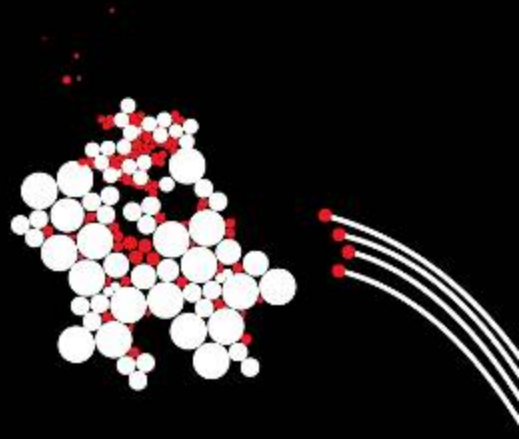
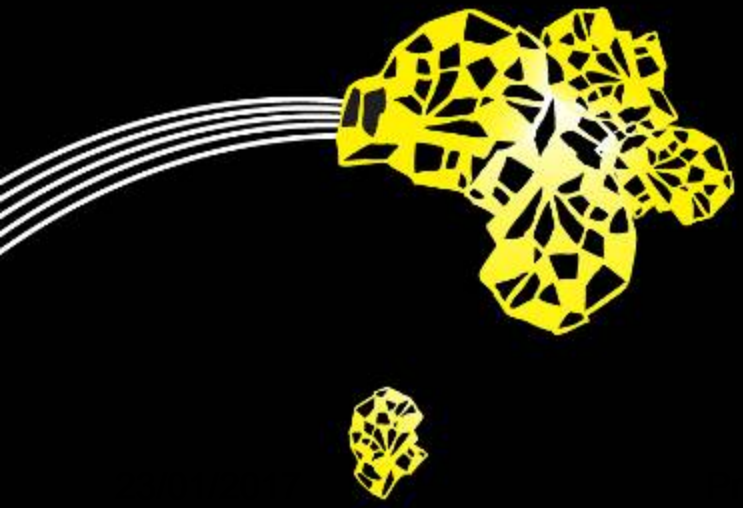
UNIVERSITEIT TWENTE.

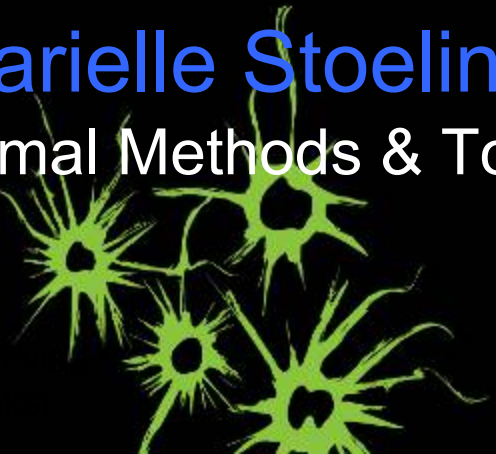


How risk happens and stochastic model checking can help

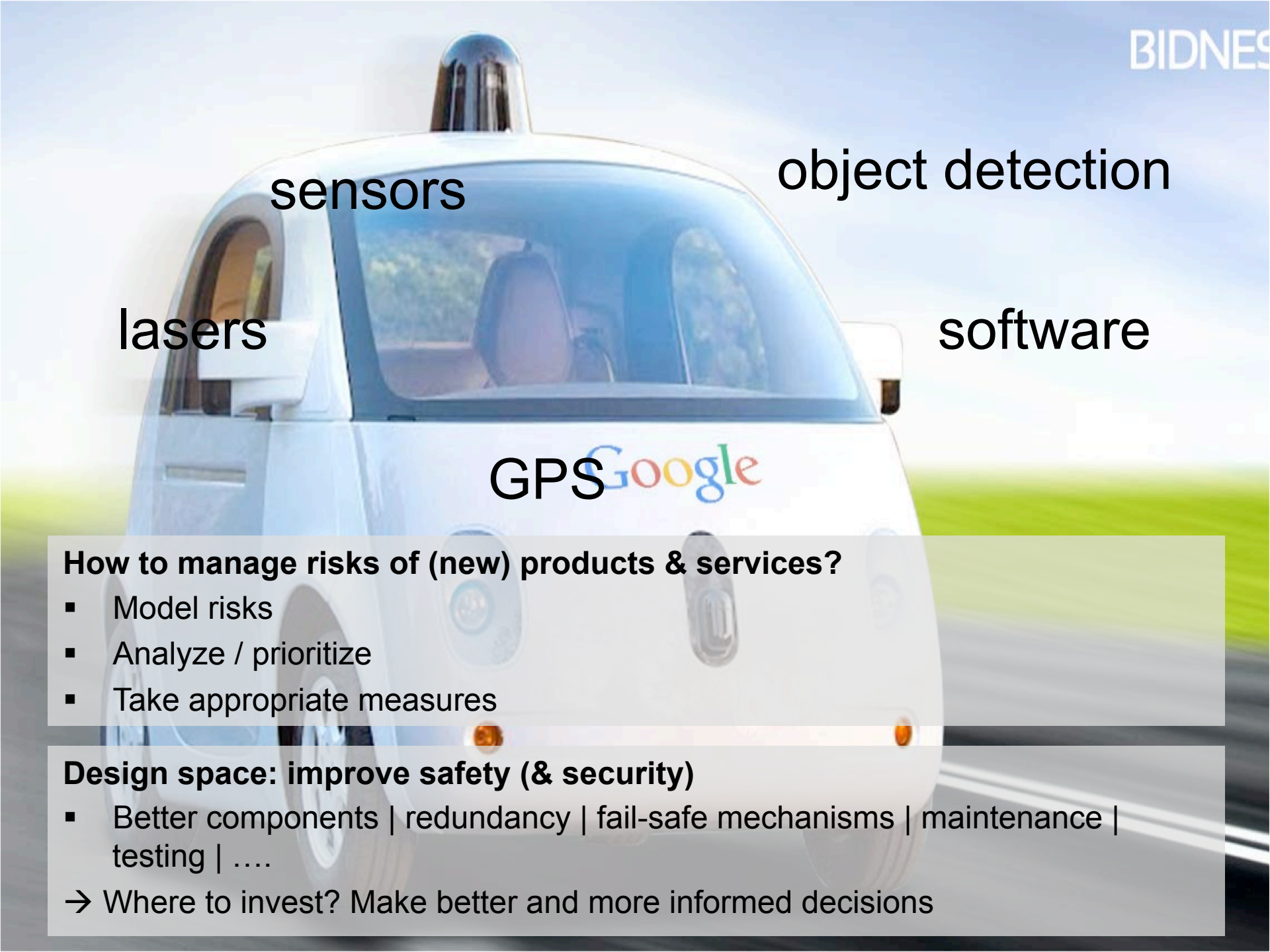


Marielle Stoelinga

Formal Methods & Tools




No risk, no fun



How to manage risks of (new) products & services?

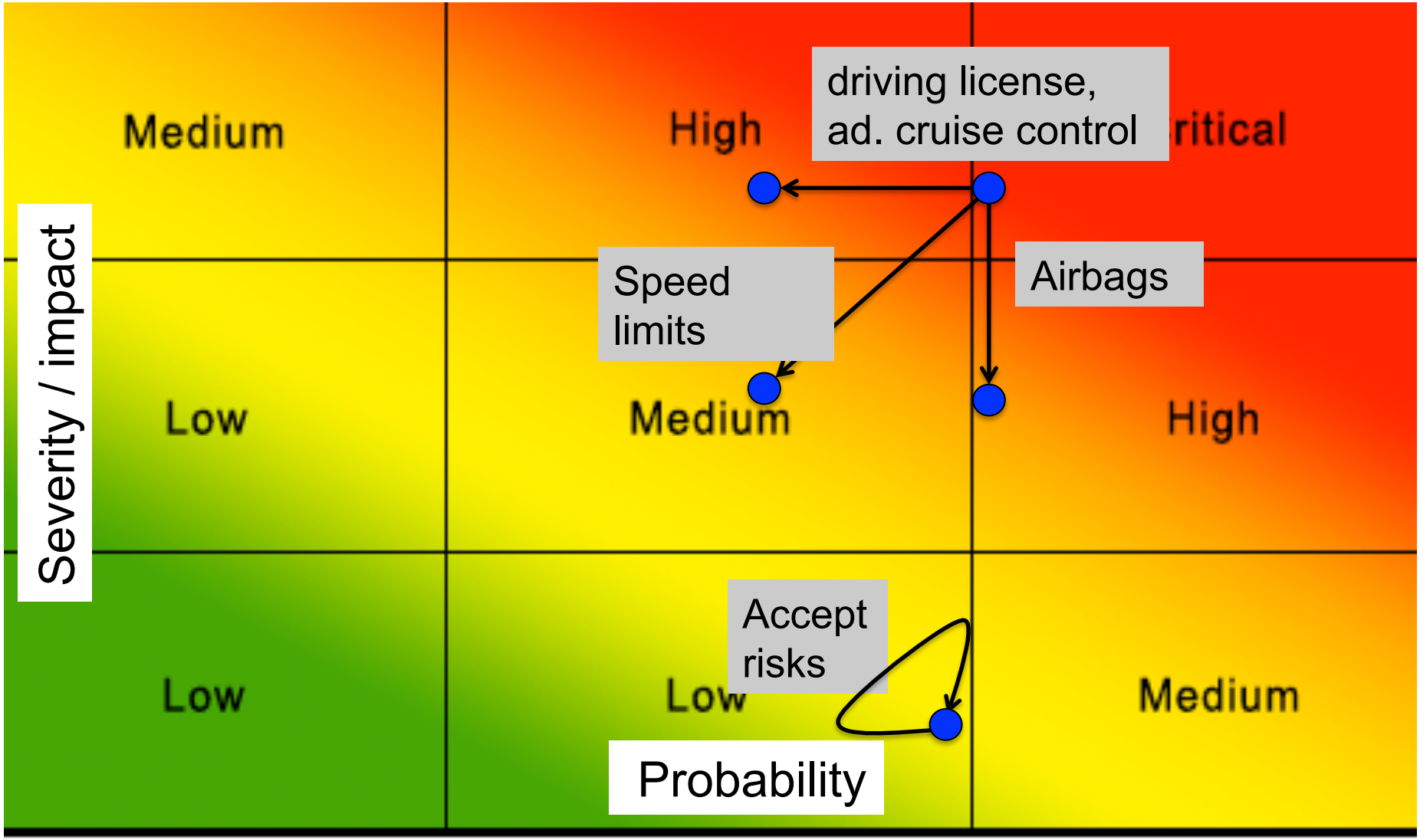
- Model risks
- Analyze / prioritize
- Take appropriate measures

