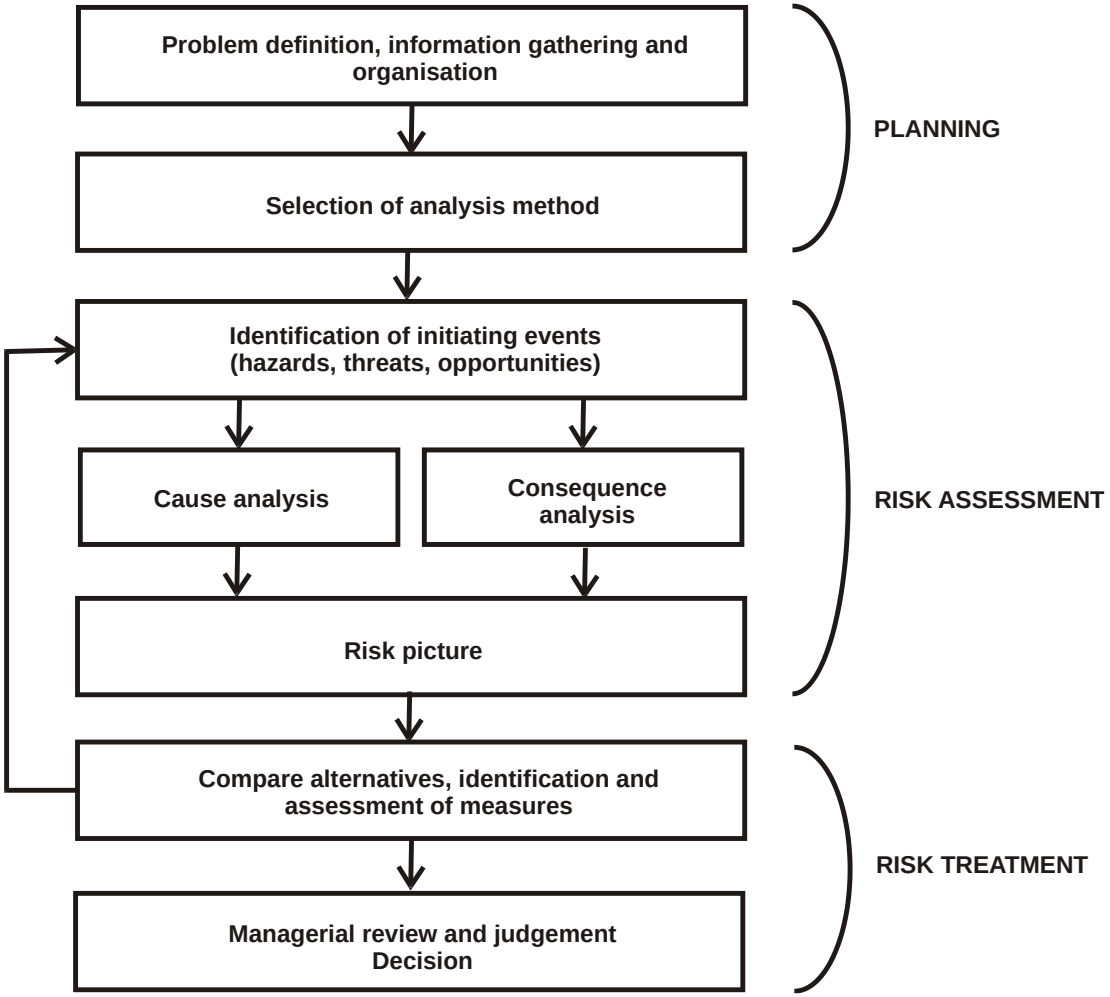
  2. <u>Validity</u> requirements of the Risk Assessment:

  - The degree to which the produced risk numbers are accurate compared to the underlying true risk
  - The degree to which the assigned probabilities adequately describe the assessor's uncertainties of the unknown quantities considered
  - The degree to which the epistemic uncertainty assessments are complete
  - The degree to which the analysis addresses the right quantities

Risk assessment: helicopter view



Zooming in: Main steps of risk assessment process (based on Aven, 2008)



Zooming in: Components of risk assessment

- Hazard identification
- Hazard categorization or classification
- Risk analysis (consequences and likelihood / exposure)
- Risk estimation (risk determination, risk picture)
- Risk evaluation (risk ranking, ALARP)

Discussion (i)

Risk Assessment = systematic investigation to determine:

- Whether there are hazards
- Whether losses can be caused
- Whether measures can be taken
- Which measures can be taken

Can be executed on different levels:

- Organisation-wide
- Level of group of workpostes or functions
- Individually

Should be applied with common sense, and results should be interpreted with critical mind!

