Engineering Risk Management
Lecture 8

Risk treatment & event analysis

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

Risk treatment/reduction

Techniques of control and risk reduction (i):

- Substitution: by replacing substances and procedures by less hazardous ones, by improving construction work, etc.
- Elimination of risk exposure: this consists in not creating or completely eliminating the condition which could give rise to the exposure.
- Prevention: combines techniques to reduce the likelihood/frequency of potential losses. Observation and analysis of past accidental events enable the improvement and intensification of prevention measures.

Risk treatment/reduction

Techniques of control and risk reduction (ii):

- Reduction/mitigation, are techniques whose goal is to reduce the severity of accidental losses when an accident occurs:
  - Measures applied before the occurrence of the event (often also have an effect on the likelihood/frequency).
  - Measures applied after the occurrence of the event (often aim to accelerate and enhance the effectiveness of the rescue).

Risk treatment/reduction

Techniques of control and risk reduction (iii):

- Segregation summarizes the techniques which are to minimize the overlapping of losses from a single event. It may imply very high costs.
  - Segregation by separation of high risk units.
  - Segregation by duplication of high risk units.

Risk treatment/reduction

Techniques of control and risk reduction (iv):

- Transfer, risk transfer by:
  - Contractual transfer of the risk financing, essentially insurance.
  - Risk financing by retention (auto financing), finance planning of potential losses by your own resources.
  - Alternative Risk. The Alternative Risk Transfer (ART) solutions comprise both elements of auto financing and contractual transfer and so cannot be classified in any of the above categories.

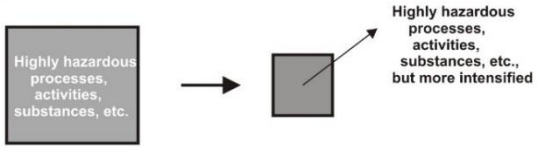
Risk treatment options

- Risk reduction:
  - Risk avoidance (inherent safety or design-based safety)
  - Risk control (prevention, protection, mitigation)

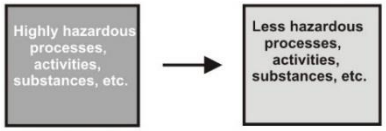
- Risk acceptance:
  - Risk retention (conscious or unconscious)
  - Risk transfer (insurance)