Design space: improve safety (& security)

- Better components | redundancy | fail-safe mechanisms | maintenance | testing | ….

→ Where to invest? Make better and more informed decisions

Risk priority heat map



Risk management: engineering a safer world

Methods

- *Textual / spread sheets:*
  - Failure Mode, Effect and Criticality Analysis (FMECA; FMEA)
  - Hazard & operability study (Hazop)
- *Architectural (system / enterprise)*
  - UML/Marte
  - AADL: error annex
- *Domain-specific:*
  - Fault tree analysis (FTA)
  - Reliability block diagrams
  - Event trees

→ Goal: reduce risks to acceptable level

→ Risk assessment often mandatory

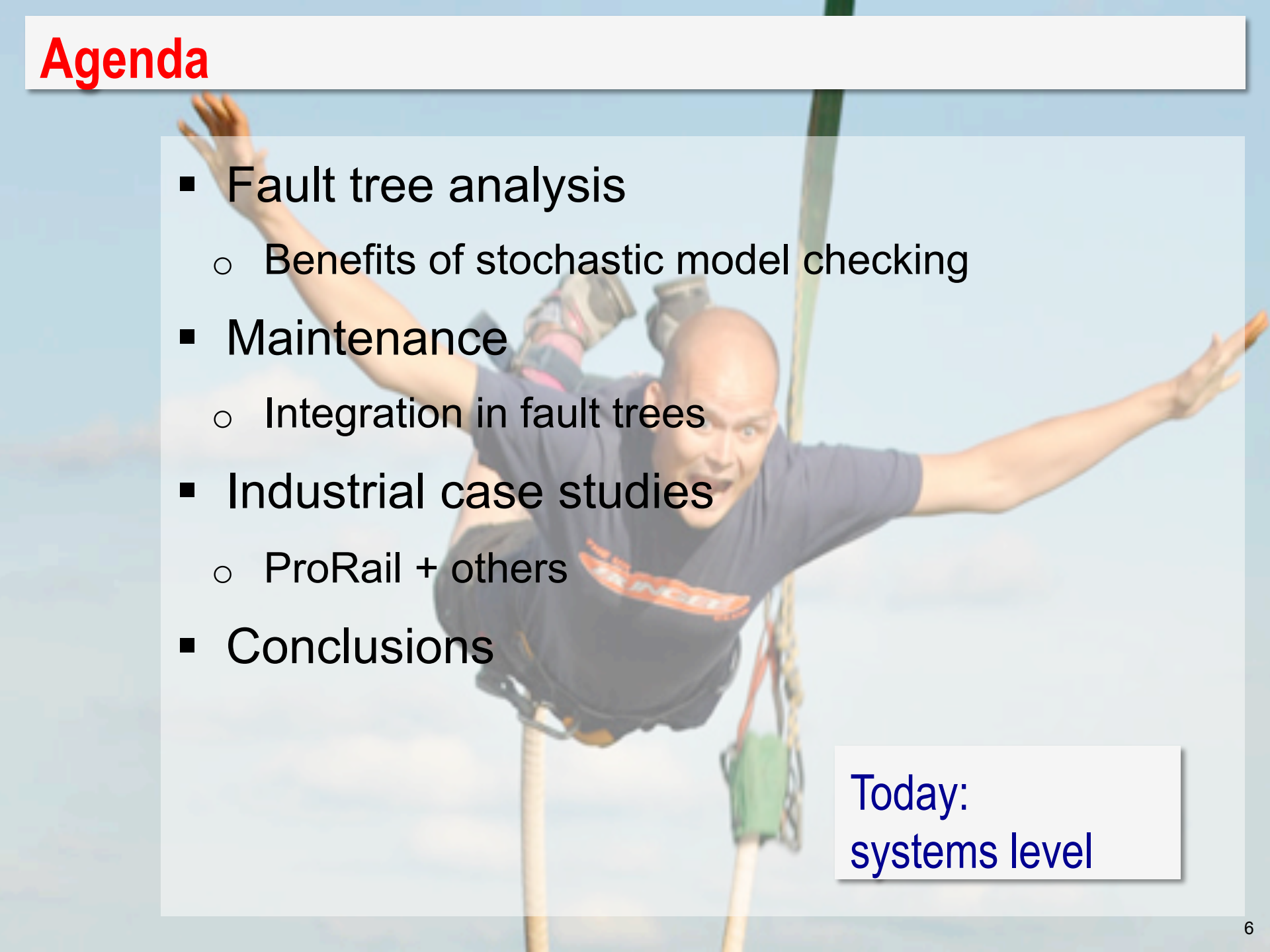
Standardization

- NRC NUREG–0492: nuclear
- SAE ARP4761: aerospace,
- IEC standard: 61025
- European NEN 61025.

Applications

- Products / systems: *data centers, rail roads, power plants, IoT …*
- Services & processes: *opening online bank account*

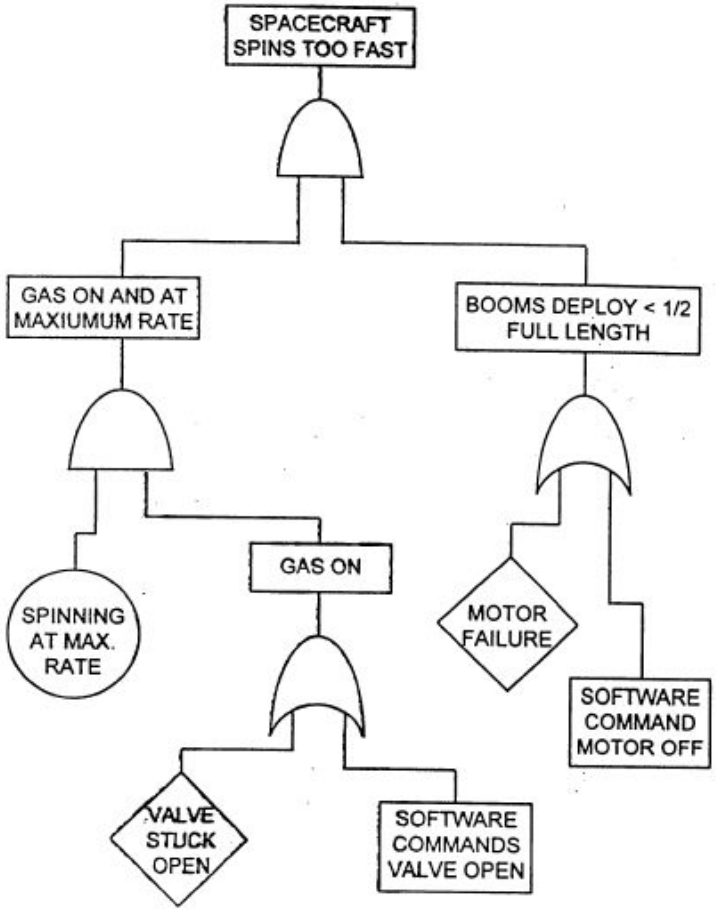
Agenda



- Fault tree analysis
  - Benefits of stochastic model checking
- Maintenance
  - Integration in fault trees
- Industrial case studies
  - ProRail + others
- Conclusions

Today:
systems level

Fault trees: what are they?