Discussion (ii): Consideration should be given to factors such as:

- Which decision alternatives have been analysed
- Which performance measures have been assessed
- The fact that the results of the analyses represent (expert) judgements
- Difficulties in assessing probabilities in the case of large uncertainties
- The fact that the assessments' results apply to models that are simplifications of the real world and real world phenomena

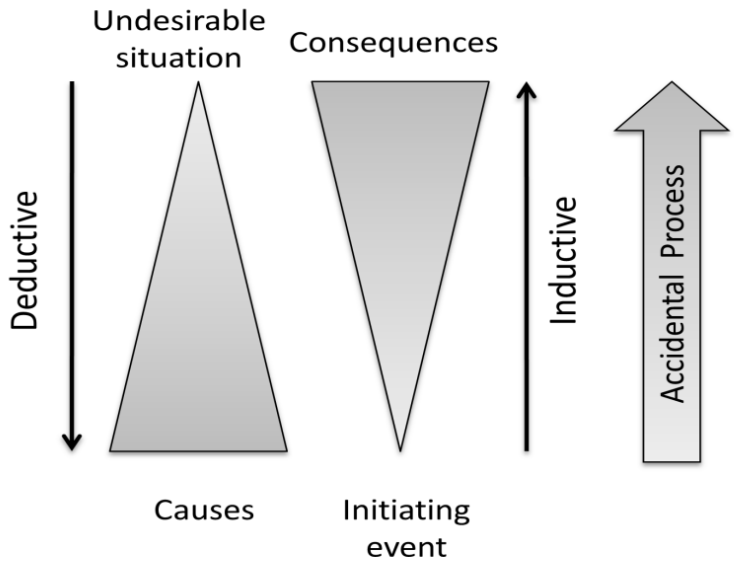
→ assessments' results need to be evaluated in the light of the premises, assumptions and limitations of these assessments!

Inductive and deductive approaches

- The **deductive methodologies analyse the causes of an adverse event** (accident) by answering the question “how is it that this event may occur (search for causes)?”

- The **inductive methodologies analyse the consequences of failure** (initiating event) and answer the question "what adverse events can result in (search for consequences)?”.

Inductive and deductive approaches



Different types of methods

- Basic methods: used during preliminary stages and proceeding towards a first global and high level analysis. (mostly inductive)

- Static methods: allow an analysis from a structural (topological) point of view. This is obtained through Boolean mathematical models which are static since they cannot model temporal effects on the system.

- Dynamic methods: were developed to take into account the temporal and compartmental effects that cannot be appropriately covered by static models.

Further division of risk analysis techniques

- Deterministic, probabilistic
- Qualitative, quantitative, semi-quantitative

Why so many methods?

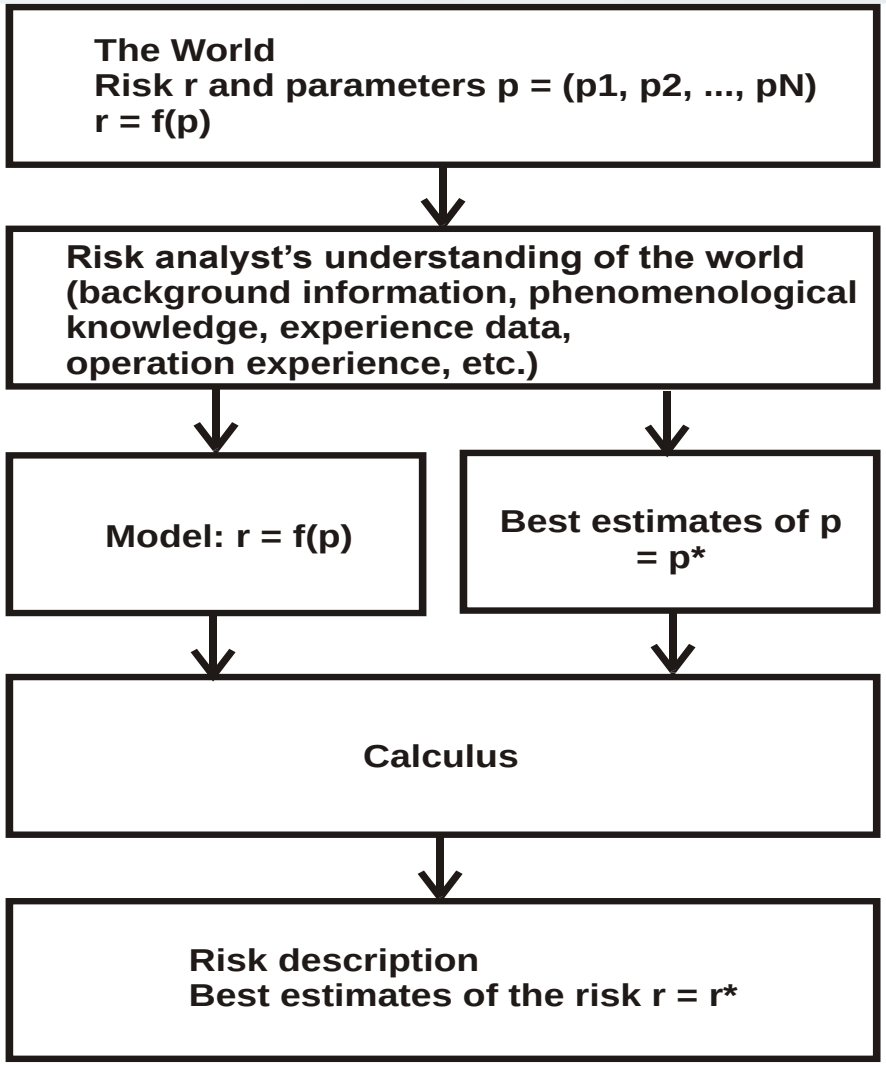
The choice of method mainly depends on:

- The nature and requirements of the study.
- The amount of knowledge of the system.
- Availability of quantitative data.
- Availability of time and resources.