Inherent safety or design-based safety

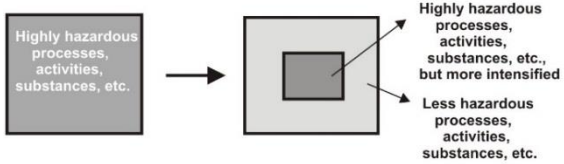
Principle 1: Intensification



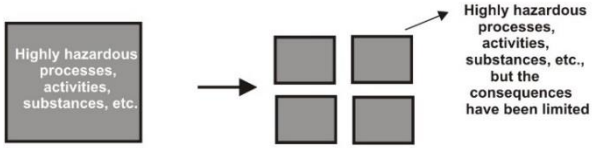
Principle 2: Substitution



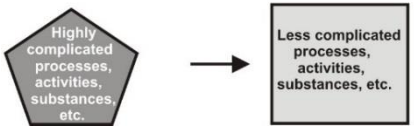
Principle 3: Attenuation by moderation



Principle 4: Attenuation by limitation of effects



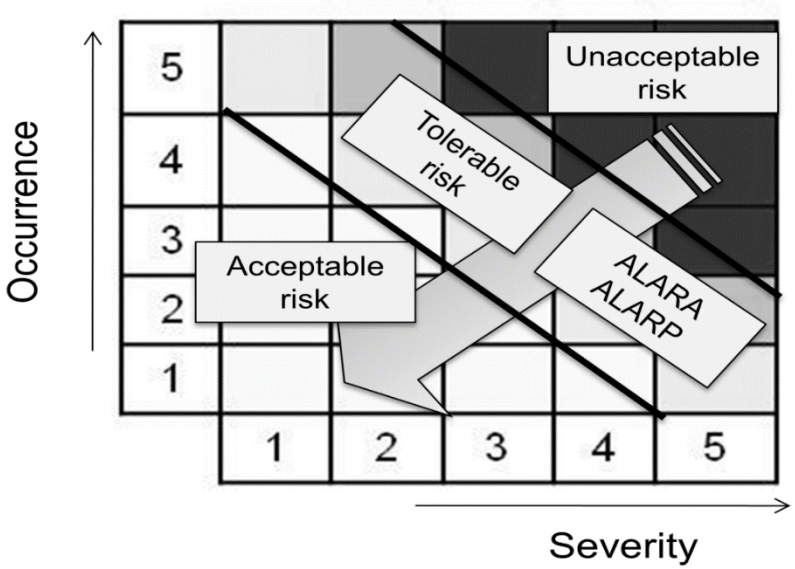
Principle 5: Simplification

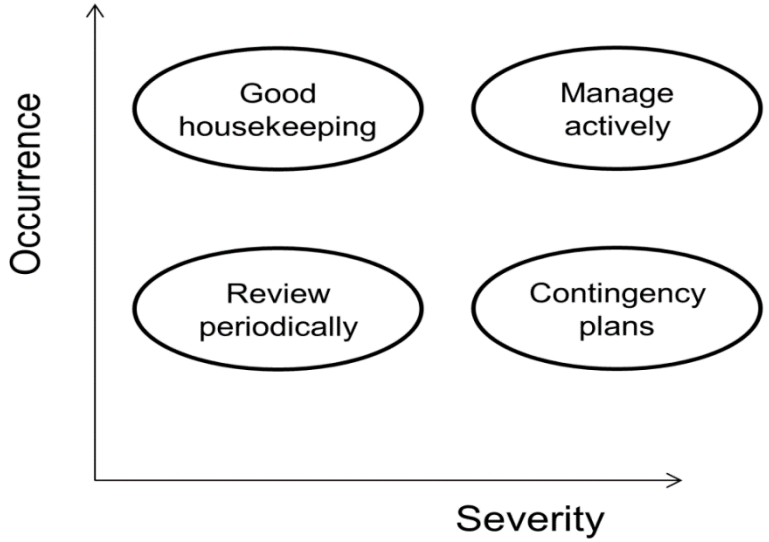


Hence: safety measures used to deal with risks

- Disincentives for avoiding the implementation of potential threats.
- Preventive measures inhibiting a threat realization (they act on causes and reduce the probability of occurrence).
- Protective (and mitigation) measures limiting the impact of a threat by reducing the direct consequences (they act on consequences without taking into account the occurrence).
- Remedial actions limiting the consequences of the threat implementation and indirect consequences.
- Recovery measures aiming to recover some of the damage by transferring the risk (e.g. insurance) to limit final losses.

Goal of risk reduction methods





Risk reduction process in 10 steps

1. Build a multidisciplinary team which includes specialists in different subject and sectors, users and a moderator. Sometimes contribution from someone “innocent” (with no or limited experience) is desired. He asks questions no one would have thought of.
2. Identify and define the risks to be reduced (hazard source, situation, requirements …).
3. Analyse the process and operating procedures (description, interaction, objectives, need, constraints …).

Risk reduction process in 10 steps

4. Generate ideas by brainstorming (a priori, all ideas are good). The multidisciplinary of the team reveals all its importance. It is crucial not to discriminate ideas at this stage; it is the moderator's role to guarantee this concept. From this step will come an accepted solution, discriminating it too early would be prejudice, especially without selection criteria
5. Establishing criteria to support the evaluation of the suggestions and ideas, a decision help and a referential for the different group members.

Risk reduction process in 10 steps

6. Evaluating all alternatives (costs (direct and indirect), risk reduction, feasibility, collateral effects, acceptation, opportunity, new hazard apparition, …
7. Retain risk reduction alternatives based on criteria
8. Implementation of the decided modification (definition of the person in charge, schedule and deadlines and which necessary means and resources).

Risk reduction process in 10 steps

9. Information and training, this step is often forgotten, but is crucial. Communication and training is inevitable in order for the users to accept and use corrective or improvement measures during a process or activity change. Without the will or acceptation of the people concerned by the result.
10. Control, it is indispensable to evaluate the new situation, evaluate the new hazards and risks that have appeared during the implementation of the measures, check the acceptance of the measure by the users and validate the project.

Prevention

Prevention is an attitude and/or a series of measures to be taken to avoid the degradation of a certain situation (social, environmental, economical, technological, etc.) or to prevent accidents, epidemics or illnesses. It acts mainly on the likelihood of occurrence and the causality chain, trying to lower the probability that an event happens. Prevention actions are also intended to keep a hazard risk problem from getting worse. They ensure that future development does not increase hazard losses.

Prevention

9 principles of prevention:

1. Avoid risks: remove the hazard or the exposure to it.
2. Assess risks that cannot be avoided: assess their nature and importance, identify actions to ensure safety and guarantee the health of workers.
3. Fight risks at the source: integrate prevention as early as possible, from the design of processes, equipment, procedures and workplaces.
4. Adapt work to man: design positions, choose equipment, methods of work and production to reduce the effects of work on health.
5. Consider the state of technological developments: implement preventive measures in line with the technical and organizational developments.

Prevention

9 principles of prevention:

