UNIVERSITY
OF TWENTE.

Risk Management

Risk Assessment Techniques #1

Fault Tree Analysis

Carlos E. Budde

Contents

- Fault Trees
  - What & Why
- Fault Tree Analysis
  - Discrete time
  - Continuous time
- FTA in practice
  - Tools & benchmarks
  - Concrete examples (the real deal)

Contents

- Fault Trees
  - What & Why
- Fault Tree Analysis
  - Discrete time
  - Continuous time
- FTA in practice
  - Tools & benchmarks
  - Concrete examples (the real deal)

Fault Trees

I beg your pardon?

- What is a fault?
- What is a tree?

Faults

- Failure = Fault

    Loss of functionality

    Bad performance

    Undesired event

"my car doesn't start"

"my car stops right after it starts"

"my car doesn't reach 60 km/h"

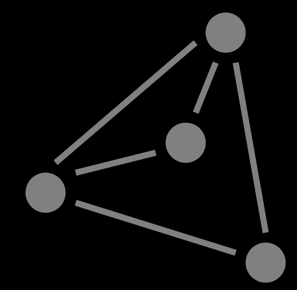
"my car burns too much oil"

"my car is stolen"

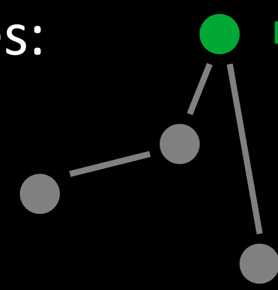
"I got lost on the way to CuriousU"

Trees

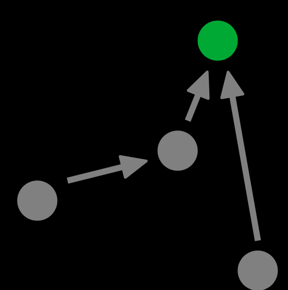
... are graphs ...



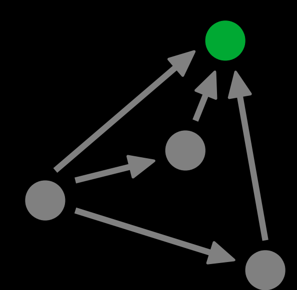
... without cycles:



Actually: **directed** graphs ...

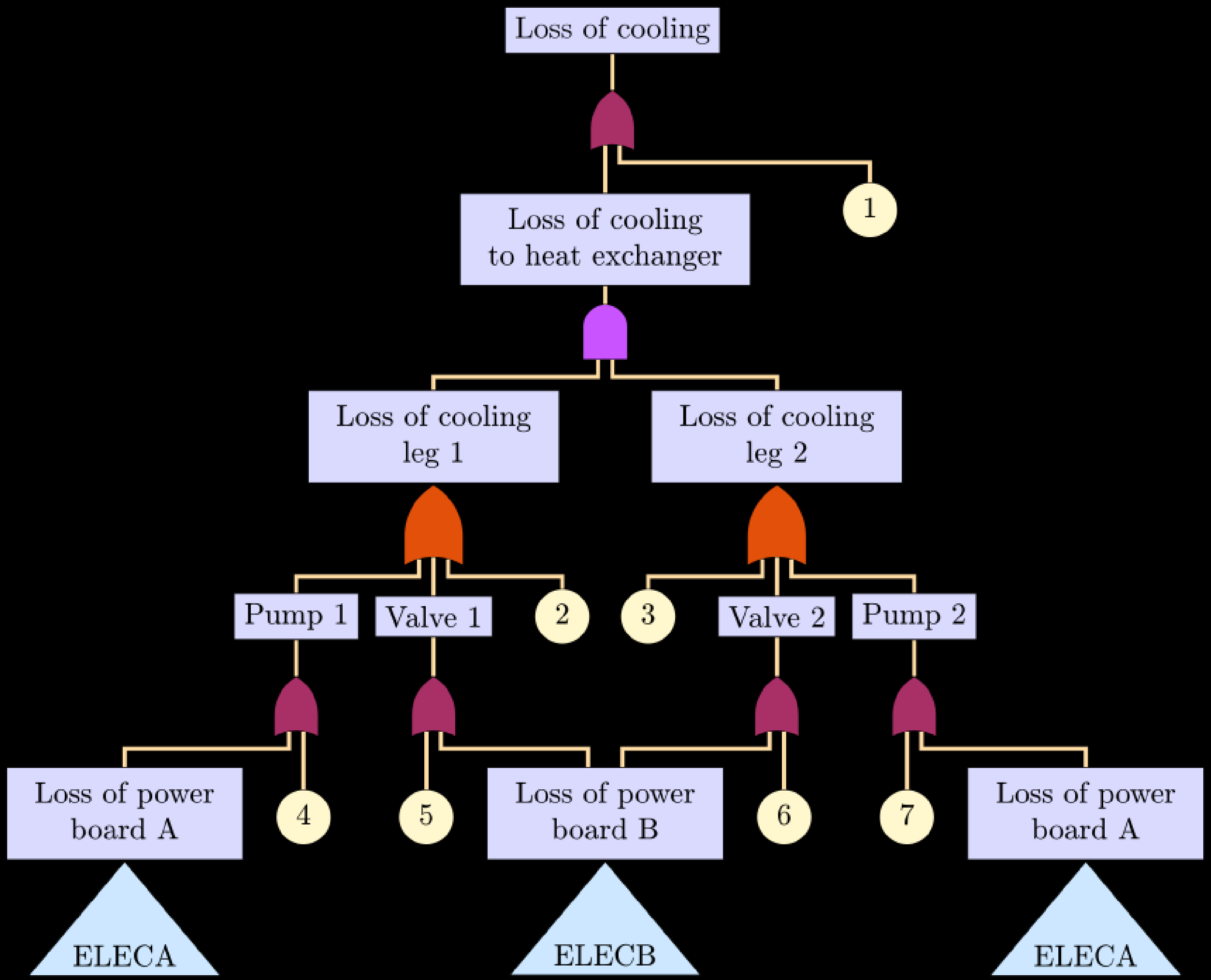


... without **directed** cycles:



