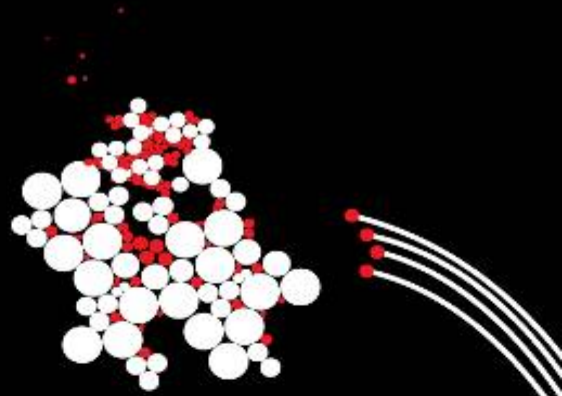
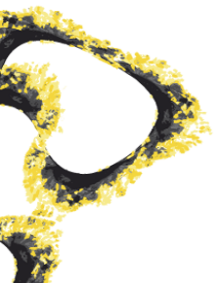
UNIVERSITEIT TWENTE.



A nice holiday
What could possibly go wrong?

Enno Ruijters
Formerly Formal Methods & Tools

INTRODUCTION



NTE.

WHO AM I ?

2008 – 2014: Operations Research
Maastricht University

2014 – 2018

PhD Student: ArRangeer project

- *Formal Methods and Tools @ UTwente*
- *Integrating maintenance in fault trees*
- *Collaboration with ProRail and NedTrain*

2018 – 2019

- Postdoc @ Utwente
- Software engineer @ BetterBe

Today's goal: case study

- Scenario: holiday
  - Climbing Mount Everest
  - Touring Chernobyl site
- Perform risk assessments for:
  - Yourself
  - Travel insurance
- Theory + practice = fun!

Other quantitative methods

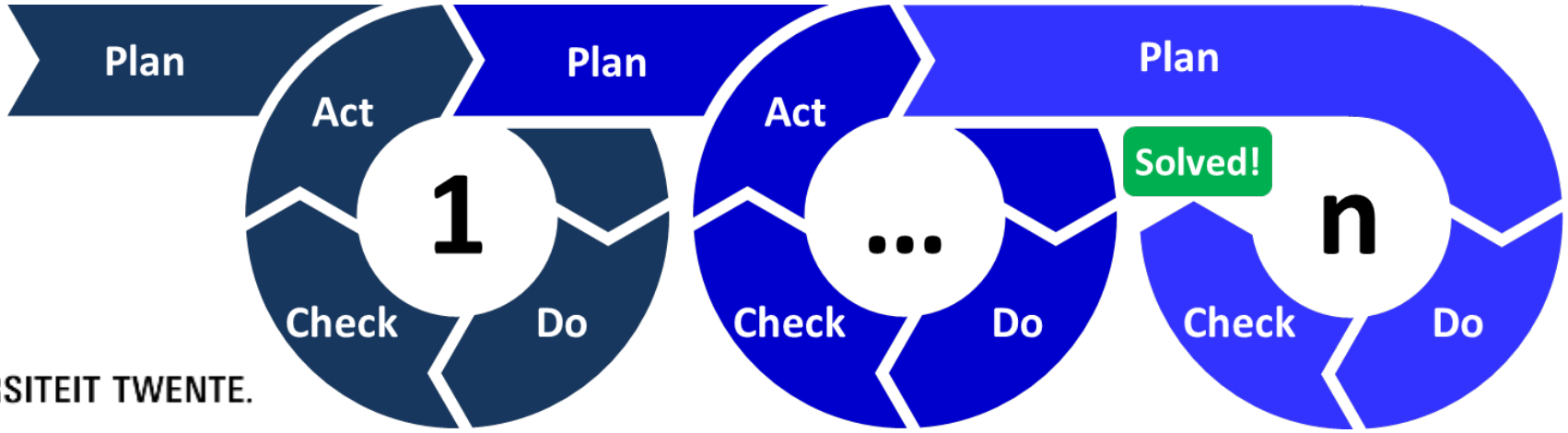
- Consider two types of risk:
  - Unsuccessful trip
  - Post-trip consequences
- Plan risk mitigations. Remember:
  - Avoidance
  - Reduction
  - Sharing/Transferrence
  - Acceptance

