Risk and safety
Part 2: Risk analysis and safety measures

EPA1132 – Technology development and impact assessment

Frank Guldenmund, Safety Science & Security Group, Faculty TPM

TU Delft Delft University of Technology

Challenge the future

Overview

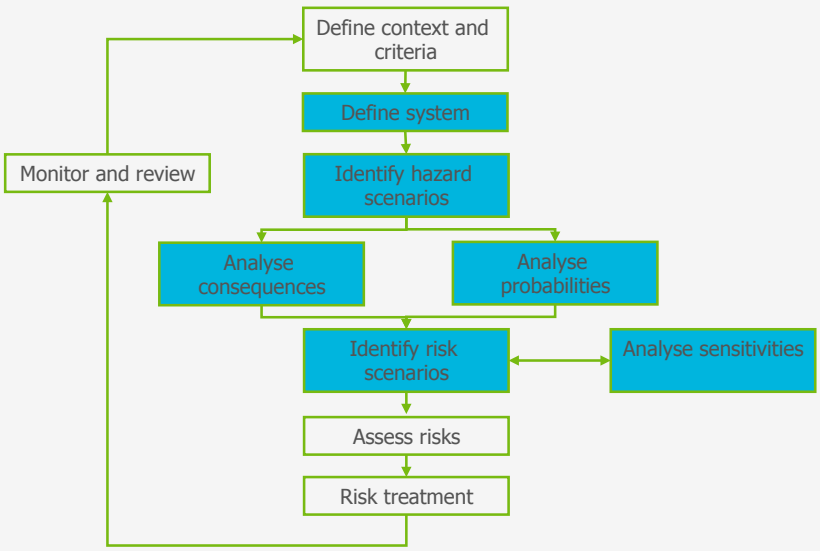
1. Risk analysis (continued)
2. Safety measures

Risk analysis (continued)

TU Delft Delft University of Technology

Challenge the future

Risk analysis



Definition of (structure of) system

Depends on defined context and chosen method for hazard identification

- Required decomposition in system parts?
- Detailed level of system description?

System definition sets the boundaries for logic and quantitative analysis in later steps

- Types of hazards and scenarios taken into account
- Type of consequences considered
- Magnitude of probability of occurrence

Identify hazard scenarios

- What might go wrong?
- How can it happen?
- What controls exist?

Crucial step:

- Detailed understanding of the system is gained
- Only identified potential hazards will be further taken into account

Methods for hazard identification

- Standard list or checklist
- Preliminary Hazard Analysis (PHA)

- Hazard Identification study (HAZID)
- Hazard and Operability study (HAZOP)

- Failure Mode and Effect Analysis (FMEA)
- Failure Mode Effect and Criticality Analysis (FMECA)

- Fault Tree Analysis (FTA)

- Past experience (incident, accident reports/databases)

Methods for hazard identification

- Standard list or checklist
- Preliminary Hazard Analysis (PHA)

- Hazard Identification study (HAZID)
- Hazard and Operability study (HAZOP)

- Failure Mode and Effect Analysis (FMEA)
- Failure Mode Effect and Criticality Analysis (FMECA)

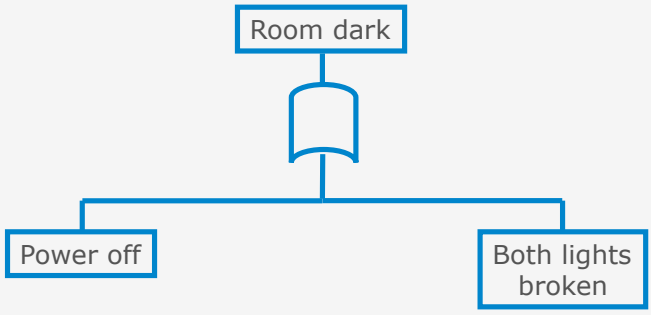
- Fault Tree Analysis (FTA)

- Past experience (incident, accident reports/databases)

