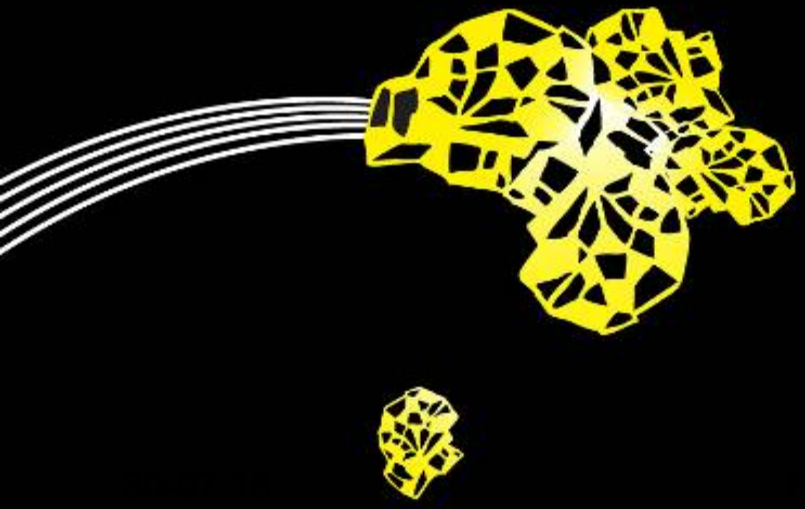
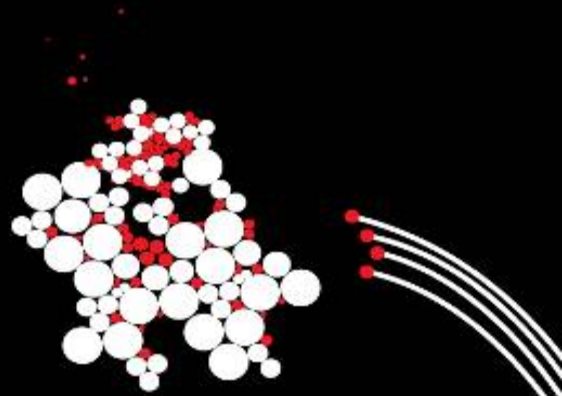
UNIVERSITEIT TWENTE.

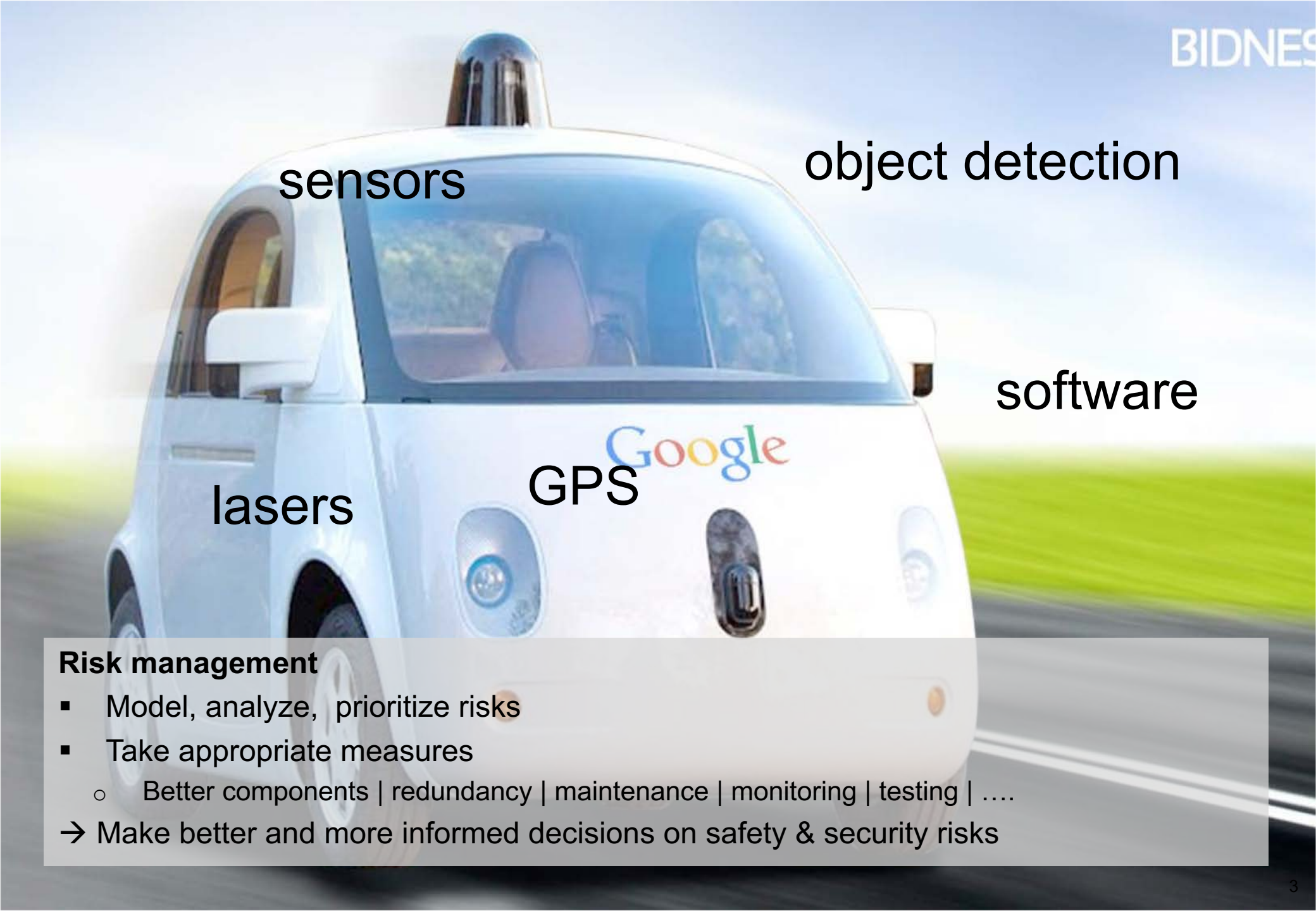




Risk happens
--- and model checking can help

Mariëlle Stoelinga
Formal Methods & Tools

No risk,
no fun



Risk management

- Model, analyze, prioritize risks
- Take appropriate measures
  - Better components | redundancy | maintenance | monitoring | testing | ….

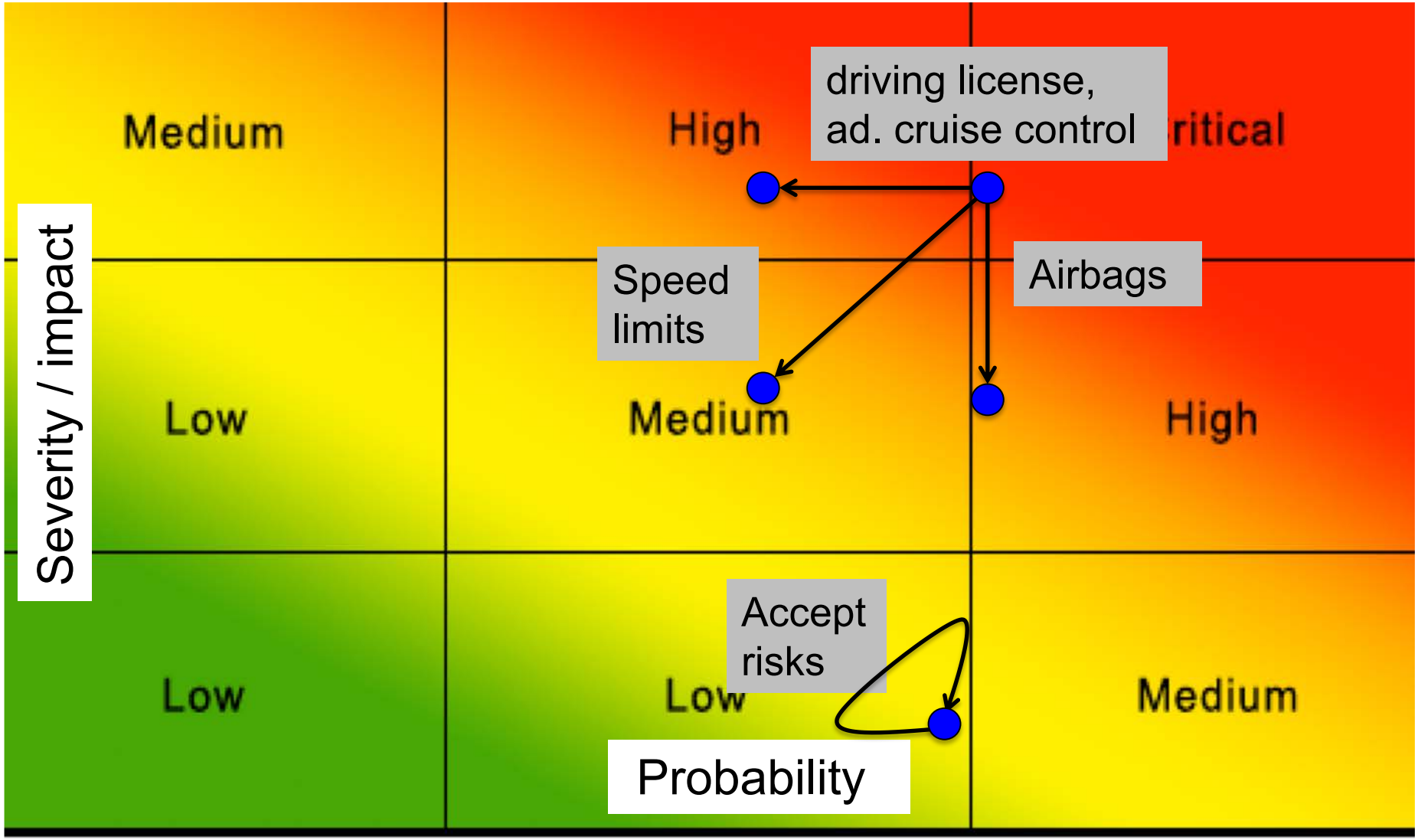
→ Make better and more informed decisions on safety & security risks

If you are Google you will …

- Hire brightest programmers & engineers
- Use state-of-art SW engineering methods
  - Model-driven development
  - Model checking
  - Rigorous (model-based) testing
  - SCRUM
  - Continuous delivery / deployment

- **Is this enough?**
  - Need more redundant sensors?
  - Better object identification algorithms?
  - More communication channels?
  - Monitors?
  - More maintenance / inspections

Risk priority heat map



Risk management: engineering a safer world

Methods

- *Informal / Spread sheets:*
  - Failure Mode, Effect and Criticality Analysis (FMECA)
  - Hazard & operability study (Hazop)
- *Architectural:*
  - UML/Marte,
  - AADL
- *Domain-specific:*
  - Fault tree analysis
  - Reliability block diagrams,
  - Event trees

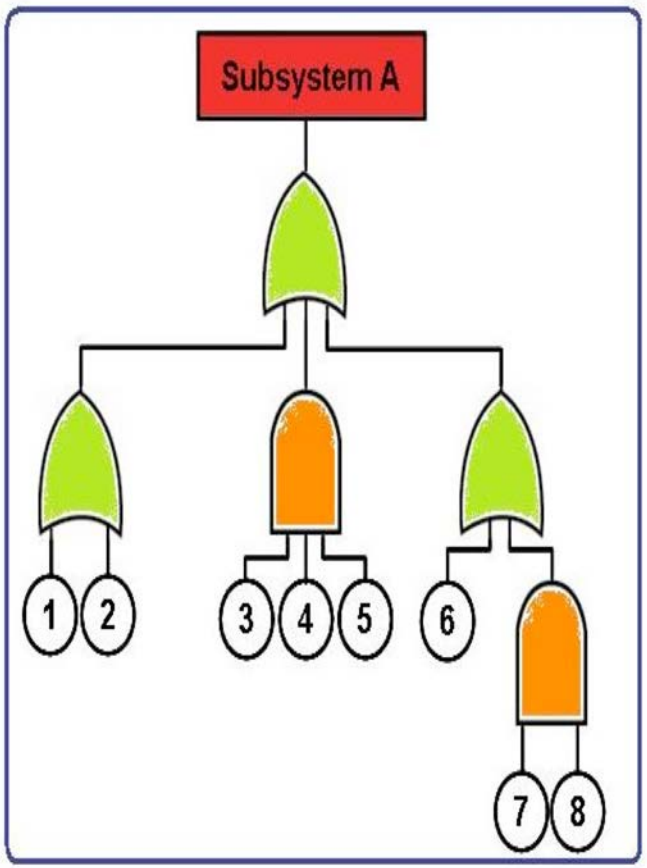
Standardization

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

→ Formal Methods can help!

→ Risk assessment often mandatory

Fault trees: what are they?



Tool in reliability engineering

- *Graphical Model*
  - Tell how systems fail:
  - How do component failures lead to system failures?
- *Qualitative Analysis*
  - *Pinpoint root causes / critical parts*
- *Quantitative Analysis: metrics*
  - Reliability: **P**[no failure during mission time]
  - Availability: **E**[up-time]
  - MTTF
  - …

Note

- Industrial software tools available
- State-of-art overwiew, > 150 FT papers

Fault trees: who uses them?

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

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cosrev

ELSEVIER

Computer Science Review

Survey

Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools

*Enno Ruijters**, *Mariëlle Stoelinga*

Formal Methods and Tools, University of Twente, The Netherlands

ARTICLE INFO

Article history:
Received 2 December 2014
Received in revised form
22 March 2015
Accepted 28 March 2015
Published online 5 May 2015

Keywords:
Fault trees
Reliability
Risk analysis

ABSTRACT

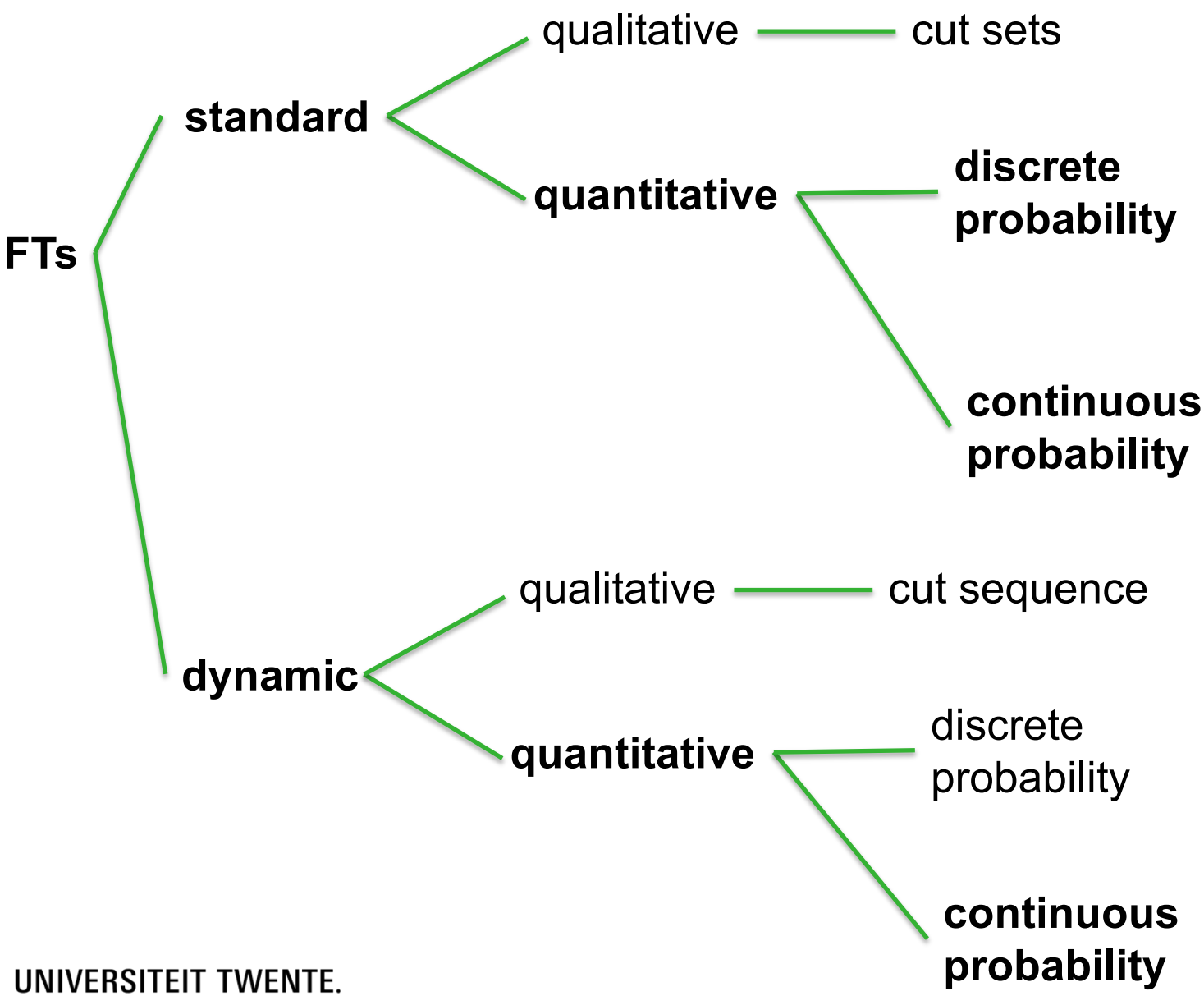
Fault tree analysis (FTA) is a very prominent method to analyze the risks related to safety and economically critical assets, like power plants, airplanes, data centers and web shops. FTA methods comprise of a wide variety of modeling and analysis techniques, supported by a wide range of software tools. This paper surveys over 150 papers on fault tree analysis, providing an in-depth overview of the state-of-the-art in FTA. Concretely, we review standard fault trees, as well as extensions such as dynamic FT, repairable FT, and extended FT. For these models, we review both qualitative analysis methods, like cut sets and common cause failures, and quantitative techniques, including a wide variety of stochastic methods to compute failure probabilities. Numerous examples illustrate the various approaches, and tables present a quick overview of results.

© 2015 Elsevier Inc. All rights reserved.

Today's Goals

- Learn about Fault Tree Analysis
- Show how Formal Methods can be used to analyze & improve industrial formalisms
- Exploiting
  - model checking
  - semantics
  - compositionality
  - BDDs
  - stochastic model checking
  - … and your own favorite method!
- … and Fun!

OVERVIEW

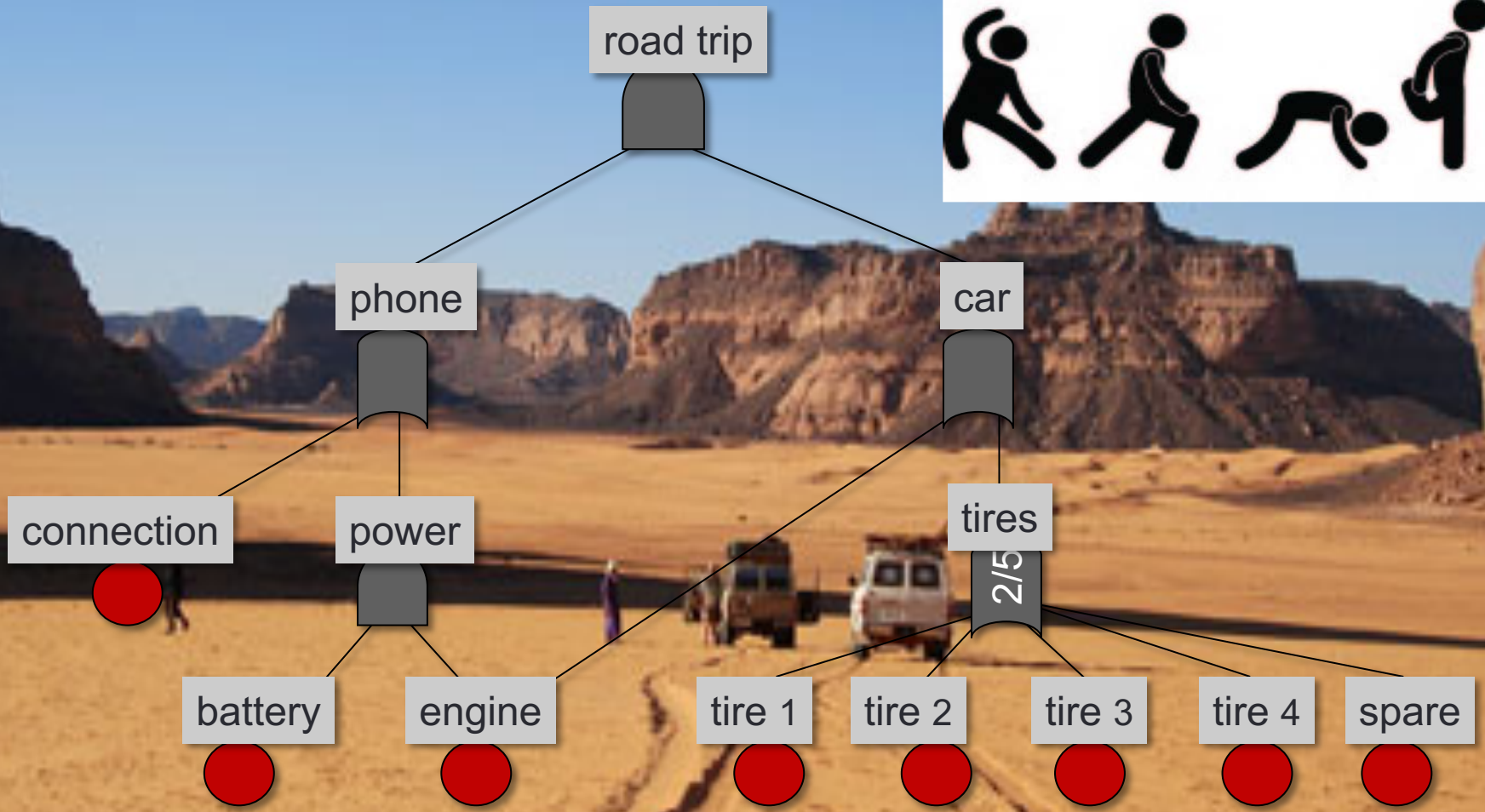

FTs
standard
qualitative
cut sets
quantitative
discrete probability
continuous probability
dynamic
qualitative
cut sequence
quantitative
discrete probability
continuous probability

FAULT TREES

Note: related to Attack Trees in security

NTE.