The key questions to be asked before choosing a method should be:

- What are the aims and what is the scope of the analysis?
- Is the analysis prospective or retrospective?
- Is the analysis specific (linked to an event, failure etc…) or does it consider the system as a whole?
- What is the required depth of analysis?
- How much time and resources are available?
- How well is the system known and which data are available?

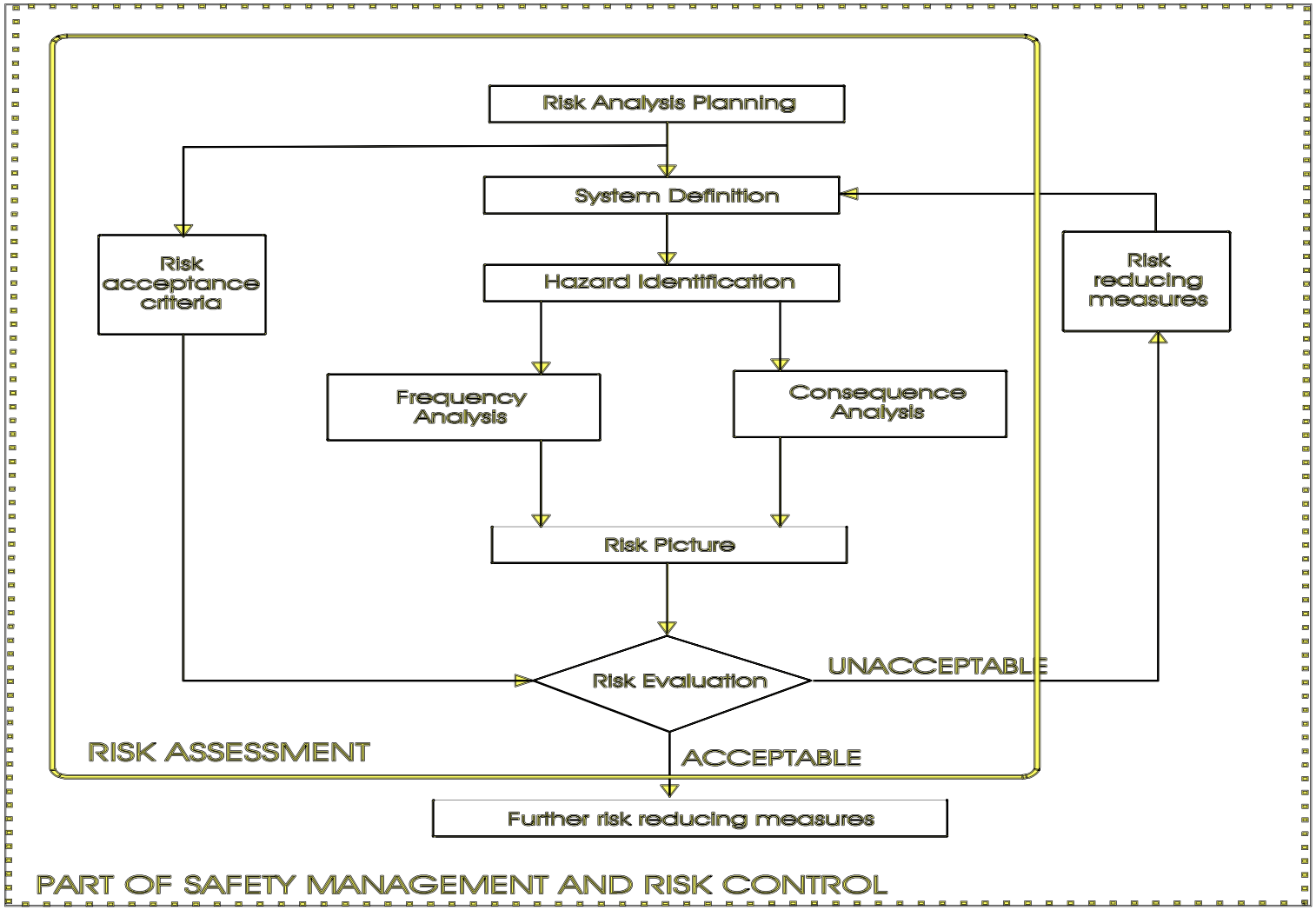
Conclusion - Classical approach of a risk assessment



Hence: components of risk assessments?

- Risk identification
- Risk categorization or classification
- Risk analysis
- Risk estimation
- Risk evaluation

Safety Risk Assessment Process



Definitions

Risk identification:

"Process of identifying situations and events that may give rise to potential losses for an organization, and includes the identification of hazards, the potential adverse events associated with these hazards, and the stakeholders who may be affected by the adverse events"

Risk classification:

"Process of categorizing risks into groups, which are identified either by their origins or by their potential impacts. Risks can be grouped either by their hazard type, such as chemical, electrical, industrial and natural sources, or by the consequences that they give rise to, such as financial, environmental, and health and safety losses."

Definitions

Risk estimation:
"Identification of the outcomes of events and an estimation of the magnitude and probability of these outcomes.
Risk estimations can be made on the basis of qualitative, semi-quantitative or quantitative predictions."