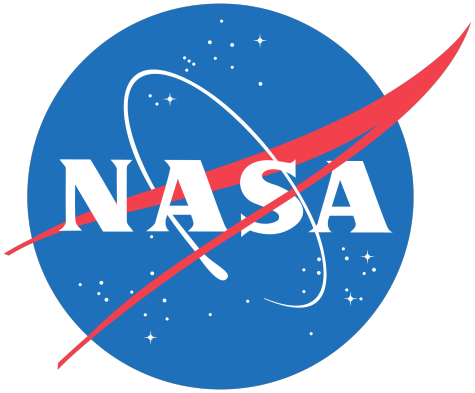


Preferred tool for RAMS

- *Graphical Model*
  - How do component failures propagate to system failures?
- *Qualitative Analysis*
  - *Pinpoint root causes and critical parts*
- *Quantitative Analysis*
  - Reliability: **P**[no failure during mission time]
  - Availability: **E**[up-time]
  - MTTF, MTBF, …..

fault trees: who uses them?

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu



FTA on twitter

- Falcon 7 rocked, SpaceX
- Led by Elon Musk, Tesla
- Ready for launch June 2015

Elon Musk @elonmusk · Jun 28

That's all we can say with confidence right now. Will have more to say following a thorough fault tree analysis.

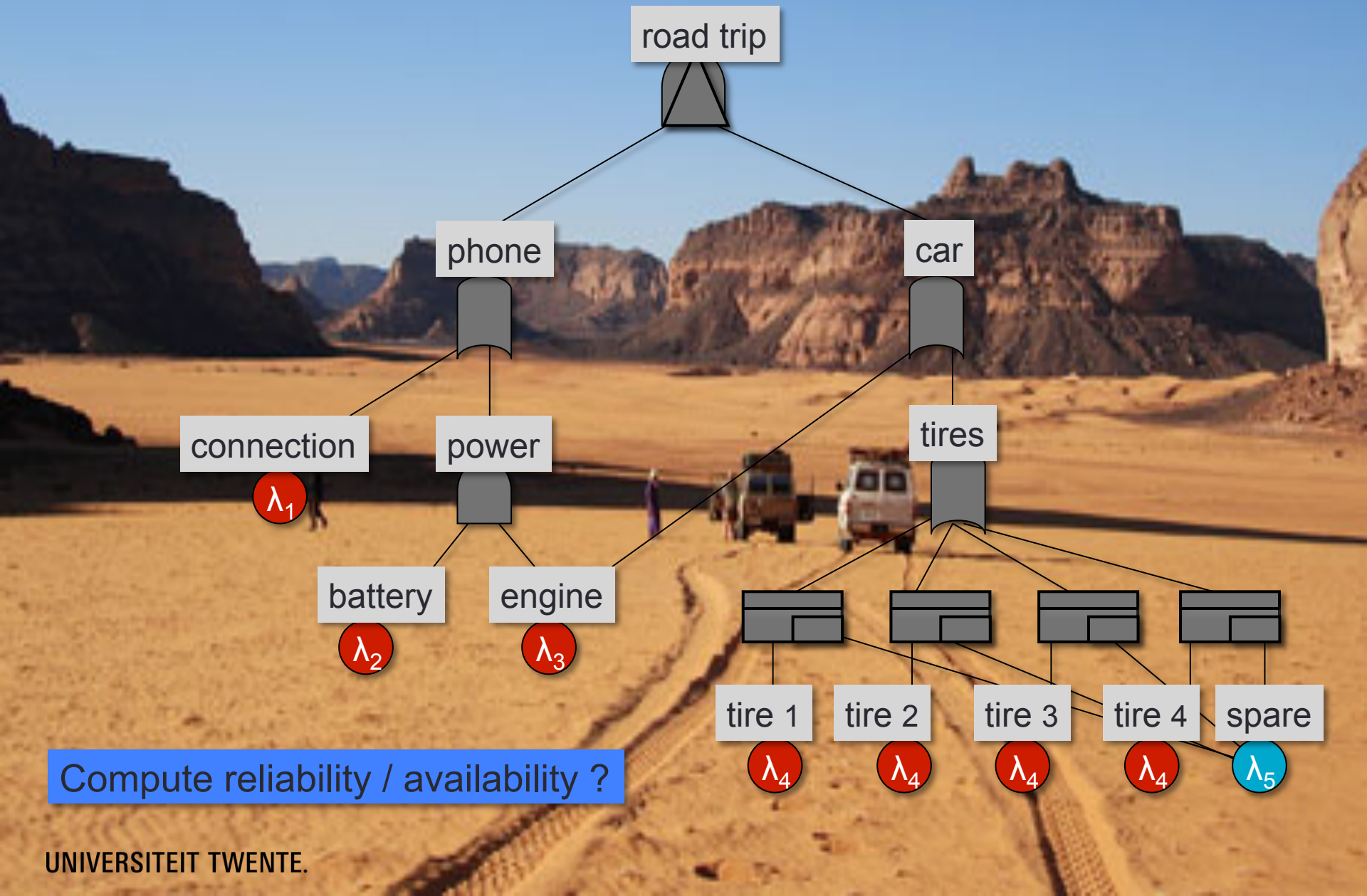
1.3K 1.9K View conversation

Elon Musk @elonmusk · Jun 28

There was an overpressure event in the upper stage liquid oxygen tank. Data suggests counterintuitive cause.