Travel insurance

- Propose a cost for an insurance policy
- Purely financial risk assessment
- Payouts:
  - Death: €50.000
  - Permanent total disablement: €100.000
  - Other costs: Cost price

General guidelines

- Focus analysis effort where needed
- Finding data is hard
- Risk management is an iterative process:
  - E.g., plan-do-check-act cycle
  - Plan for future adjustment
- Risks vary over time and mission phase.



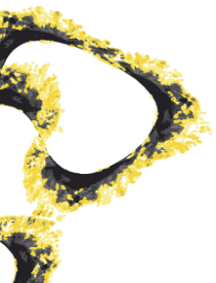
Continuous refinenement

- Progressive insight and actual events may require adjustments.
- Such adjustments can be planned:
  - “If I am injured early on, cancel the holiday”
  - “On arrival, I expect to see X. If I do not, reconsider the risk assessment”
- SMART criteria: Specific, measurable, achievable, relevant, time-bound

People are a problem

- Humans have been known to fail at every step of risk management:
  - Analysis (Therac-25)
  - Production (also Therac-25)
  - Operation (Chernobyl)
  - Fault detection (EAL 401)
  - Fault correction (TNA 235)

QUANTITATIVE RISK ANALYSIS



NTE.

Focusing effort

- Risk analysis is typically performed in stages, for example:
  - FME(C)A
  - Fault tree analysis
  - Domain-specific analysis
- Risk that are sufficiently known may not require additional stages

Failure Mode and Effect Analysis

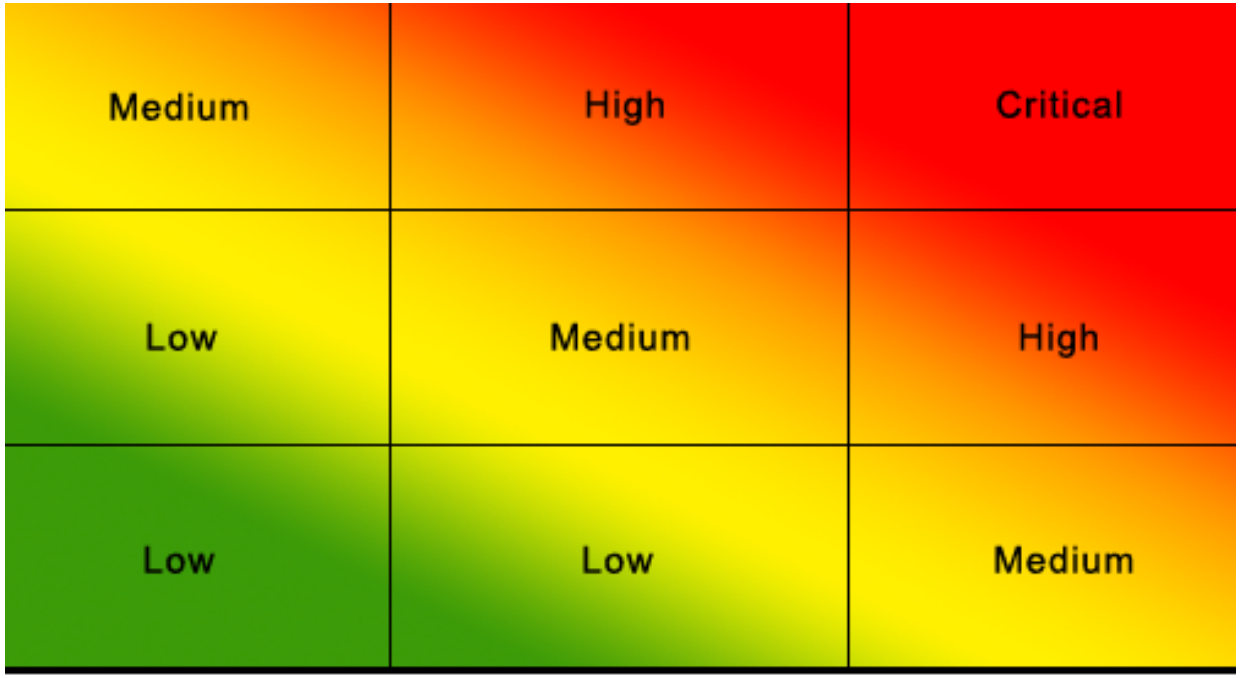
- Spreadsheet based method
- Enumerate all (single) failure modes and their effects
- Different standard have different fields
- Example (for this presentation):