Example: Safe road trip



Cut sets: Which BEs make FT fail?

{battery, engine, tire 1, spare}

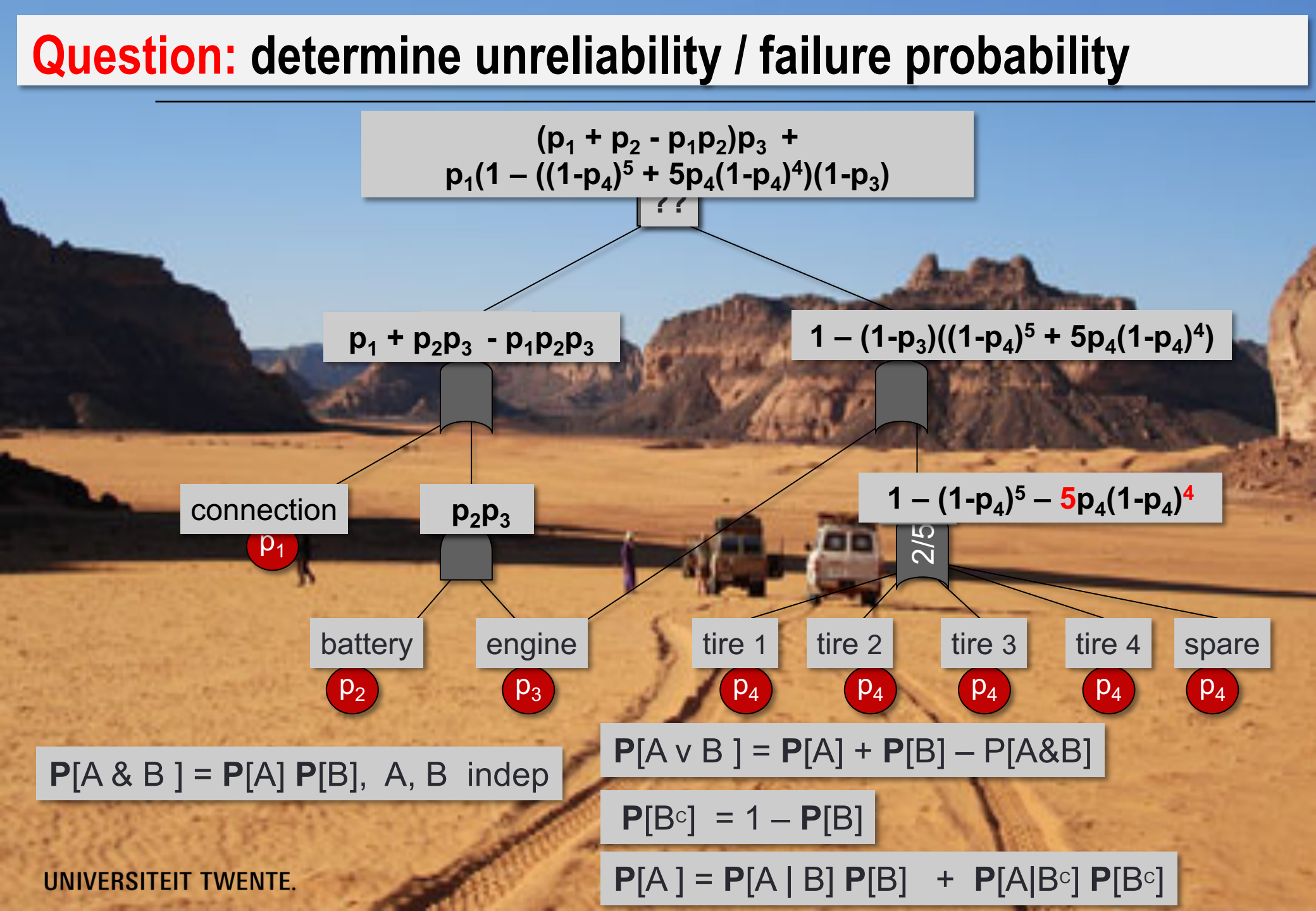
{engine, tire 1, spare} **minimal cut set**

{no connection, engine} **minimal cut set**

How to determine system reliability?

= probability of no failure during mission time

Question: determine unreliability / failure probability

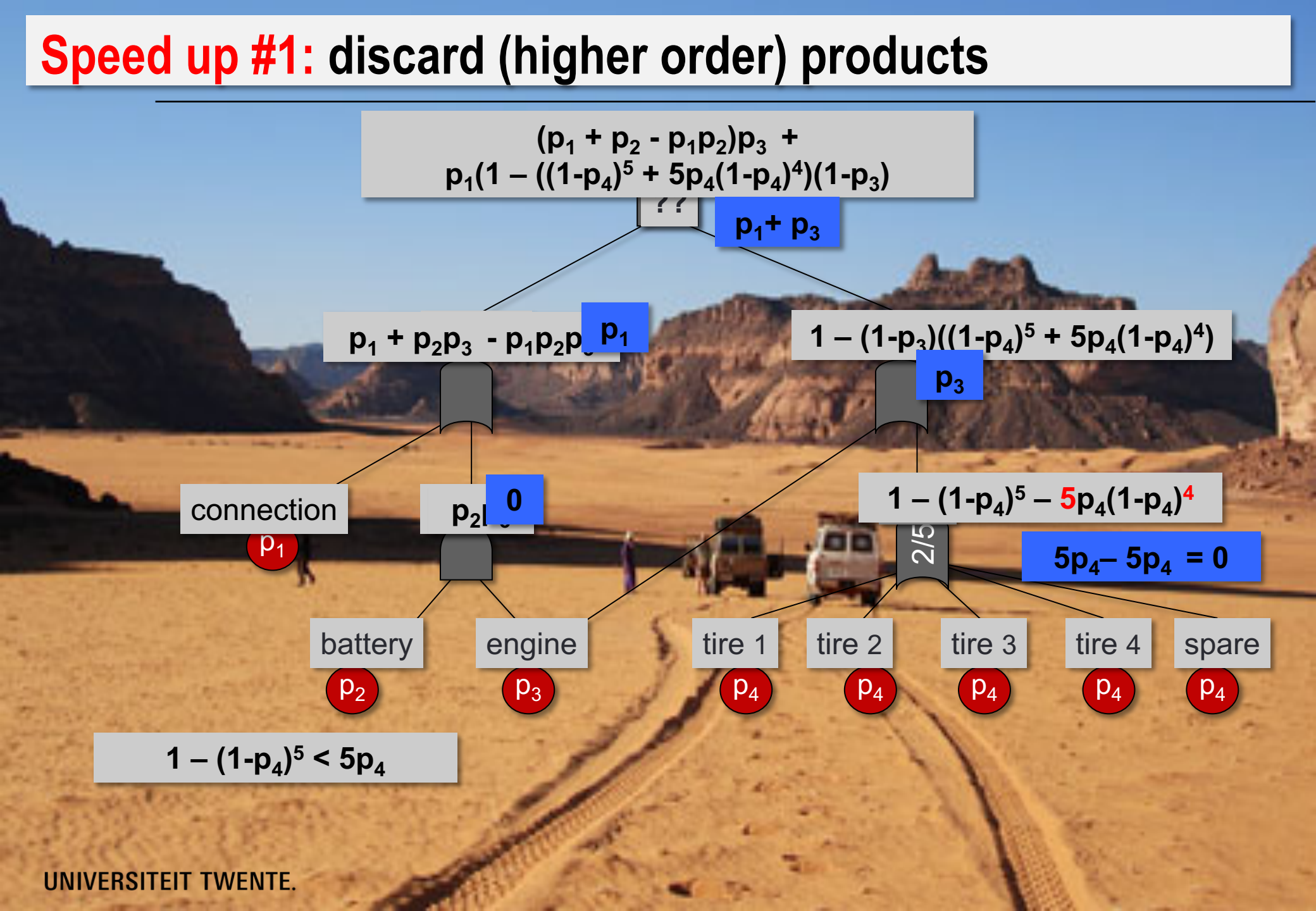


Find 3 ways to speed up this computation

Simplify the computation

1. Disregard higher order products
2. Use minimal cut sets
3. Combine 1 & 2
4. Use BDDs

Speed up #1: discard (higher order) products

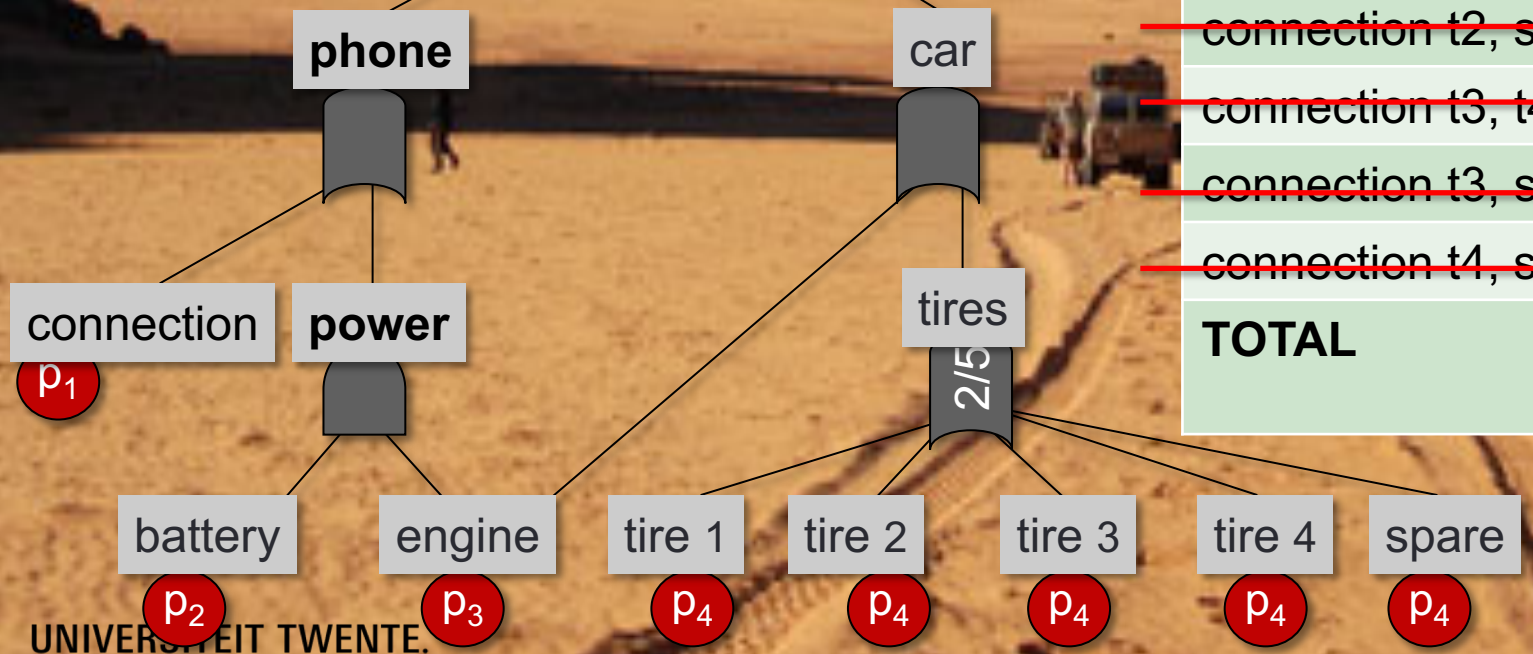


Speed up #2 & 3: Using cut sets

Under- or overapproximation? Why?

$P[C_1 \vee C_2 \vee C_3] = P[C_1] + P[C_2] + P[C_3] - P[C_1]P[C_2] - P[C_1]P[C_2] - P[C_2]P[C_2] + P[C_1]\,P[C_2]\,P[C_3] \leq P[C_1 \vee C_2 \vee C_3] = P[C_1] + P[C_2] + P[C_3]$

$p_1(1 - ((1-p_4)^5 + 5p_4(1-p_4)^4)(1-p_3)$



Min cut set	prob
connection, engine	$p_1 * p_3$
battery, engine	$p_2 * p_3$
~~connection, t1, t2~~	~~$p_1 * p_4^2$~~
~~connection, t1, t3~~	~~$p_1 * p_4^2$~~
~~connection t1, t4~~	~~$p_1 * p_4^2$~~
~~connection t1, spare~~	~~$p_1 * p_4^2$~~
~~connection t2, t3~~	~~$p_1 * p_4^2$~~
~~connection t2, t4~~	~~$p_1 * p_4^2$~~
~~connection t2, spare~~	~~$p_1 * p_4^2$~~
~~connection t3, t4~~	~~$p_1 * p_4^2$~~
~~connection t3, spare~~	~~$p_1 * p_4^2$~~
~~connection t4, spare~~	~~$p_1 * p_4^2$~~
TOTAL	$p_1*p_3 + p_2*p_3$ ~~$+ 10* p_1 * p_4^2$~~

Note: p_1 , p_4 should be low

Speed up #2 & 3: Using BDDs

BDDs

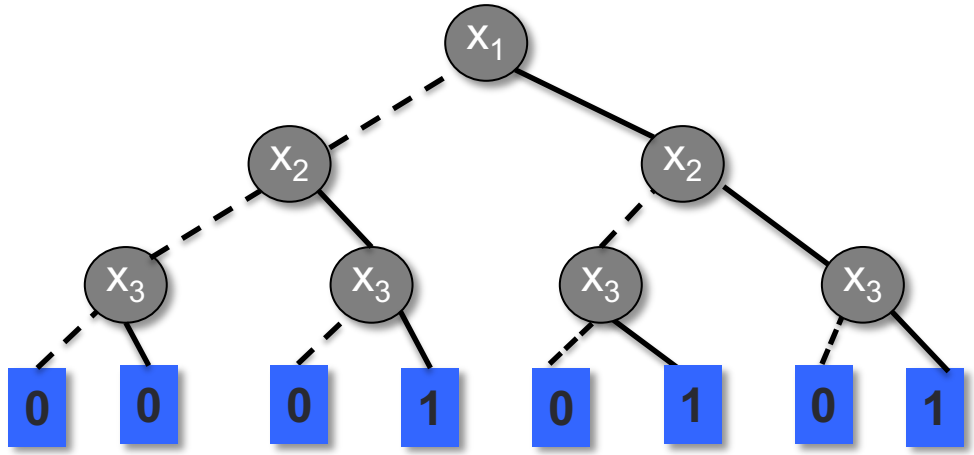
- Compact representation for Boolean functions $f(x_1,x_2,\ldots,x_n)$
  - eg the structure function of a FT
- Heavily used in model checking
  - (intial) condition
  - (reachable) state space
- Based on Shannon expansion / pivotal decomposition
  - $f(x_1,x_2,\ldots,x_n) = \underline{x_1} f(0,x_2,\ldots,x_n) + x_1 f(1,x_2,\ldots,x_n)$
  - fixed variable ordering
  - shared subtrees

Example: $(x_1 + x_2)$ & x_3

Truth Table

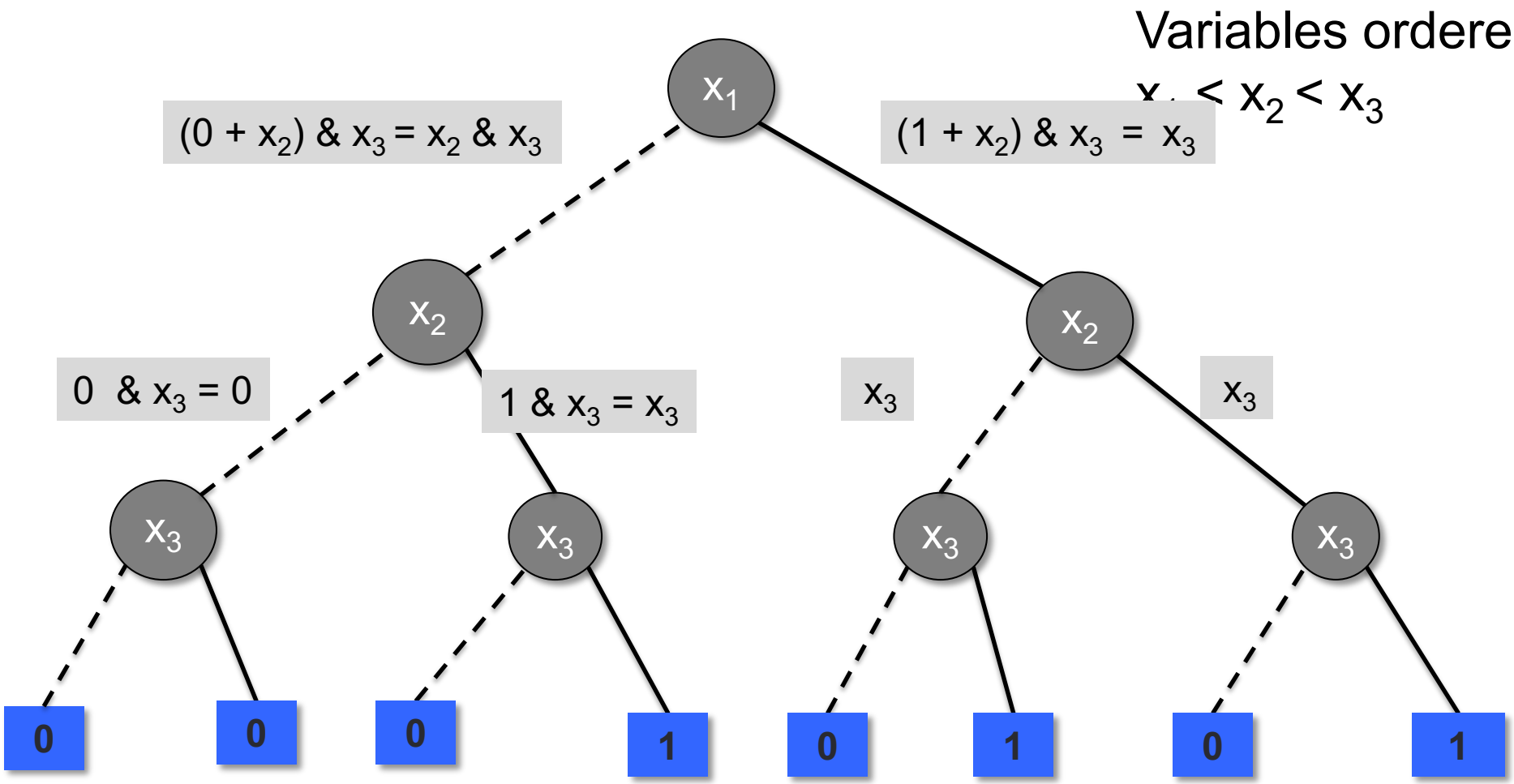
x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Decision Tree



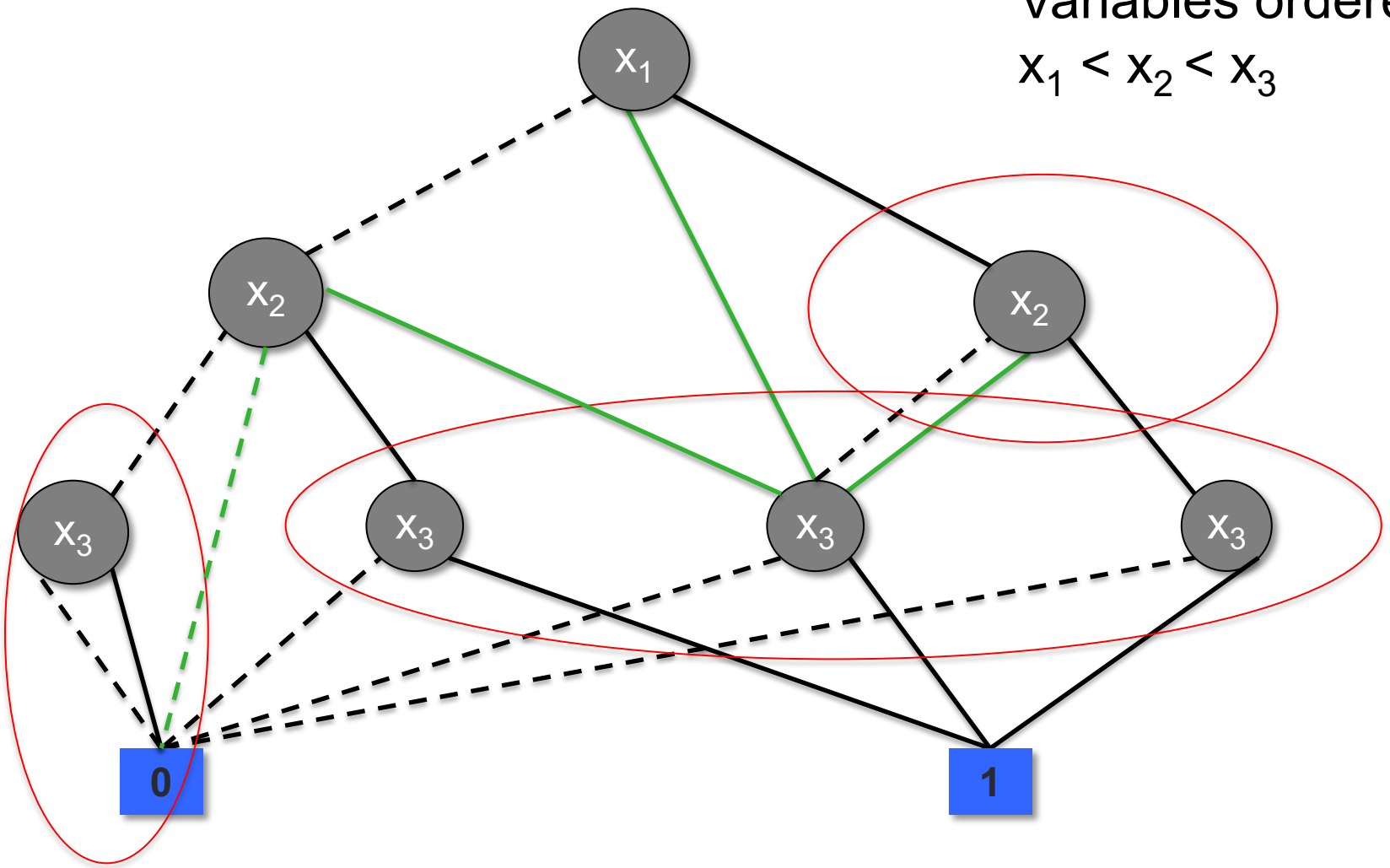
- Vertex represents decision
- Follow dashed line for value 0
- Follow solid line for value 1
- Function value in leave.