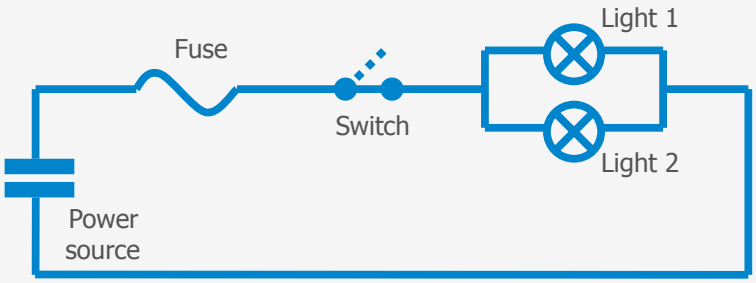
FTA – Fault Tree Analysis

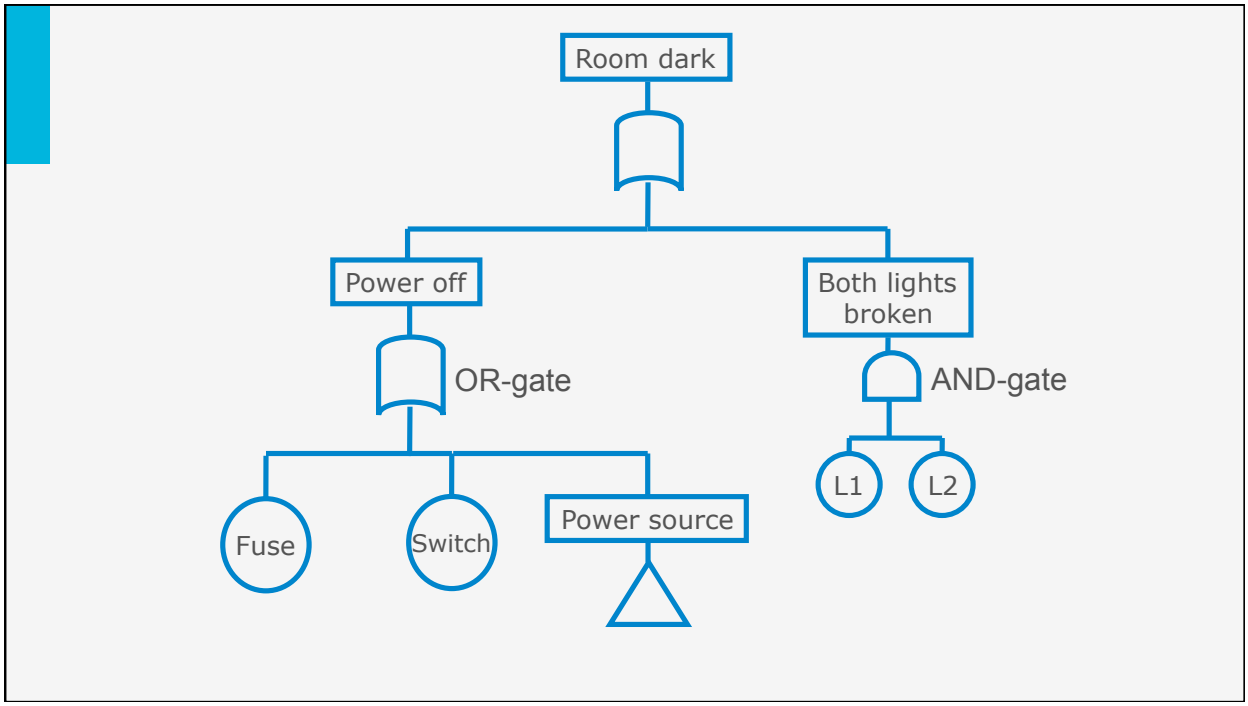
- Logical structure of sequences of events that lead to the event/accident
- Allows quantification of probability of failure or of the accident
- Can be used both in a retrospective way (accident analysis) and in a prospective way (process analysis)
- Tree structure:
  - Starting point: top event (the accident, the system failure)
  - End point: basic failure events (component failures)