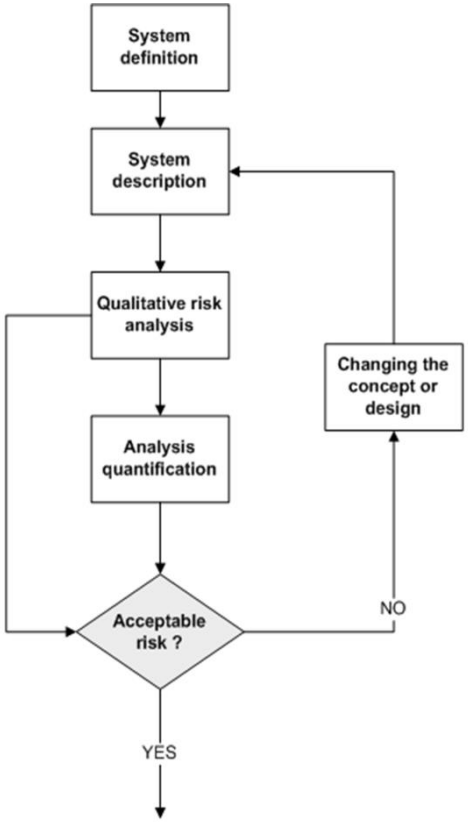
Risk evaluation:
"Process of determining the acceptability of estimated risks."

Suited methods for engineering projects?

Depends on the project phase:

- Conception
- Preliminary
- Detailed engineering
- Construction
- Equipment hand-over
- Pre-operation
- Before start-up
- Pre-production

General risk assessment procedure



General process for all risk analysis techniques

- Step 1: Identify the hazards
- Step 2: Decide who or what might be harmed and how
- Step 3: Evaluate the risks and decide on precautions
- Step 4: Record your findings and implement them
- Step 5: Review your assessment and update if necessary

General 9-step process for all risk analysis techniques

1. Definition of the system

- Objective(s) and scope of the study, definition of the system to be studied, identify the elements to be analysed, subdivide complex processes.

2. Team selection

- Choose experts according to the process, important factors are: multidisciplinary, expertise, availability.
- Designate a secretary (generally the future user) or a moderator who will record the identified risks, causes, corrective measures, unsolved problems, etc.

3. Information gathering

- Collect all the necessary information before the analysis (products and equipment properties and description, operating procedures, technical drawings, process and flow diagrams, schemes, general drawings, process manuals, heat and mass flows, emergency procedures, weather conditions, environment, topography, human reliability, etc.).
- Identify intended use.

General 9-step process for all risk analysis techniques

4. Perform the analysis with the adequate chosen method.

- Identify and list the elements to assess, make risk analysis meetings, save the results of the analysis in a table form or appropriate document, control the evaluation table by a system engineer, follow the methodology without introducing "feelings" statements, etc.

5. Recommend corrective actions and action plan

- Define preventive and corrective solutions.
- Recommend actions to reduce unacceptable risks.
- Assign responsibility and schedule for corrective actions.

6. Monitor the solutions' implementation

- Regularly monitor the implementation of corrective measures.
- Update the analysis in case of major changes

General 9-step process for all risk analysis techniques

7. Record hazards

- Record identified hazards in the safety quality assurance system (if any).
- Establish record keeping
- Establish documents of the complete analysis with diagrams, drawings, tables, processes.
- Update information according to the completion of corrective measures.

8. Forecast to update the system

- It must evolve to reflect changes in raw materials, formulation (recipe), market, habits or consumer demands, new hazards, scientific information, or inefficiency.
- It must provide at the outset why, when and how the system will be reviewed.

9. Continuous monitoring and follow-up

- Once the analysis is completed, the story does not stop there, as time is a factor of change, iteration of the procedure must be performed when (sometimes minor, certainly major) changes happen.

Some remarks on the quantification of risks

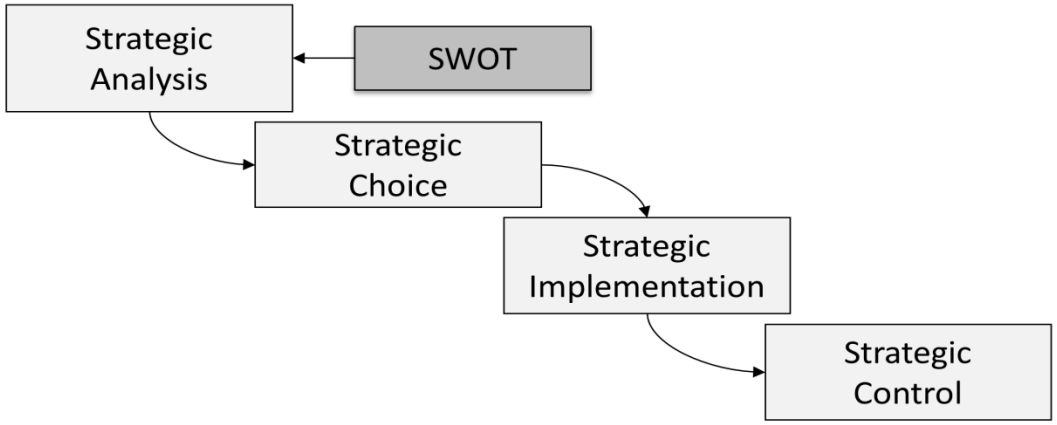
- All risk assessments involve human judgements → based to some degree on subjective criteria
- However, interpretation and communication of quantified risks and their consequences and probabilities lead to different perceptions and ideas about risk control strategies
- Statistics is not exact science!!! (but will lead to more objective cost/benefit analyses and hence to better and more optimal decisions)