Component	Failure mode	Effect
Projector	Lamp fails	Change rooms, delay
Computer	Does not start	Use different computer
Laser pointer	Empty batteries	Point manually
Presenter	Oversleeps	Late start

Failure Mode, Effect and Criticality Analysis

- Extend FMEA with probability and severity:

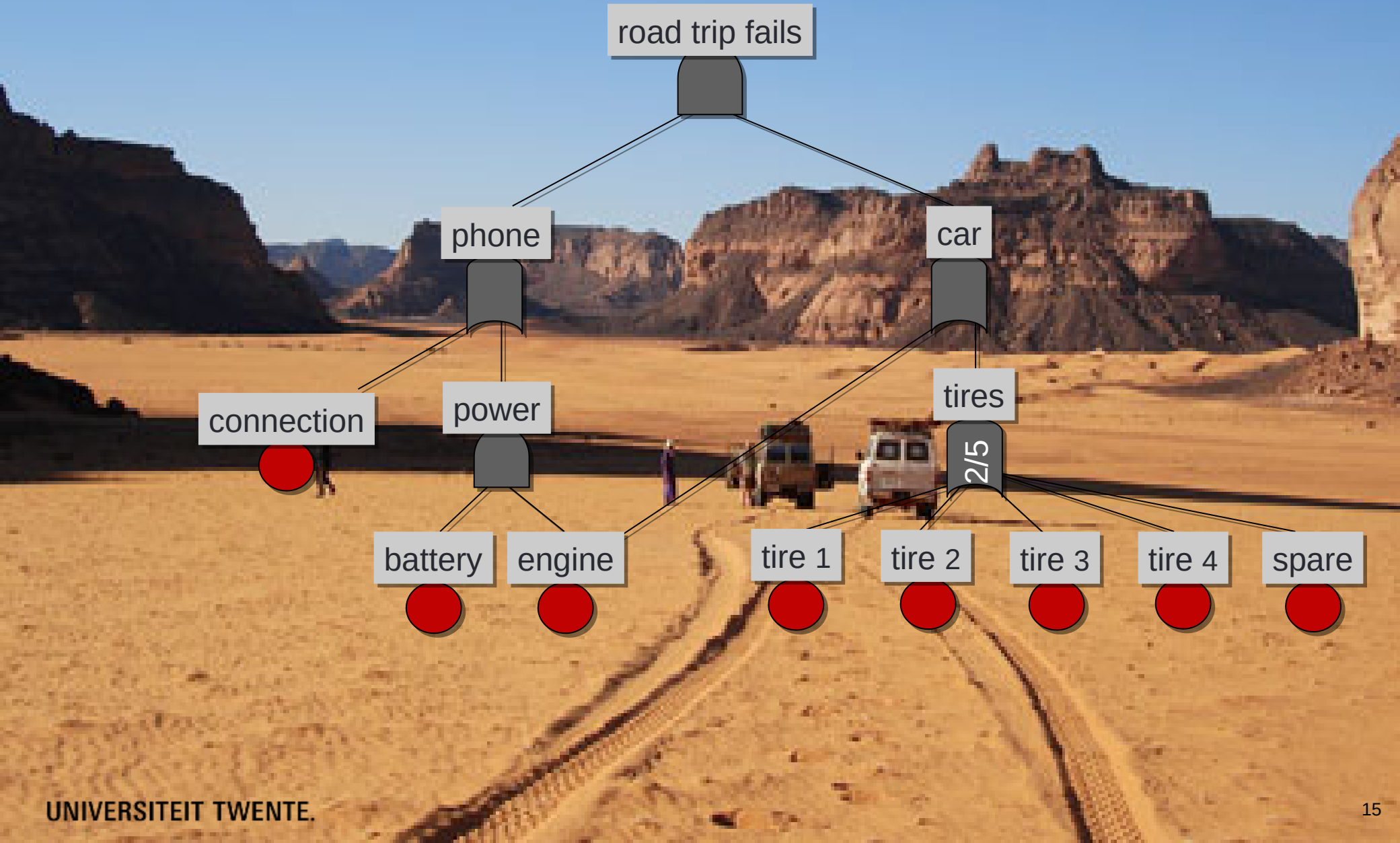
Component	Failure mode	Effect	Prob.	Severity	Criticality
Beamer	Lamp fails	Change rooms, delay	Low	Medium	Low
Computer	Does not start	Use different computer	Medium	Medium	Medium
Laser pointer	Empty batteries	Point manually	High	Low	Medium
Presenter	Oversleeps	Late start	Low	High	Medium