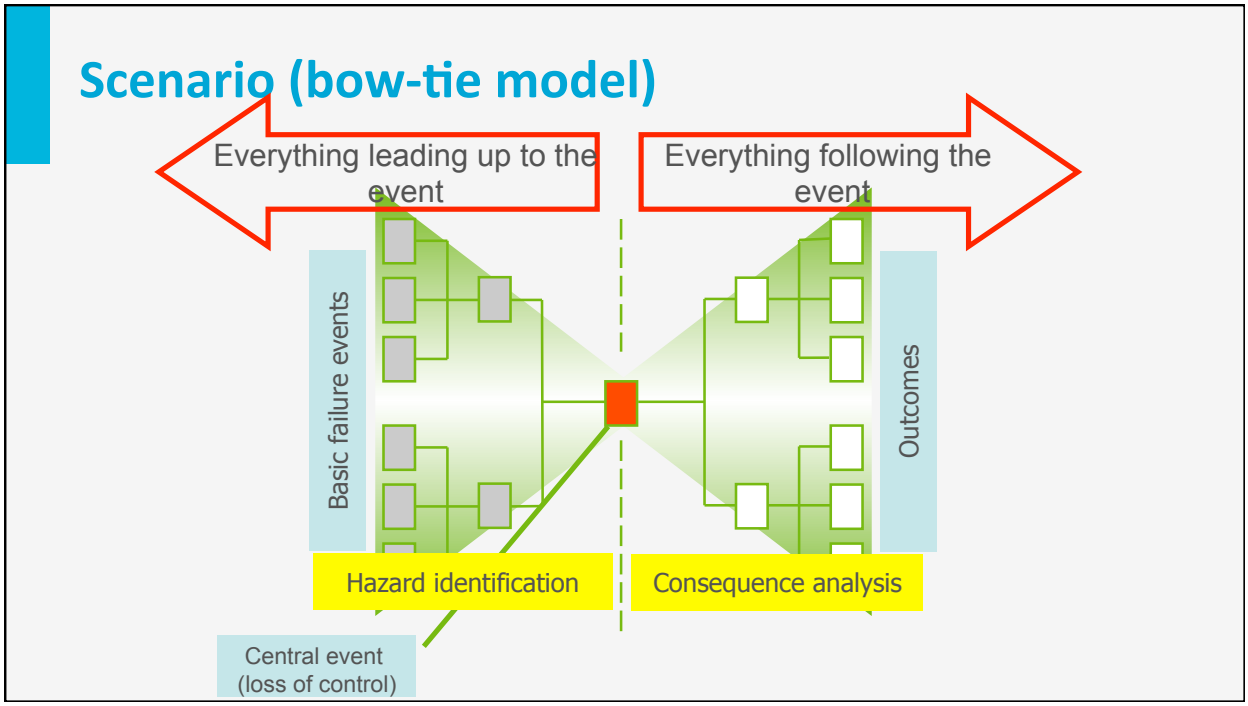
FTA – example


Room dark
Power off
Both lights broken

System


Fuse
Switch
Light 1
Light 2
Power source


Room dark
Power off
Both lights broken
OR-gate
AND-gate
Fuse
Switch
Power source
L1
L2


Scenario (bow-tie model)
Everything leading up to the event
Everything following the event
Basic failure events
Outcomes
Hazard identification
Consequence analysis
Central event (loss of control)

Consequences

- Often used to define consequences
  - Loss of life
  - Injury
  - Economical loss
- Issue: what common denominator to use?
  - Comparability of direct losses and indirect losses?
- Influence of time
  - Benefits and costs often do not occur at the same time
- For consequence analysis domain expertise is required