Example: $(x_1 + x_2) \& x_3$

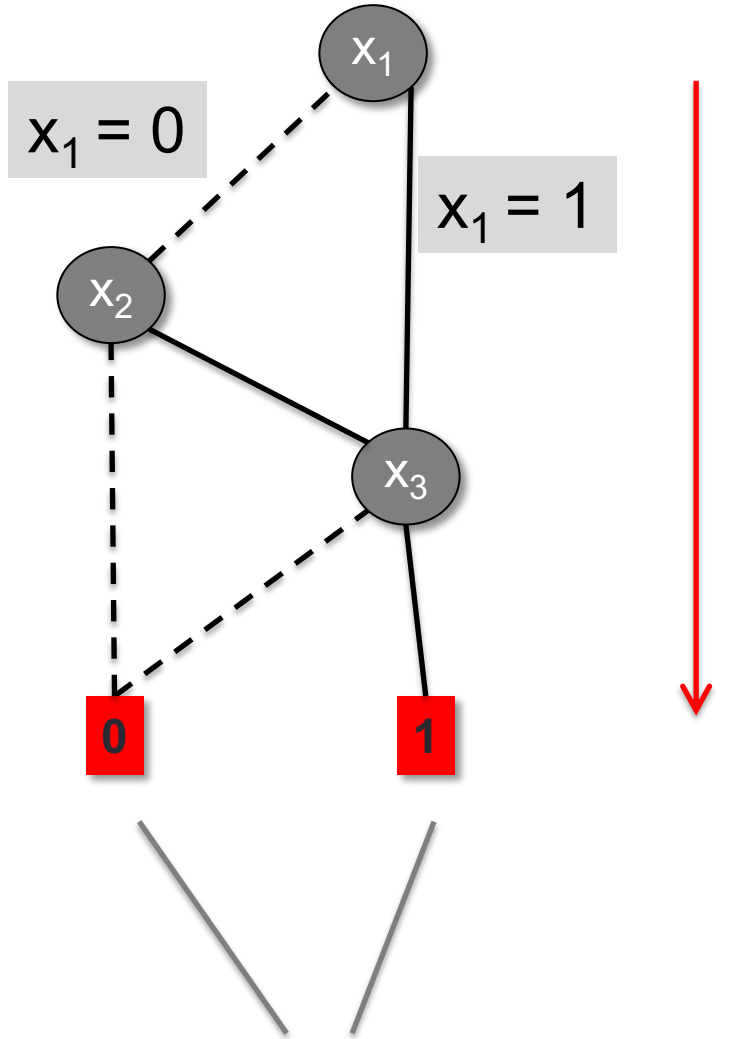


Example: $(x_1 + x_2) \& x_3$

Variables ordered
$x_1 < x_2 < x_3$



Example: $(x_1 + x_2) \& x_3$

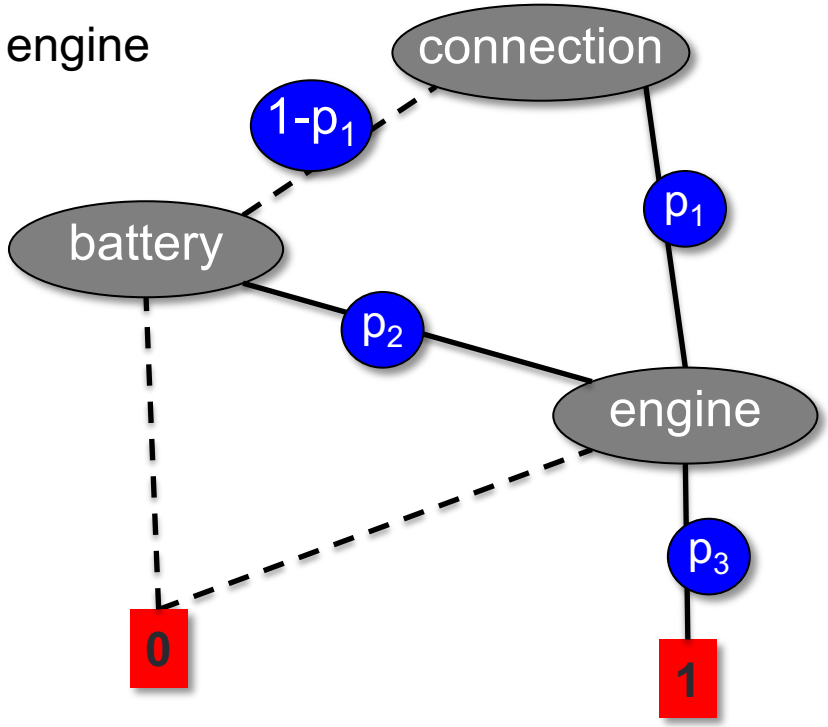


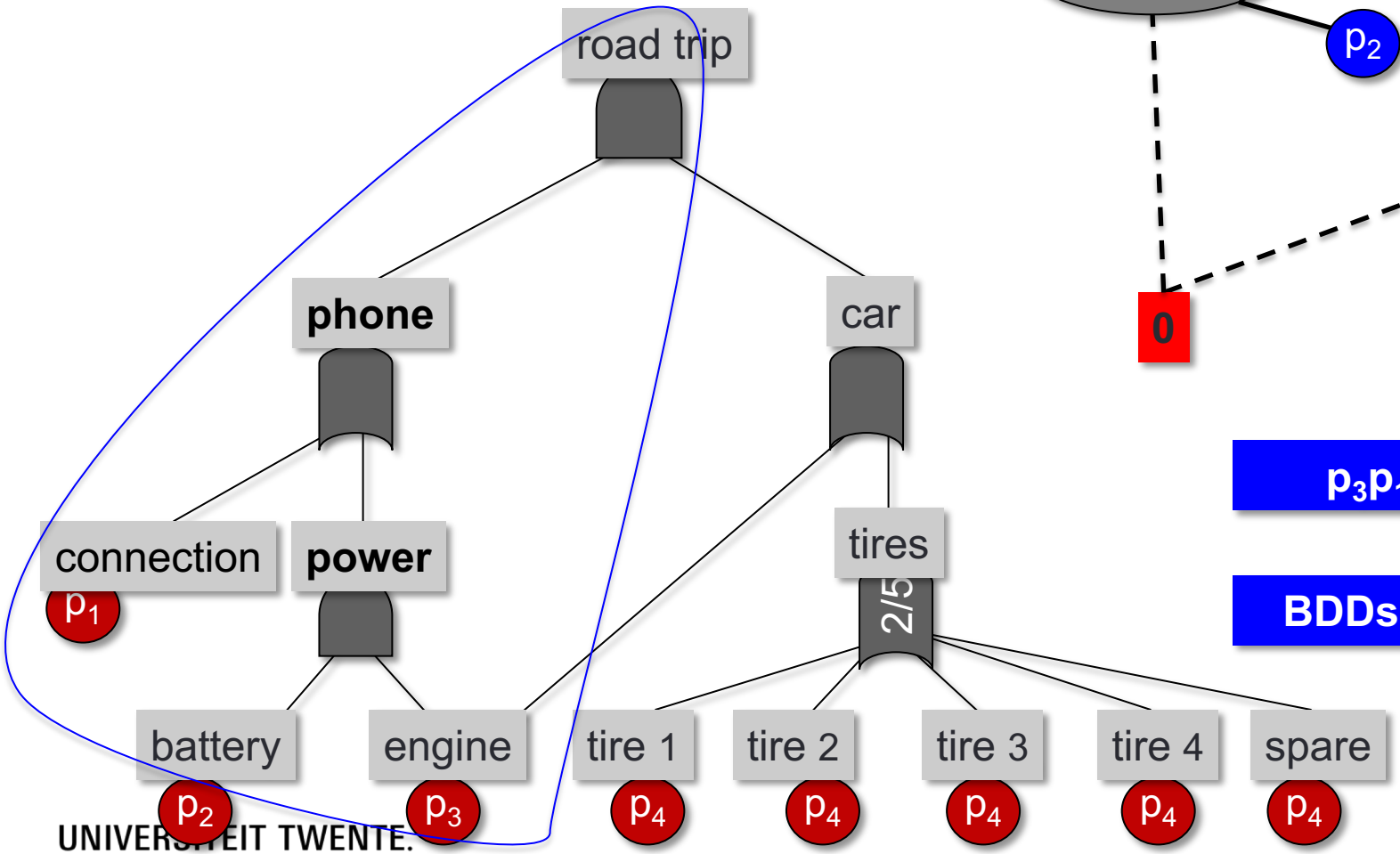
Variables ordered
$x_1 < x_2 <\ldots,< x_n$

- Size of BDDs heavily depends on variable order
$x_1 < x_2 <\ldots,< x_n$
- Finding best order is NP hard
- Good algos in practice

Using BDDs

(connection + battery) & engine





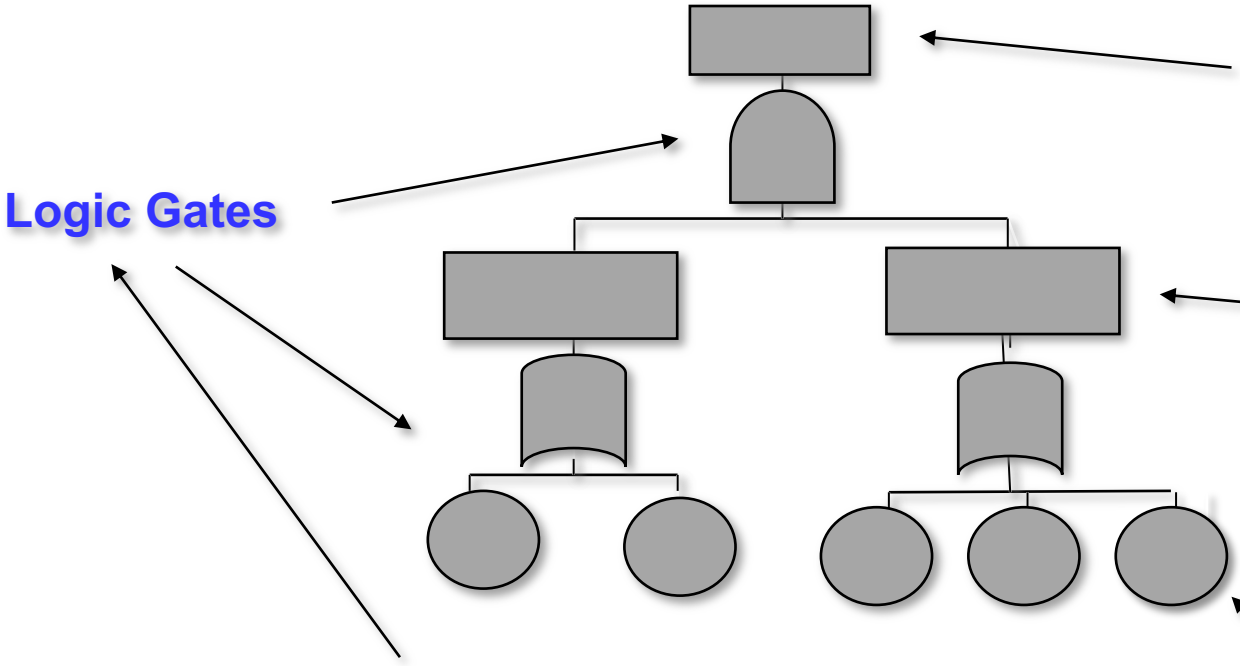
$p_3p_1 + p_3p_2(1-p_1)$

BDDs also find MCS

FAULT TREES
SOME REMARKS

Note: related to Attack Trees in security

The fault Tree Model: Structure



Top Undesired Event

- usually several TUEs / FTs

Logic Gates

Intermediate Events

- documentation
- standard naming
- tie to information systems

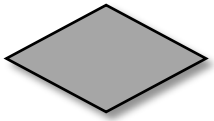
Elements

Basic Events (BE)

Many guidelines for FT modeling

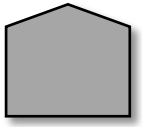
- Top-down, from TUE
- Establish boundaries & conditions
- Include human behaviour

The Fault Trees Model: more elements



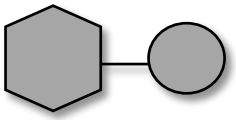
Incomplete/Undeveloped Event
relevant but not further developed, usually because of insufficient data.

- E.g. SW malfunction, Human Error
- Analytically omitted



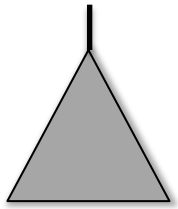
External / House Event: An event external to the system which can cause failure.

- E.g. Fire
- Analytically same as BE

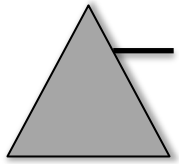


Inhibit Gate: The top event occurs only if the bottom event occurs and the inhibit condition is true.

- Analytically same as AND

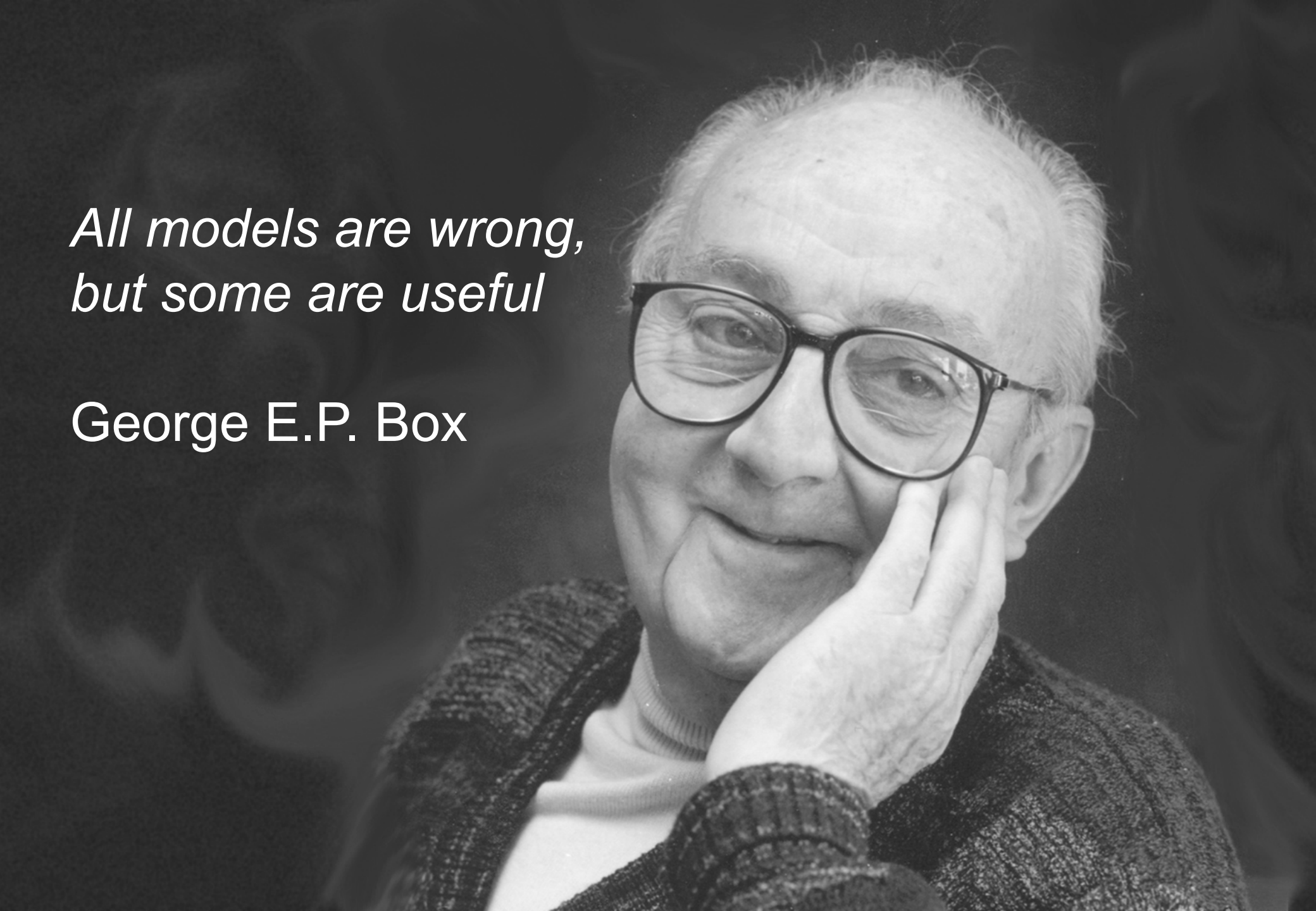


Transfer in
Input FT in gate



Transfer out
Use FT in other parts

There are many other gates; extensions → it's a fault tree jungle


All models are wrong,
but some are useful
George E.P. Box

FT history

- **1962:** H.A. Watson @ Bell Labs
  - FT for Minute Man Launch Control System
- **1965:** David Haasl @ Boeing
  - Introduced FTA
- **1966** Boeing developed FTA simulation programme
- **1981** NASA Fault Tree Handbook
- **2002** NASA Fault Tree Handbook v2

Ericson, Clifton (1999). "Fault Tree Analysis - A History"

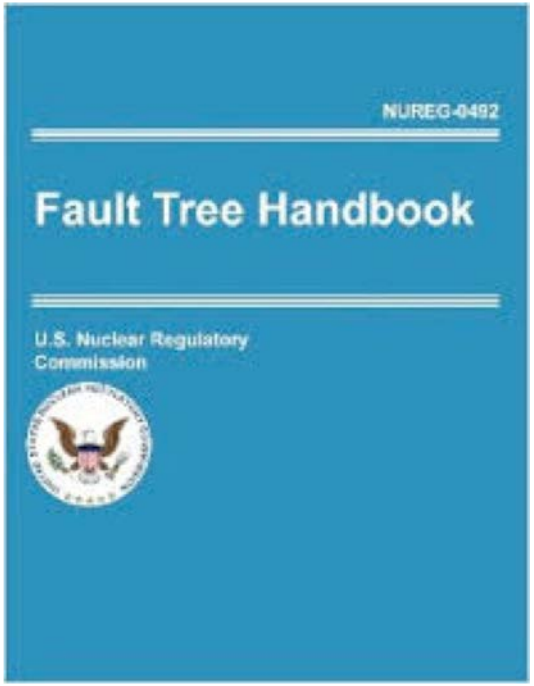
Qualitative vs Quantitative Analysis

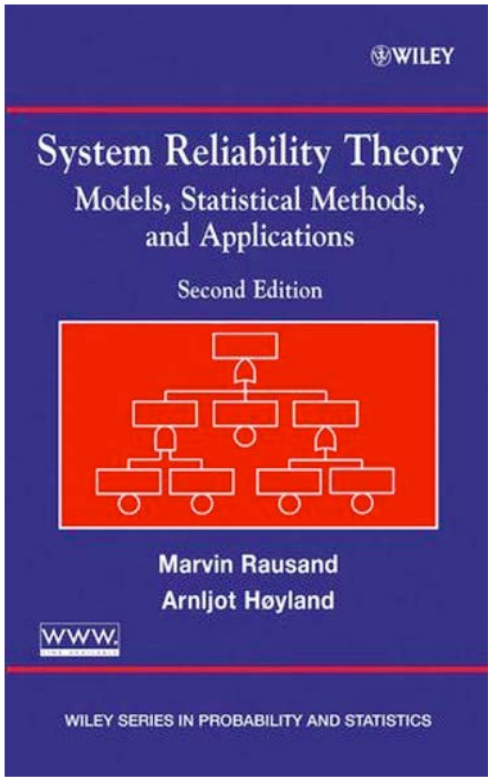
Qualitative analysis

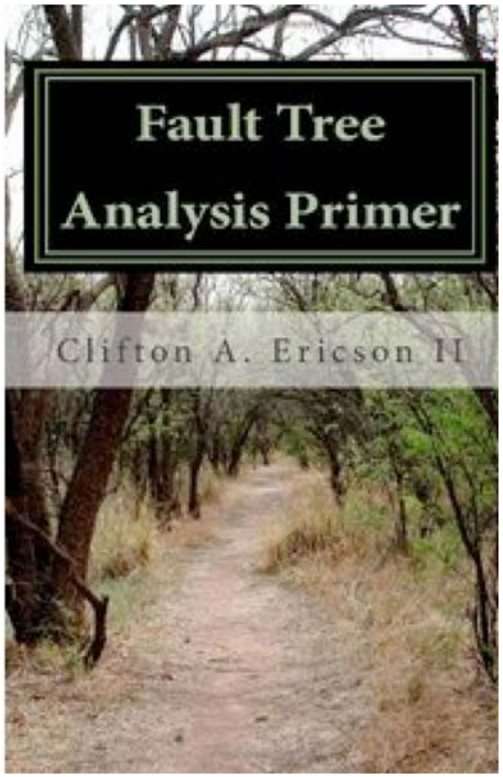
+ Insight in main risks
+ Quick
- Less informative on priorities