SWOT analysis

A SWOT analysis is a useful technique for understanding your Strengths and Weaknesses, and for identifying both the Opportunities open to you and the Threats you face. Used in a business context, a SWOT analysis helps you carve a sustainable niche in your market. Used in a personal context, it helps you develop your career in a way that takes best advantage of your

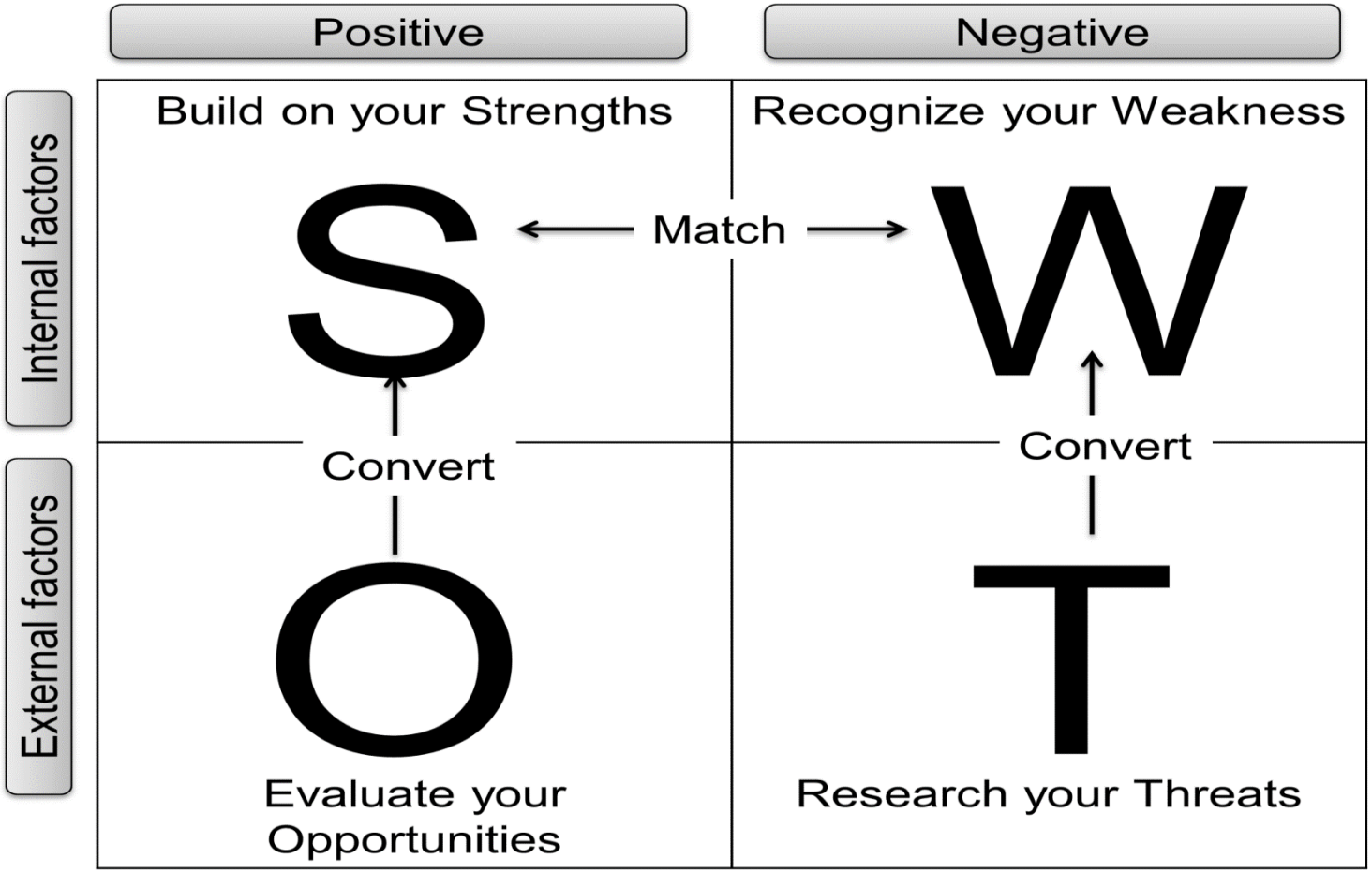
talents, abilities and opportunities.

SWOT analysis



SWOT analysis

- Internal and external environment



SWOT analysis sample questions

	Positive	Negative
Internal factors	• Which strengths are unique to the team? • What are we good at doing? • What are the things that had gone well?	• What should be done better in the future? • What knowledge do we lack? • Which skills do we lack? • What system do we need to change?
External factors	• What are the key success enablers? • Which additional services can we offer? • What new market should we investigate?	• Barriers to progress • What are the possible impacts of what competitors are doing? • Which regulatory issue might cause us concern?