Different loss categories

	Minor	Critical	Severe	Catastrophic
Plant damage and lost production	Short-term loss of production	Damage to machines. Reparable in short term	Damage to plant. Major repair costs. Serious loss of production	Substantial damage to plant. Potential loss of overall plant
Environment damage	Temporary excursion in emission levels	Significant release. Effluent clean up required	Ecological damage for up to 1 year. Risk of penalties	Ecological damage for more than 1 year. Pressure to cease business
Harm to personnel	Reportable but non-disabling injuries causing over 3 days absence	Disabling injury or severe injury requiring extensive recovery. 1 to 10 chance of fatality	Critical injuries, and possible 1 fatality	One or more fatalities

Probabilities: the probability that a given event will occur

Dying in an airplane crash	10^{-6} per flight
Having a car accident	0.6 x 10^{-5} per km travelling in the Netherlands
Human error on a simple, frequently performed task, under minimal stress	10^{-3} per demand

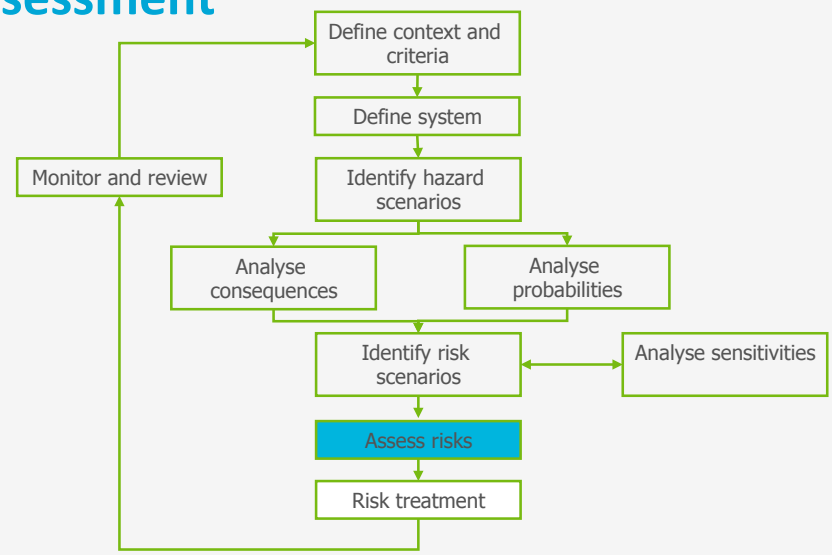
Ranking of scenarios

Scenario	Likelihood (probability)	Consequence (large to small)
s_1	p_1	x_1
s_2	p_2	x_2
.	.	.
.	.	.
s_i	p_i	x_i
.	.	.
.	.	.
s_{N-1}	p_{N-1}	x_{N-1}
s_N	p_N	x_N

Sensitivity

- Needed since risk analysis is associated with uncertainty/ incompleteness
- Sources
  - Inherent or natural variability
  - Modelling uncertainty (all factors, relationships)
  - Statistical uncertainty (data availability, data quality)
- Analysis
  - Effect of changes in input variables, relations and/or data
  - Effect of changes in model assumptions

Risk assessment



Risk assessment matrix

	Hazard Categories			
Frequency of Occurrence	I Catastrophic	II Critical	III Marginal	IV Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Example of risk matrix used in the chemical industry

SEVERITY	CONSEQUENCES				INCREASING LIKELIHOOD				
	People	Assets	Environment	Reputation	A	B	C	D	E
					Never heard of in the Industry	Heard of in the Industry	Has happened in the Organisation or more than once per year in the Industry	Has happened at the Location or more than once per year in the Organisation	Has happened more than once per year at the Location
0	No injury or health effect	No damage	No effect	No impact					
1	Slight injury or health effect	Slight damage	Slight effect	Slight impact					
2	Minor injury or health effect	Minor damage	Minor effect	Minor impact					
3	Major injury or health effect	Moderate damage	Moderate effect	Moderate impact					
4	PTD or up to 3 fatalities	Major damage	Major effect	Major impact					
5	More than 3 fatalities	Massive damage	Massive effect	Massive impact					