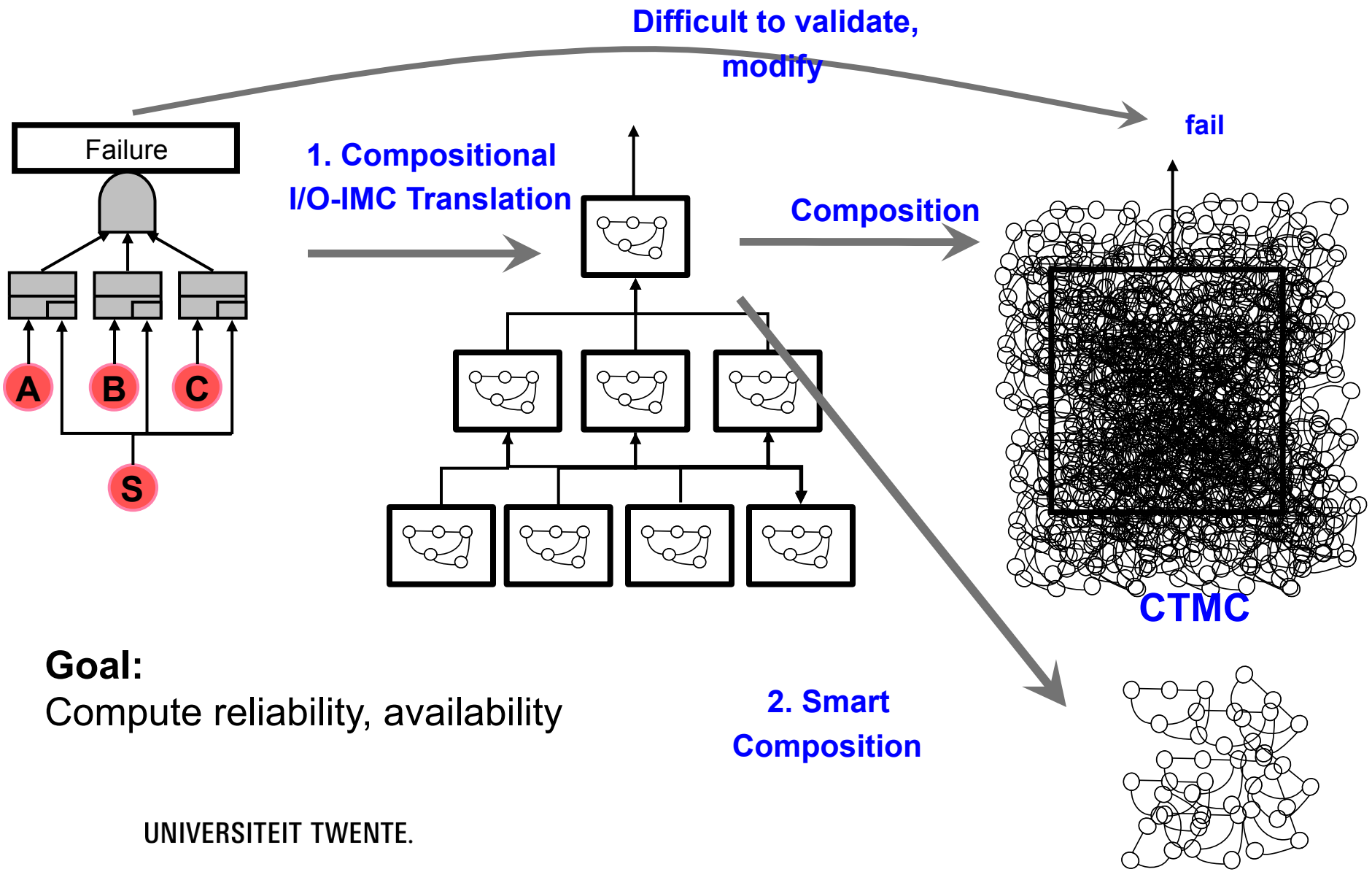
4.3K 3.3K

Example: Safe road trip



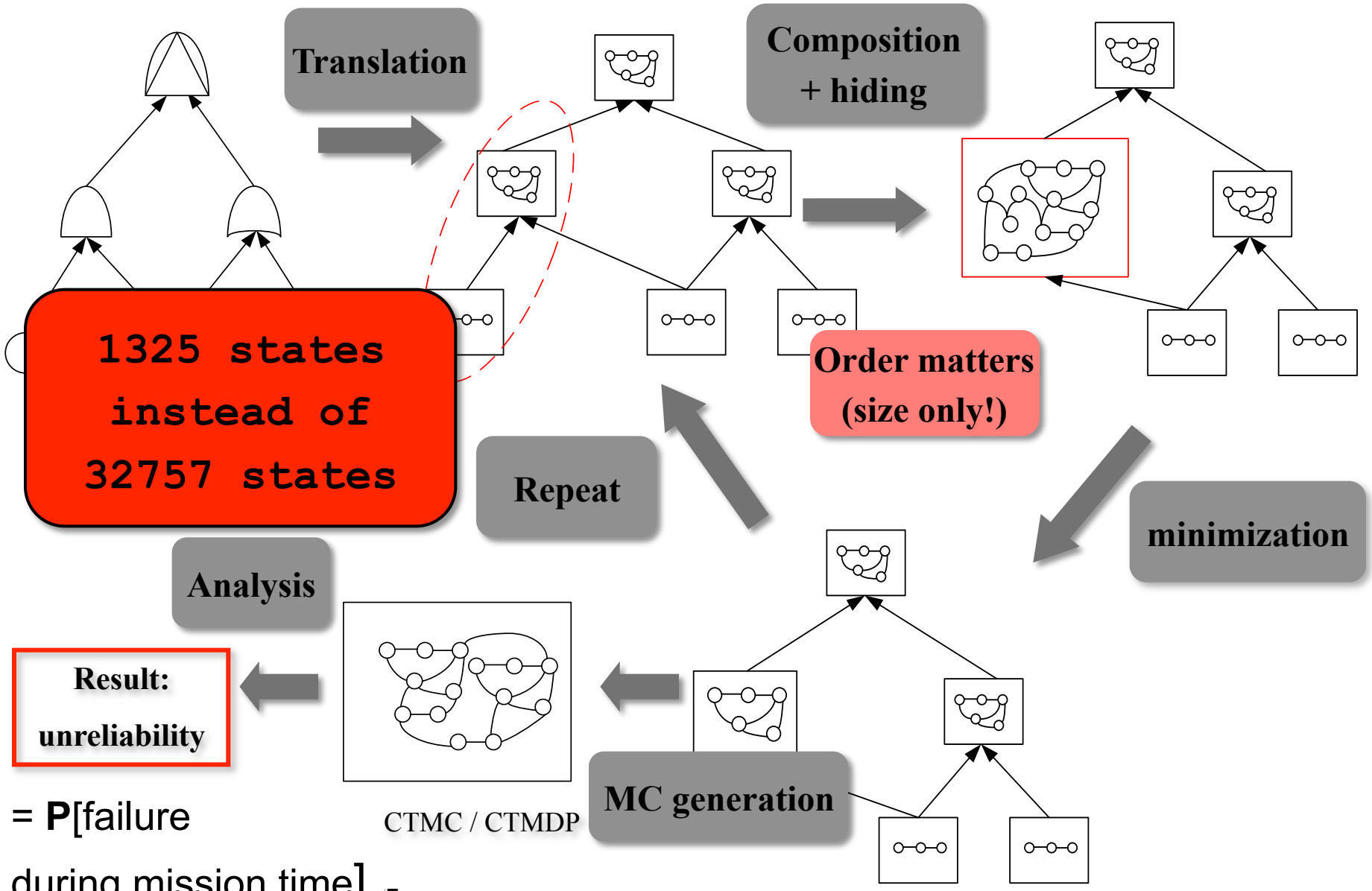
Compute reliability / availability ?

Fault tree analysis: how to compute reliability?



Goal:
Compute reliability, availability

Deep compositionality [IEEE TDSC'10]



= **P**[failure during mission time] E.

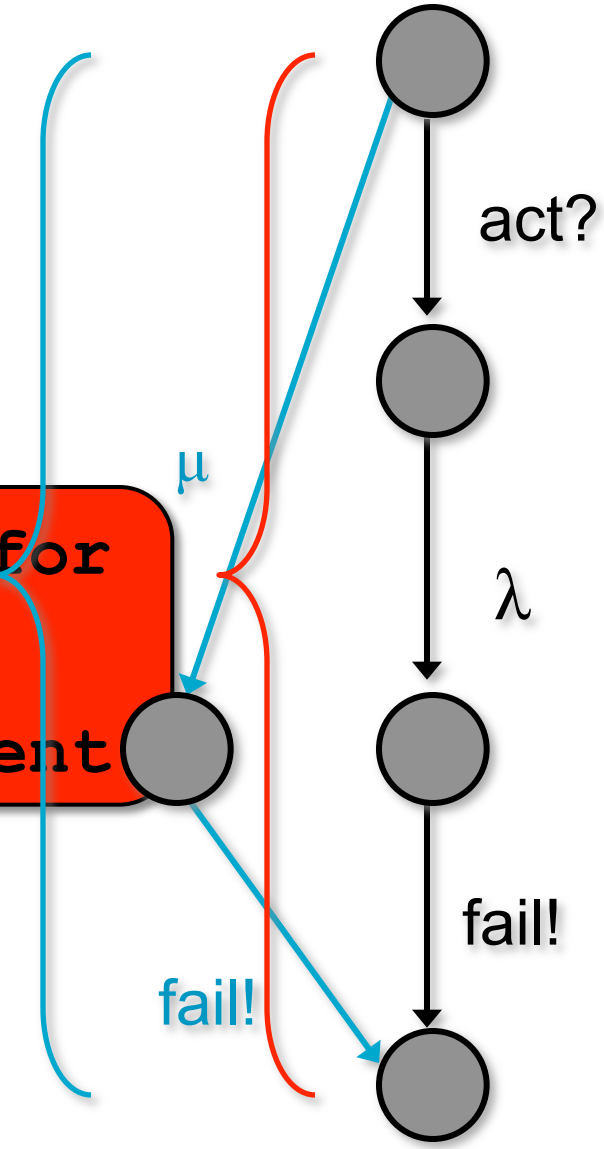
Interactive Markov Chains (I/O-IMC)

- I/O-Automata + CTMC
- Markovian transitions (CTMC)
  - labeled with rates λ
  - delays governed by exponential distribution
  - **P**[transitio
- Interactive
  - labeled wit
  - synchroniz
- Action signature
  - ? - Input actions: *delayable*
  - ! - Output actions: *immediate*
  - ; - Internal actions: *immediate*
- Compositional performance modeling