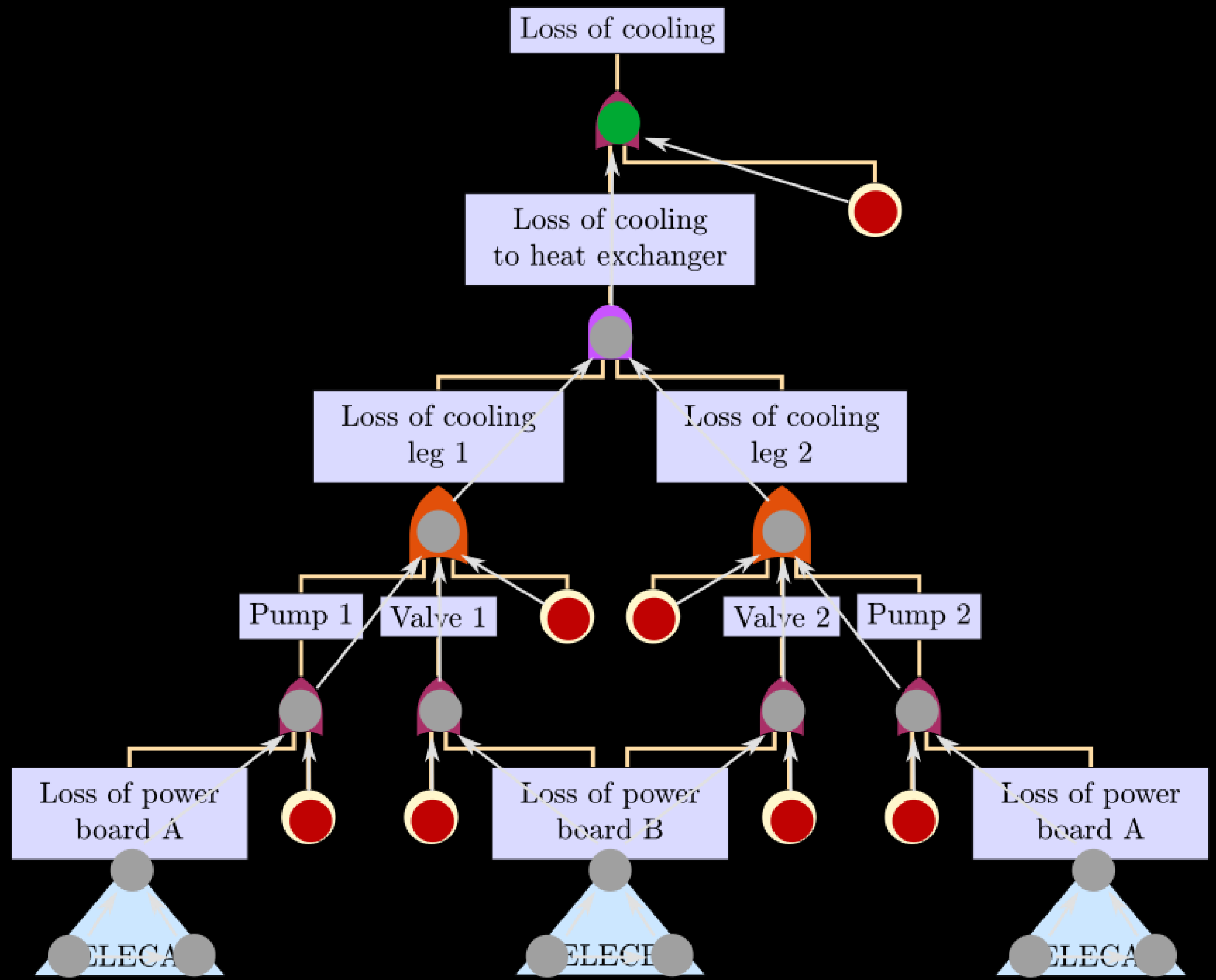
Directed
Acyclic
Graph

Fault Trees



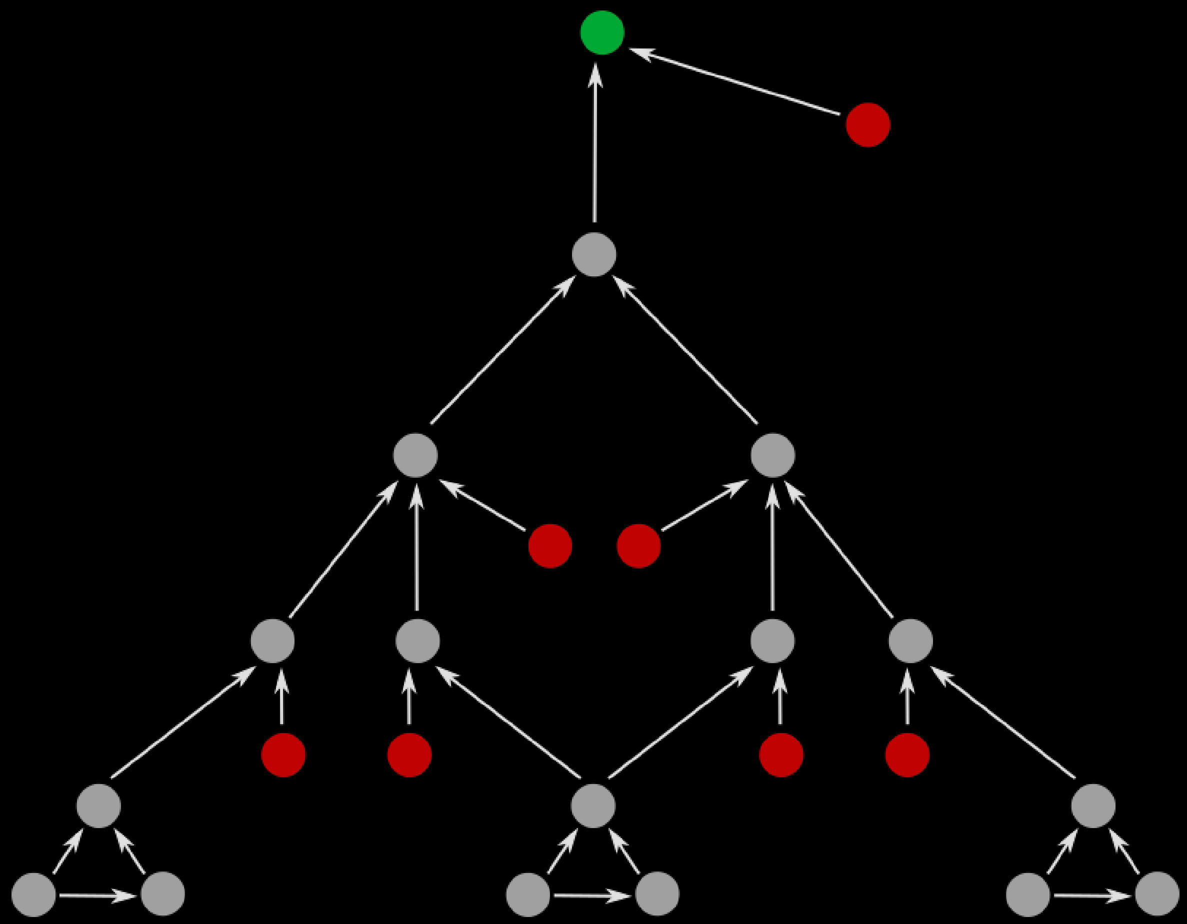
Loss of cooling
1
Loss of cooling to heat exchanger
Loss of cooling leg 1
Loss of cooling leg 2
Pump 1
Valve 1
2
3
Valve 2
Pump 2
Loss of power board A
4
5
Loss of power board B
6
7
Loss of power board A
ELECA
ELECB
ELECA