Quantitative analysis

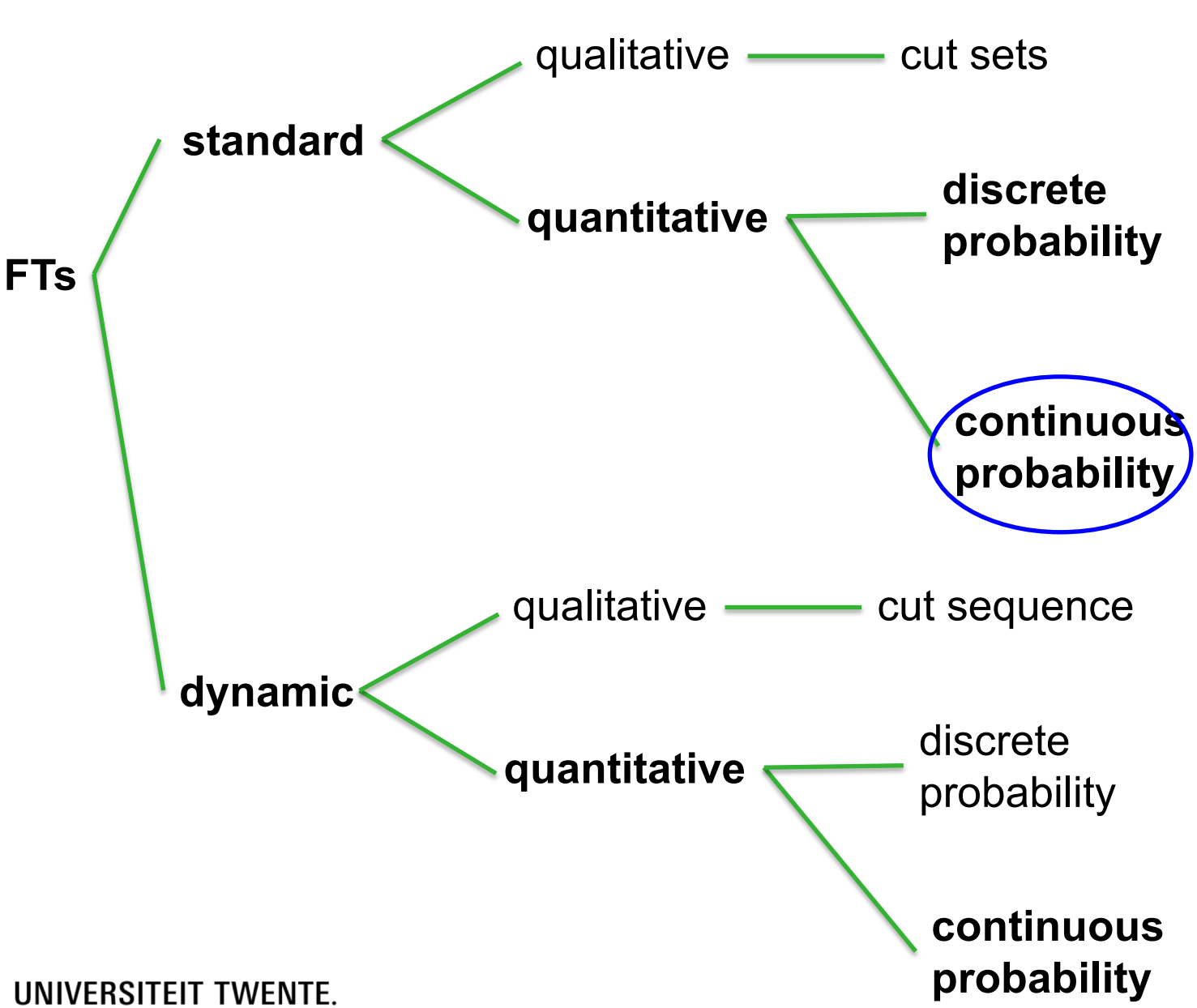
+ Provable evidence of safety requirements
+ Info on priorities & effect of measures taken
- Takes time and effort
- Numbers “lead their own lives,” assumptions forgotten


NUREG-0492
Fault Tree Handbook
U.S. Nuclear Regulatory Commission


WILEY
System Reliability Theory
Models, Statistical Methods, and Applications
Second Edition
Marvin Rausand
Arnljot Høyland
WWW.
WILEY SERIES IN PROBABILITY AND STATISTICS


Fault Tree Analysis Primer
Clifton A. Ericson II

Overview

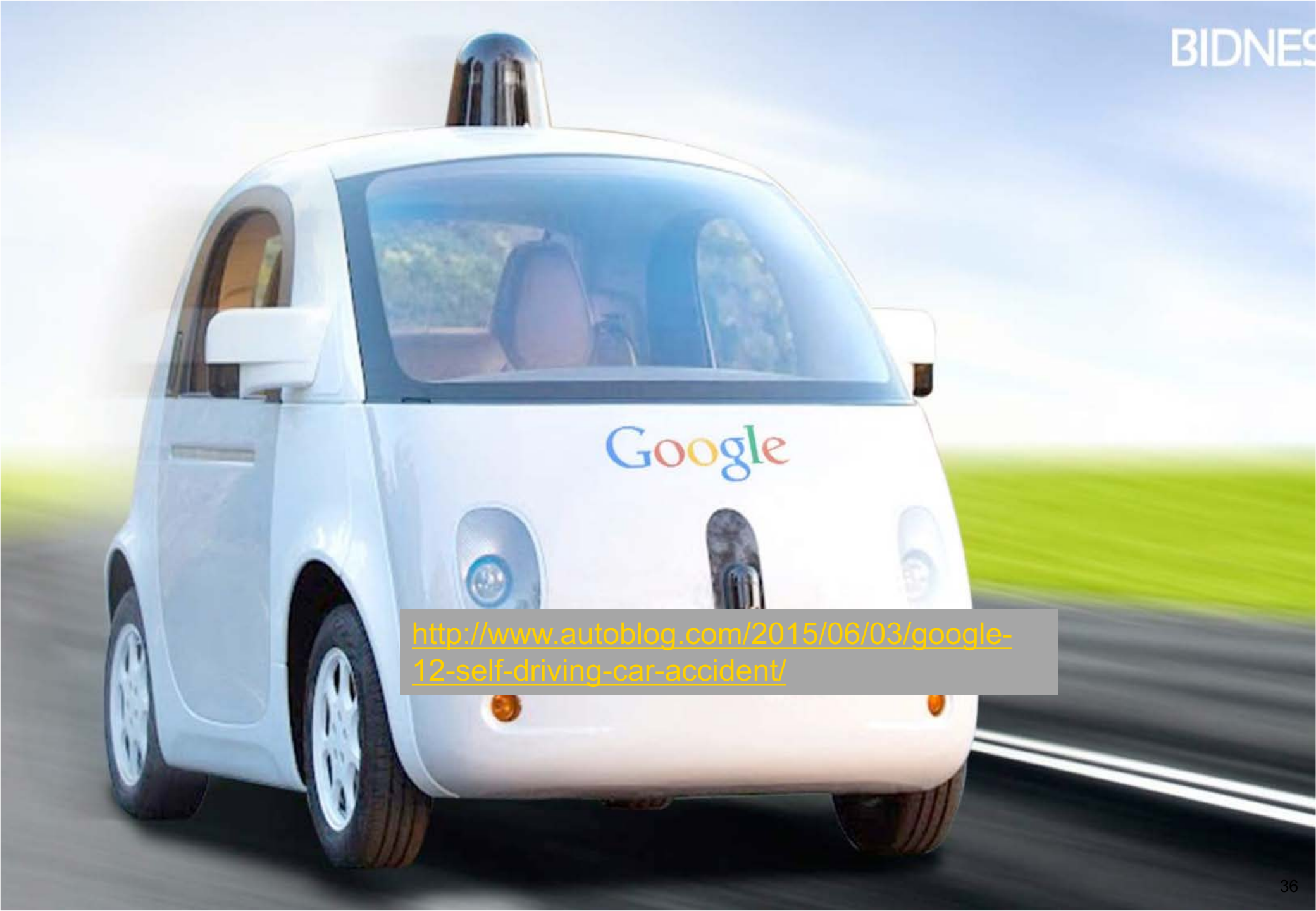


Technique

- Recursive
- BDDs

Technique

- Bottom up
- Cut sets
- BDDs


BIDNES
Google
http://www.autoblog.com/2015/06/03/google-12-self-driving-car-accident/

FAULT TREES IN CONTINUOUS TIME

Note: related to Attack Trees in security

System (un)reliability

- Unreliability

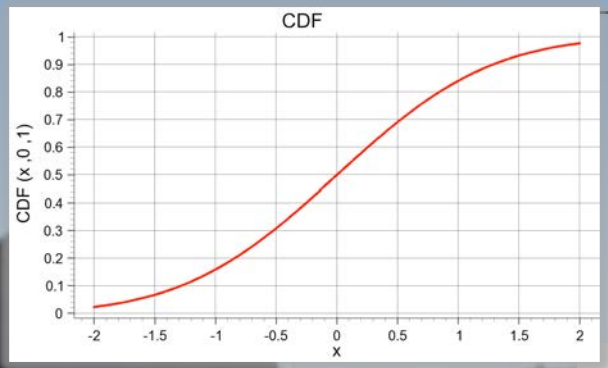
  U(t) = **P**[failure before time *t*]

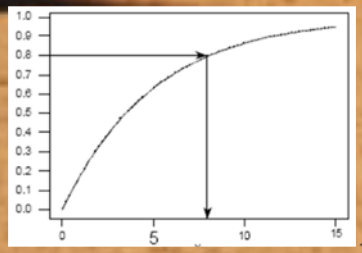
- Reliability / Survivor function

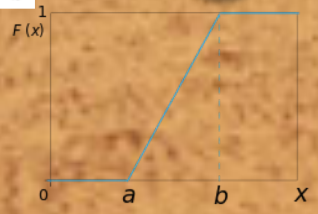
  R(t) = **P**[no failure until time *t*]

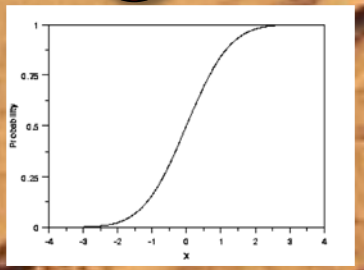
  = 1- U(t)

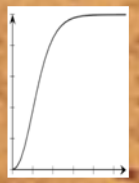
Continuous probability: failure behaviour over time

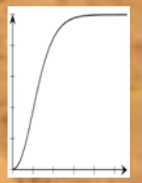


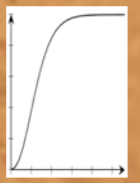






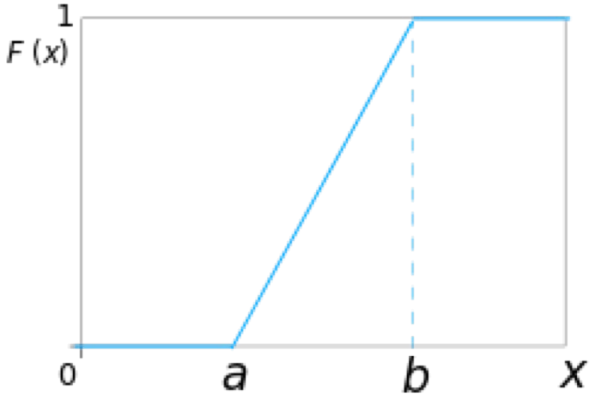


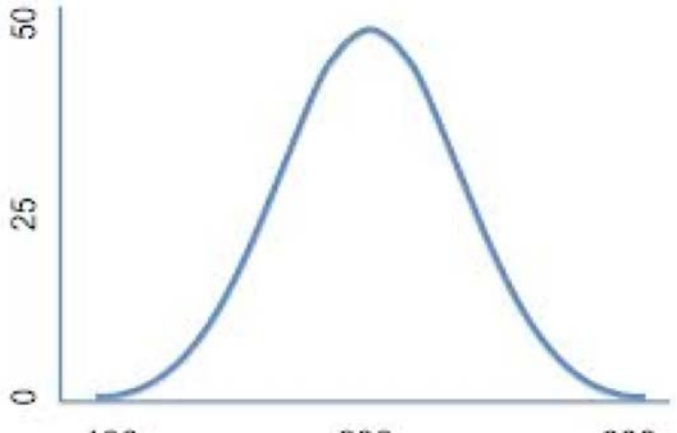




Continuous probability distributions: which one?

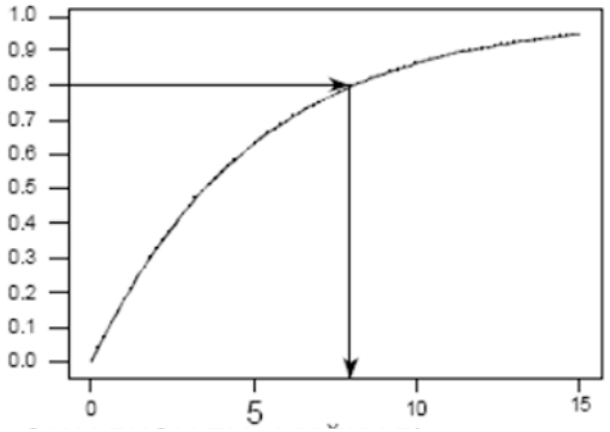
- Uniform distribution
- Gaussian
- Exponential
  - realistic model for degradation
  - mathematically tractable
  - approximation via composed exponentials
- Weibull
  - generalized exponential
  - often used
  - not discussed

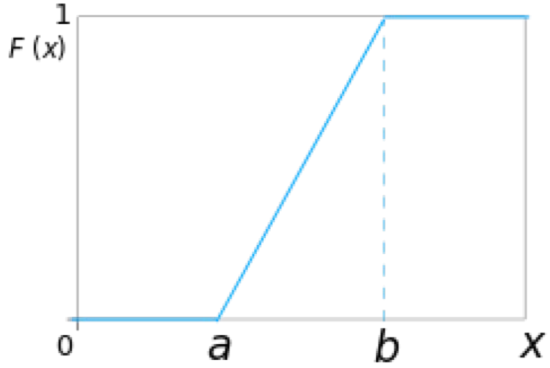


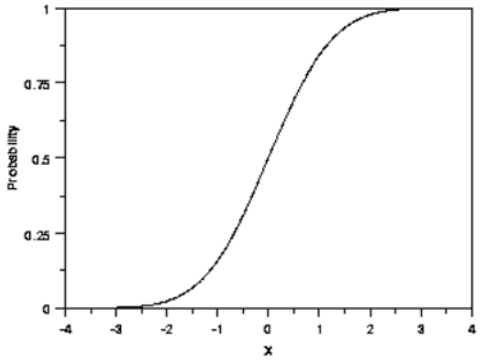


Repap: Continuous probability distributions

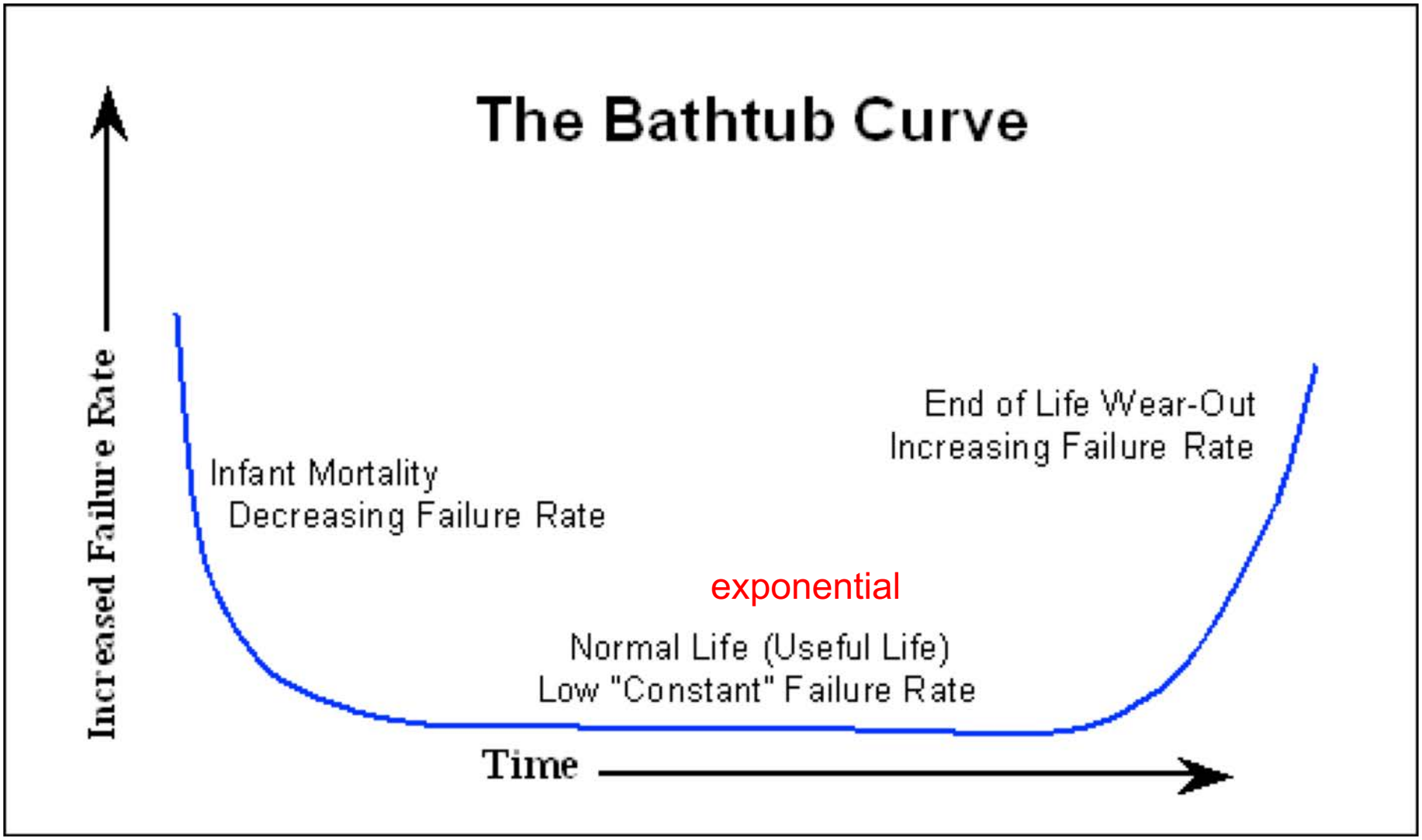
- Often: **P**[X = x] = 0
- Hence: F(x) = **P**[X ≤ x]
- **P**[x ≤ X ≤ y] = **P**[X ≤ y] – P[X ≤ x]
- Where does the probability increase most?
  - f(x) = F'(x) density function



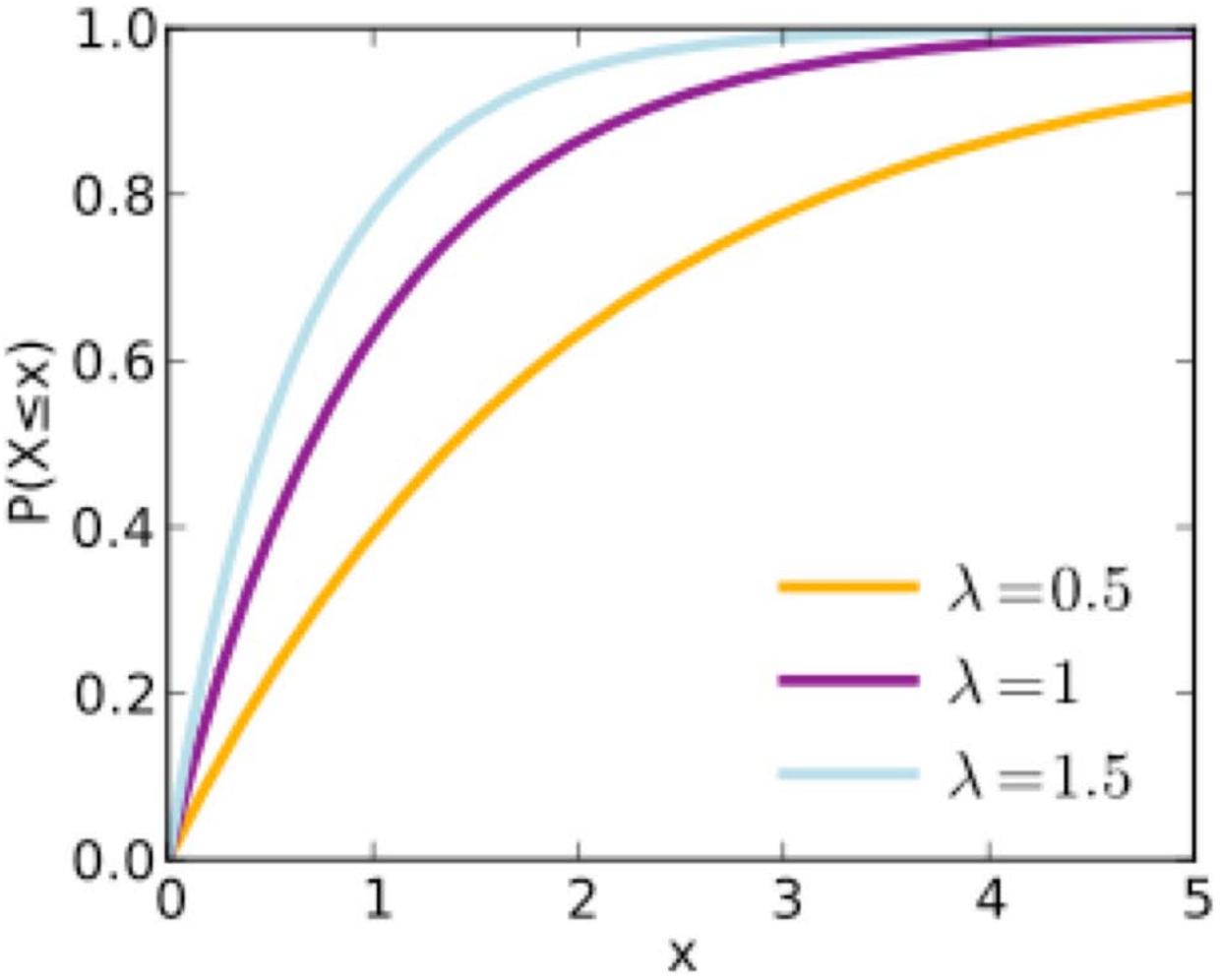




Bath tub curve: degradation behaviour of systems



Exponential probability distribution



Higher λ = more failures = lower average failure time

Components fail with fixed rate / time

Unreliability / CDF =

P[fail before x] =

P[X ≤ x] = $1 - e^{-\lambda x}$

Reliability =

P[fail after x] =

P[X > x] = $e^{-\lambda x}$

PDF

$f(x) = F'(x) = \lambda e^{-\lambda x}$

Expected value

E[x] = $1/\lambda$

Some known facts about exponential distributions

"BACK IN 15
MINUTES!"
(on average)

Question

You are waiting in front of your professor's office. There is a note on the door

Back in Exp(1/15) minutes

Questions

1. What is the expected amount you have to wait?
2. What is the probability that you wait
   A. less than 5 minutes?
   B. more than 10 minutes?
   C. exactly 10 minutes?
   D. between 10 and 25 minutes?
3. You have been waiting for 15 minutes
   - What is the probability that you have to wait less than 5 minutes?
   - What is the probability that you have to wait more than 10 minutes?
   - exactly 10 minutes?
   - between 10 and 25 minutes?