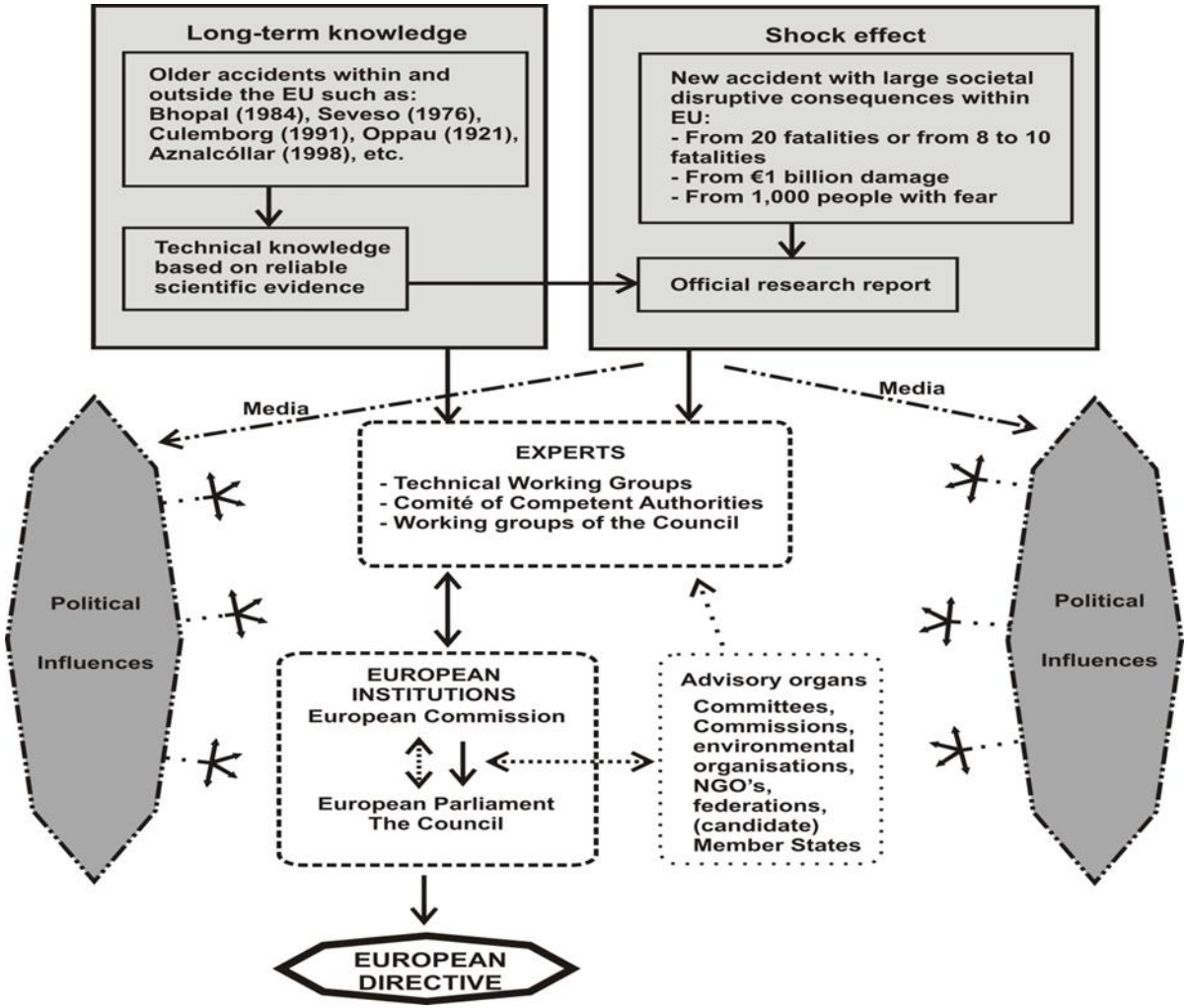
6. Replace the hazardous by what is less hazardous: avoid the use of harmful processes or products when the same result can be obtained with a method with less hazards.
7. Plan prevention integrated in a coherent package: a) technique, b) work organization, c) working conditions, d) social relations, e) environment.
8. Take collective protection measures and give them priority over individual protective measures: use of personal protective equipment's (PPE) only to supplement collective protection or their defaults.
9. Give appropriate instructions to employees: provide them the necessary elements for understanding the risks and thus involve them in the preventive approach.

Preventive measures examples

Preventive measures	Example
Fire risk elimination	Using non-flammable materials
Limiting hazardous functioning parameters	Continuous following and automatic control of the functioning parameters classified as critical
Installing isolation, blocking and restriction devices.	Rendering flammable liquids inert, locking down electrical equipment
Installing a failsafe after a failure	Use of electrical fuses and circuit breakers
Reducing the likelihood of breakdowns and errors	Oversizing important elements, using redundancy
Substance leak recuperation	Neat floor cleaning.

Prevention barrier	PFD	Commentary
“All or nothing” valve	$5 \cdot 10^{-3}$ to 10^{-1}	Valid with complete and planned maintenance
Prevention or overpressure/sub-pressure protection valve	10^{-3} to 10^{-1}	Safety valve function (no-opening when asked)
Rupture disk	10^{-3}	Typical values

Seveso Directive: prevention of major accidents in Europe



Protection and mitigation

Protection and mitigation consist of all measures reducing consequences, severity or development of a disaster.

There are two types of protection measures (safeguards):

- Before the event (“protection”): reducing the size of the object of risk exposure when an event occurs.
- After the event (“protection by means of mitigation”): are usually emergency measures to stop the damage accumulation or counteract the effects of the disaster.