Fault Trees



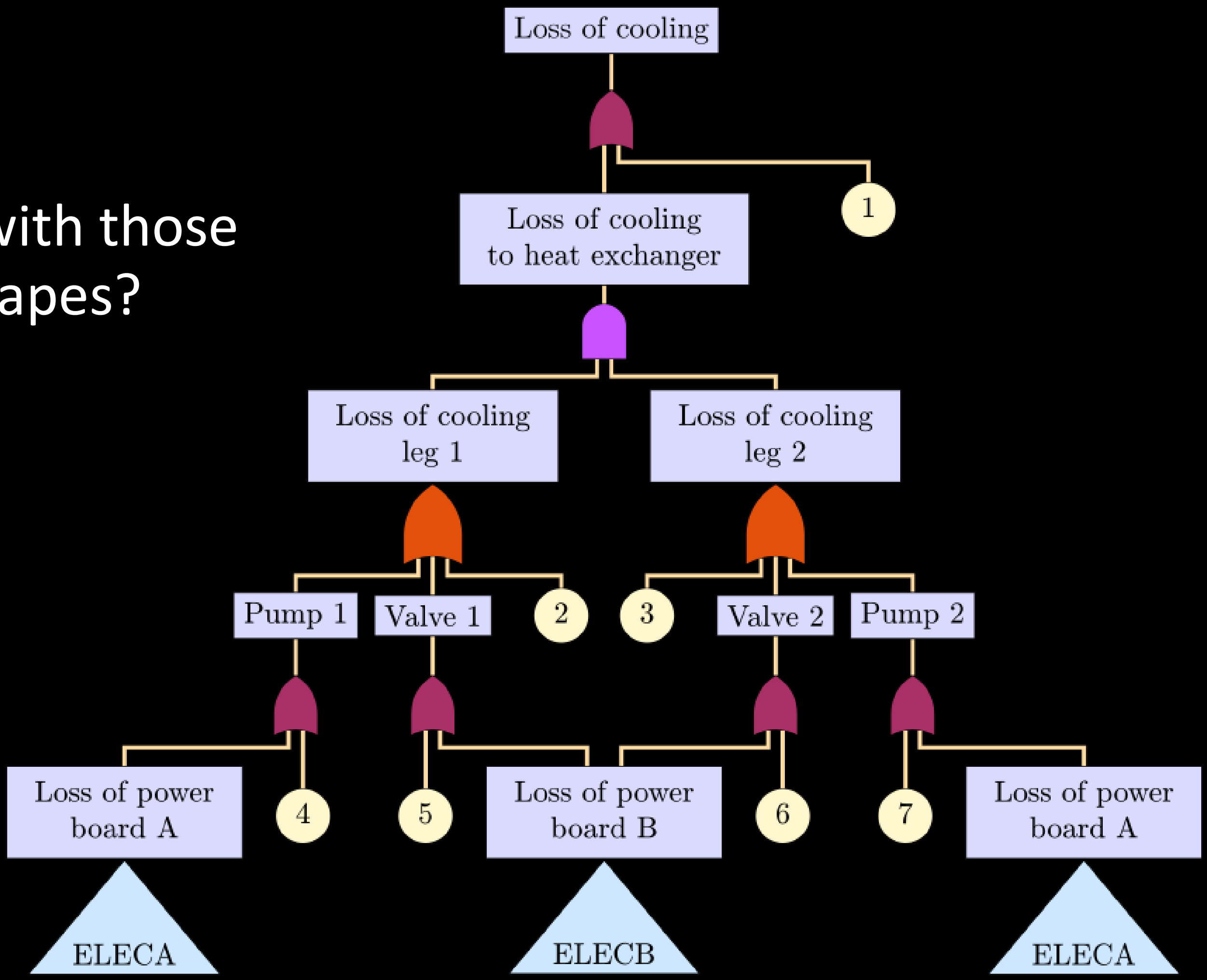
Loss of cooling
Loss of cooling to heat exchanger
Loss of cooling leg 1
Loss of cooling leg 2
Pump 1
Valve 1
Valve 2
Pump 2
Loss of power board A
Loss of power board B
Loss of power board A