Preliminary hazard analysis (PHA)

A Preliminary hazard analysis (PHA) is a risk analysis technique that is performed to:

1. Identify all potential hazards and accidental events that may lead to an accident
2. Rank the identified accidental events according to their severity
3. Identify required hazard controls and follow-up actions

Several variants of PHA are used, and sometimes under different names like: Rapid Risk Ranking or Hazard identification (HAZID)

Preliminary hazard analysis (PHA)

- Three info inputs are needed: design knowledge, hazard knowledge, preliminary hazard list (collection of identified hazards)

- A PHA is applied in two ways:
  - alone as risk analysis for systems with simple or easily identifiable hazards and not complex accidental process;
  - in combination with other methods. In this case, a PHA is seen as a preliminary risk study to prepare the complex or poorly defined case. In this sense, it is mainly used in the early design phase of a project.

Preliminary hazard analysis (PHA) – Example of storage tank

Element	Hazard	Hazardous event	Causes	Consequences	Measures
Tank	Heat stress (fire outside the tank)	Explosion of the tank and important release of gases	Presence of combustibles elements near the tank	Fire Property damage Casualties	Changing logistics storage. Move individual hazards away
Tank	Mechanical impact against the shell of the tank	Gas release	Accident with a crossing vehicle, intentional damage	Fire Property damage Casualties	Inspection program Continuous monitoring of air quality
Tank	Weakening of the tank shell	Gas release Explosion of the tank and important release of gases	Corrosion, fatigue (crack), not well sized tank (do not stand up to pressure imposed).	Fire Property damage Casualties	Inspection program Verification of design
Valve	Unexpected opening	Gas release	Valve or control system failed, error during routine maintenance, ...	Gas release	Inspection program Continuous monitoring of air quality

Checklist

Checklist analysis is a systematic evaluation against pre-established criteria in the form of one or more checklists.
It is a systematic approach built on the historical knowledge included in checklist questions. It is used for high-level or detailed analysis, including root cause analysis. It is applicable to any activity or system, including equipment issues and human factors issues.
It is generally performed by an individual trained to understand the checklist questions. It generates qualitative lists of conformance and non-conformance determinations, with recommendations for correcting non-conformances.
The quality of evaluation is determined primarily by the experience of people creating the checklists and the training of the checklist users.

Steps of checklist

Identify hazards

→ establish risk catalogue with categorization

→ risk mitigation

Checklists

- Easy to use, simple
- Passing on valuable experience/expertise
- Limited to the experience/expertise/knowledge/imagination of authors of checklist
- Cheap
- Not suitable for complex analyses