Protection measures - examples

Protection measures	Human	Material	Organizational
Passive: which act by their presence alone	• Mastering the urbanisation • Seclusion rooms • Escape ladders	• Firewalls • Storage underground • Retentions basin	• Emergency plan existence
Active: which act only with a specific human or material action	• Following orders • Wearing personal protective equipment's • Using portable extinguishers	• Sensor activating safety systems: cut off valves, water curtain • Valves, rupture disks	• Operator training • Activating the emergency plan • Implementing crisis' cell

Prevention barrier	PFD	Commentary
Fix fire-fighting equipment	10^{-2}	Typical value if tested regularly
Catalytic gas detection with associated alarm	$5 \cdot 10^{-3}$	Valid with tests and calibration once every two-three months for a redundant mechanism
Alarm triggering	10^{-3}	Typical value (probability of failure on siren request)
Confinement against explosion/toxic risks	0	Value close to 0

Safety barriers (active/passive devices)

Safety Barrier		Definition	Example
Technical	Passive safety devices	Unitary elements whose objective is to perform a safety function, without external energy contribution coming from outside the system of which they are part and without the involvement of any mechanical system.	• Retention basin. • Rupture disk.
	Active safety devices	Non passive unitary elements whose objective is to fulfil a safety function, without contribution from energy from outside the system of which they are part.	• Discharge valve. • Excess flow lid.
	Safety Instrumented systems	Combination of sensors, treatment units and terminal elements whose objective is to fulfil a safety function or sub-function.	• Pressure measure chain to which a valve or a power contractor is linked.
Organizational		Human activities (operations) which do not include technical safety barrier to oppose the progress of an accident.	• Emergency plan. • Confinement.
Manual action systems		Interface between a technical barrier and a human activity to ensure the success of a safety function.	• Pressing on an emergency button. • Low flow alarm, followed by the manual closing of a safety valve.

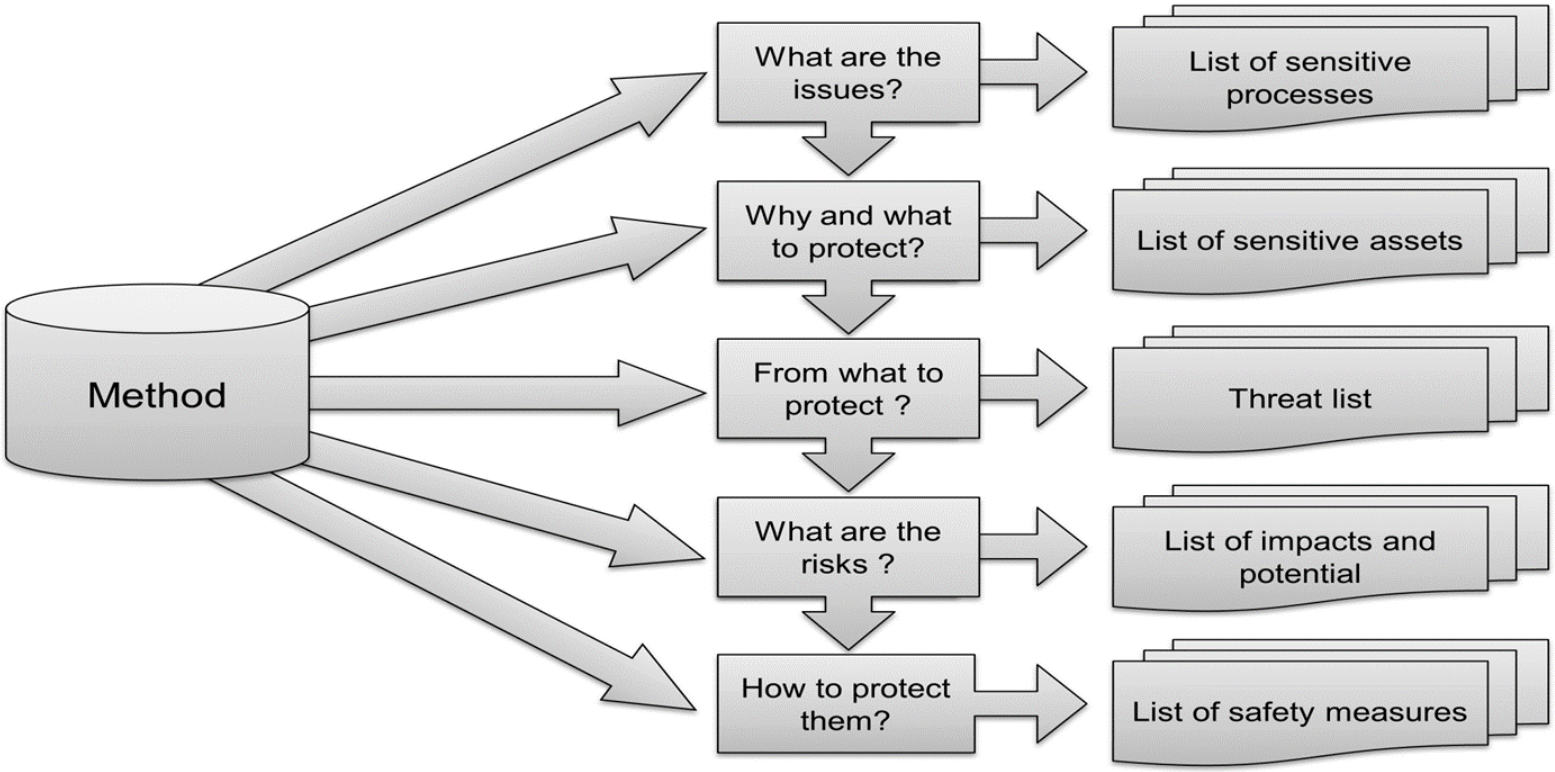
Risk Treatment

Three specific steps are involved in the treatment of risk:

1. Identification of potential measures under the prevention, preparedness, response and recovery domains.
2. Evaluation and selection of measures.
3. Planning and implementation of chosen measures.