Fault Trees

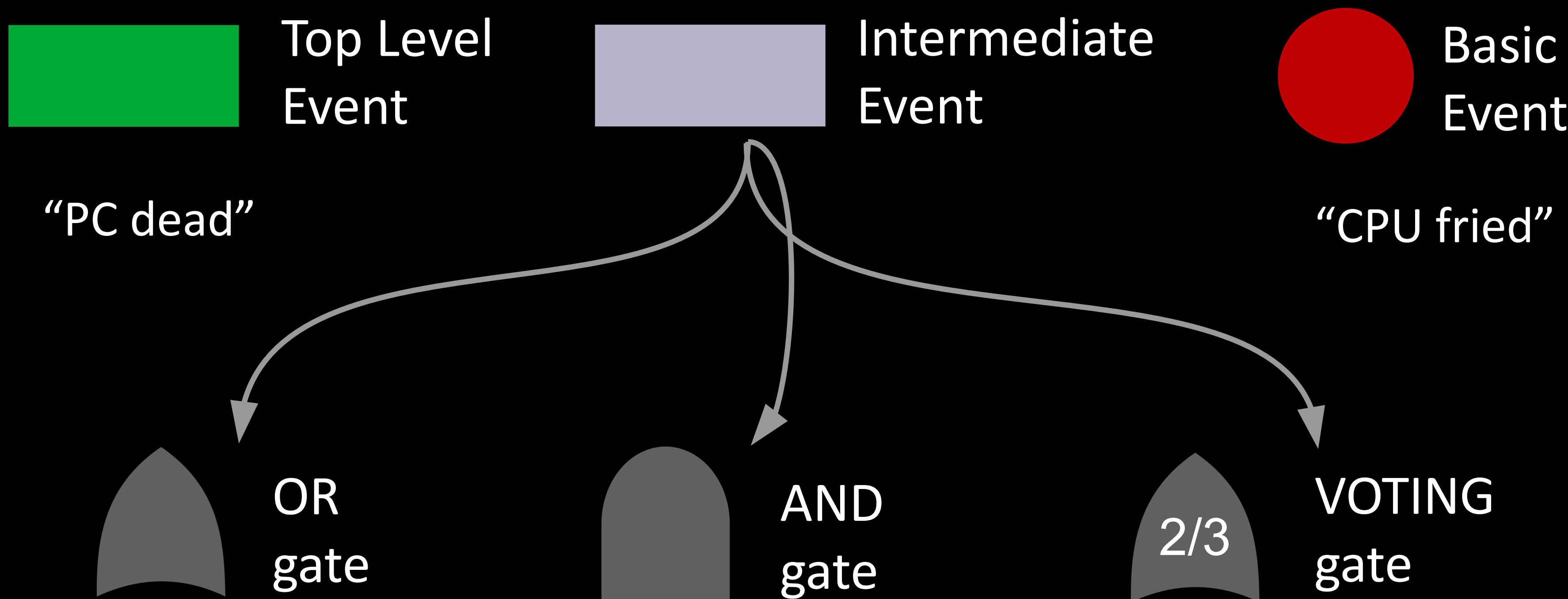


Fault Trees

What's with those weird shapes?



FT building blocks



PC dead if:

"CPU fried"
OR
"no power"

No power if:

"no AC"
AND
"UPS insufficient"

UPS insufficient if:

"2 out of 3
UPS fail"

FT building

- Describe how component failures interact:

  1. Define top undesired event (**TLE**)

  2. List all causes that could lead to it (1st level **IE**)

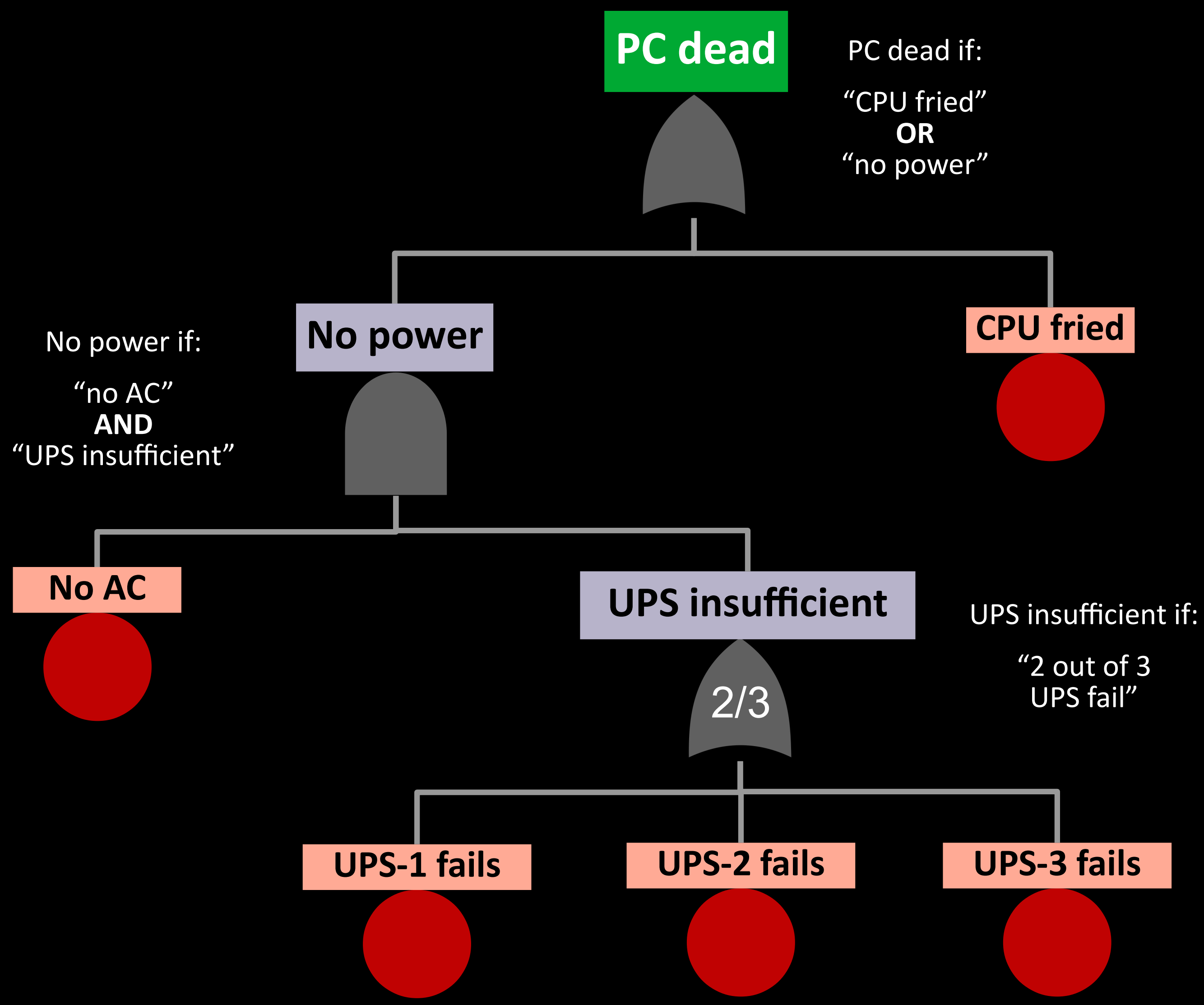
     ➔ Think of everything needed to keep the system operating normally