Failure Mode and Effect Analysis

- Other fields sometimes included:
  - Function (of system and/or component)
  - Failure cause
  - Consequences of different types (e.g. cost, risk to public, reputation damage, etc.)
  - Mitigation, residual effects
  - Detection options
  - Other internal fields (reporting codes, historic occurrence, etc.)

Fault Tree Analysis

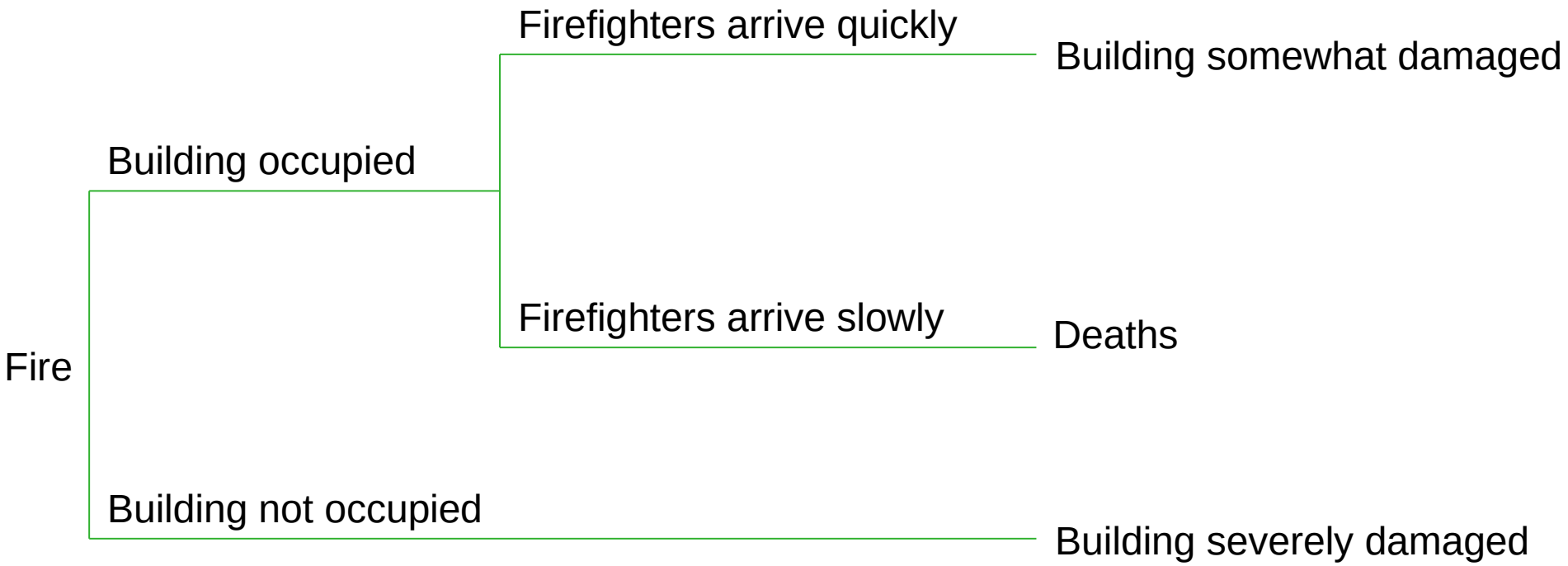


Event trees

- Describe possible consequences of events.
- Quantitative if probabilities known