Question

You are waiting in front of your professor's office. There is a note on the door

Back in Exp(1/15) minutes.

X denotes your waiting time. Then X~ Exp(1/15)

Questions

1. What is the expected amount you have to wait? $\mathbf{E}[X] = 15$
2. What is the probability that you wait
   A. less than 5 minutes? $\mathbf{P}[X < 5] = 1 - e^{-5/15}$
   B. more than 10 minutes? $\mathbf{P}[X > 10] = e^{-10/15}$
   C. exactly 10 minutes? $\mathbf{P}[X > 10] = 0$
   D. between 10 and 25 minutes? $\mathbf{P}[10 < X < 25] = \mathbf{P}[X < 25] - \mathbf{P}[X < 10] =$

   $1 - e^{-25/15} - (1 - e^{-10/15}) = -e^{-25/15} + e^{-10/15}$

Question

You are waiting in front of your professor's office. There is a note on the door

Back in Exp(1/15) minutes.

X denotes your waiting time. Then X~ Exp(1/15)

Questions

1. You have been waiting for 15 minutes
   - What is the probability that you have to wait more than 10 minutes?

   - **P**[X > 25 | X > 15] =
   - **P**[X > 25 **&** X > 15] / **P**[X > 15] =
   - **P**[X > 25] / **P**[X > 15] =
   - $e^{-25/15}$ / $e^{-15/15}$ = {use $e^a e^b = e^{a+b}$}
   - $e^{-25/15 +15/15}$ =
   - $e^{-10/15}$ =
   - **P**[X > 10]

Exponential distribution **memoryless:** past waiting time has not influence on future waiting time

Note: can be approximated with a dice

Question

You are waiting in front of your professor's office. There is a note on the door

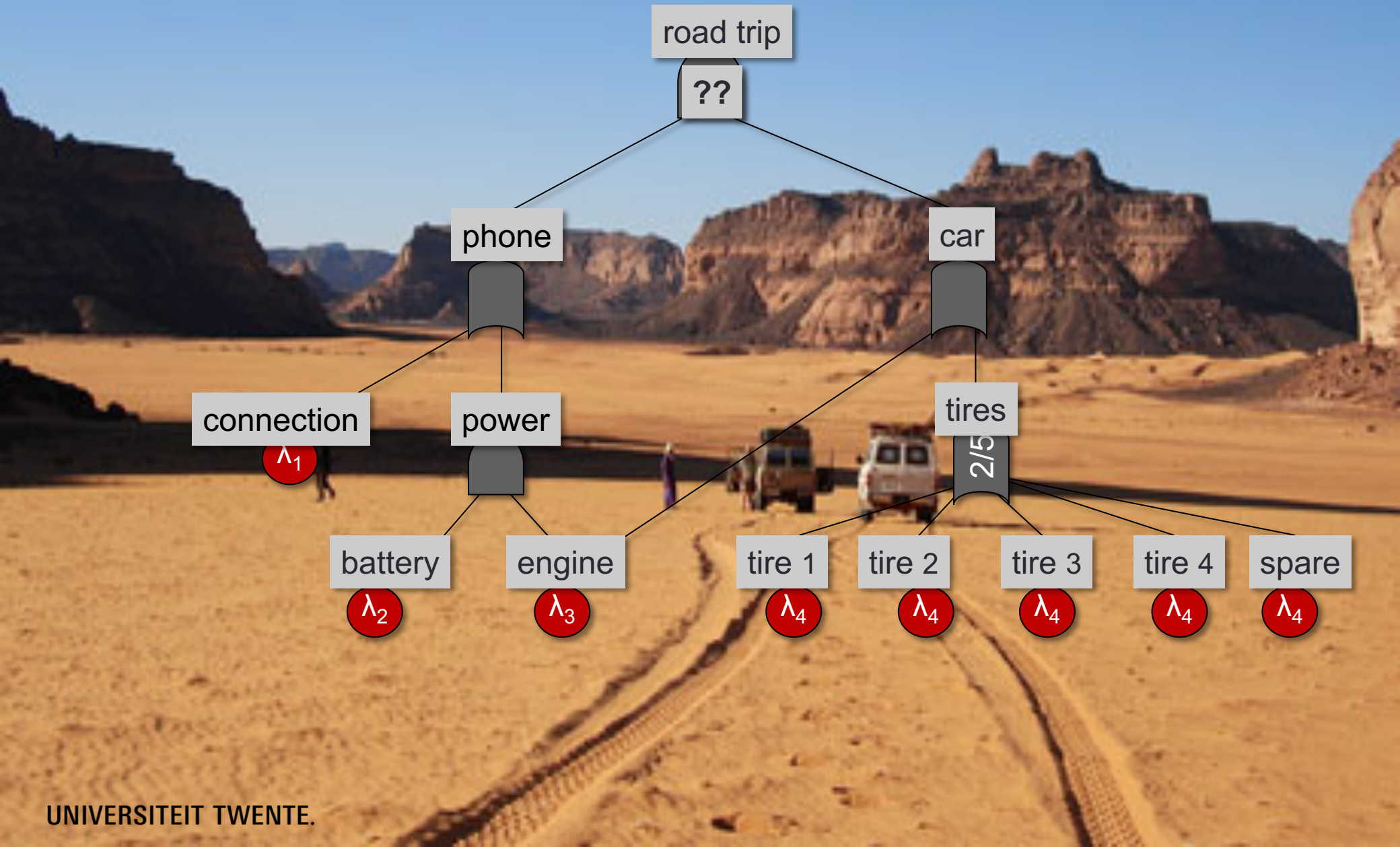
Back in Exp(1/15) minutes.

X denotes your waiting time. Then X~ Exp(1/15)

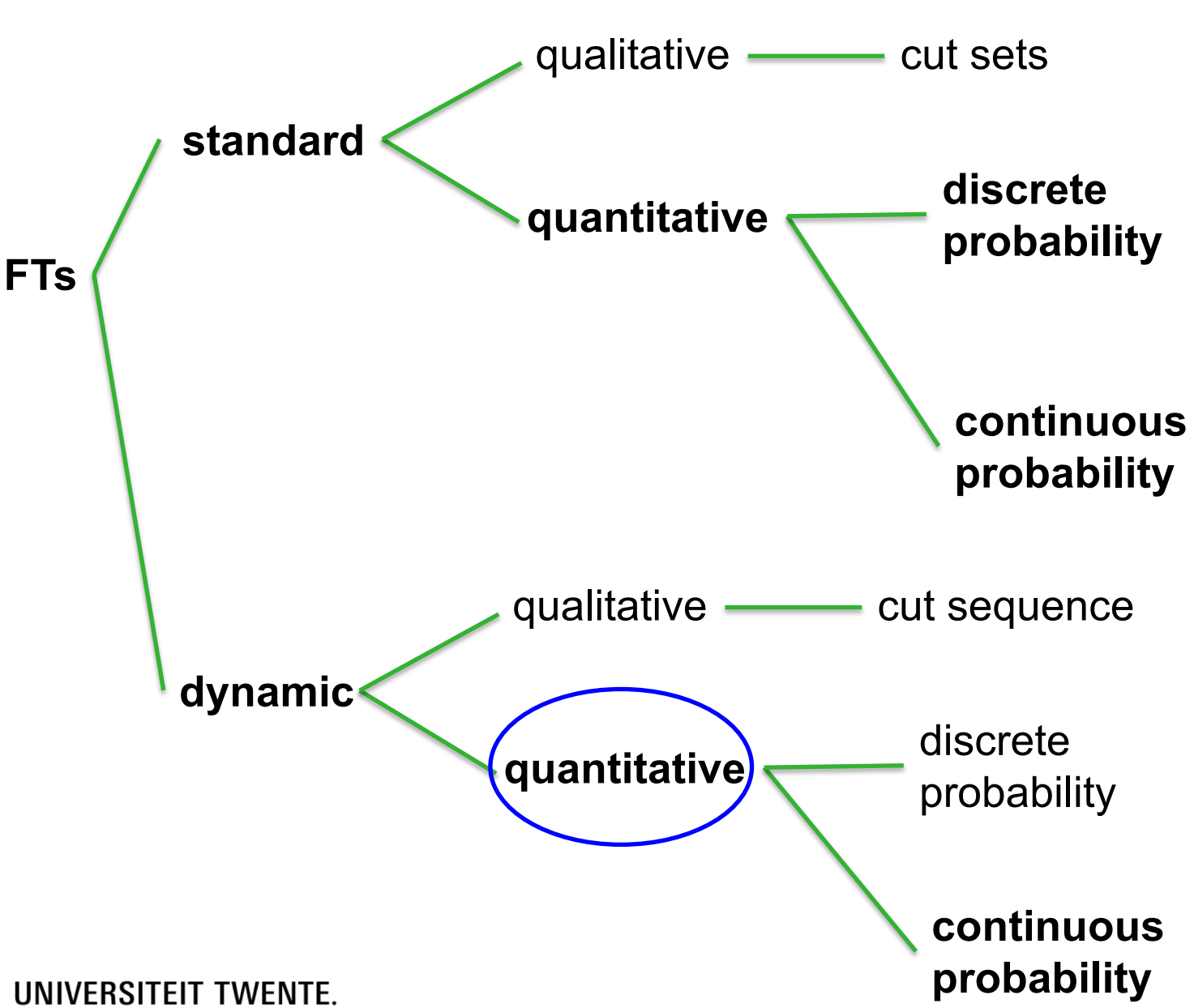
Questions

1. What is the expected amount you have to wait? $\mathbf{E}[X] = 15$
2. What is the probability that you wait
   A. less than 5 minutes? $\mathbf{P}[X < 5] = 1 - e^{-5/15}$
   B. more than 10 minutes? $\mathbf{P}[X > 10] = e^{-10/15}$
   C. exactly 10 minutes? $\mathbf{P}[X > 10] = 0$
   D. between 10 and 25 minutes? $\mathbf{P}[10 < X < 25] = \mathbf{P}[X < 25] - \mathbf{P}[X < 10] =$
   $1 - e^{-25/15} - (1 - e^{-10/15}) = -e^{-25/15} + e^{-10/15}$
3. You have been waiting for 15 minutes
   - What is the probability that you have to wait less than 5 minutes? $1 - e^{-5/15}$
   - What is the probability that you have to wait more than 10 minutes? $e^{-10/15}$
   - exactly 10 minutes? $\mathbf{P}[X > 10] = 0$
   - between 10 and 25 minutes? $-e^{-25/15} + e^{-10/15}$

Example: probabilistic analysis



Overview



Technique
- Recursive
- BDDs

Technique
- Bottom up
- Cut sets
- BDDs

Technique
- The same!

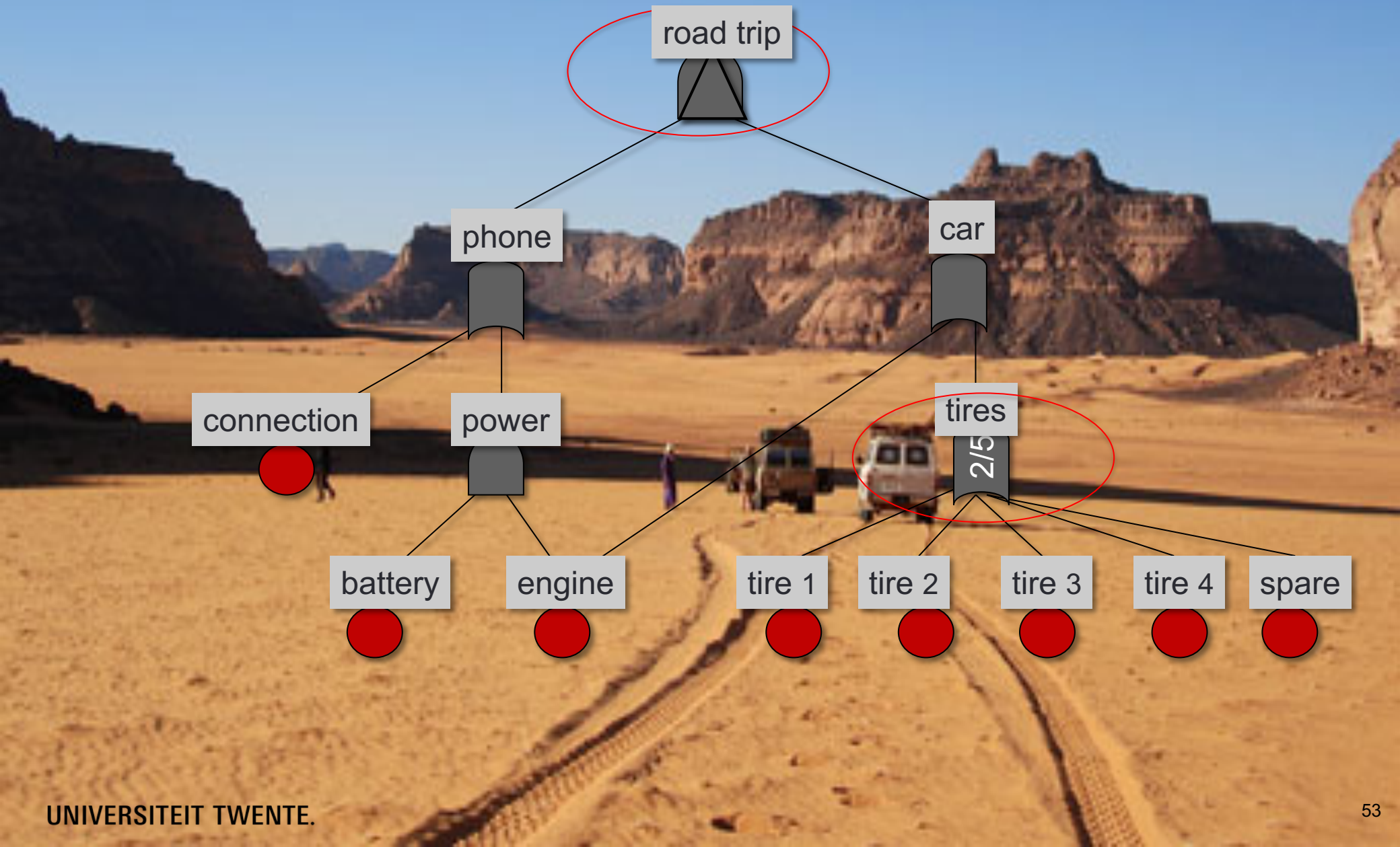
Technique
- Model checking

DYNAMIC FAULT TREES

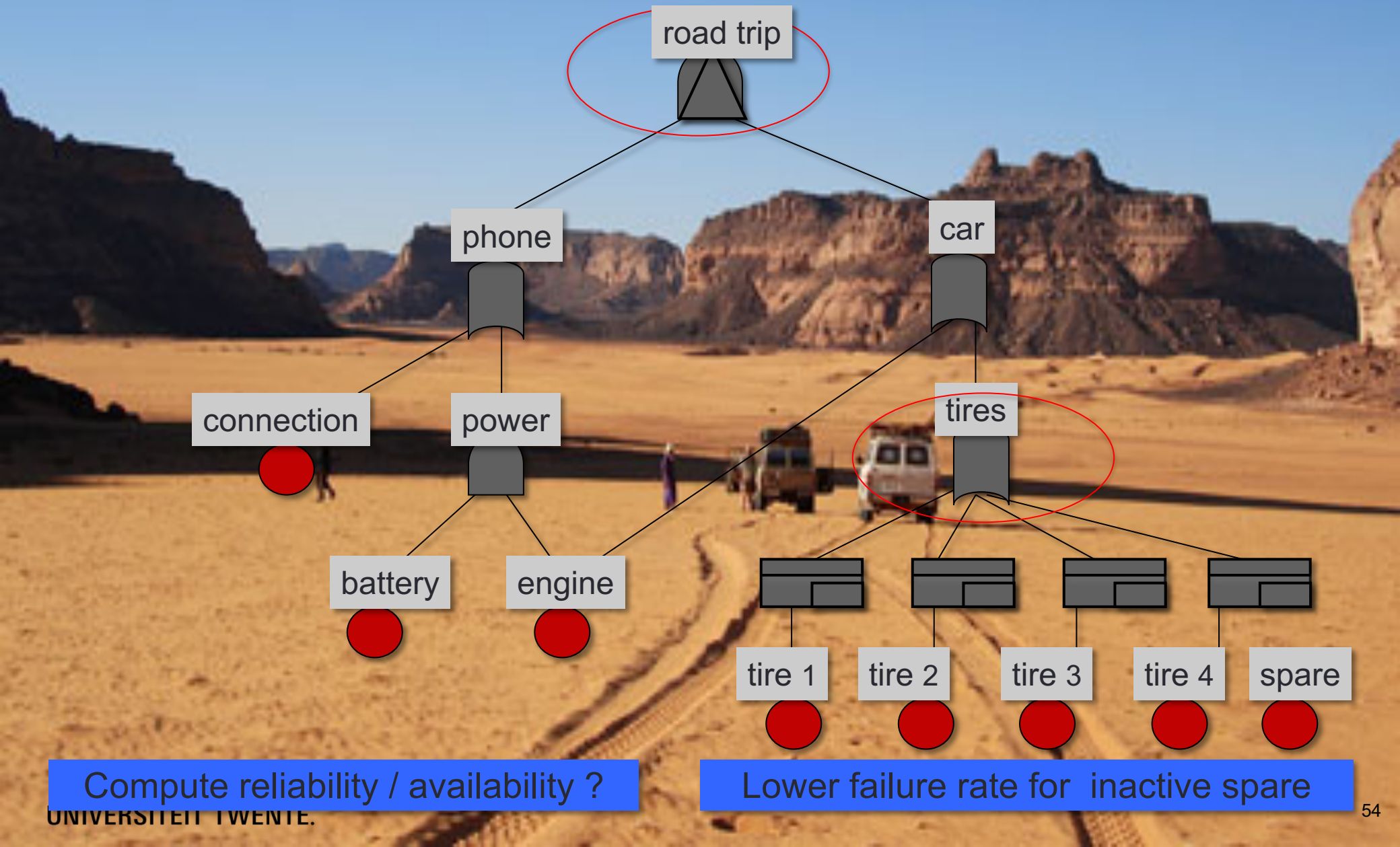
Note: related to Extended Attack Trees in security

NTE.

Example: Safe road trip



Example: Safe road trip



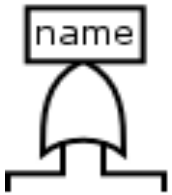
Compute reliability / availability ?