Warm BE: can fail before activation, with reduced rate

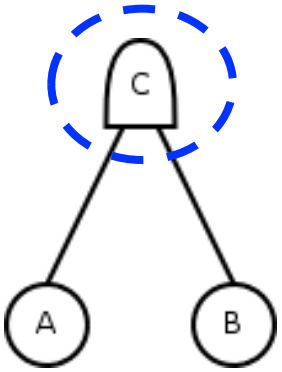
for

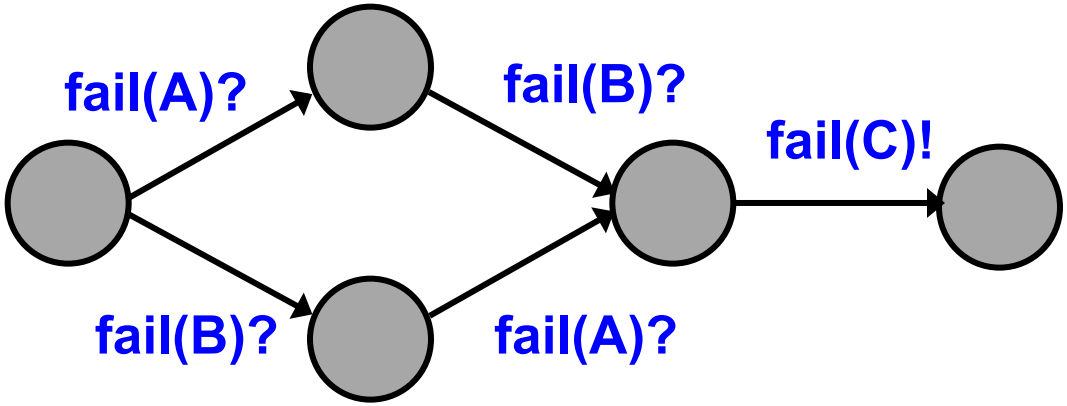
ent



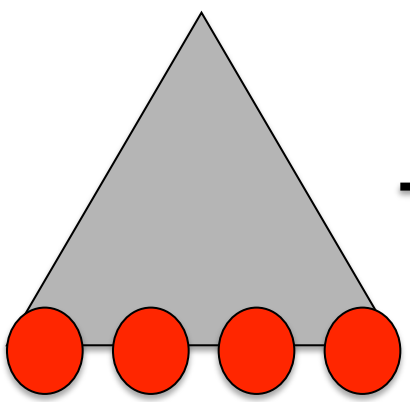
semantics for DFT gates

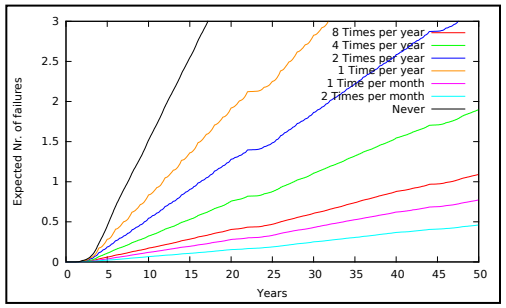
AND gate





Tool implementation: DFTcalc





Metrics

Results:
reliability
availability
costs
strategy
diagnostics, …

Agenda

- Fault tree analysis
  - Standard approaches
  - Benefits of stochastic model checking
- **Maintenance**
  - Integration in fault trees
- Industrial case studies
- Conclusions

Maintenance optimization via Fault Trees

Maintenance

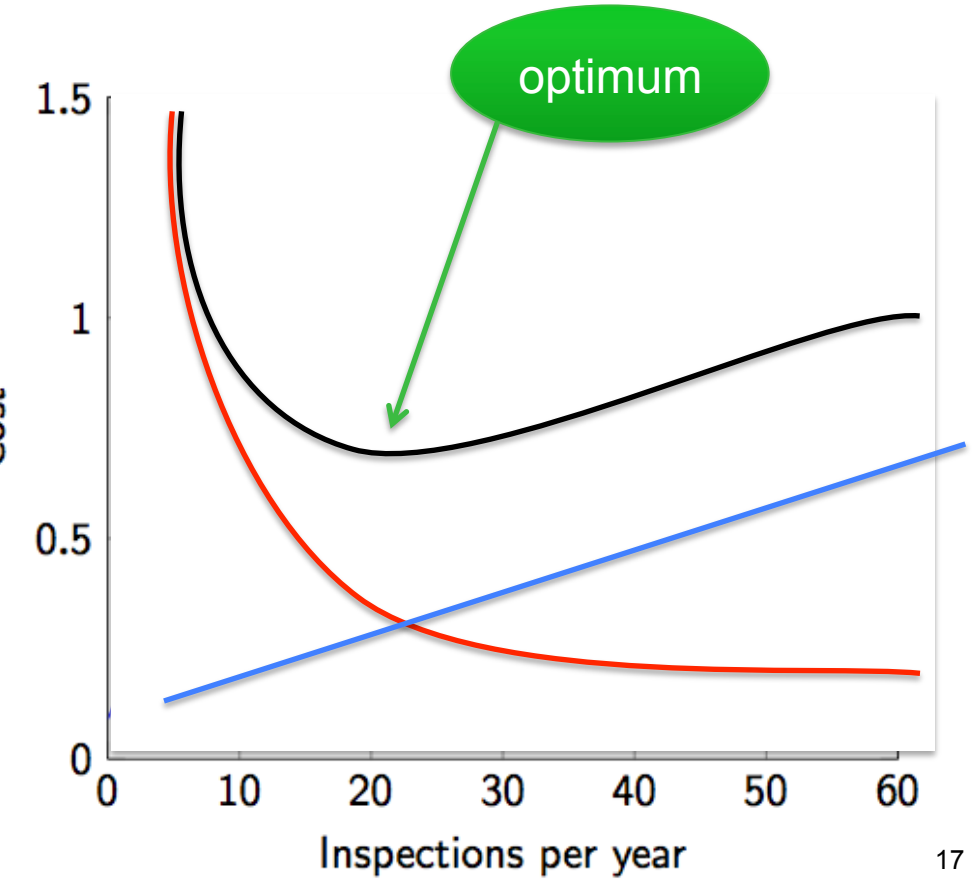
- **Crucial:** Large impact on reliability / availability / life span
- **Costly:** labour / equipment / unplanned down time

Optimize

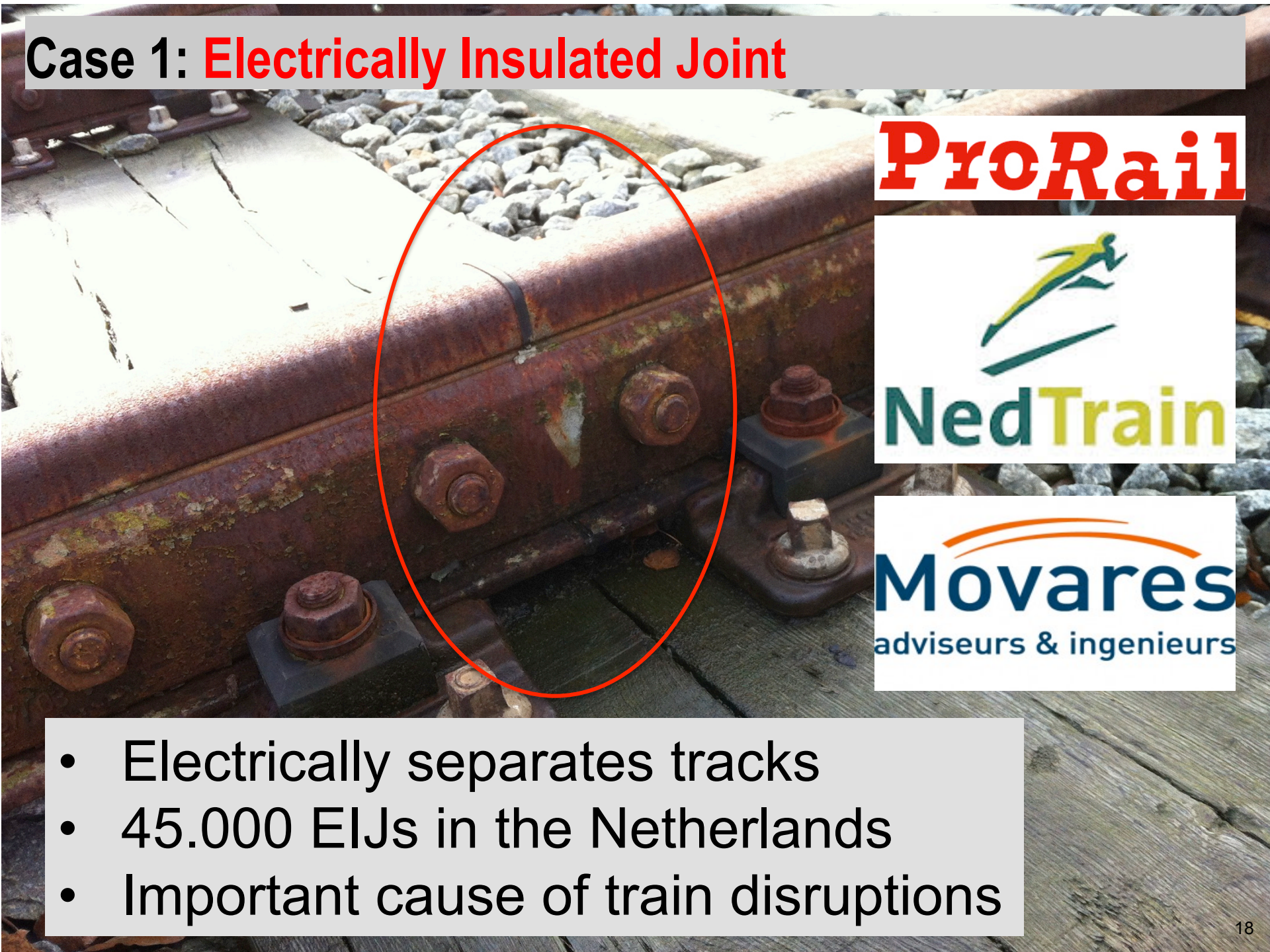
- Performance benefits
  → fault trees
- Maintenance cost
  → in leaves