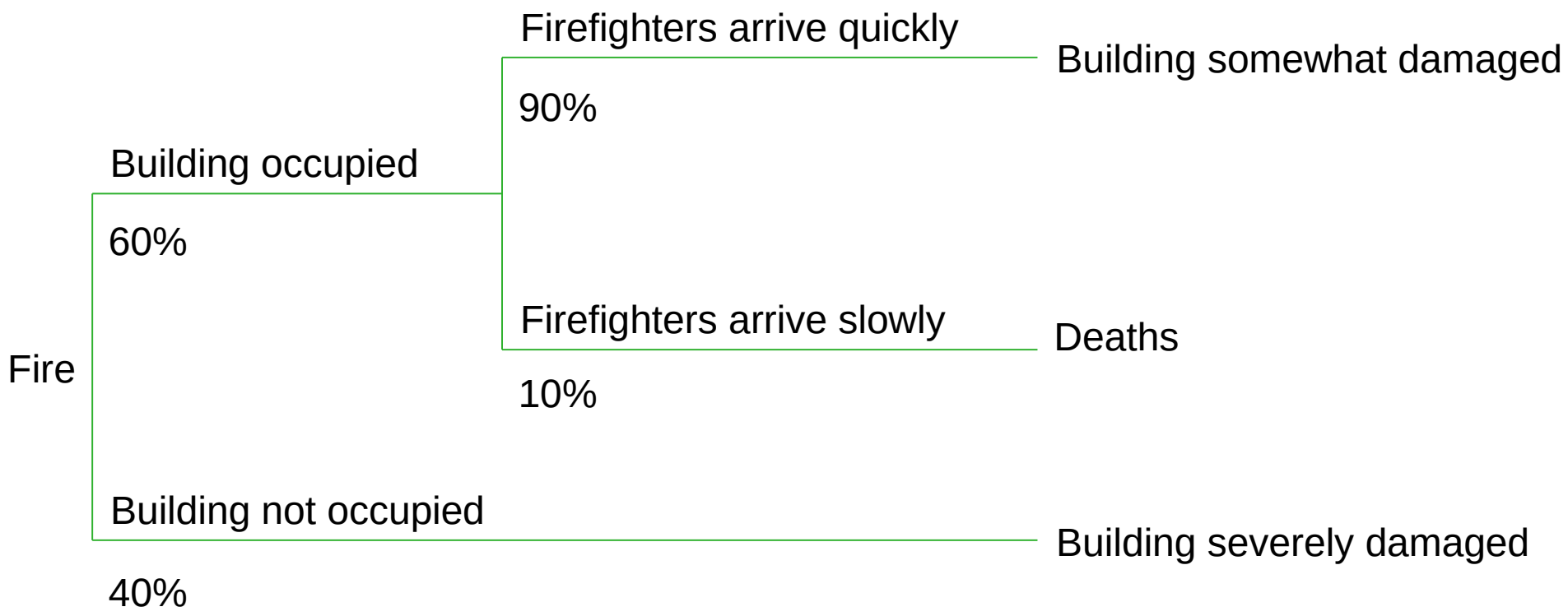
- Process:
  - Start with *initiating* event.
  - Determine possible immediate consequences.
  - Examine what decides which consequences occur.
  - Repeat

Event trees (example)