  3. What could cause each branch to fail?

     ➔ Repeat on each **IE** as in item 1.

  4. Stop when root causes reached (**BE**)

FT building


PC dead
PC dead if:
“CPU fried”
OR
“no power”
No power
CPU fried
No power if:
“no AC”
AND
“UPS insufficient”
No AC
UPS insufficient
UPS insufficient if:
“2 out of 3
UPS fail”
2/3
UPS-1 fails
UPS-2 fails
UPS-3 fails

So what?

Who cares?

¯_(ツ)_/¯

Let's see who cared…

- 1962: FTs developed in Bell Labs
  - Evaluate ICMB launch control system (**I**nter**C**ontinental **B**allistic **M**issile)

- FTs were originally designed for killing **lots** of people

Let’s see who cared...

- 1966: Boeing starts to use FTs
  - Civil aircraft design, e.g. Boeing 747

- FTs start to help keeping people safe

Let’s see who cared…

- 1975: FT analysis standardised
  - “Fault Tree Handbook” (1981 by Vesely et al.)
  - Nuclear power plants regulations

- FTs help to keep **lots** of people safe

Let’s see who cared…

- 2000: FTs in government and industry standards
  - “Fault Tree Handbook with Aerospace applications” (2002 by Vesely et al.)
  - Dynamic FTs and more
- FTs to the moon and back

Are FTs any good ***today***?

Movares
adviseurs & ingenieurs

Honeywell

VolkerRail

BOEING

AIRBUS

ARCADIS

NRG

Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

TOYOTA

delta π
performance improvement

esa

DB BAHN

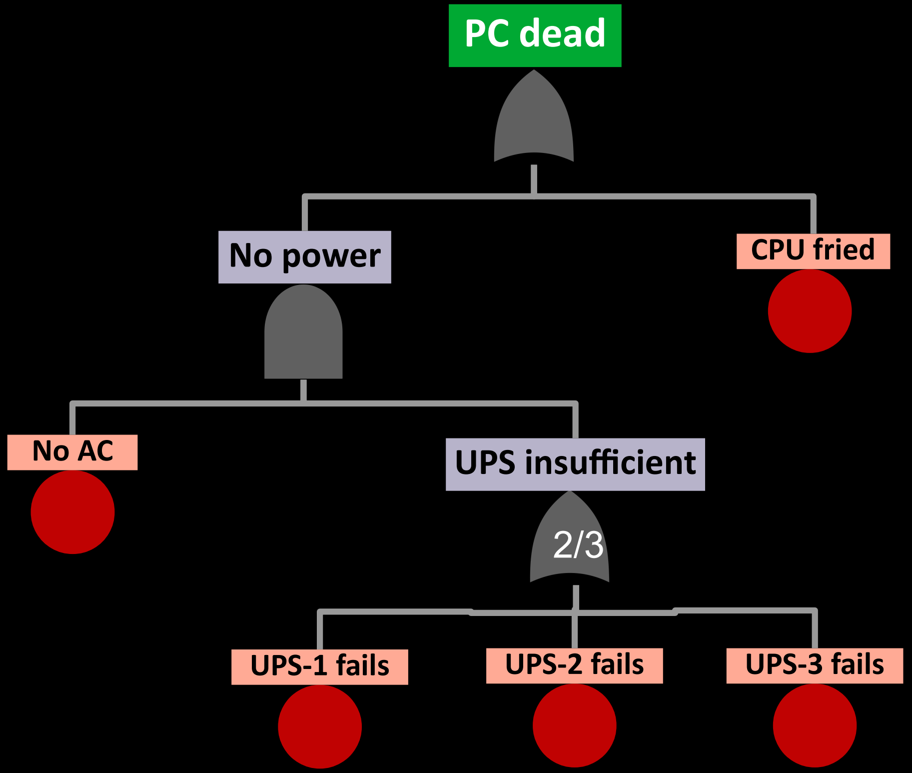
NASA

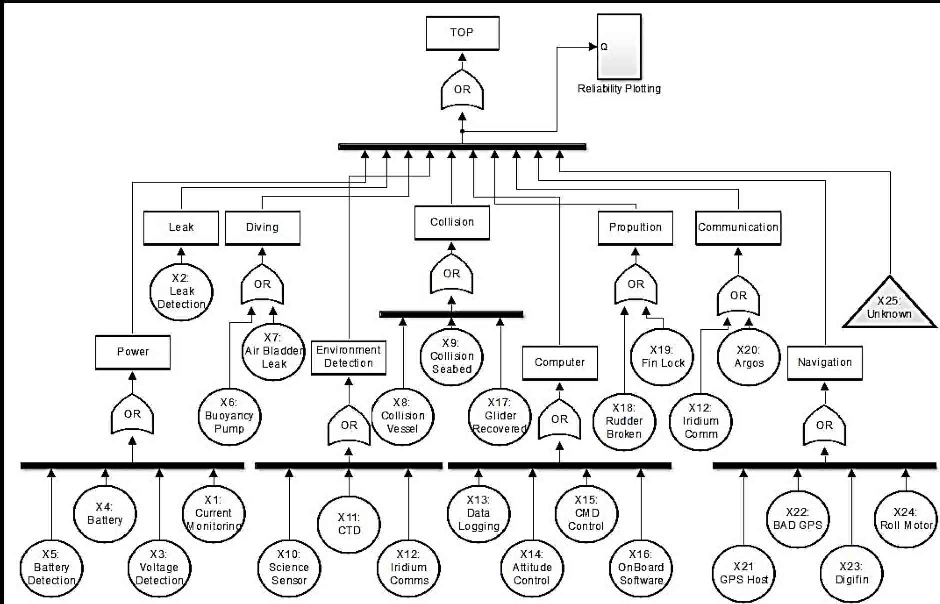
ProRail

Are FTs any good ***today***?