Risk assessment matrix

Frequency of occurrence	Hazard categories I Catastrophic	II Critical	III Marginal	IV Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

High risks: changes must be made

Serious risks: make changes if possible

Medium risks: acceptable with management review

Low risks: acceptable without review

Risk assessment matrix

Frequency of occurrence	Hazard categories I Catastrophic	II Critical	III Marginal	IV Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

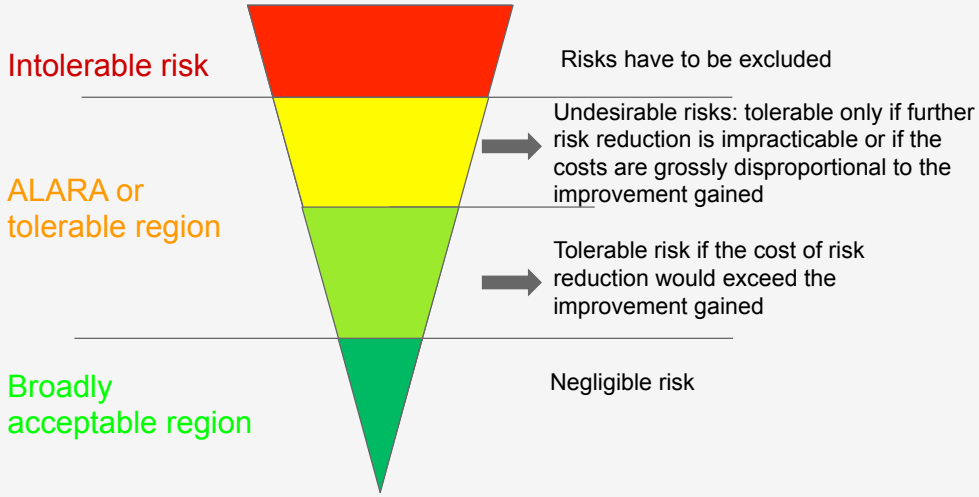
High risks: changes must be made

Serious risks: make changes if possible

Medium risks: acceptable with management review

Low risks: acceptable without review

ALARA-principle: As Low As Reasonable Achievable



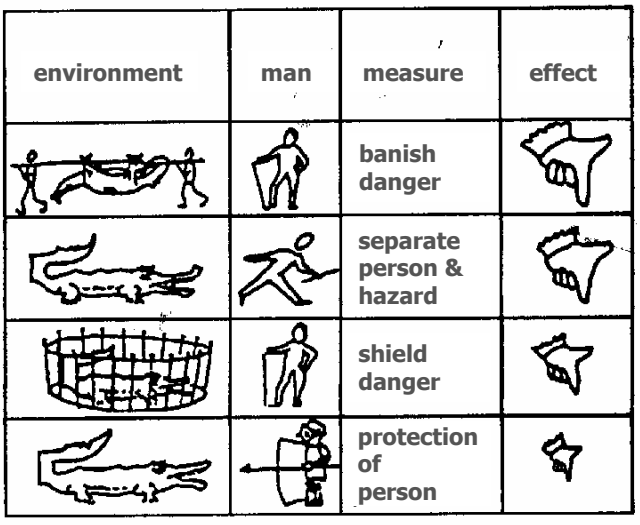
Safety measures

TU Delft Delft University of Technology

Challenge the future

Risk treatment

1. Risk avoidance
   - Eliminate the hazard, not continue with system (e.g. chlorine transport by train)
2. Risk reduction
   - Reduce probability of occurrence of events
   - Reduction of severity of consequences (mitigation)
3. Risk transfer
   - E.g. insurance or other financial mechanisms
4. Risk acceptance
   - Until other measures can and must be taken