Risk treatment is hence described as a selection and implementation process of measures which are destined to reduce (negative) risks.

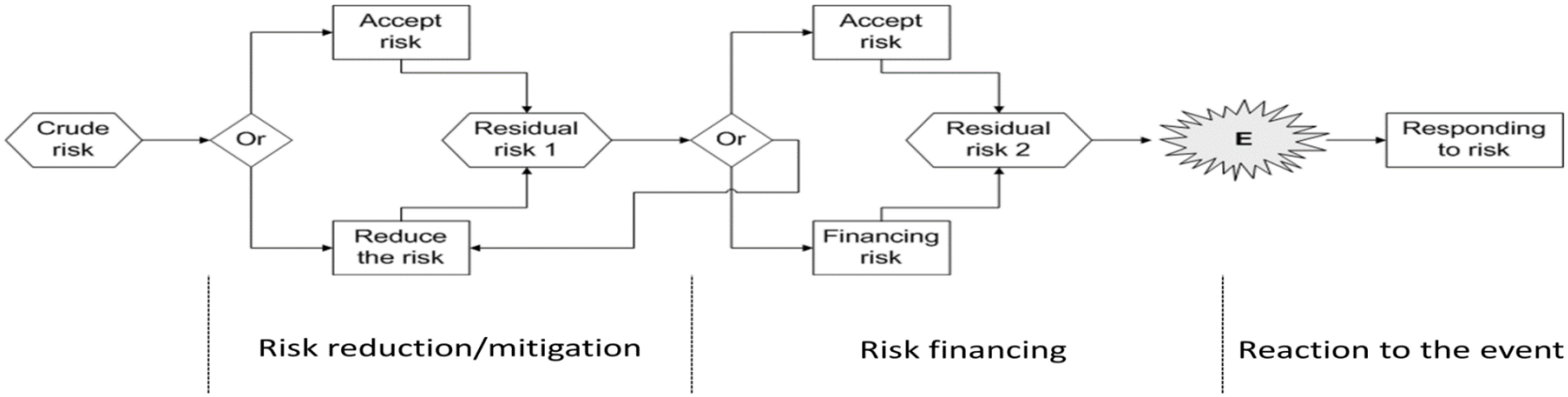
Risk Treatment



Risk treatment flowchart

At every step, one asks himself the following questions:

- Is the risk acceptable?
- Should the risk be reduced?



Some criteria for assessing risk treatment options

Criteria	Question to be answered
Cost	Is this option affordable? Is it the most cost-effective?
Equity	Do those responsible for creating the risk pay for its reduction?
Timing	Where there is no man-made cause, is the cost fairly distributed?
Leverage	Will the application of this option lead to further risk-reducing action by others?
Administrative efficiency	Can this option be easily administered or will its application be neglected because of difficulty of administration or lack of expertise?
Continuity of effect	Will the effects of the application of this option be continuous or merely short-term?
Compatibility	How compatible is this option with others that may be adopted?
Jurisdictional authority	Does this level of government have the legislated authority to apply this option? If not, can higher levels be encouraged to do so?
Effects on the economy	What will be the economic impacts of this option?
Effects on the environment	What will be the environmental impacts of this option?
Risk creation	Will this option itself introduce new risks?
Risk reduction potential	What proportion of the losses due to this risk will this option prevent?
Political acceptability	Is this option likely to be endorsed by the relevant governments?
Public and pressure group reaction	Are there likely to be adverse reactions to implementation of this option?
Individual freedom	Does this option deny basic rights?

Risk Control

- Risk control includes methods by which firms evaluate potential losses and take action to reduce or eliminate such threats.
  It is a technique that utilizes findings from risk assessments (identifying potential risk factors in a firm's operations, such as technical and non-technical aspects of the business, financial policies, and other policies that may impact the well-being of the firm), and implementing changes to reduce risk in these areas.

Risk Control

Risk control measures are based on:

- Prevention measures whose role is to reduce the probability of occurrence of feared events being the source of hazard for damaging targets.
- Protection measures whose role is to protect targets against the effects of such as heat flow, pressure or projectiles, which are associated with the release of dangerous phenomena.
- Mitigation measures whose role is to limit the effects due to the appearance of feared events.

S.T.O.P. Principle: measures in the following order:

- ***S*** measures: strategic, substitution of processes or substances giving a less hazardous result (examples: substituting, eliminating, lowering, modifying, abandoning, etc.); abandon process or product, modify final product.
- ***T*** measures: technical protection against hazardous phenomena which cannot be eliminated, lowering the likelihood of occurrence of an event and reducing the spread of the damage, (examples: replacing, confining, isolating/separating, automating, fire-wall, EX zones, bodyguards, etc.).
- ***O*** measures: organizational modifications of the work, training, work instructions, information concerning residual risk and how to deal with it (examples: training, communicating, planning, supervising, warnings signs, etc.)
- ***P*** measures: personal, relative to people (examples: personal protective equipment, masks, gloves, training, communication, coordinating, planning, etc.)