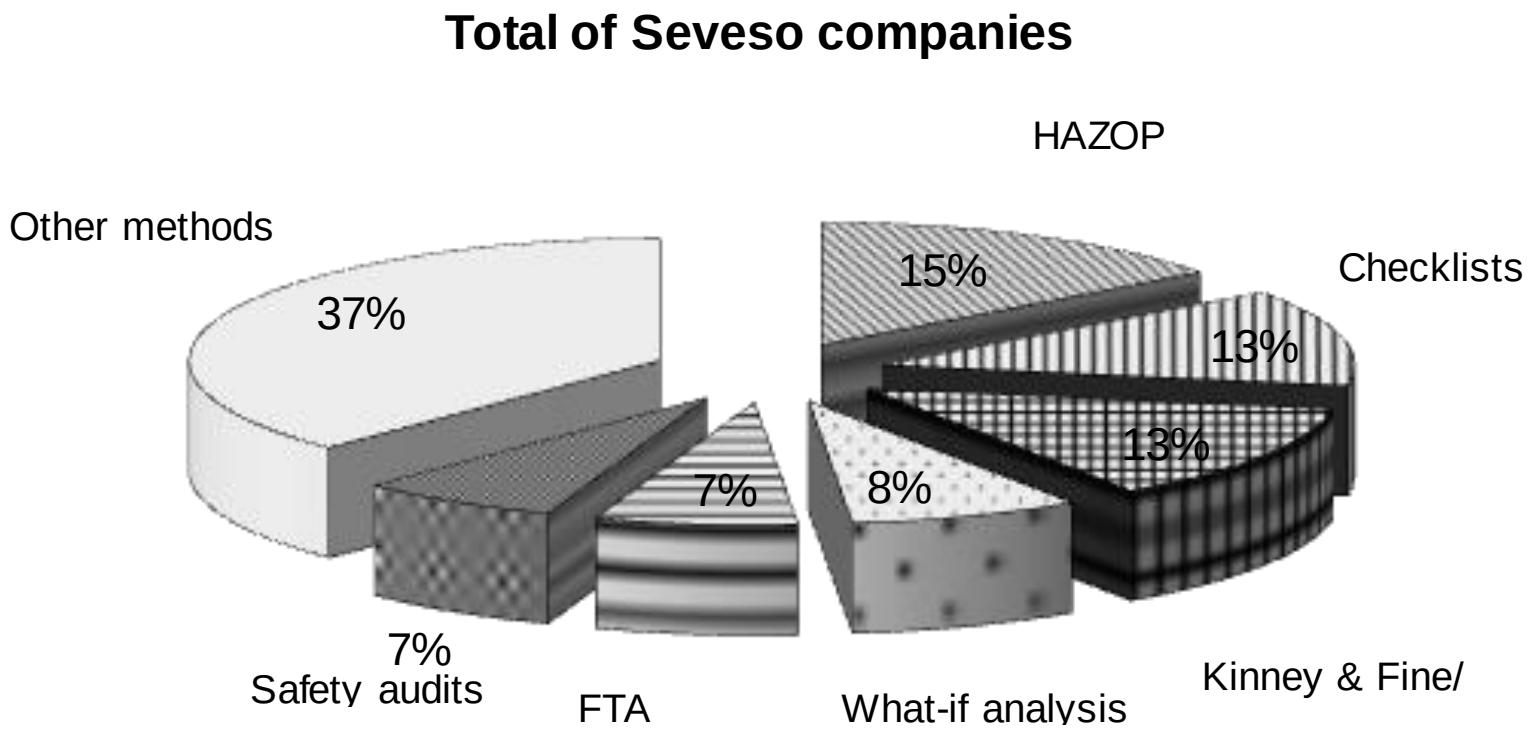
Exercise

- Actions that need to be taken in case of receiving a bomb threat:

  Assume that there is no possibility to record the conversation between your receptionist and the terrorist.

  Draft a checklist for the company receptionist (he/she should be able to use it in the unfor-tunate case of a bomb threat) to use during and right after the telephoe cponversation, so that the checklist can be employed by the firefighters and police to determine what actions to take (e.g. to evacuate completely, partially, or not).

Risk analysis methodes: popularity in the chemical industry (2003):



HAZOP

Hazard and Operability Analysis is a structured and systematic technique for system examinationand risk management. In particular, it is often used as a technique for identifying potential hazards in a system and identifying operability problems likely to lead to nonconforming products. It is based on a theory that assumes risk events are caused by deviations from design or operating intentions. Identification of such deviations is facilitated by using sets of “guide words” as a systematic list of deviation perspectives.

HAZOP

- "deviation analysis", inductive
- Use of "guidewords": more, less, no, higher, smaller, partial, equal, opposite,…
- Use of "operating parameters": flow, pressure, temperature,…
- Combination is applied on "study nodes" (i.e., specific points)
- Multidisciplinary team
- Use on existing equipment (e.g. using PID, PFD)