Bron: Social- und Preventiv Medizin, Dec. 1981, Volume 26

Avoid

Reduce probability

Reduce probability

Reduce consequence

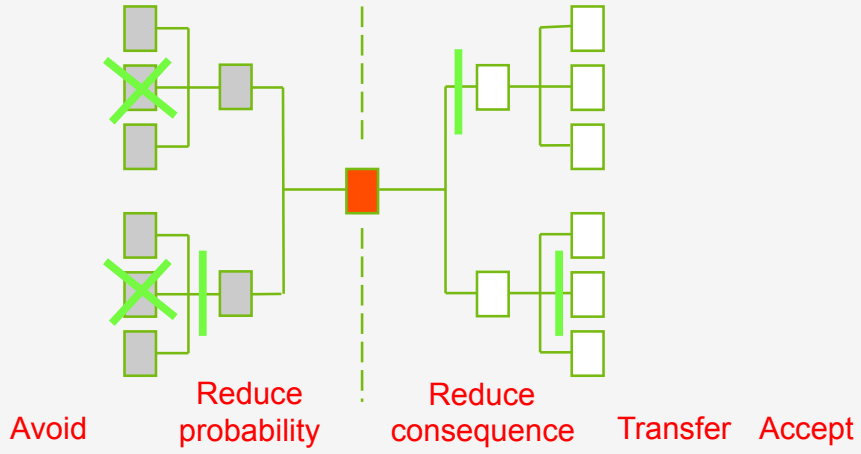
What to do with the hazard? Haddon's ten strategies

1. Eliminate hazard source
2. Lower, diminish, reduce hazard source
3. Prevent release of hazard
4. Modify rate of release of hazard source
5. Separate in space and time hazard source and objects
6. Use a barrier between the hazard and the objects
7. Modify contact surface of hazard source (rounding, softening)
8. Strengthen objects against hazard
9. Mitigation (after initial release)
10. Reparative strategies, stabilisation

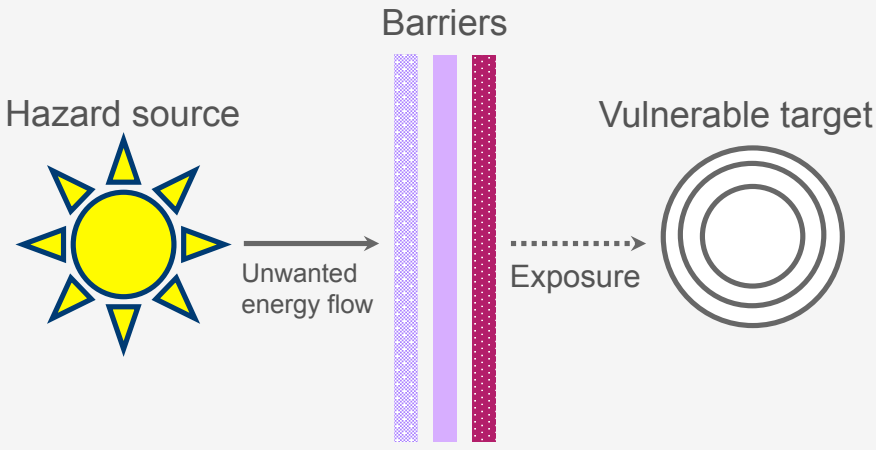
What to do with the hazard? Haddon's ten strategies