S.T.O.P. Principle: hierarchy in the following order:

- **Acting at the source:** Deleting the risk (substituting product or process, in situ neutralization), limiting leak risks (re-enforcing the system, lowering the energy levels), predictive measures (rupture disk, valves) and surveillance (integrity and functionality of the system, energy levels).
- **Acting at the interface** (on the trajectory between the source and the target): limiting the propagation (active barriers/ passive barriers), catching/neutralizing (local or general ventilation, air purification, substance neutralization), people control (raising barriers, access restrictions, evacuation signs) and surveillance (energy levels in the zone, excursions or deviations (alarms)).
- **Acting at the target:** lowering the vulnerability (personal protective equipment selection, special training), reducing exposure (e.g. automation), reducing the time (job rotation) and supervising (individual exposure, biological monitoring, medical survey, correct PPE use and followings rules).

STOP Table

	1. At the source	2. At the interface	3. At the target
Measures **S** (strategy)	Substitution Change process	Automation, telemanipulation Room subdivision	Criteria for selection of licensed operators
Measures **T** (technical)	Reactant production or use in continuous mode Safety relieve valves.	Fumes extraction process enslaved Physical access restrictions	Selection and purchase of personal protective equipment (PPE) and community protective equipment (CPE)
Measures **O** (organizational)	Response instructions	Extraction of fumes manually controlled Access restrictions markup	Prescription for PPE and CPE Organization of first aid
Measures **P** (personal)	Education / training of the process operation	Information / instruction on the process hazards	Instruction for the use of PPE

STOP principle pros and cons

	Pros	Cons
Measures **S** (strategical)	• Cancel or reduce the considered hazard. • Intervene at the beginning of the process.	• In case of a substitution, it is possible to create other hazards or risks. • Deletion needing a strategic decision.
Measures **T** (technical)	• Fixed. • Difficult to bypass.	• Costs. • Deadlines.
Measures **O** (organizational)	• Quick. • Moderate costs.	• Controllability. • Easy to bypass.
Measures **P** (personal)	• Quick. • Moderate costs • Simple implementation.	• Controllability. • Acceptability. • Convenience. • Omission.

Resilience

Definition: The intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.

Abilities essential for resilience:

- To respond to what happens
- To monitor critical developments
- To anticipate future threats and opportunities
- To learn from past experience – successes as well as failures

Resilience

A resilient system possesses 4 attributes (and design principles):

- Capacity (absorption, redundancy, functional, layer defensive)
- Flexibility (reorganization design, human backup, complexity avoidance, drift correction)
- Tolerance (localized capacity, loose coupling, neutral state, reparability design)
- Cohesion (inter-node interaction)

Resilience Engineering is based on following premises:

- Performance conditions are always underspecified
- Some adverse events can not be expected
- Safety mgt must be proactive and reactive
- Safety cannot be isolated from the core (business) process

Four basic abilities for understanding how organisations function

- Systems of first kind
- Systems of second kind
- Systems of third kind
- Systems of fourth kind

Event analysis

Event analysis
(event = accident, incident, near-miss)

Why analyze accidents?

- To understand by analysing the objective causes related to the accident.
- To prevent a recurrence.
- To determine which measures will improve safety.
- To act by implementing adequate solutions.
- To show employees that safety and health protection must be taken seriously.
- To communicate and therefore cool down debates.
- Savings for companies.
- To meet regulations.

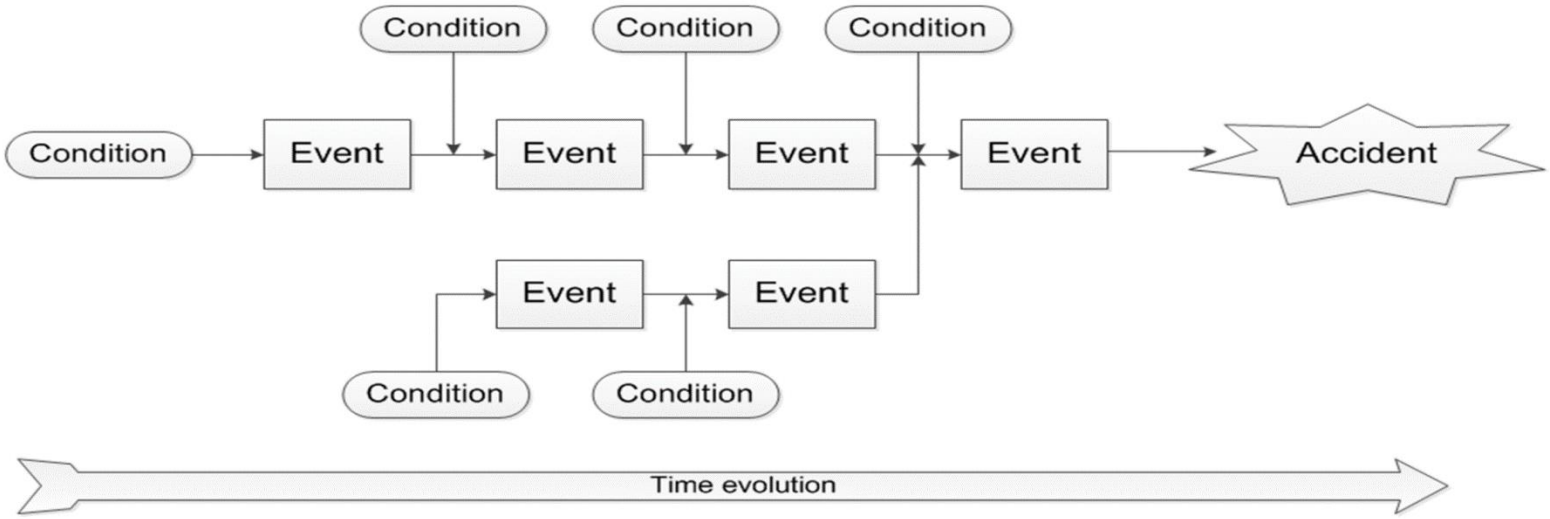
Common denominators among major analytical techniques