Lower failure rate for inactive spare

DFTs gates

static: as before

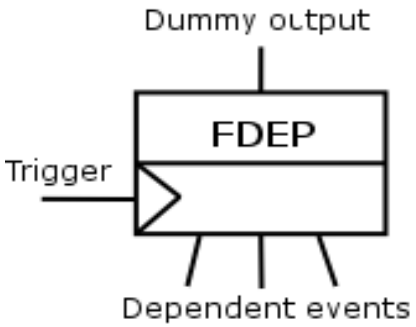
AND



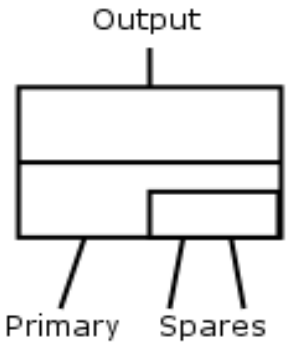
OR

(k,m)
VOTING

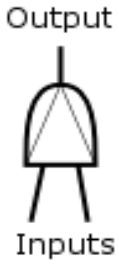
dynamic: failure order matters



FDEP

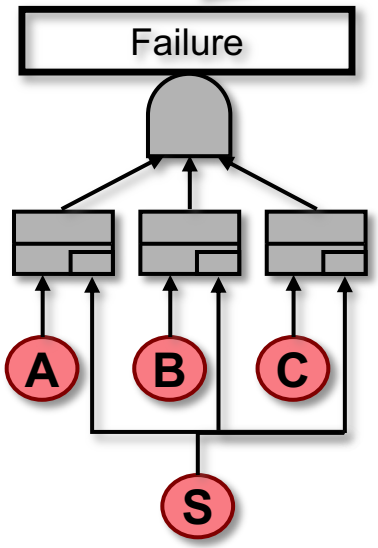


SPARE



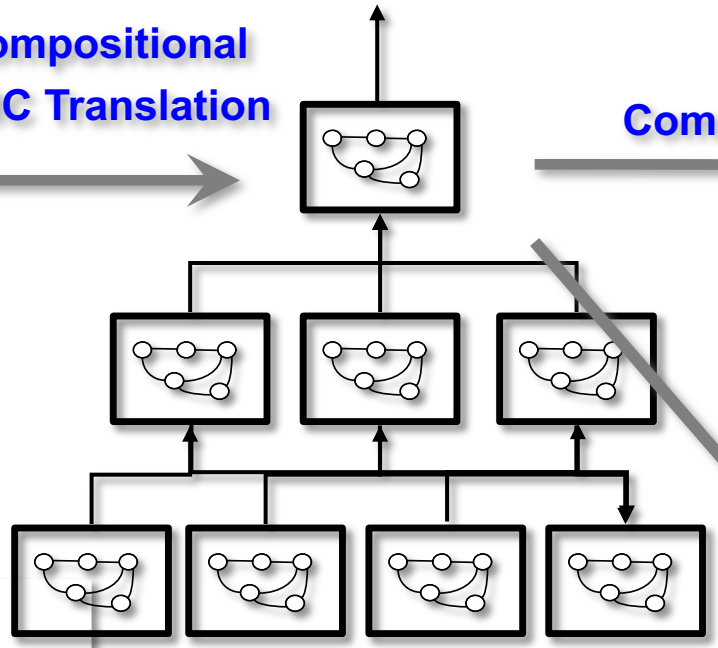
PAND

Fault tree analysis

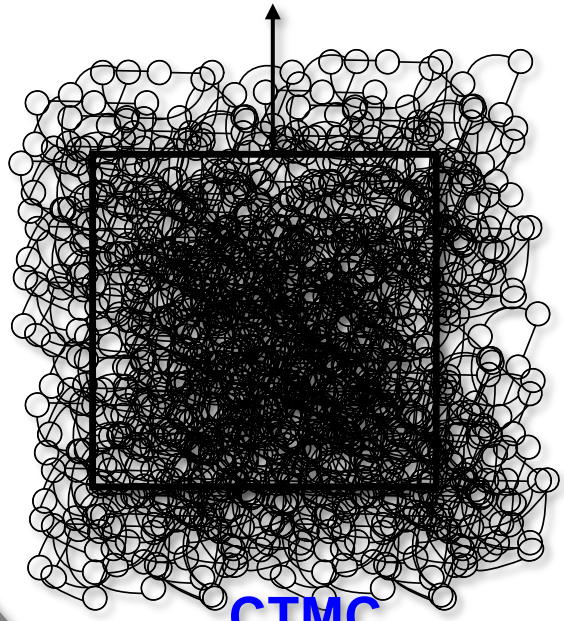


Difficult to validate, modify

1. Compositional I/O-IMC Translation



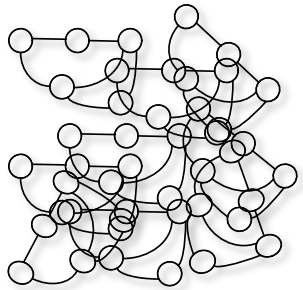
Composition



fail

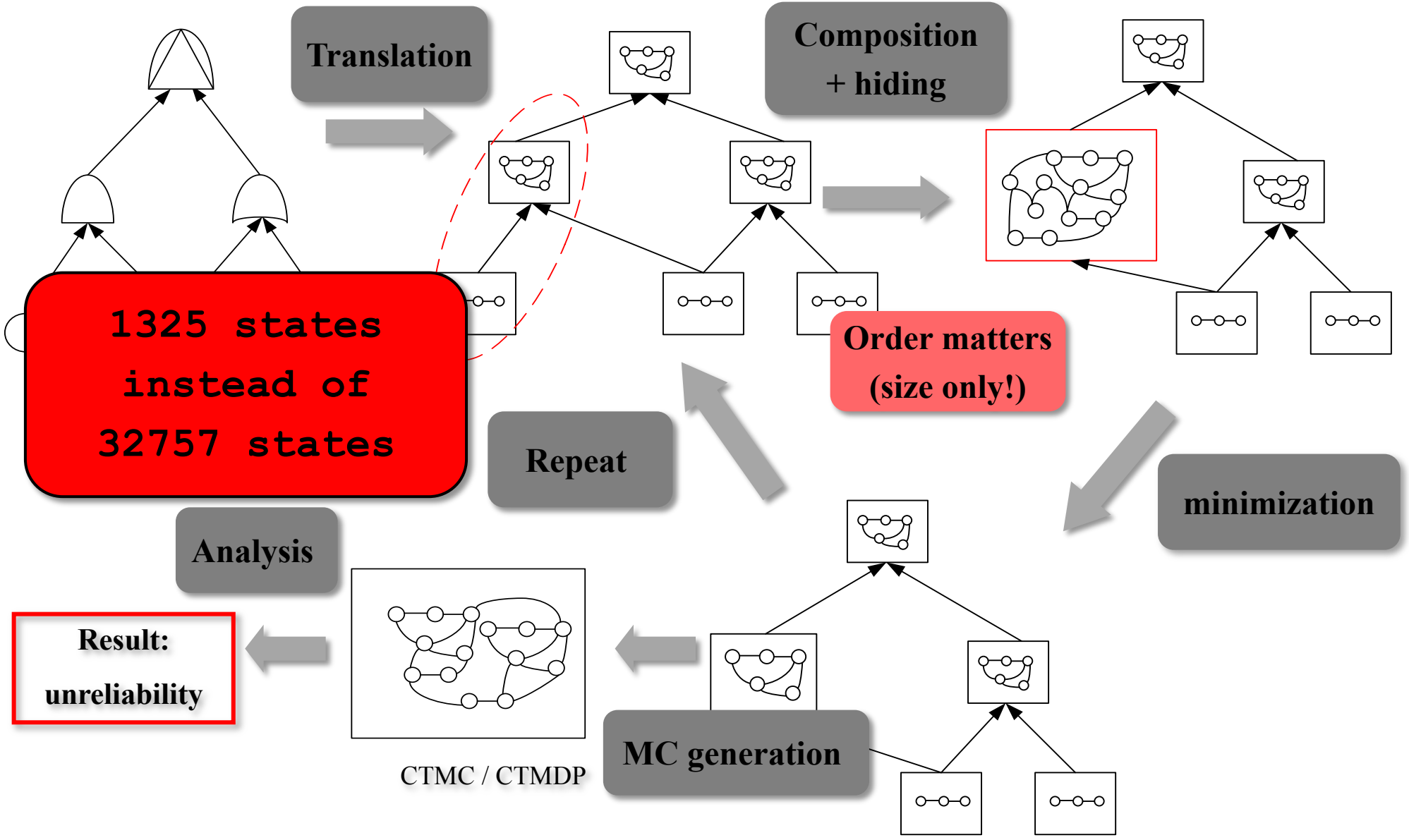
CTMC

2. Smart Composition



Easy to include:
Costs, parameters,
fail-over times,
Recovery,
spare management,
inspections, maintenance,
YOUR WISHLIST

Deep compositionality



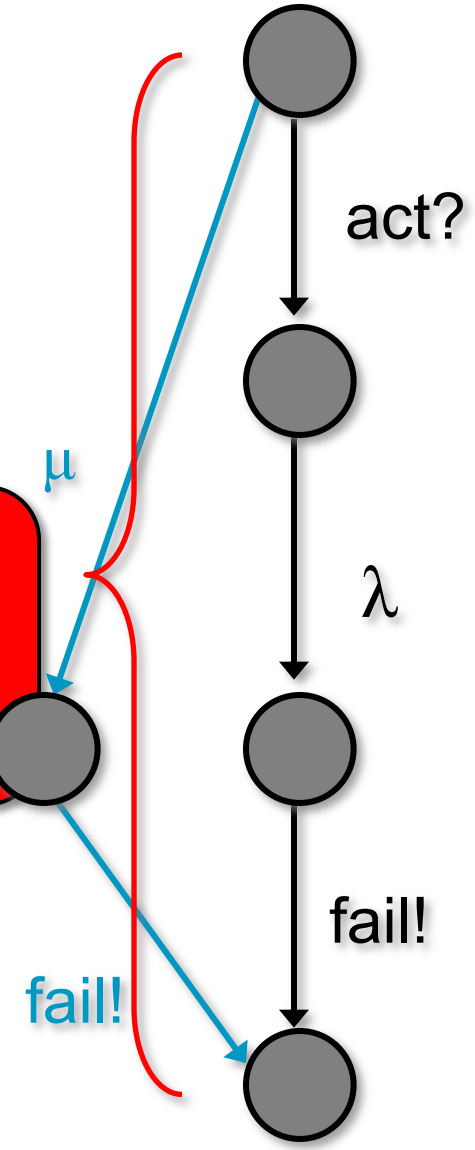
Interactive Markov Chains (I/O-IMC)

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

Warm BE: can fail before activation, with reduced rate

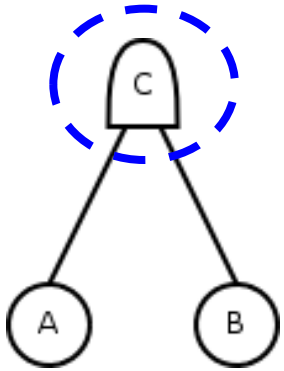
for

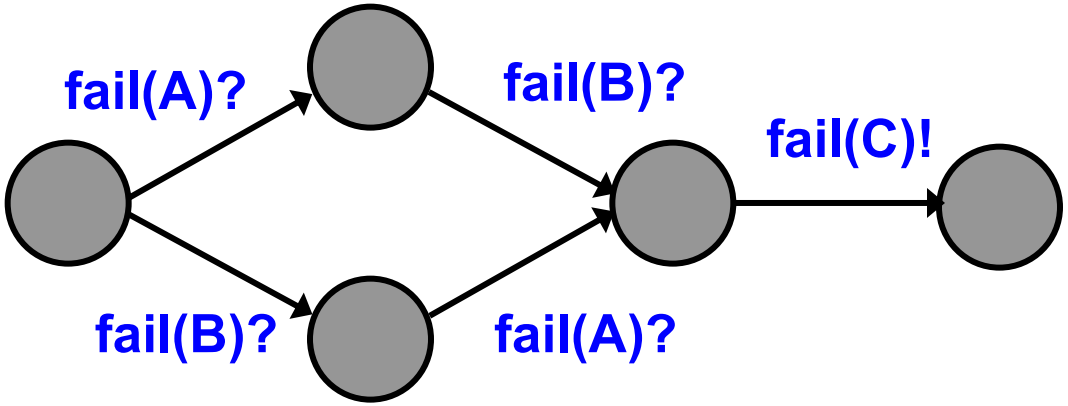
ent



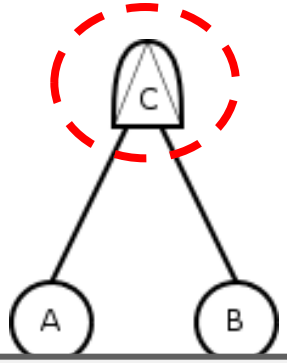
semantics for FT gates

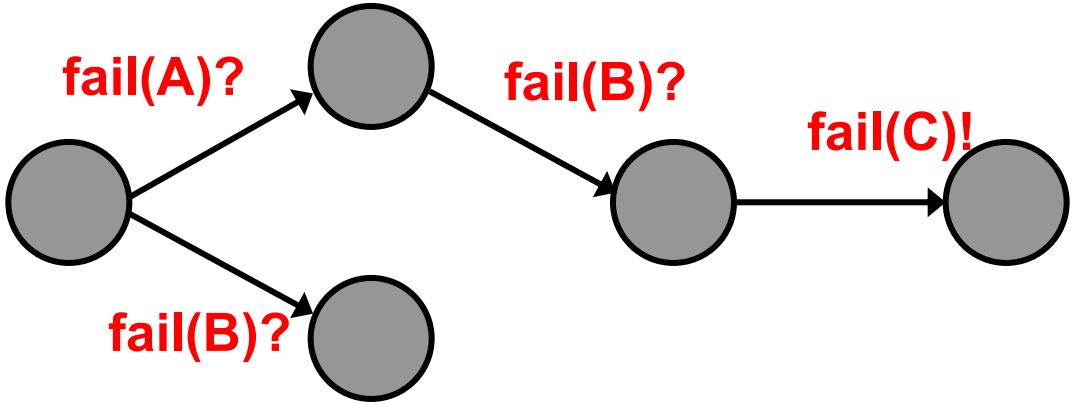
AND gate





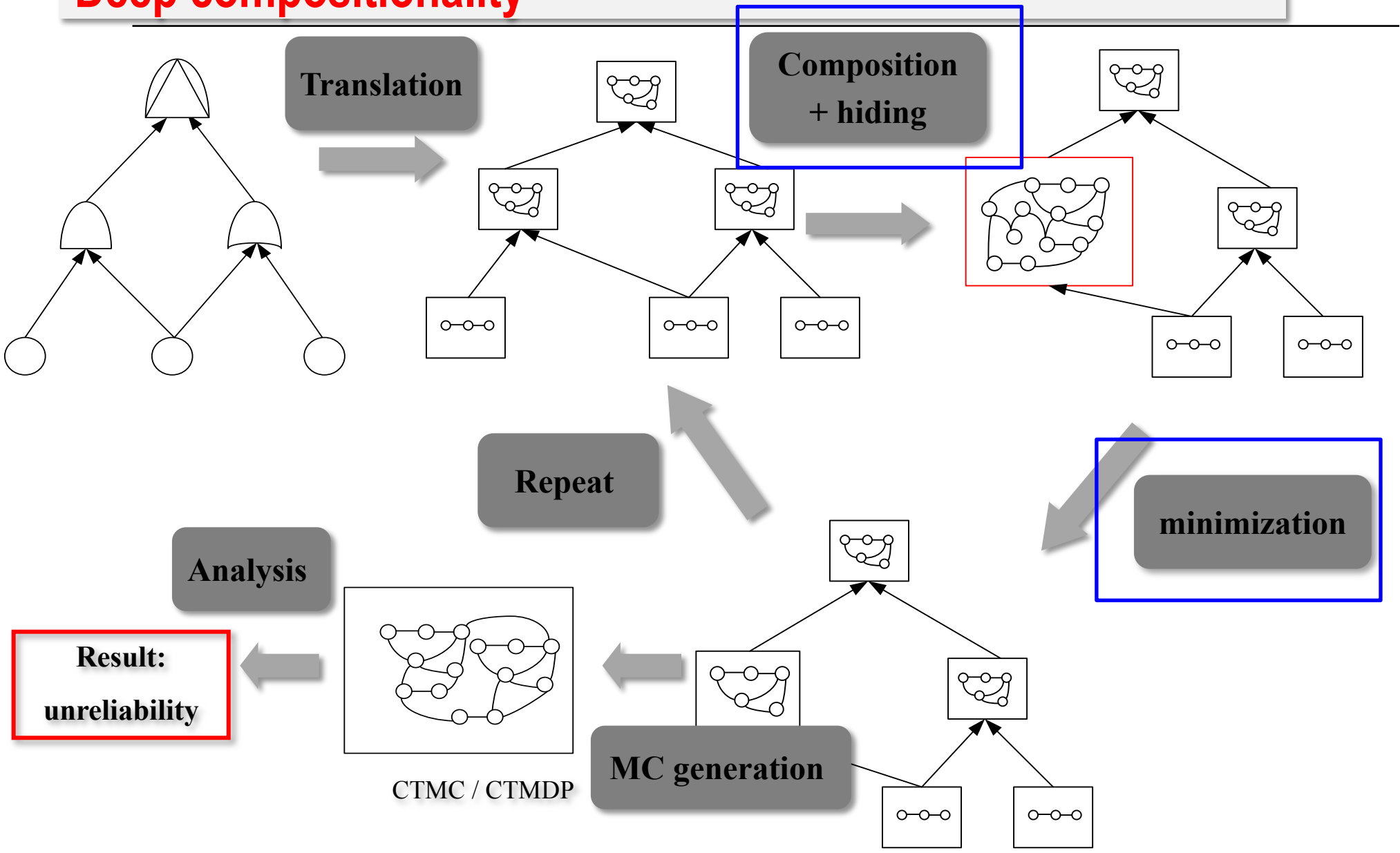
PAND gate



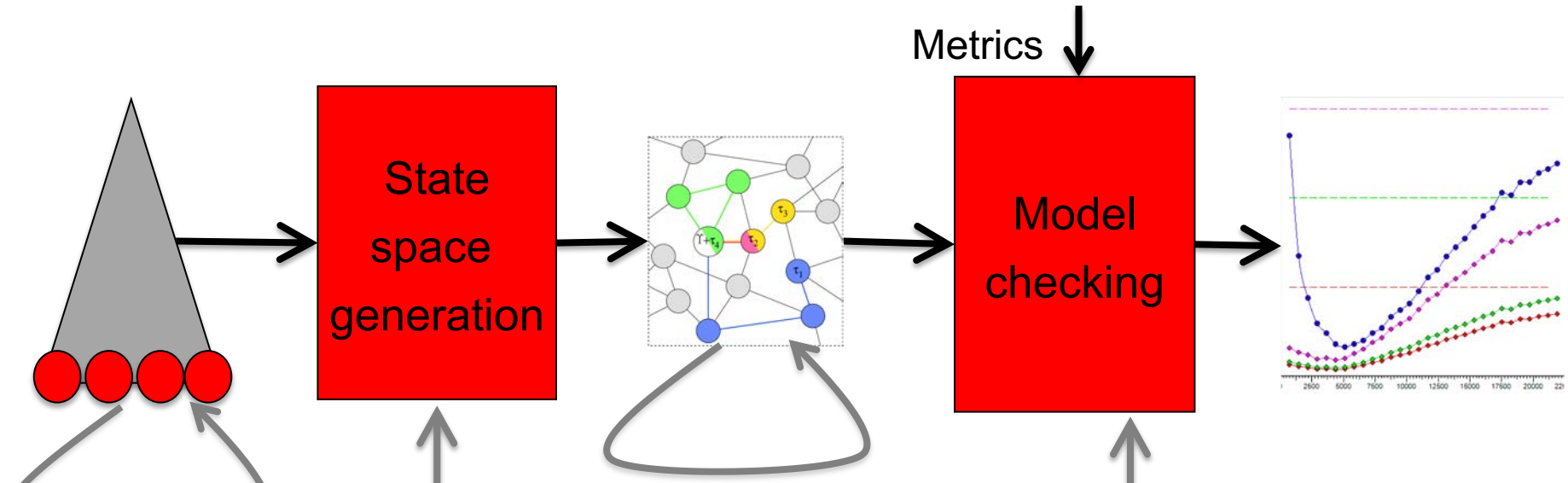


Similar, but more complex for other gates

Deep compositionality



FT analysis: more, faster, bigger, better



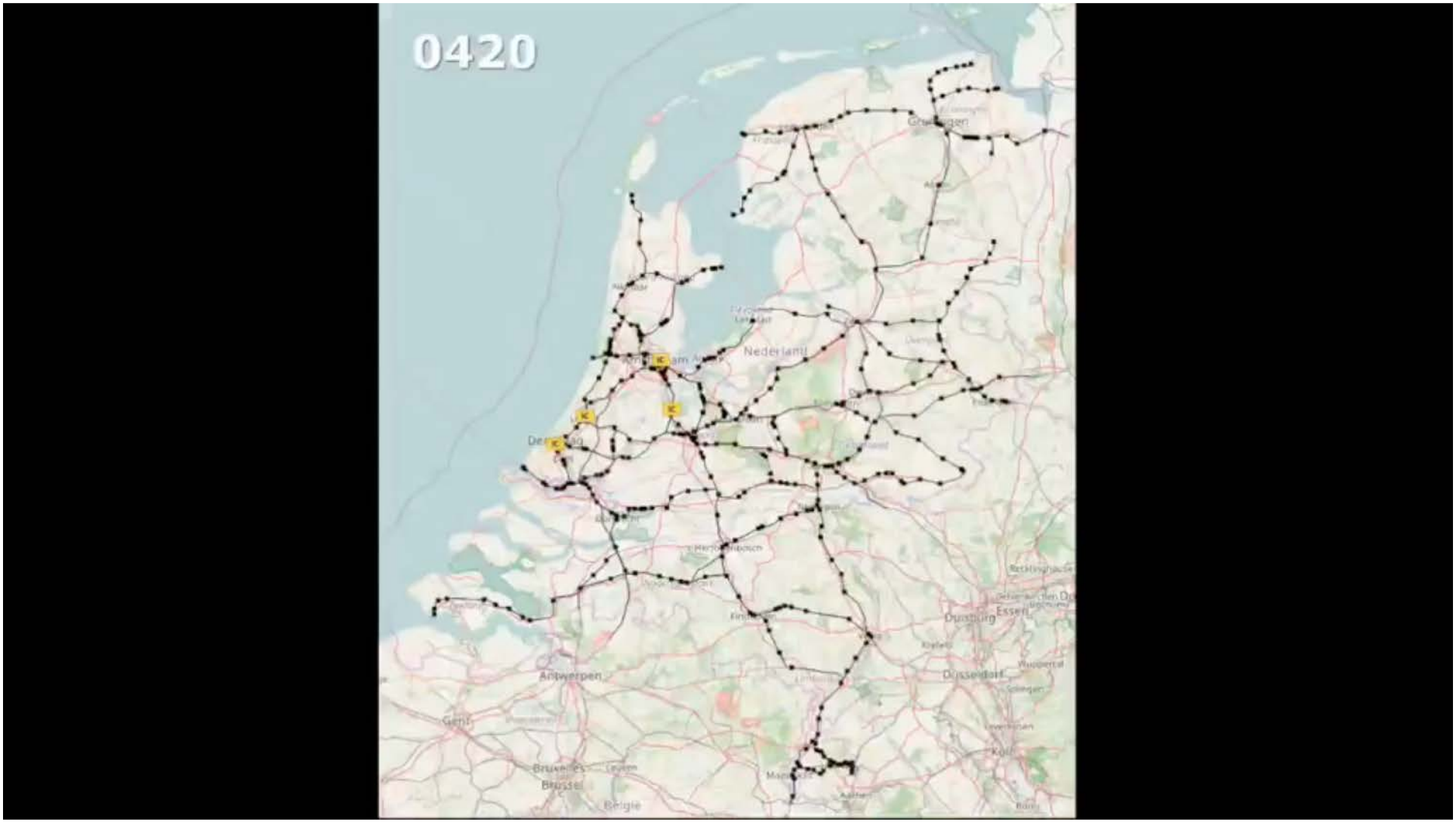
FTs on a diet
Graph rewriting

Reduce, reduce, reduce
- symmetry reduction
- partial-order reduction
- don't care detection