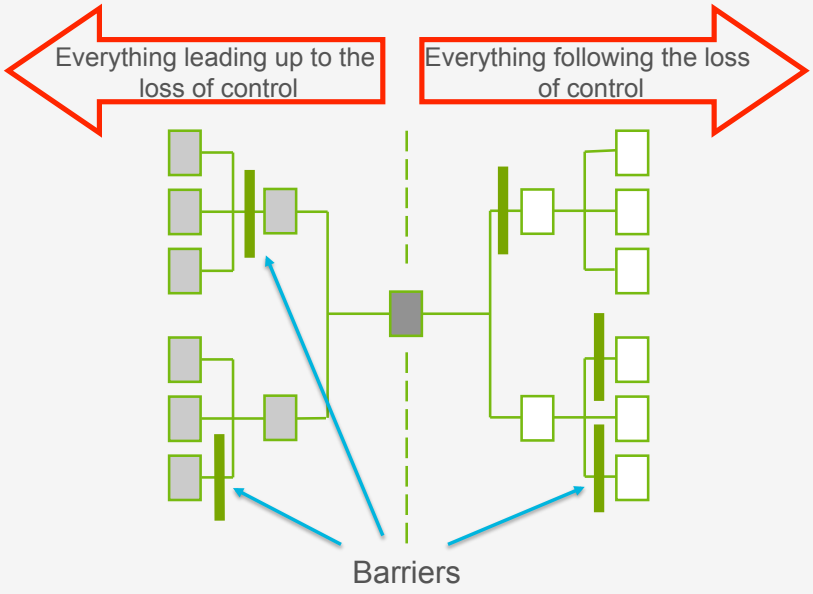
1. Eliminate hazard source
2. Lower, diminish, reduce hazard source
3. Prevent release of hazard
4. Modify rate of release of hazard source
5. Separate in space and time hazard source and objects
6. Use a barrier between the hazard and the objects
7. Modify contact surface of hazard source (rounding, softening)
8. Strengthen objects against hazard
9. Mitigation (after initial release)
10. Reparative strategies, stabilisation

Implement barriers ≠ fully eliminate

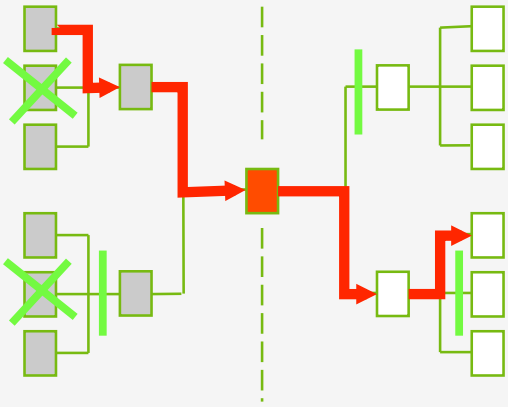


The Hazard-Barrier-Target (HBT) model

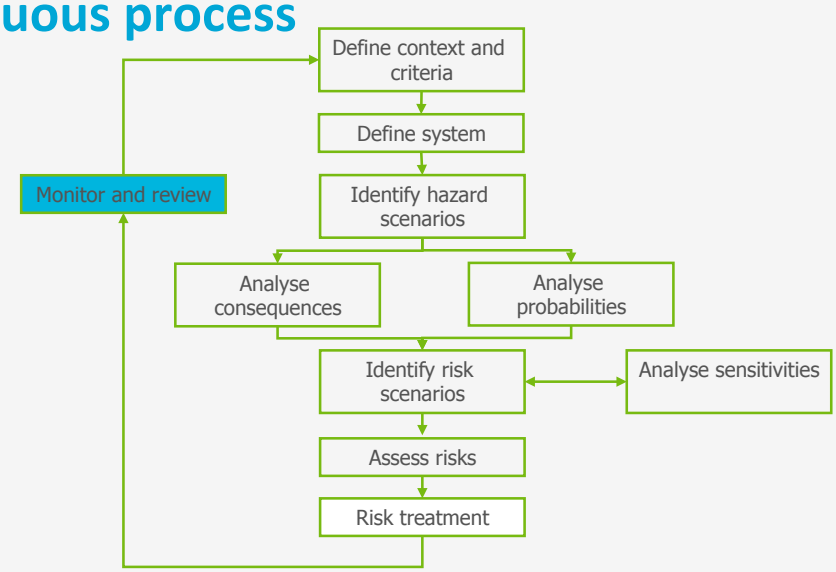




Implement barriers ≠ fully eliminate



Continuous process



Monitor and review

- Risk analysis is a continuous process. It requires regular monitoring and revision
- Due to:
  - System modifications
  - Changes in use/ operation
  - Increased operating experiences (short and long term)
  - Accidents
  - Other new information relevant to system performance

Thank you for your attention!

TU Delft Delft University of Technology

Challenge the future