- One does not seek for responsibilities but for solutions.
- An accident is always a combination of several factors.
- On should retain only facts, no judgments nor interpretations.
- The analysis is interesting only if it leads to the implementation of solutions.
- The analysis of accidents is a collective work.

Event investigation?

- Accident = chain of sequential events (cfr. Heinrich)
- Swiss cheese model (holes, pathogens) (cfr. Reason)

Multilinear events sequencing



Root cause analysis

1. **Data collection and gathering**

Without complete information and an understanding of the event, the causal factors and root causes associated with the event cannot be identified.

2. **Causal factor charting**

The causal factor chart is simply a sequence diagram with logic tests that describes the events leading up to an occurrence, plus the conditions surrounding these events.

3. **Root cause identification**

After all the causal factors have been identified, one can begin root cause identification. This step involves the use of a decision diagram called the Root Cause Map to identify the underlying reason or reasons for each causal factor. The map structures the reasoning process to help answering questions about why particular causal factors exist or occurred.

4. **Recommendation generation and implementation**

Following identification of the root causes for a particular causal factor, achievable recommendations for preventing its recurrence are then generated and must be implemented.

Causal tree analysis

- Causal tree analysis provides a means of analysing the critical human errors and technical failures that have contributed to an incident or accident in order to determine the root causes.
  It is a graphical technique that is simple to perform and very flexible, allowing mapping out exactly what one thinks happened rather thanbeing constrained to an accident causation model.
  The diagrams developed provide useful summariesto include in incident and accident reports that give people a good overview of the key issues.

Causal tree analysis – method description

The method has four main steps as:

I. Search for facts
- Without any judgment
- Without interpreting
- By treating each fact one by one
- One fact must be measurable and/or photographable

II. Build the tree
- Begin with the last fact,
- Develop branches by asking the three following questions:
  - -What is the direct cause which provoked this?
  - -Was this cause really necessary for the occurrence of that fact?
  - -Was this cause sufficient to provoke the event?

Causal tree analysis – method description

The method has four main steps as:

III. Search for measures
- Begin with the first fact
- Search measures for each fact
- Accept all ideas

IV. Define measures
- Efficiency, use
- Measures not displacing a risk
- Simple measures, sustainable
- Measures complying with laws and regulations

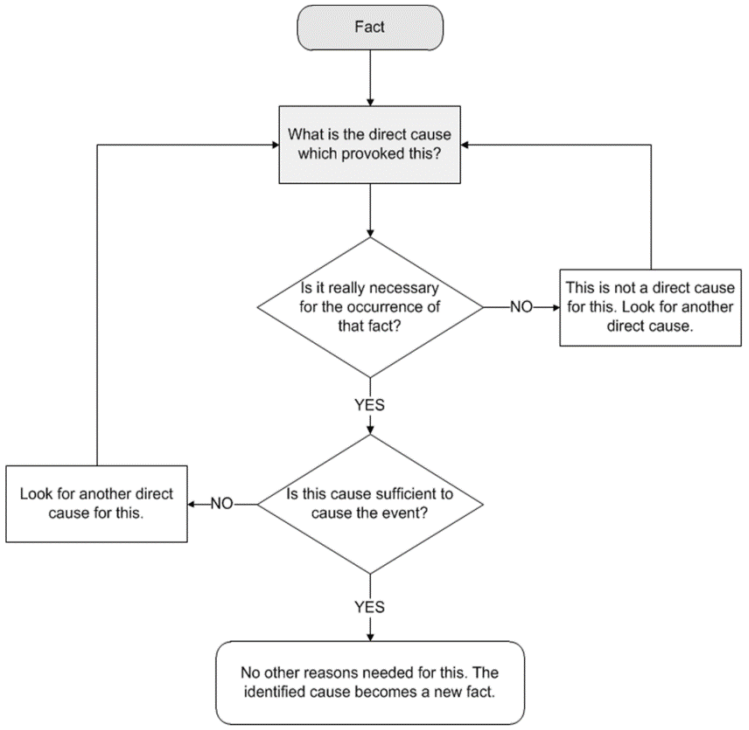
Interviewing basic tips for an investigator