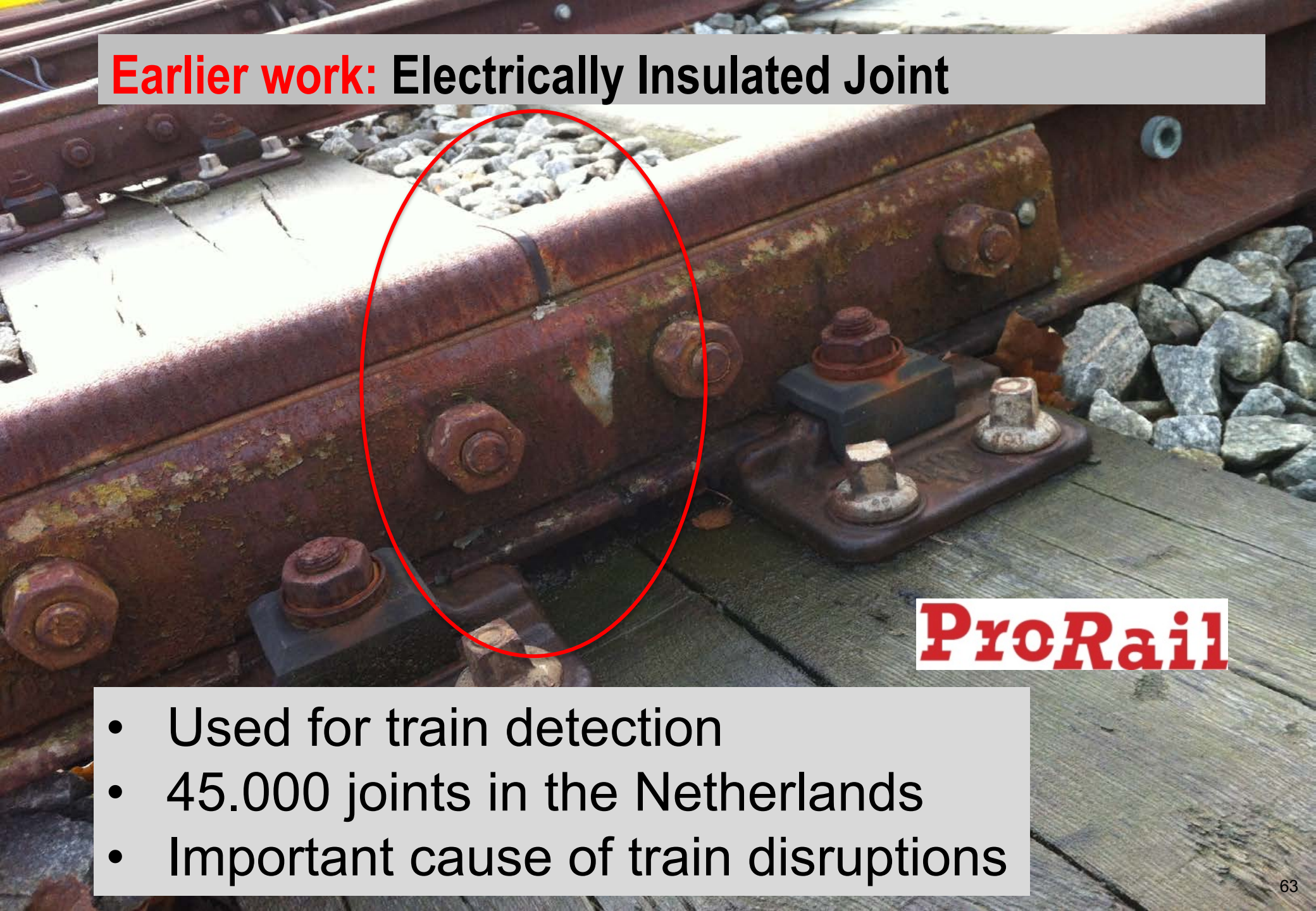
Smart state space generation
- Compositionality
- don't care detection
- Partial: optimistic / pessimistic

Smart algos
- Stochastic MC
- Metric specific computations
- Statistical MC
- Rare event simuluation

Fitting all together: meta modeling

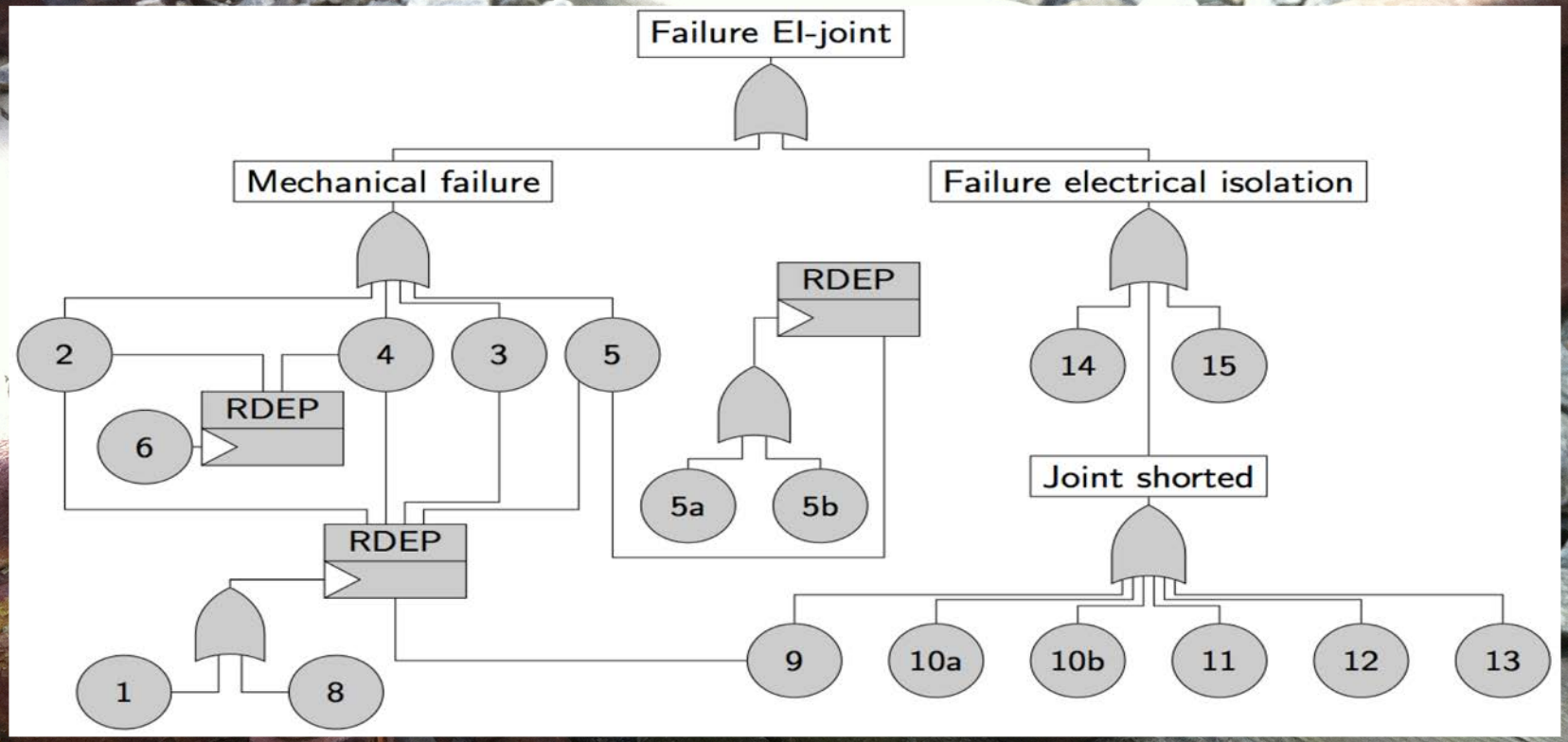

0420
Nederland
Antwerpen
Gent
Brussel
België
Duisburg
Essen
Düsseldorf

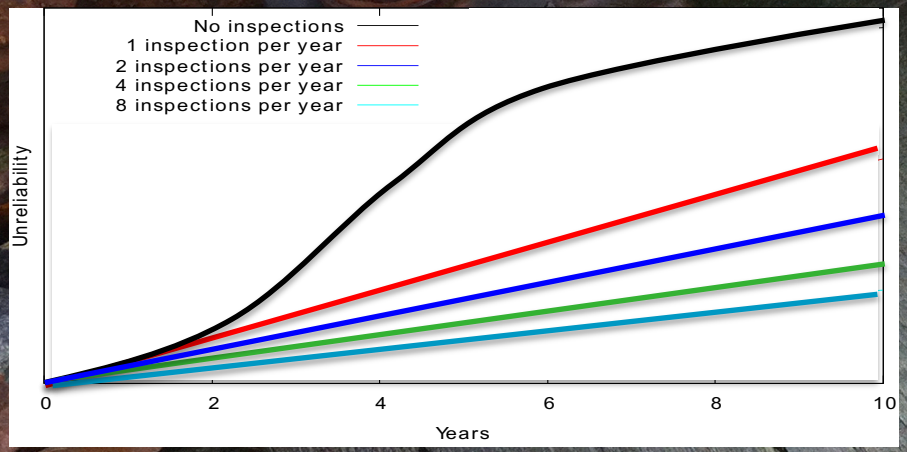
Earlier work: Electrically Insulated Joint

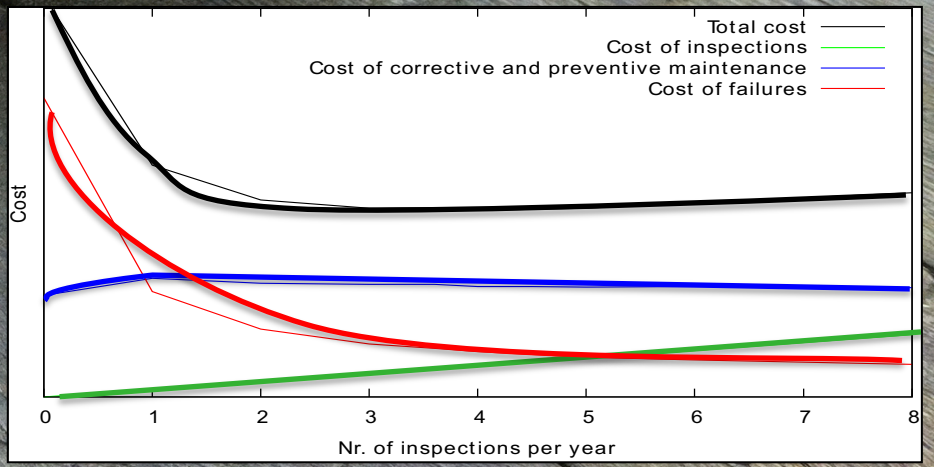


- Used for train detection
- 45.000 joints in the Netherlands
- Important cause of train disruptions

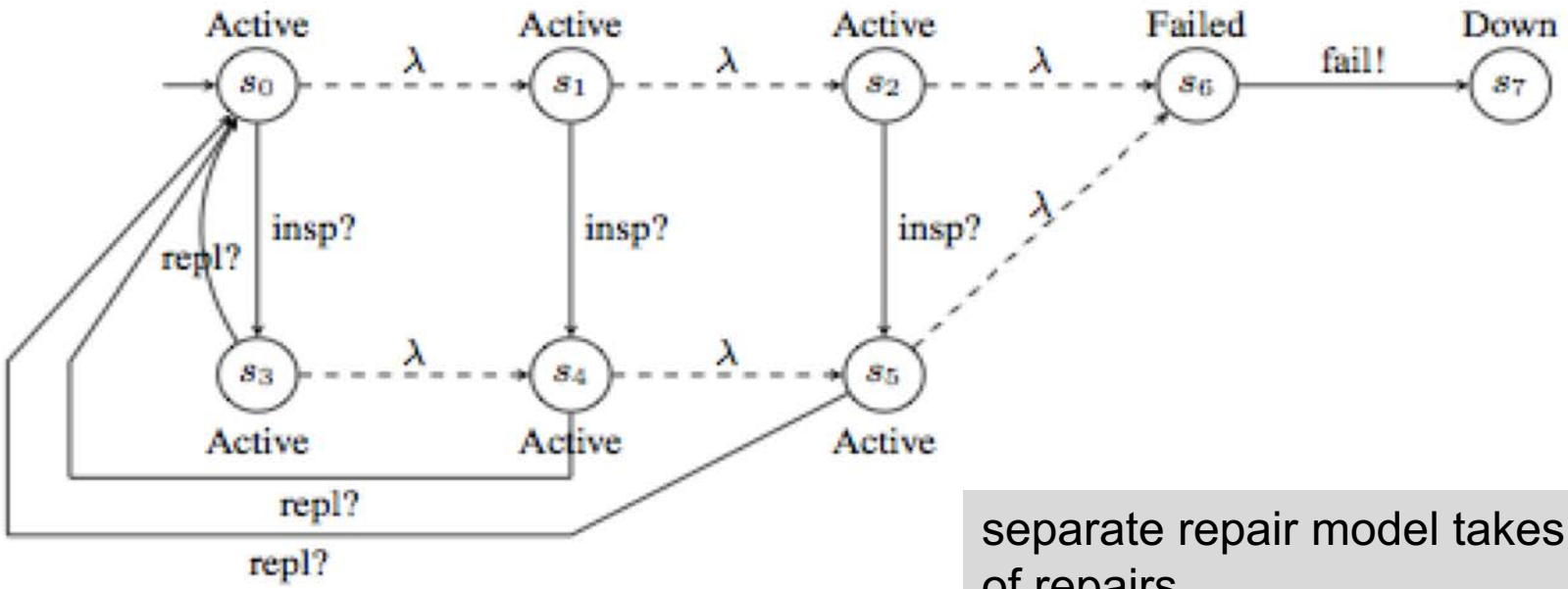
EI Joint: analysis results







Maintenance models (simplification)

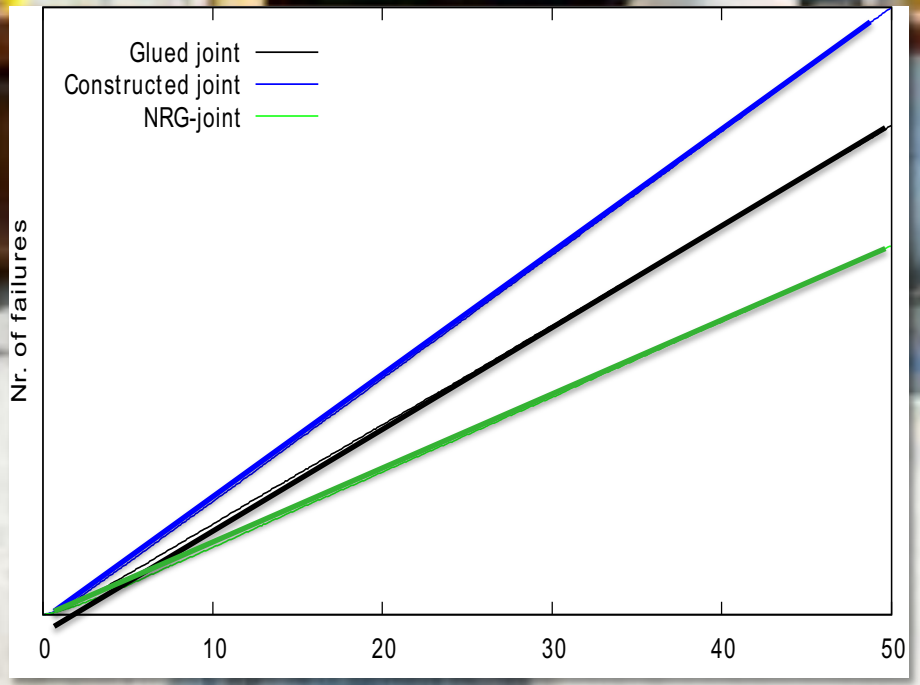


separate repair model takes care of repairs

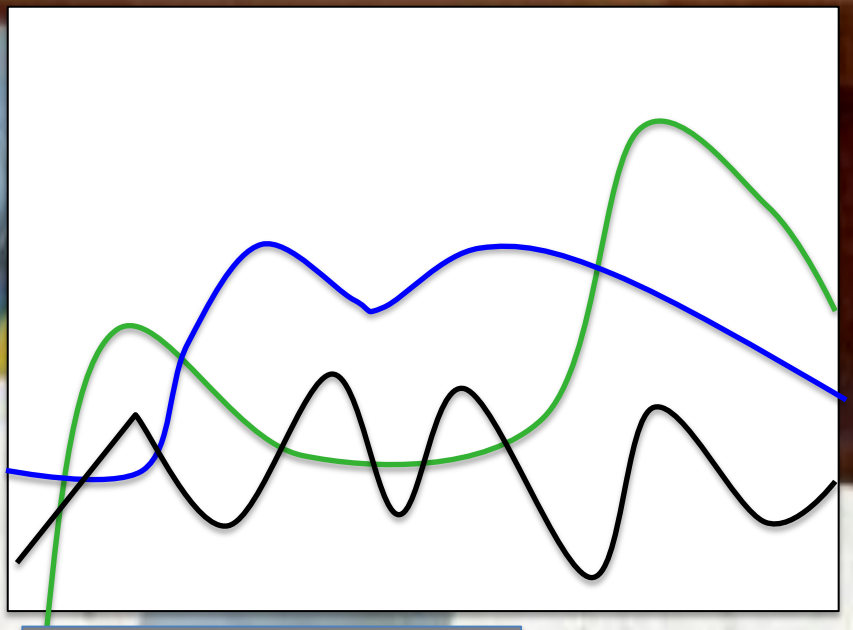
NedTrain models very similar

New joint type: NRG joint

- Investment cost effective?