“ Today FTA is widely used in system safety and reliability engineering, and in all major fields of engineering.”

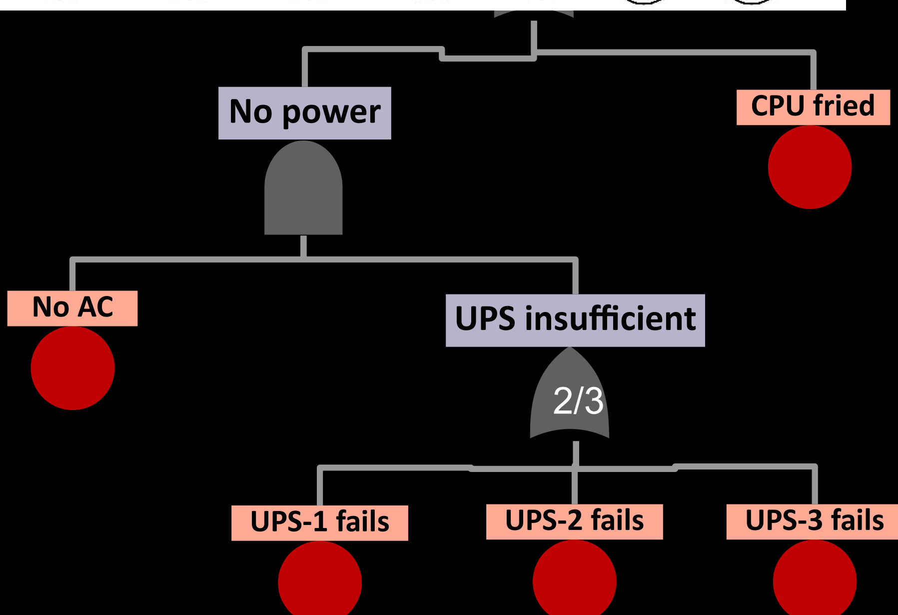
FTs are (graphical) **models**





TOP
OR
Reliability Plotting
Leak
Diving
Collision
Propultion
Communication
X2: Leak Detection
OR
OR
OR
OR
X25: Unknown
Power
X7: Air Bladder Leak
Environment Detection
X9: Collision Seabed
Computer
X19: Fin Lock
X20: Argos
Navigation
OR
X6: Buoyancy Pump
OR
X8: Collision Vessel
X17: Glider Recovered
OR
X18: Rudder Broken
X12: Iridium Comm
OR
X4: Battery
X1: Current Monitoring
X11: CTD
X13: Data Logging
X15: CMD Control
X22: BAD GPS
X24: Roll Motor
X5: Battery Detection
X3: Voltage Detection
X10: Science Sensor
X12: Iridium Comms
X14: Attitude Control
X16: OnBoard Software
X21 GPS Host
X23: Digifin