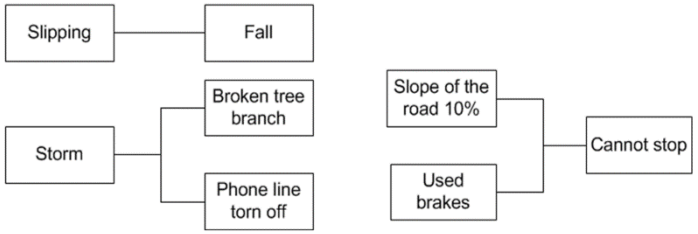
- Explain who the investigator is
- Explain why the accident is being investigated
- Discuss the purpose of the investigation (for example, to identify problems and not to determine fault or blame)
- Provide assurances that the witness is not in any danger of being compromised for testifying about the accident
- Inform the witness of who will receive a report of the investigation results
- Ensure witnesses that they will be given the opportunity to review their statements before they are finalized
- Absolutely guarantee the privacy of the witness during the interview
- Remain objective – do not judge, argue, or refute the testimony of the witness

Minimum questions to be covered: focus on 'who', 'what', 'when', 'where', and 'how' ('why' at the end!)

- *What* was the exact or approximate time of the event?
- *What* was the condition of the working environment at the time of the event; before the event; after the event (e.g., temperature, noise, distractions, weather conditions, etc.)?
- *Where* were people, equipment, and materials located when the event occurred; and *what* was their position before and after the event?
- *Who* are the other witnesses of the event (if applicable) and *what* is their job function?
- *What* and/or *who* was moved from the scene, repositioned, or changed after the event occurred?
- *When* did the witness first become aware of the event and *how* did he or she become aware?
- *How* did the response or emergency personnel perform, including supervisors and outside emergency teams?
- *How* could the event have been avoided?

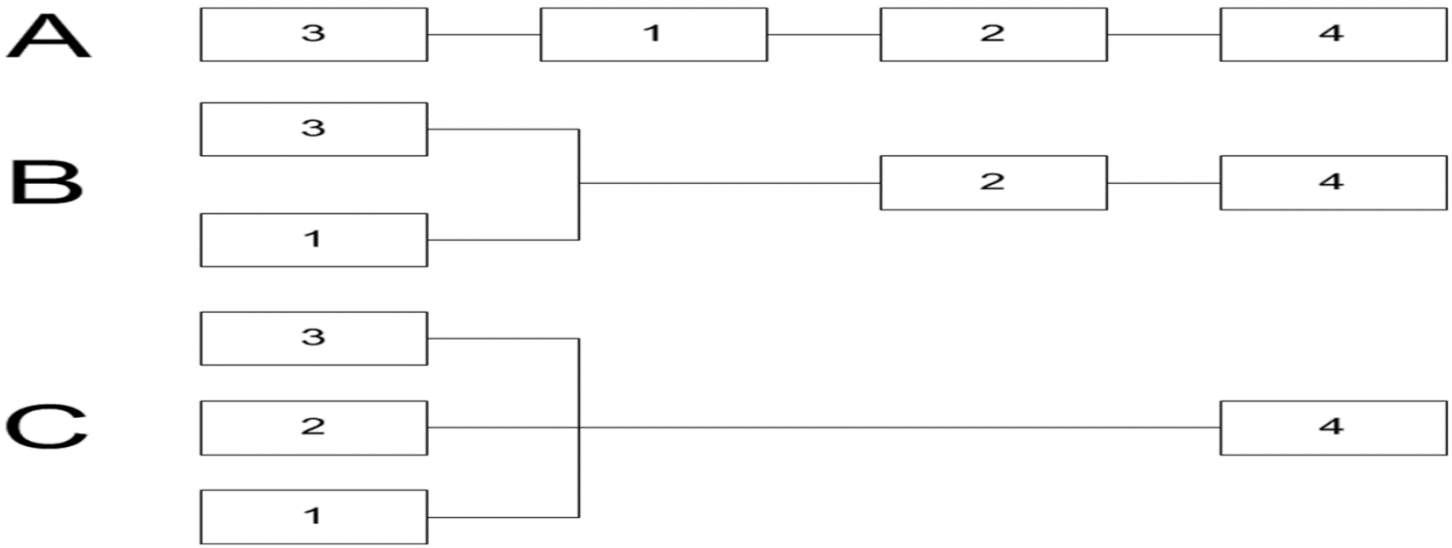
Building the tree





Simple example

1. The faucet is left open.
2. The tub overflows.
3. The siphon is blocked.
4. The carpet bathroom is full of water.



Exercise: build the causal tree

1. Workers must take the bottles out of crate to be sorted by type.
2. Mr X does not wear protective gloves.
3. The customer is not refunded for broken and/or missing bottles.
4. Protective gloves are not designed for the specific task – hazard.
5. The customer puts the number per supplier in crates without separating by content.
6. Mr X holds the broken bottle.
7. There is a broken bottle in the crate.
8. Mr X has a reflex movement.
9. The driver does not control the bottles when taking them from the customer.
10. Mr X does not meet the guidelines of wearing gloves.
11. Mr X does not see that the bottle is broken.
12. Mr X has a significant injury to his right hand.
13. The customer puts broken bottles in the crate.
14. There is an absence of regulation, “Control of crates by the driver”.
15. There is a lack of control by the supervisor.