Goal

Decision support for cost-effective maintenance



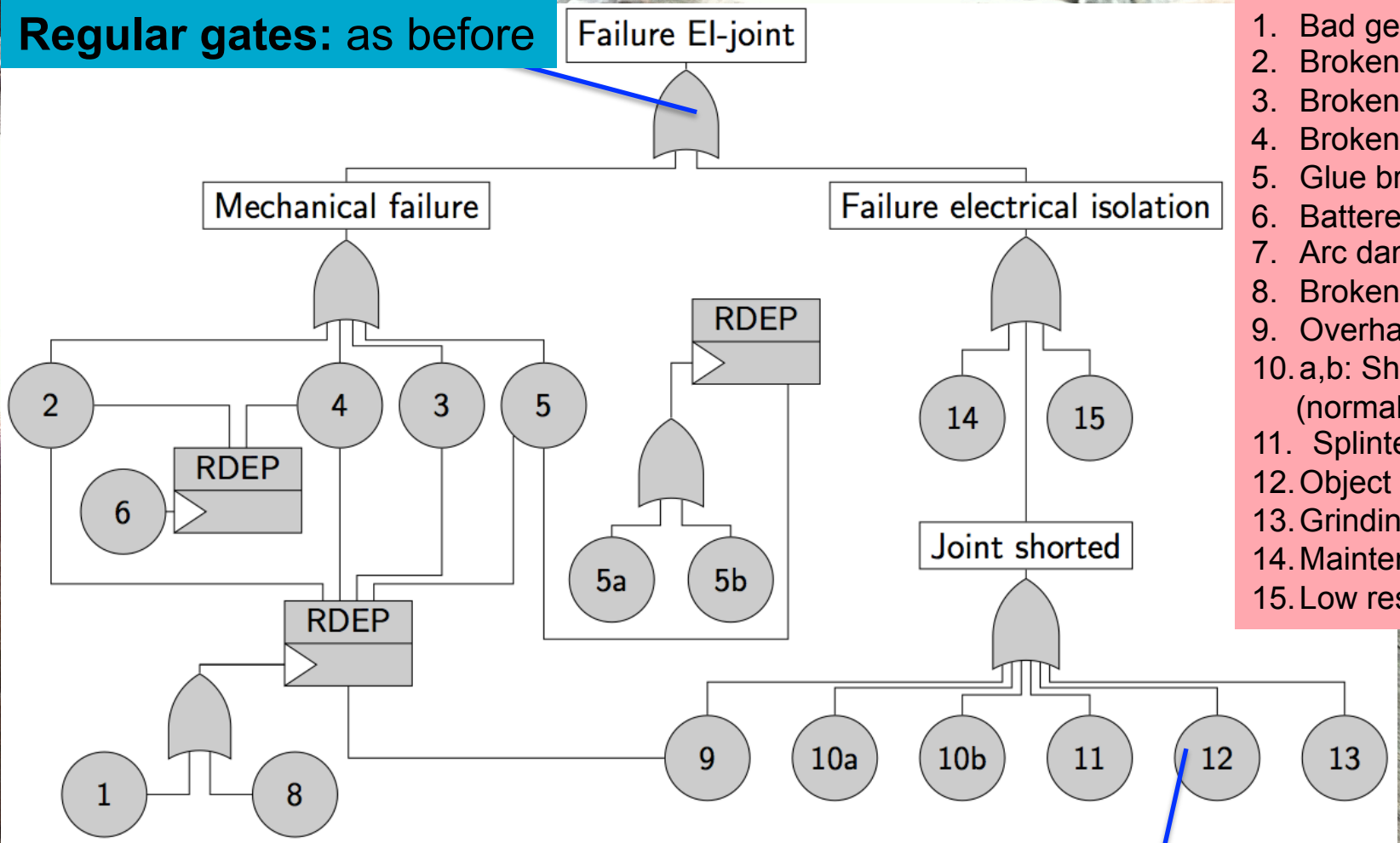
Case 1: Electrically Insulated Joint



- Electrically separates tracks
- 45.000 EIJs in the Netherlands
- Important cause of train disruptions

El joint: modeling

Regular gates: as before

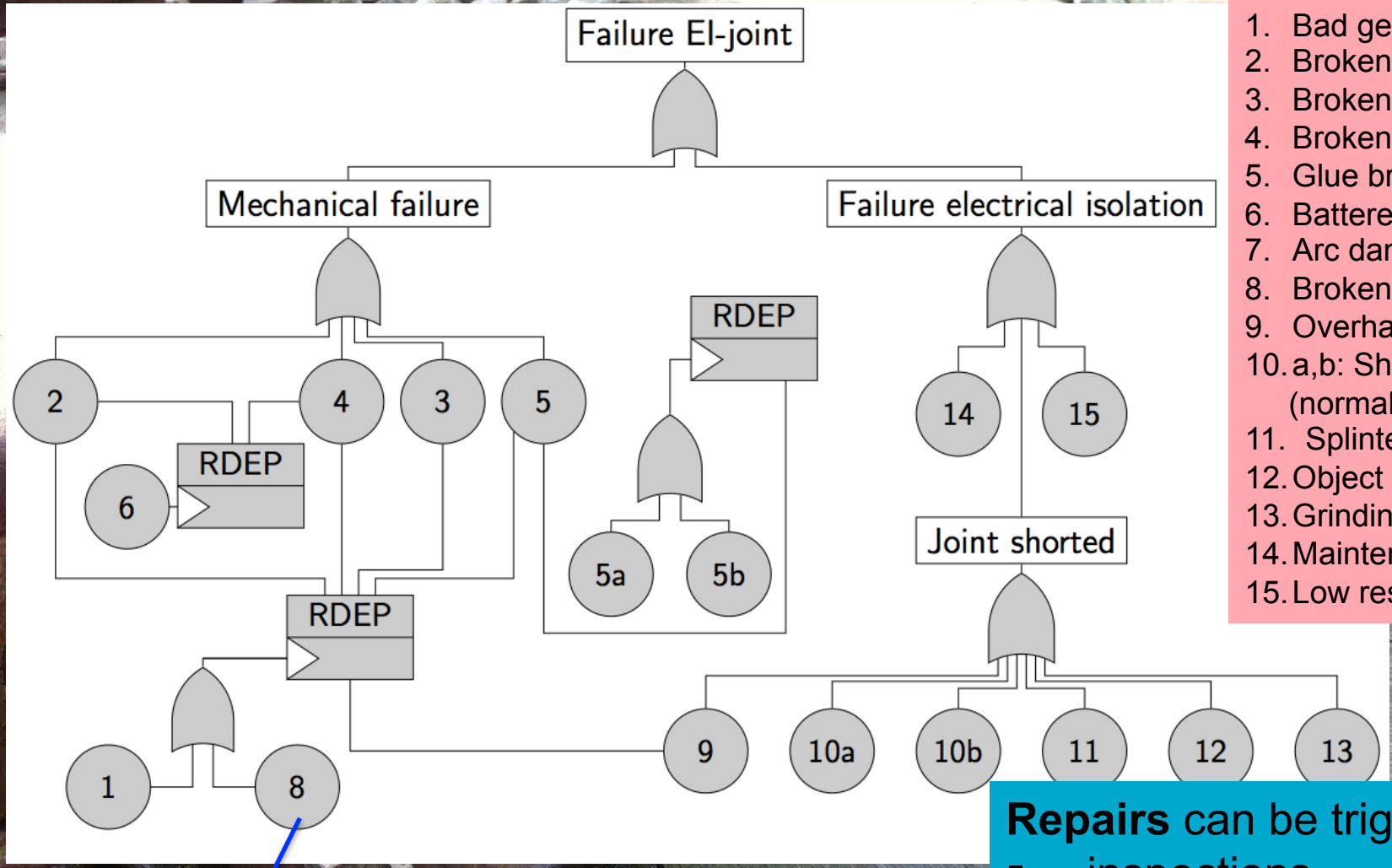


1. Bad geometry
2. Broken fishplate
3. Broken bold
4. Broken rail head
5. Glue broken
6. Battered head
7. Arc damage
8. Broken end plate
9. Overhang
10. a,b: Shavings (normal/ coated)
11. Splinters
12. Object
13. Grinding
14. Maintenance
15. Low resistance