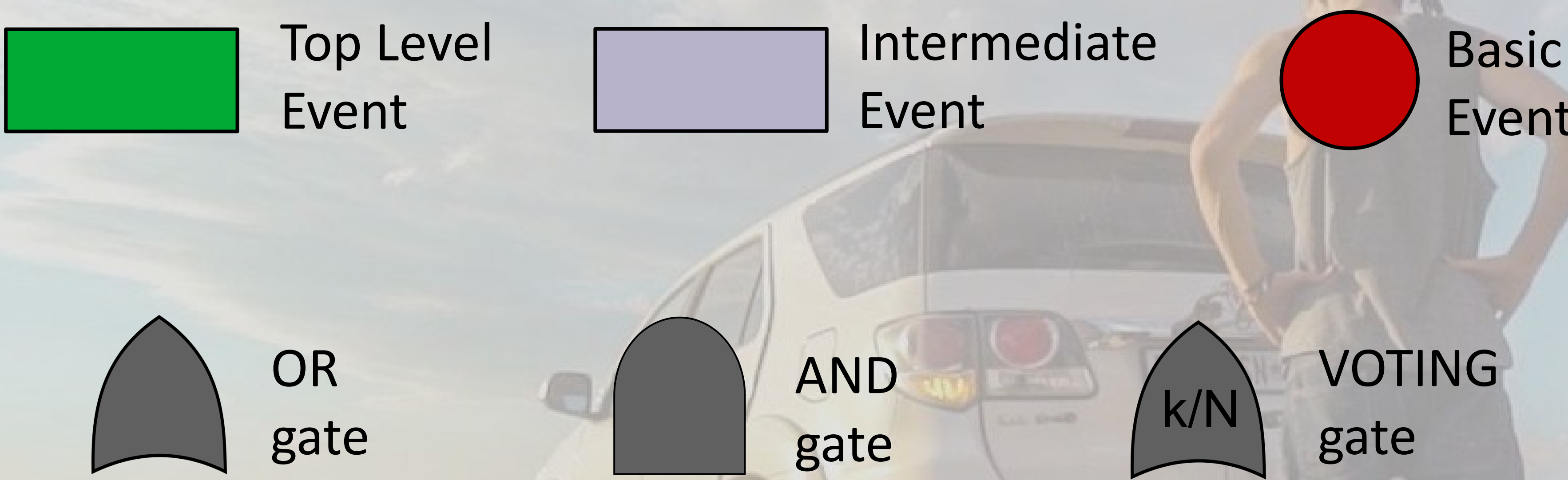
models



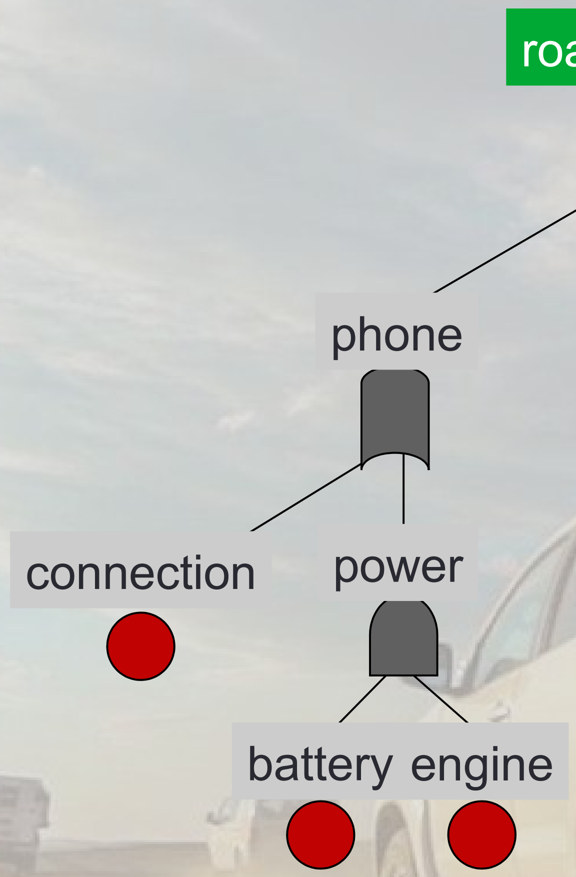
No power
CPU fried
No AC
UPS insufficient
2/3
UPS-1 fails
UPS-2 fails
UPS-3 fails