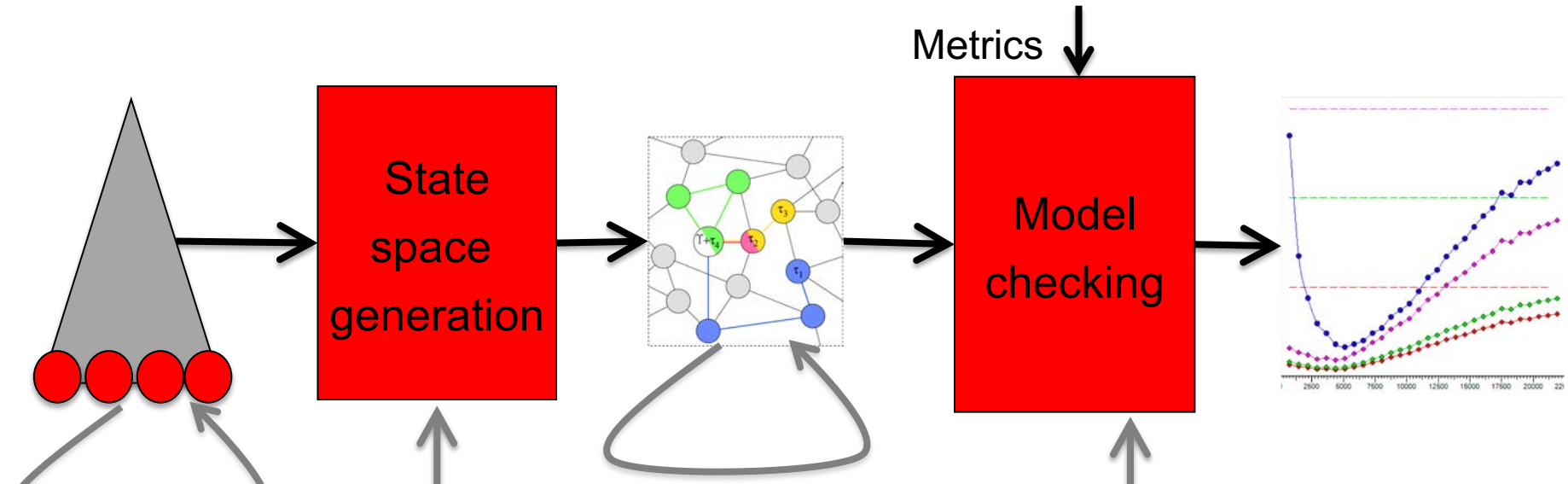
failures



costs

- More sensitive to variations in maintenance policy
- Currently extending the model

FT analysis: more, faster, bigger, better



FTs on a diet
Graph rewriting

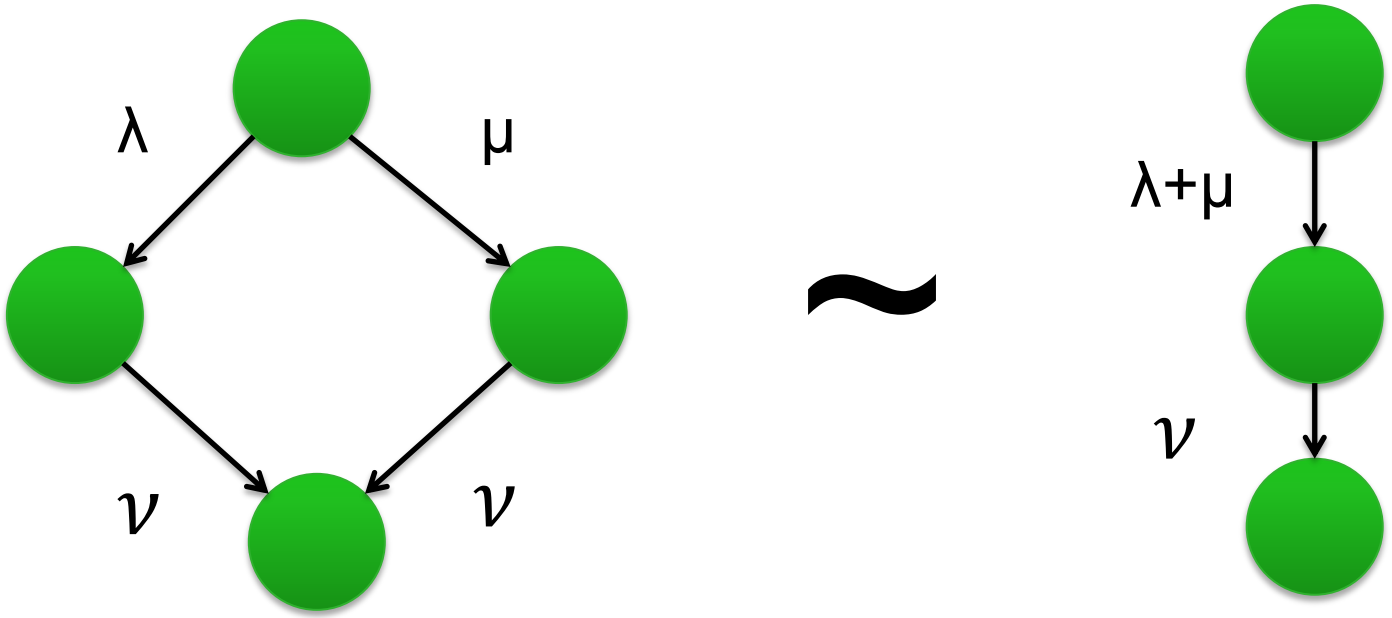
Reduce, reduce, reduce
- symmetry reduction
- partial-order reduction
- don't care detection

Smart state space generation
- Compositionality
- don't care detection
- Partial: optimistic / pessimistic

Smart algos
- Stochastic MC
- Metric specific computations
- Statistical MC
- Rare event simuluation

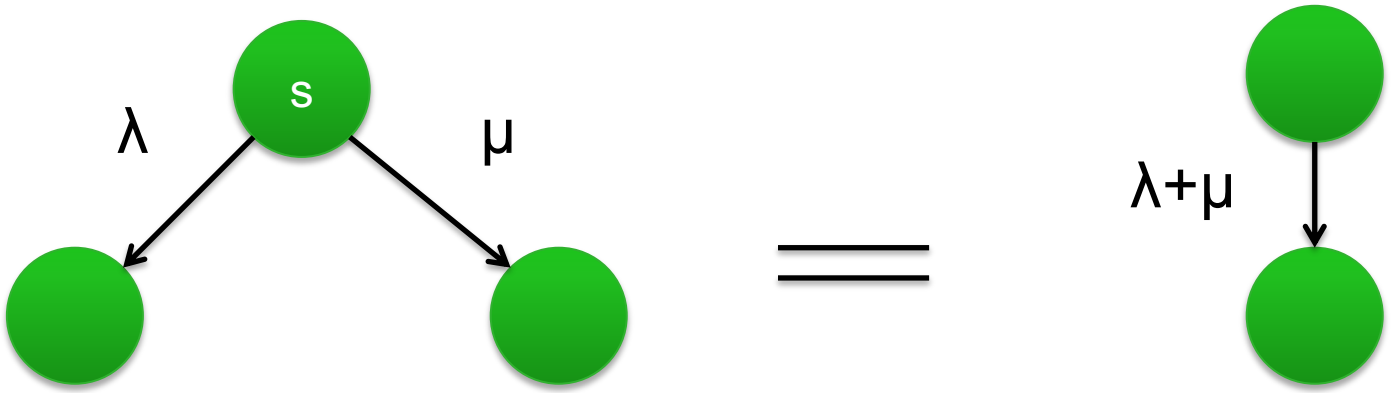
Fitting all together: meta modeling

Strong Bisimulation



Why is this correct ?

Bisimulation



operational / simulation view:

- race condition between exponentials
- take the one that expires first

→ minimum of two exponential distributions

operational / simulation view:

- take 2 random samples from exponential distributions
- look which is smallest
- take that transition

→ minimum of two exponential distributions

Minimum of exponentials

$X \sim \text{Exp}(\lambda)$ X, Y independent

$Y \sim \text{Exp}(\mu)$

$\min(X,Y) \sim \text{Exp}(\lambda+\mu)$

Strong Markovian bisimulation (sketch!)

Let R be an equivalence relation over S.

Then R is a strong Markovian bisimulation relation if for all (s,t) in **R**

- for interactive transitions

s – a → s’ implies t – a → t’ for some t’ with (s’, t’) in **R**

- for Markovian transitions

sum all outgoing Markovian rate has to be the same in s and t.

Definition 5 (Strong bisimulation). *Let $\mathcal{I} = (S, Act, \longrightarrow, \Longrightarrow, s_0)$ be an IMC. An equivalence relation $R \subseteq S \times S$ is a* strong bisimulation *on $\mathcal{I}$ if for any $(s,t) \in R$ and equivalence class $C \in S/R$ the following holds:*

1. *for any $\alpha \in Act$, $\mathbf{T}(s,\alpha,C) = \mathbf{T}(t,\alpha,C)$, and*
2. *$s \stackrel{\tau}{\not\longrightarrow}$ implies $\mathbf{R}(s,C) = \mathbf{R}(t,C)$.*

States s and s' are strongly bisimilar, denoted $s \sim s'$, if $(s,s') \in R$ for some strong bisimulation R.

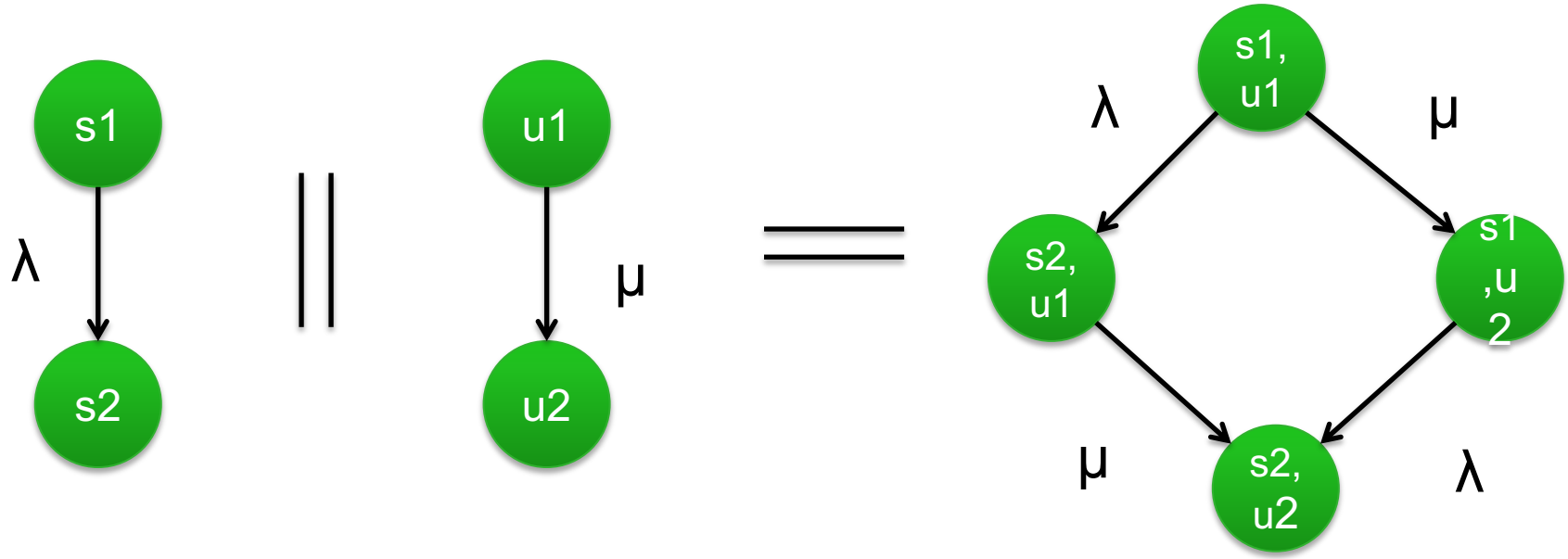
UN

Congruence properties: Hiding & composition

~ is a congruence wrt parallel composition and hiding

- What does this mean?
- Why is it important?
- How to prove this statement?

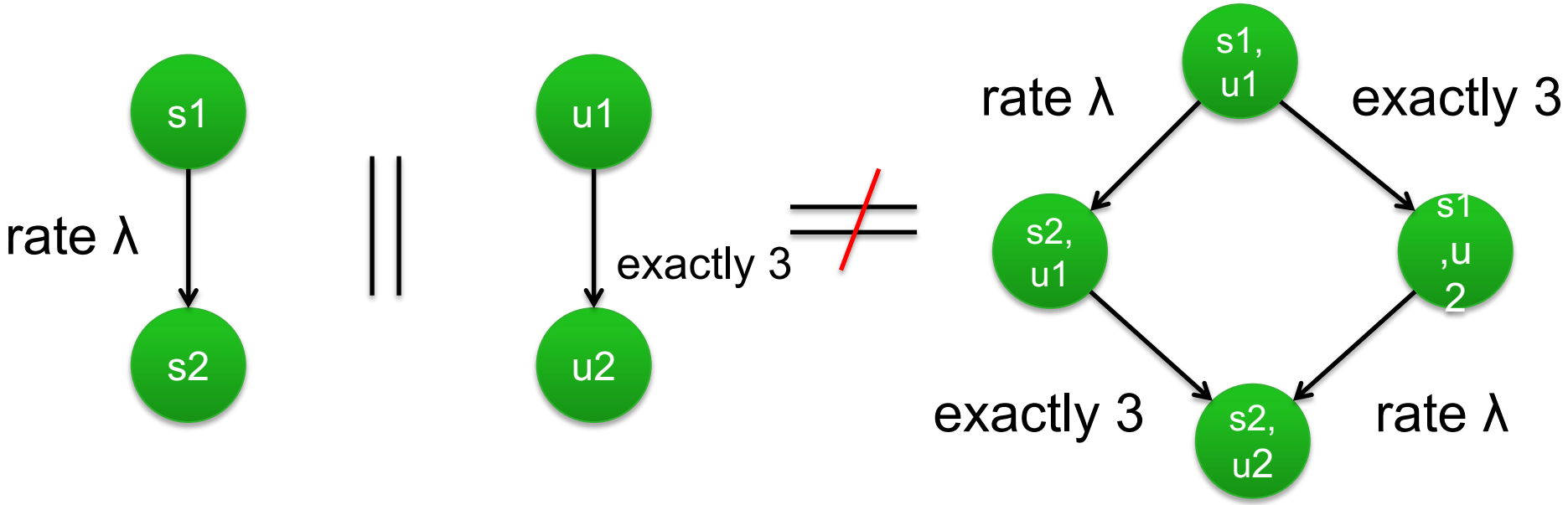
Parallel composition



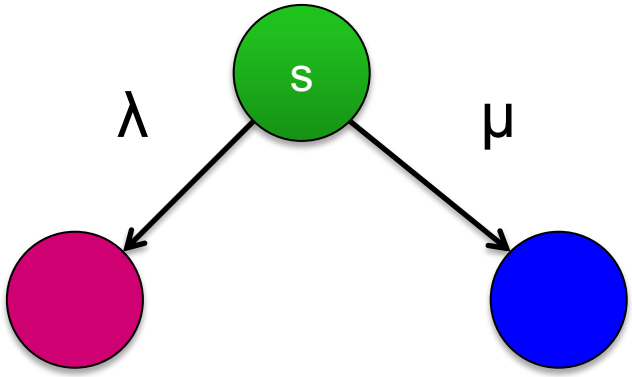
Why is this correct ?

Assignment (homework)

This only works for exponentials !

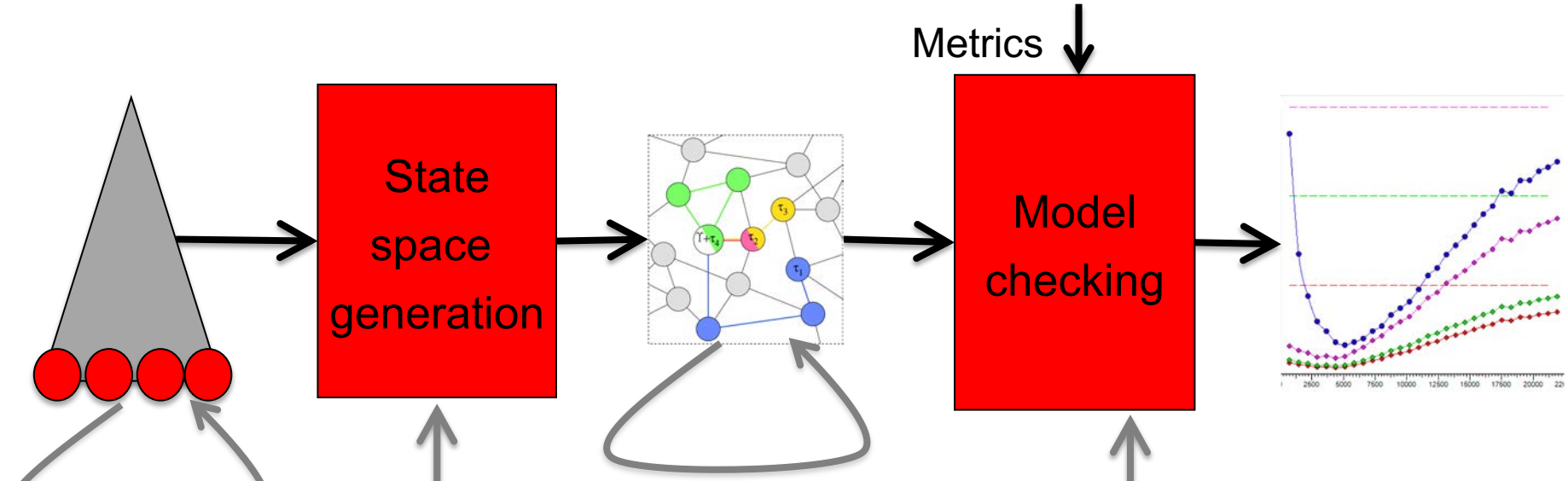


More Probabilities



What is the probability to end up in pink?

FT analysis: more, faster, bigger, better



FTs on a diet

Graph rewriting

Reduce, reduce, reduce

- symmetry reduction
- partial-order reduction
- don't care detection

Smart state space generation

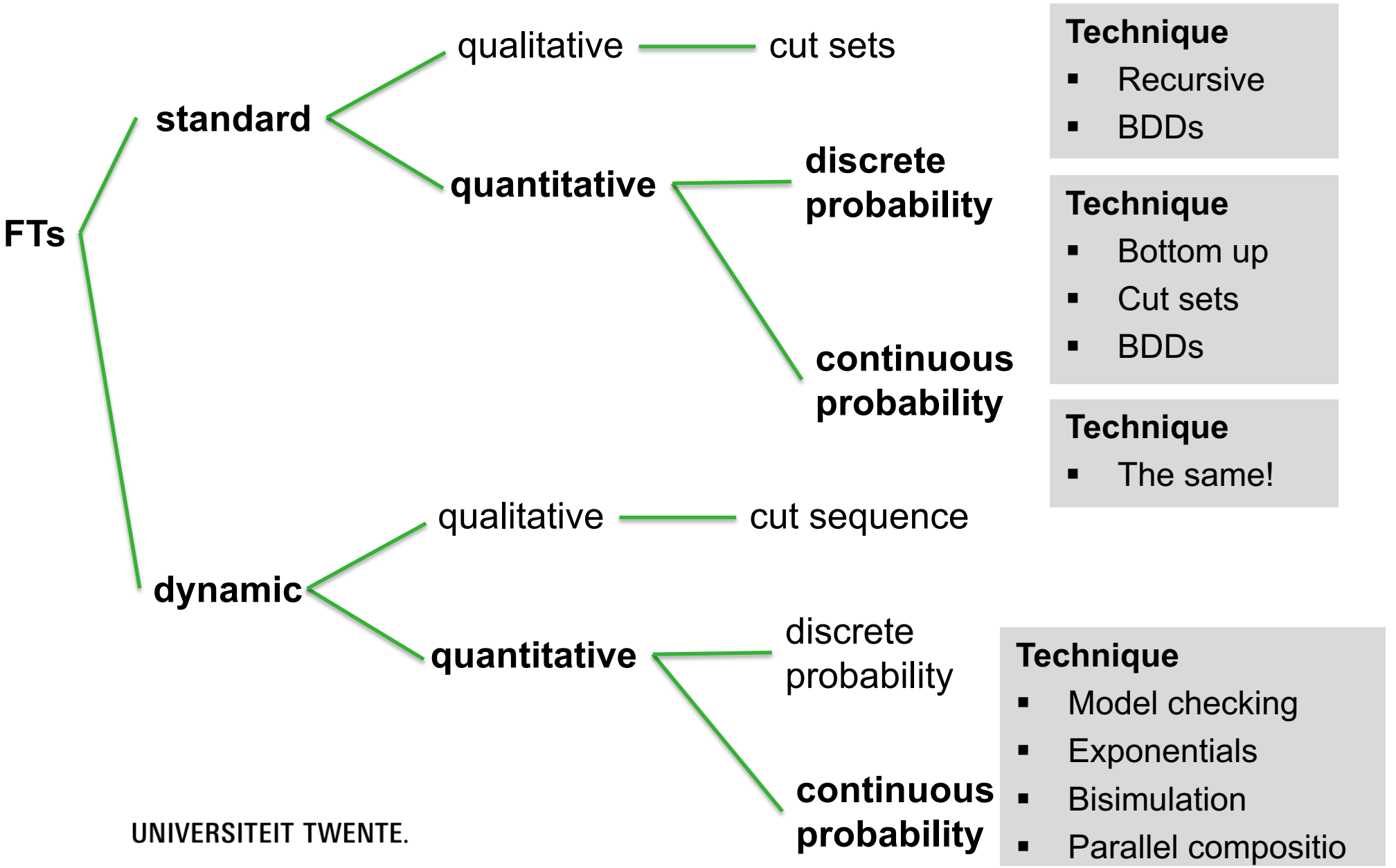
- Compositionality
- don't care detection
- Partial: optimistic / pessimistic

Smart algos

- Stochastic MC
- Metric specific computations
- Statistical MC
- Rare event simuluation

Fitting all together: meta modeling

Overview


FTs
standard
qualitative
cut sets
quantitative
discrete probability
continuous probability
dynamic
qualitative
cut sequence
quantitative
discrete probability
continuous probability
Technique
Recursive
BDDs
Technique
Bottom up
Cut sets
BDDs
Technique
The same!
Technique
Model checking
Exponentials
Bisimulation
Parallel compositio