new BEs: maintenance

- Constructed from ProRail's FMECA
- Connected to failure database

El joint: modeling



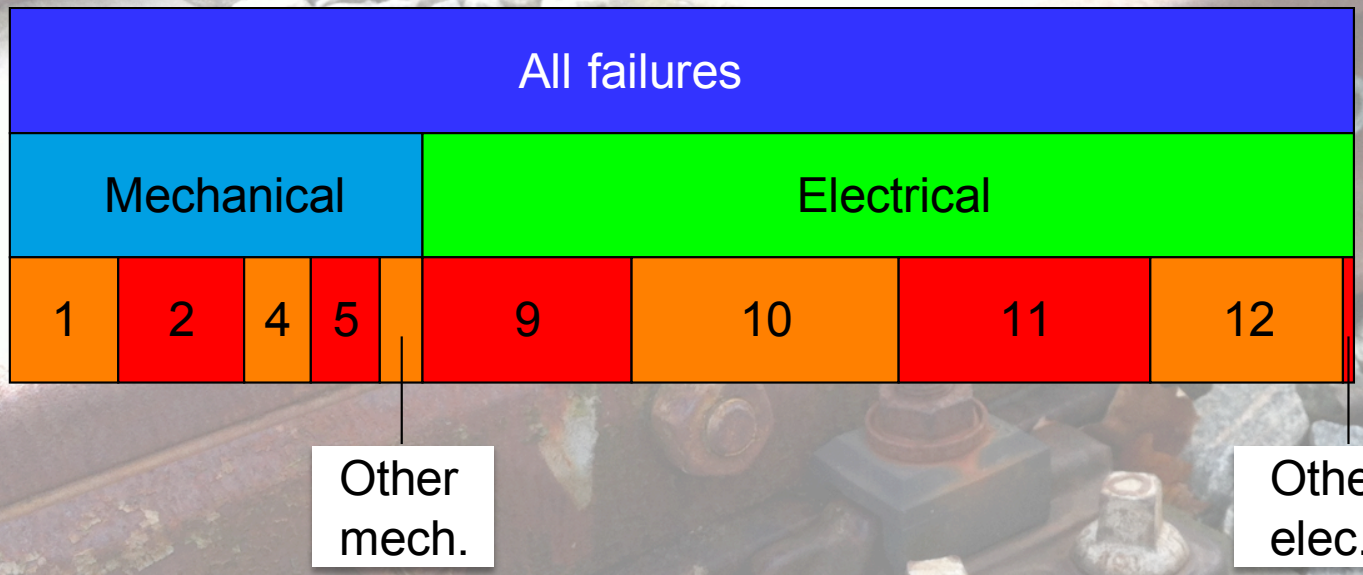
1. Bad geometry
2. Broken fishplate
3. Broken bold
4. Broken rail head
5. Glue broken
6. Battered head
7. Arc damage
8. Broken end plate
9. Overhang
10. a,b: Shavings (normal/ coated)
11. Splinters
12. Object
13. Grinding
14. Maintenance
15. Low resistance

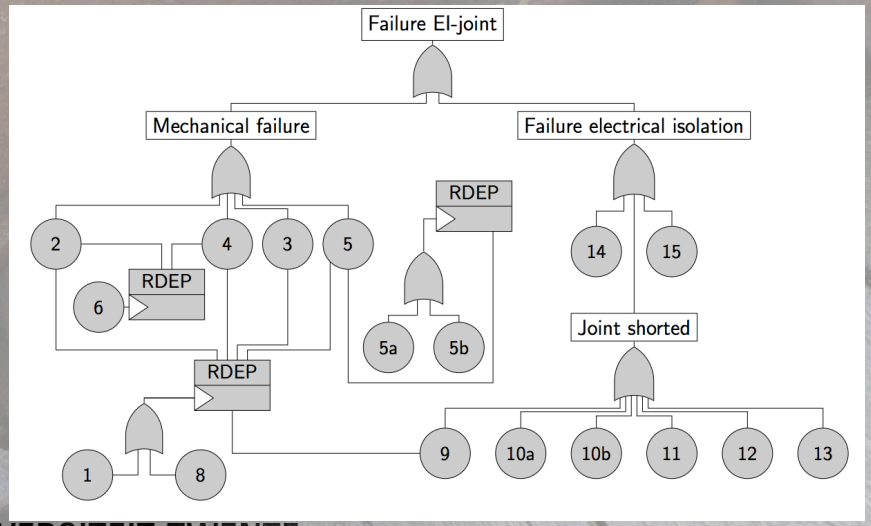
new BEs: maintenance

Inspections
fixed frequency

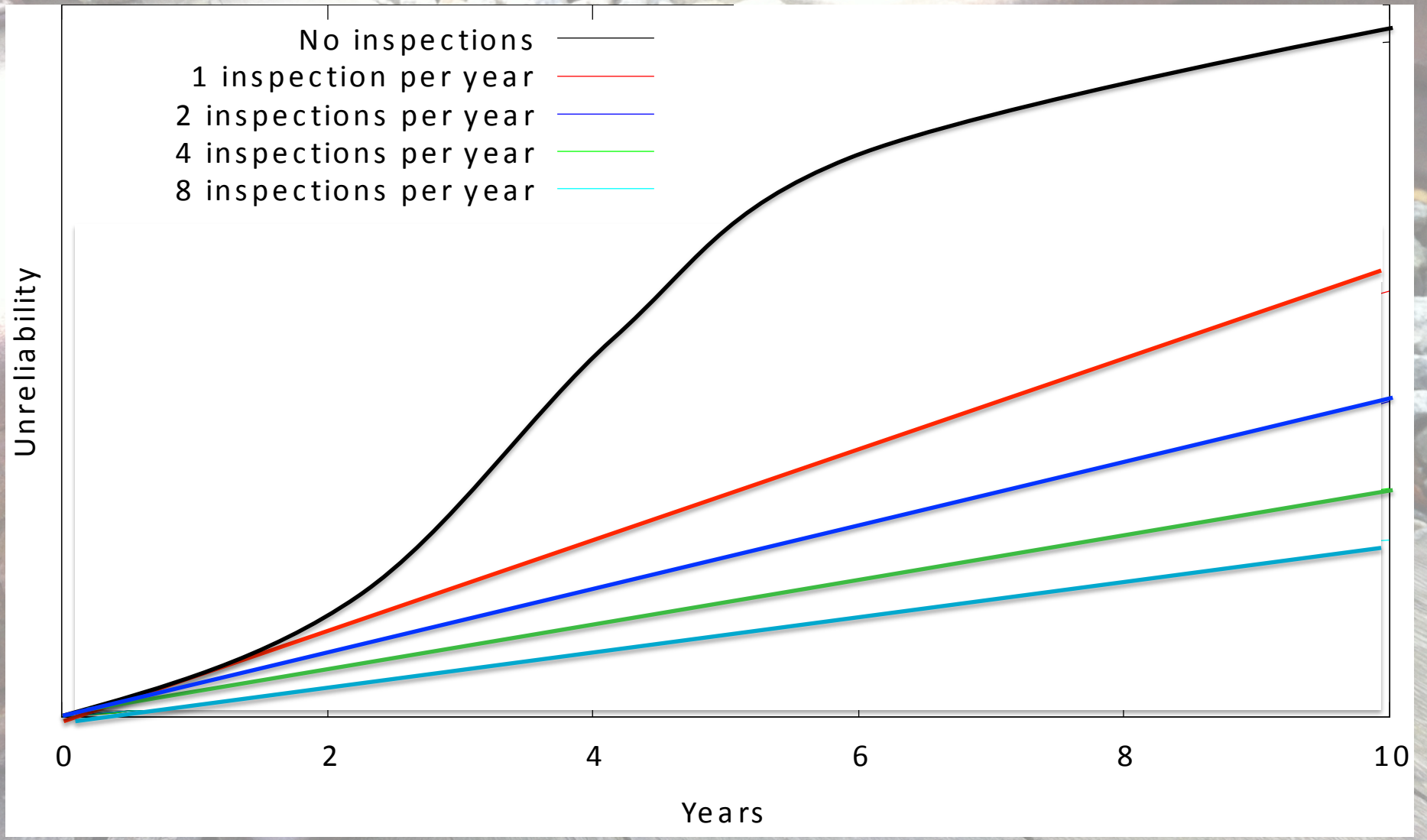
Repairs can be triggered by
- inspections
- other repairs
- failures
- periodic