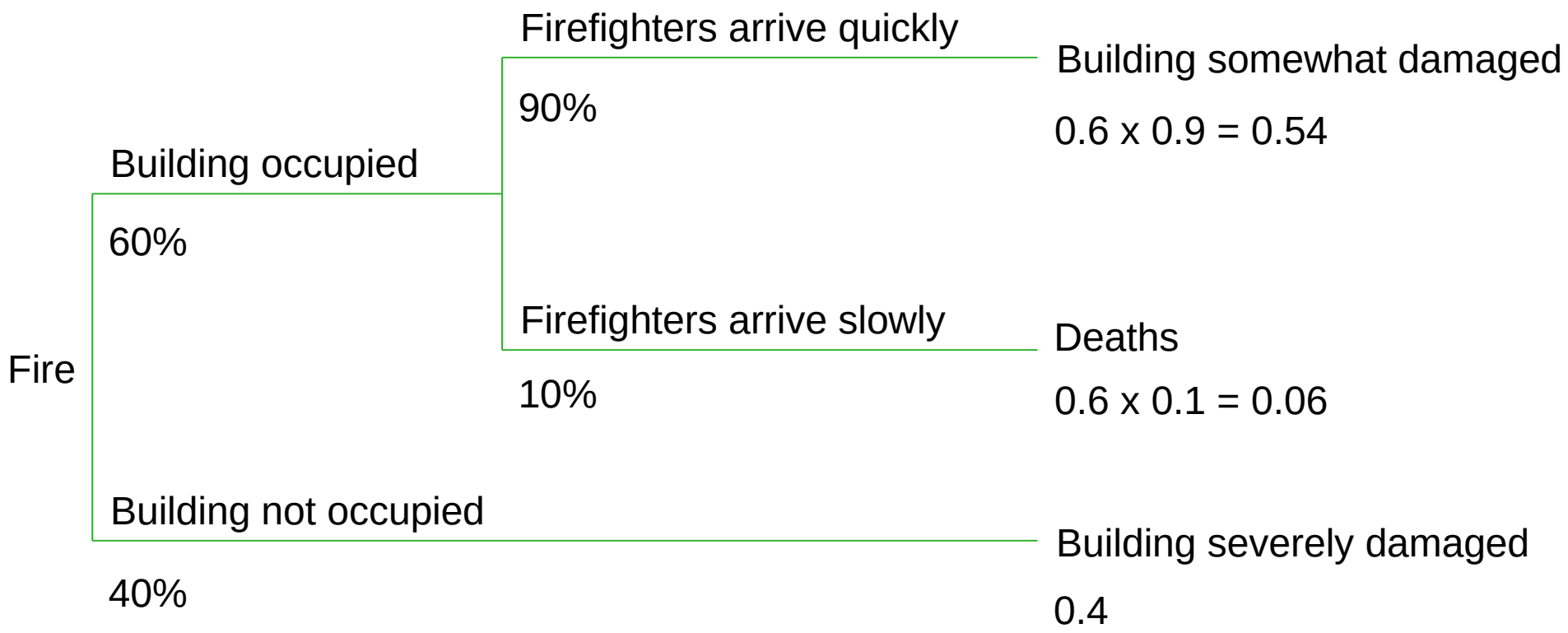
Event trees quantification

- Assign probabilities to conditions



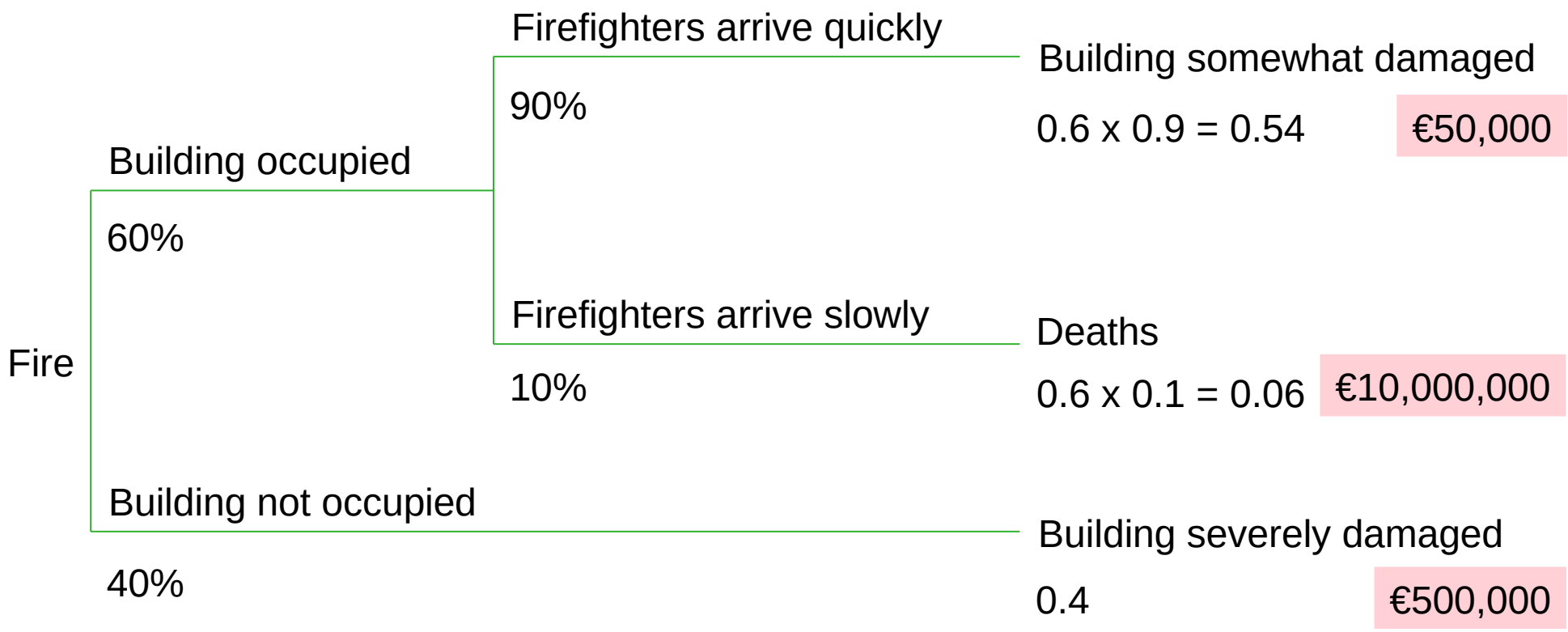
Event trees quantification

- Compute probabilities of outcomes



Event trees quantification

- Assign impact and compute risk

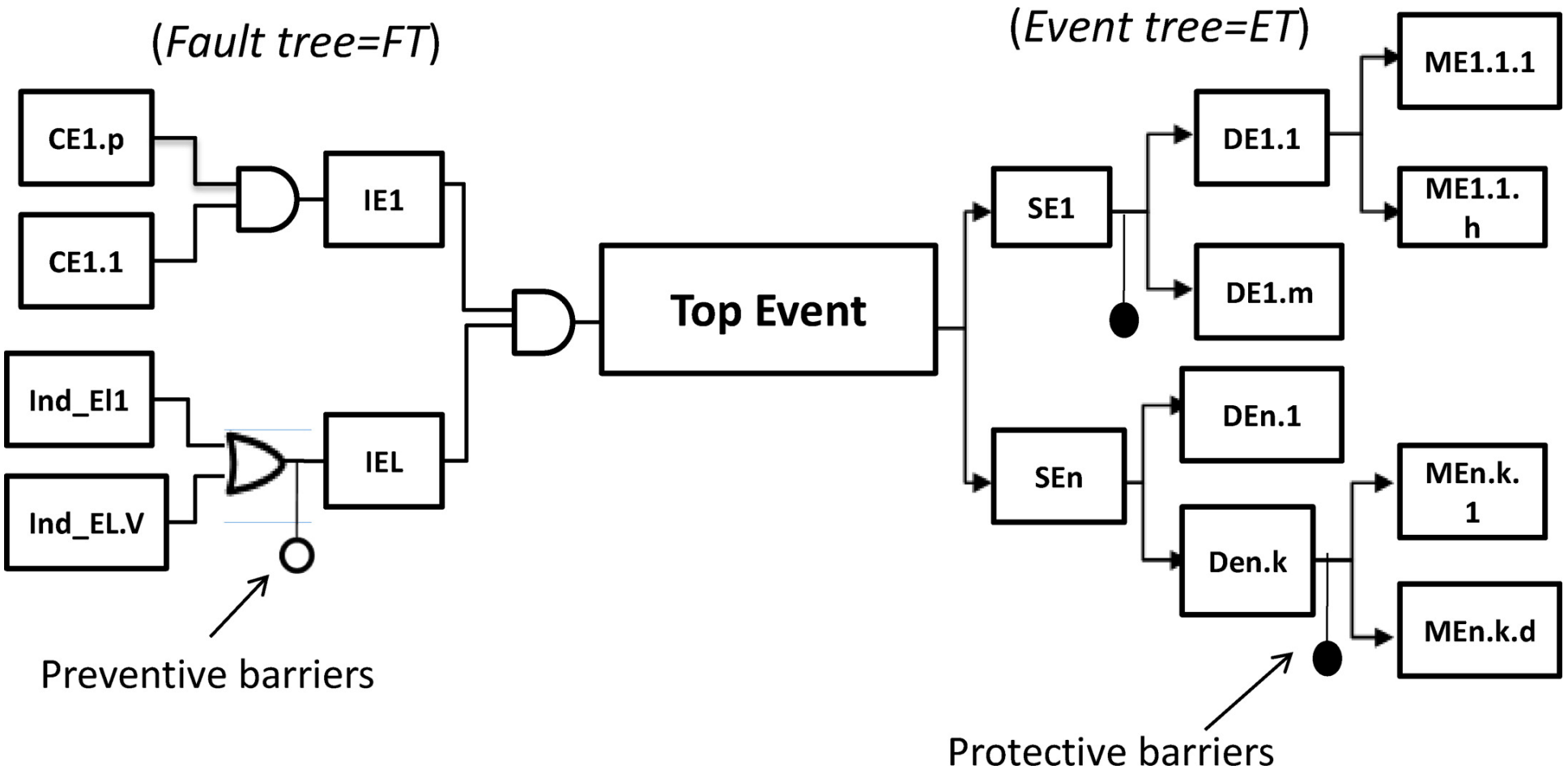


0.54 x 50,000 + 0.06 * 10,000,000 + 0.4 * 500,000 = €827,000 **If a fire occurs**

Bow-tie diagram

- Combine fault tree and event tree
  - Use fault tree to analyze occurrence of initiating event.
  - Use event tree to analyze consequences of event.

Bow-tie diagram (example)



Getting failure probabilities and costs

- Historical data (statistics)
- Domain-specific models (physics-of-failure)
- Expert judgement

Getting failure probabilities from statistics

- Look at past occurrences of potential risks