Hazop process

Input

- PID/PFD
- Process
- Team leader
- Team members
- Directives, methodology

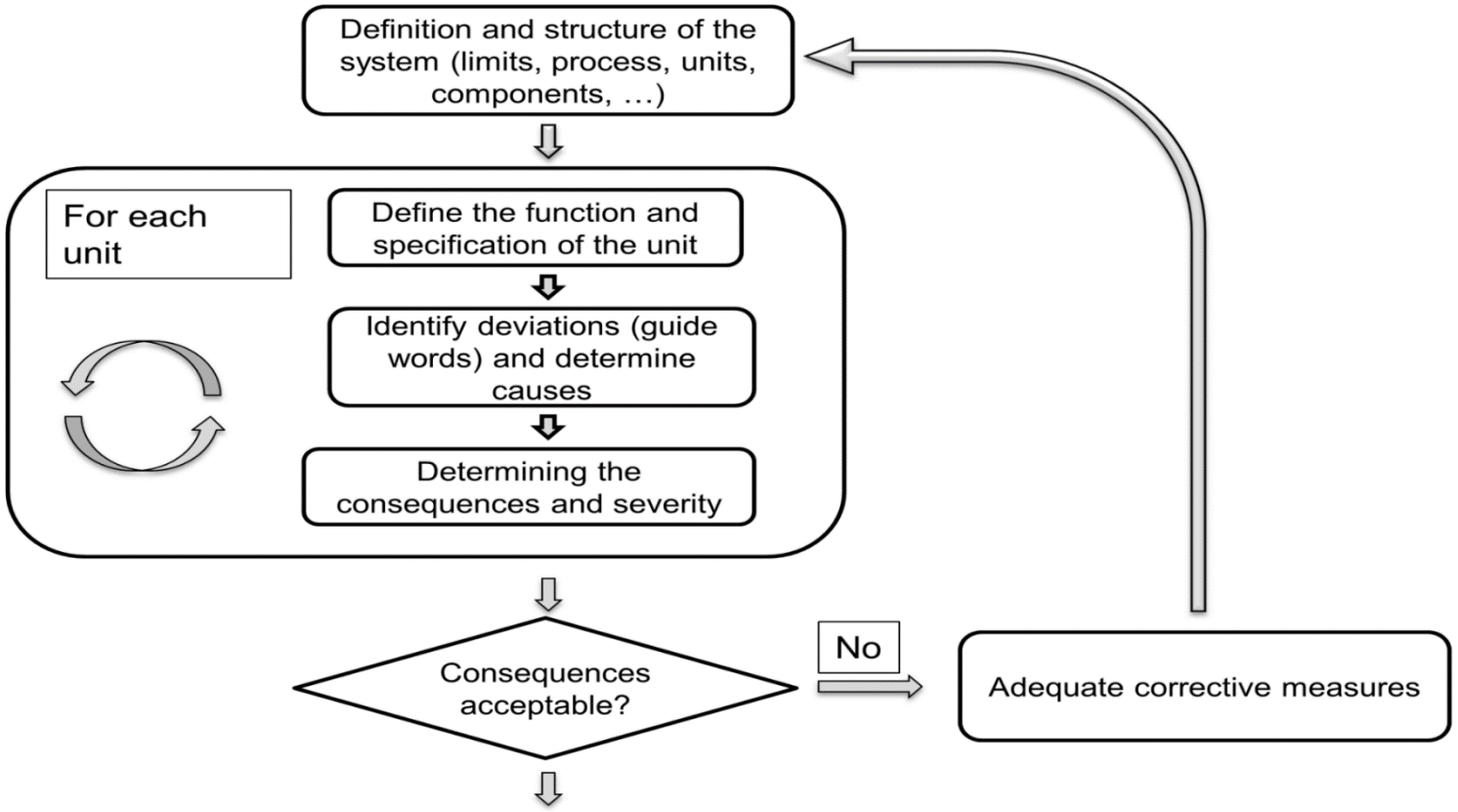
HAZOP process

1. Establish HAZOP plan
2. Select team members
3. Identify system elements
4. Choose guide/key words
5. Perform the analysis
6. Documenting the HAZOP

Output

- Hazards
- Risks
- Correctives measures/actions

Hazop methodology



How to conduct a Hazop analysis

1. Initially, choose a line of process. It generally covers equipment and connections, all performing a function in the process identified in the functional description.
2. Choose an operating parameter.
3. Identify a guide/keyword and generate a deviation.
4. Verify that the deviation is credible. If yes, proceed to step 5, otherwise return to step 3.
5. Identify causes and potential consequences of this deviation.
6. Examine ways to detect this drift as well as those provided to prevent the occurrence or mitigate its effects.
7. Propose, where appropriate, recommendations and improvements (see table 4.10).
8. Choose a new guide/keyword for the same parameter and return to step 3.
9. When all guide/keyword have been considered, choose another operating parameter and go back to step 2.
10. When all operating phases have been studied, choose another process line and go back to step 1.

Hazop guidewords

Keywords	Signification	Commentary	Examples
No or not	No part of the intention is fulfilled	The purpose or function is not fulfilled at all, not even partially.	No agitation No flow
More	Overrun, or increase, quantitatively	Refers to the quantities and properties (T, P), but also activities (heating, reaction).	Higher temperature Too much product
Less	Insufficient or quantitative reduction.		Lower flow rate than expected Less agitation
As well as	Qualitative increase	The intent (design and procedure) is performed with additional activity. Concomitant adverse effect.	Heating started at the same time as the addition of reagent A.
Part of	Qualitative modification/diminution	Only part of the intention is realized.	Only part of the reagent is added
Reverse	The logical opposite of the intention	Reversal of the activity or sequence	Liquid flows in the opposite direction It heats instead of cooling
Other than	Total substitution	Result different from that of intention.	Reagent A is loaded in place of B
Earlier than	On the time clock	The action takes place before or after a defined time.	We started heating 15 minutes before the deadline.
Later than	On the time clock		It has been left the reaction taking place over two hours.
Before	On the sequence or order	Action is taken before or after the defined sequence	A was loaded before B
Later	On the sequence or order		It was cooled after stirring

Hazop operating parameters

Measurable physical quantities		Operations		Actions	Functions-situations
Temperature	pH	Loading	Control	Start-up	Protection
Pressure	Intensity	Dilution	Separation	Sampling	Utility default
Level	Speed	Heating	Cooling	Stop	Freezing
Flow rate	Frequency	Stirring	Transfer	Isolate	Spill
Concentration	Amount	Mixing	Maintenance	Purge	Earthquake
Contamination	Time	Reaction	Corrosion	Close	Malevolence

Example of safety barriers

Safety Barriers		Definition	Example
Technical	Passive safety devices	Unitary elements aiming to fulfil a safety function without external energy supply system which he belongs, and without the involvement of any mechanical system.	• Holding tank/tray. • Rupture disc.
	Active safety devices	Items not passive aimed to perform a safety function without external energy supply system to which it belongs.	• Safety valve • Excess flow valve
	Safety instrumented systems	Combination of sensors, processing units and terminal elements aiming to fulfil a function or a sub-safety function.	• Measuring elements which controls a valve or switch power.
Organizational		Human activities (operations) that do not involve technical safety barriers to oppose the conduct of an accident.	• Emergency plan. • Containment.
Systems with manual action		Interface between a technical barrier and human activity to carry out a safety function.	• Pressing an emergency button. • Low flow alarm, followed by manual closing of a safety valve.

Hazop example

n°	Object	Function	Parameter	Key-word	Conse-quence	Cause	Hazard	Risk P/G	Recomm endation	Risk 2 P/G	Who	When
1	Line	Bring water to the system	Fluid	No	Loss of cooling of the pump	Line rupture	Damage d pump	LM	-	LM	-	-
2				More	Pressure rise in the line	No pressure regulatio n	Line rupture	LM	Add a safety valve to the loop	LL	TJ	2012.10
3				Less	Not enough cooling capacity of the pump	Leakage at the pipe and fittings	Damage d pump	MH	Periodic control of fittings	LM	TJ	Bimonthl y
4	Electrical supply	Supply power to the motor M23	Electricity	No	Loss of power to the pump	Short-circuit, power failure	Loss of control	LH	Backup Power	LL	JK	2013.01

What-if analysis

A brainstorming approach in which a group of experienced people familiar with the subject process ask questions or voice concerns about possible undesired events

- Not super-structured
- Easy to use at every stage of the life of a process
- Typically “What-if”-questions