Electrically Insulated Joint: failure causes

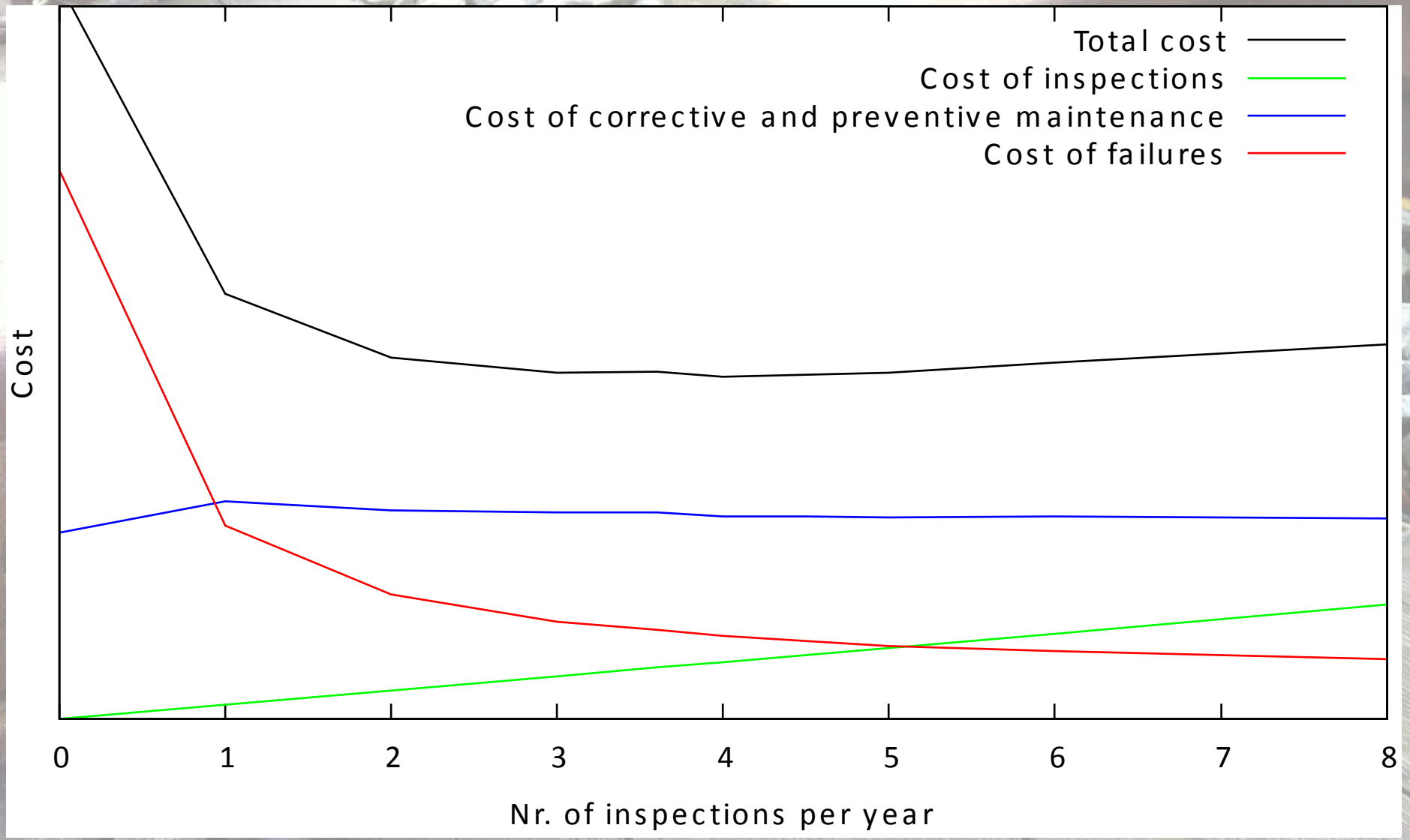




Results: unreliability



Results: price / performance



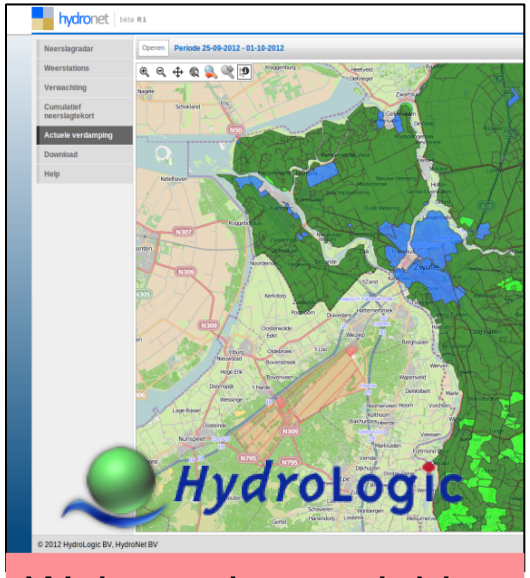
New joint type: NRG joint vs current joints

Same analysis for NGR joint:

- NRG joint is cost-effective
- More sensitive to variations in maintenance policy

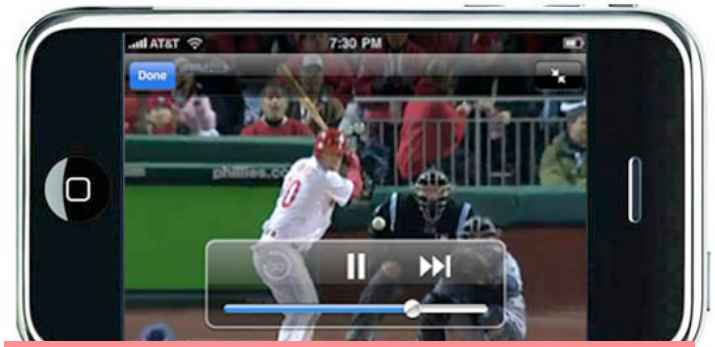
More software: other cases

Cardiac assist system reliable enough?

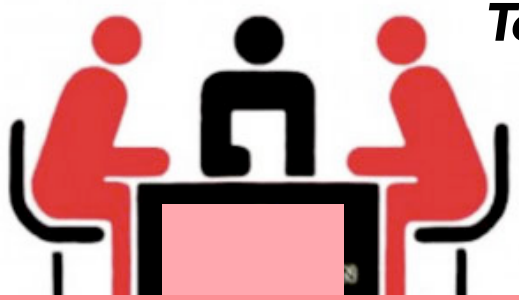


Web service scalable enough?

E-payment secure enough?



Reduce energy in streaming applications?



Tech4people

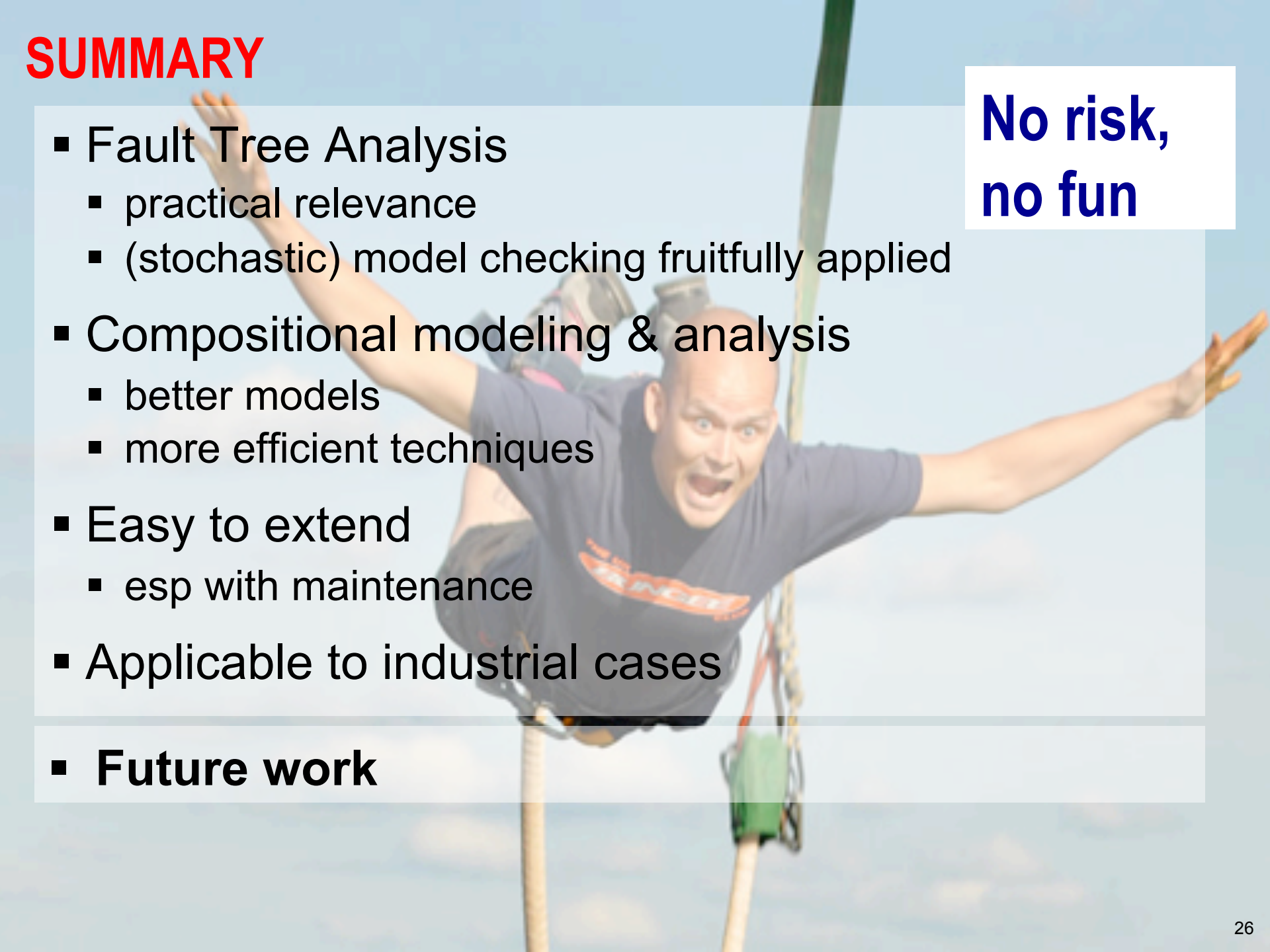
Risks in digital victim-offender mediation: with FTs

SUMMARY

- Fault Tree Analysis
  - practical relevance
  - (stochastic) model checking fruitfully applied
- Compositional modeling & analysis
  - better models
  - more efficient techniques
- Easy to extend
  - esp with maintenance
- Applicable to industrial cases

No risk, no fun

- **Future work**



FUTURE WORK

Fault trees + big data analytics

- understand failure causes better
- Fault trees provide domain knowledge

Hiring:

2 PhD students

https://www.utwente.nl/en/organization/careers/vacancies/!/vacature/888350