- Pitfalls:
  - Sampling bias
  - Different operating conditions
  - Accuracy of data (entry)

Getting failure probabilities from domain-specific models

- Very useful for very specific risks
  - Metal fatigue
  - Electronic component failure
  - Diseases (under normal conditions)
- Often require very specific input data
  - Exact metal composition and forces
  - Operating temperature, vibration, etc.
  - Age, profession

Getting failure probabilities from experts

- Generally a last resort
- Don’t expect exact numbers, prefer linguistic scales
  - “very low” (<0.1%), “high (>10%)”, etc.
- Prefer relative judgements
  - How much more likely is a plastic cog to fail than a metal one?
- Be cautious in averaging away outliers, they may reflect real knowledge.

Bad data kills

- The Therac-25 incident:
  - Radiation therapy machine for cancer treatment
  - Major overdoses due to malfunctions
  - First ‘fix’ after discovery was useless
  - Cause: software bug
  - Root cause: Probability of software bug was estimated as 0

CASE STUDY

NTE.

Today's goal: case study

- Scenario: holiday
  - Climbing Mount Everest
  - Touring Chernobyl site
- Perform risk assessments for yourself and for a travel insurer.
  - These will probably differ only in effect analysis
- Evaluate each other's risk assessment
  - Pretend you are the insurance company
- Refine your assessments based on the evaluation

Today's goal: case study

- Schedule (subject to change):
  - 14:00 Present first risk assessment
  - 14:45 Provide evaluations
  - 15:30 Present final risk assessment
  - Tomorrow Present poster