USA

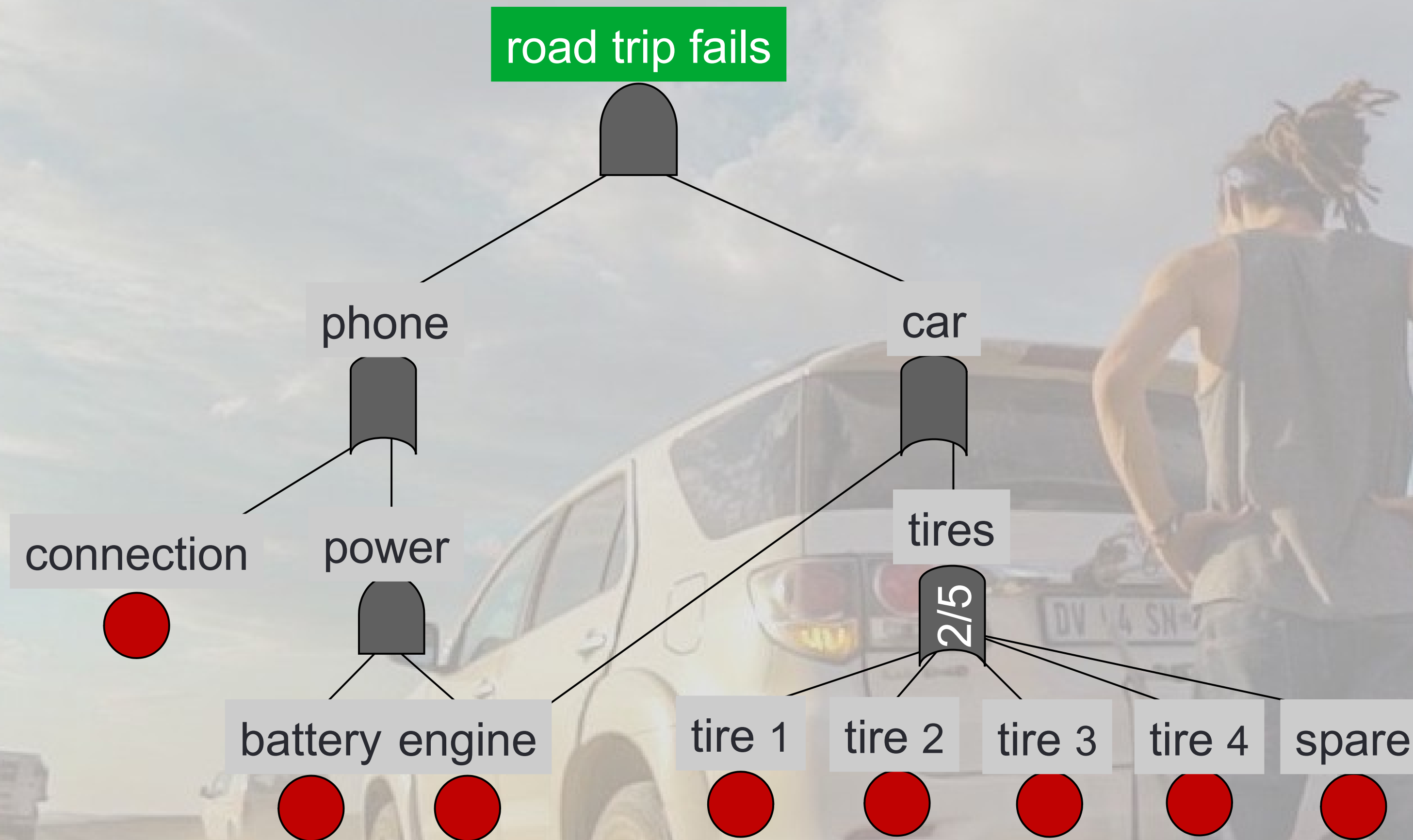
Running example: safe road trip



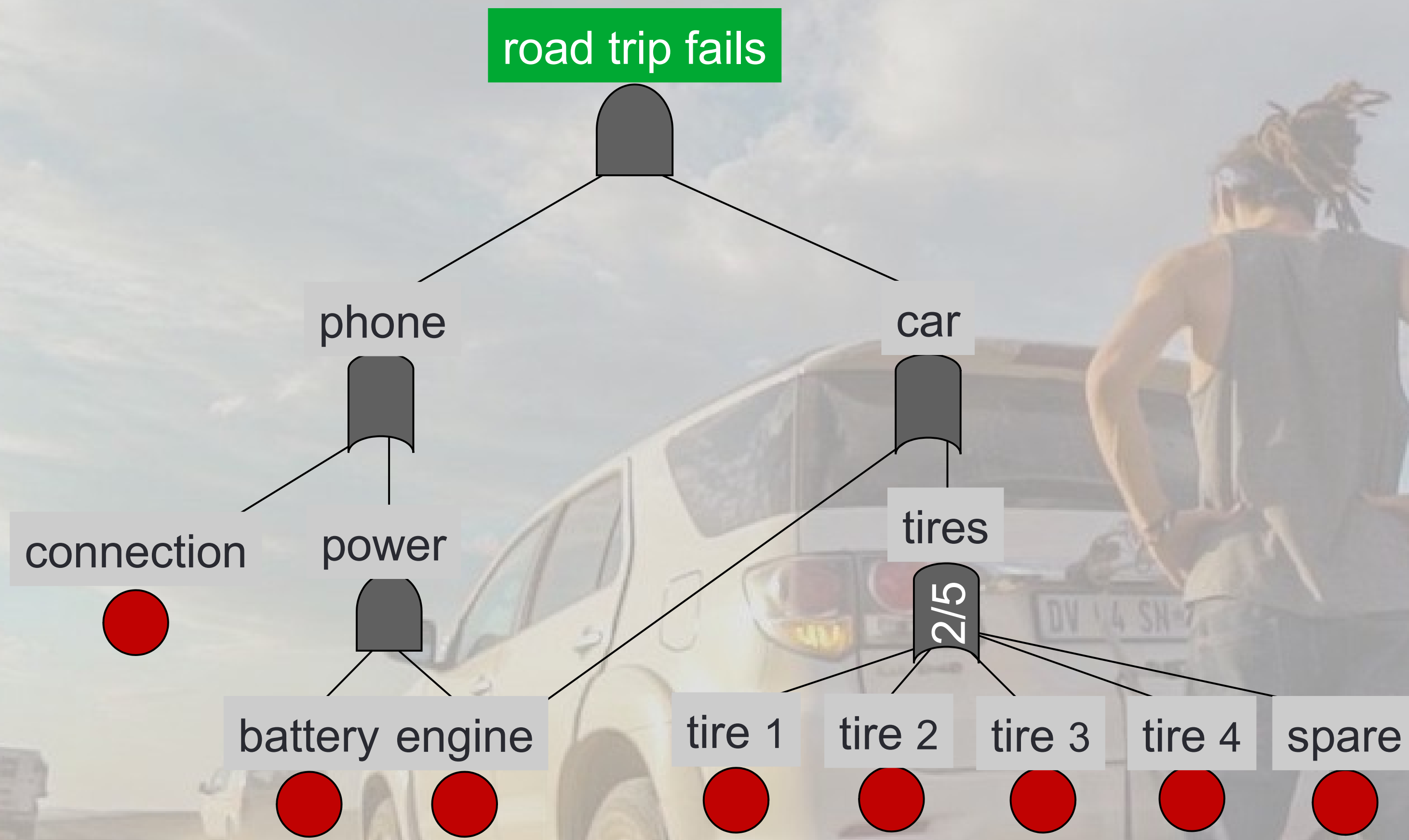
Running example: safe road trip



Running example: safe road trip



Running example: safe road trip



Cut sets: Which BEs make FT fail?

{battery, engine, tire 1, spare}

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

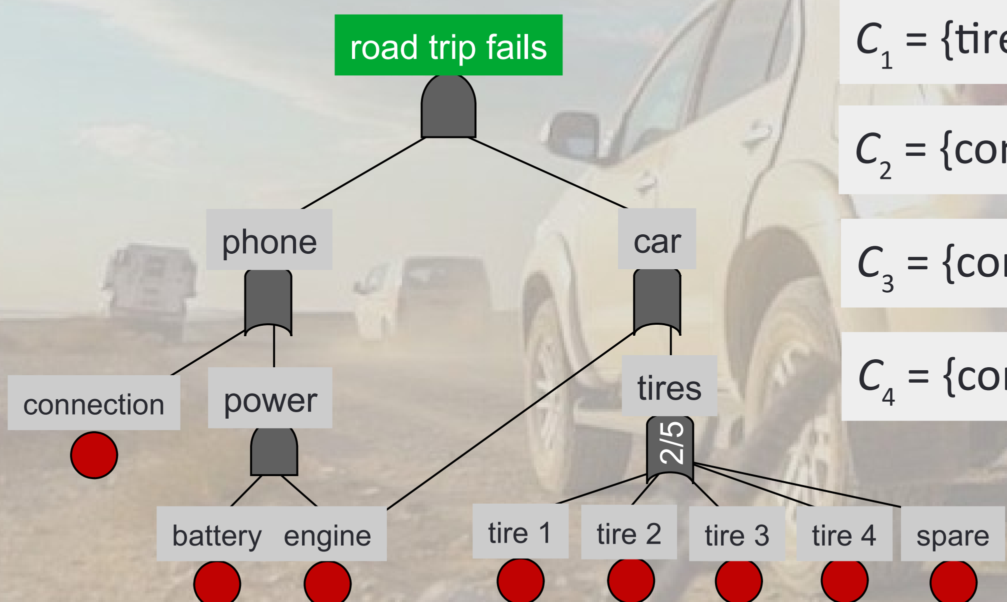
{connection, engine} **minimal cut set**

(Minimal) cut sets

- **Cut set**
  - Set ‘*C*’ of Basic Events that cause the Top Level Event
- **Minimal cut sets**
  - Cut set that is minimal: no proper subset of *C* is a cut set

(Minimal) cut sets

- **Cut set**
  - Set '*C*' of Basic Events that cause the Top Level Event
- **Minimal cut sets**
  - Cut set that is minimal: no proper subset of *C* is a cut set



C_1 = {tire 1, tire 2, tire 3, tire 4, battery}

C_2 = {connection, battery, engine, tire 1, spare}

C_3 = {connection, tire 1, spare}

C_4 = {connection, engine}

C_5 = {battery, engine}

(Minimal) cut sets

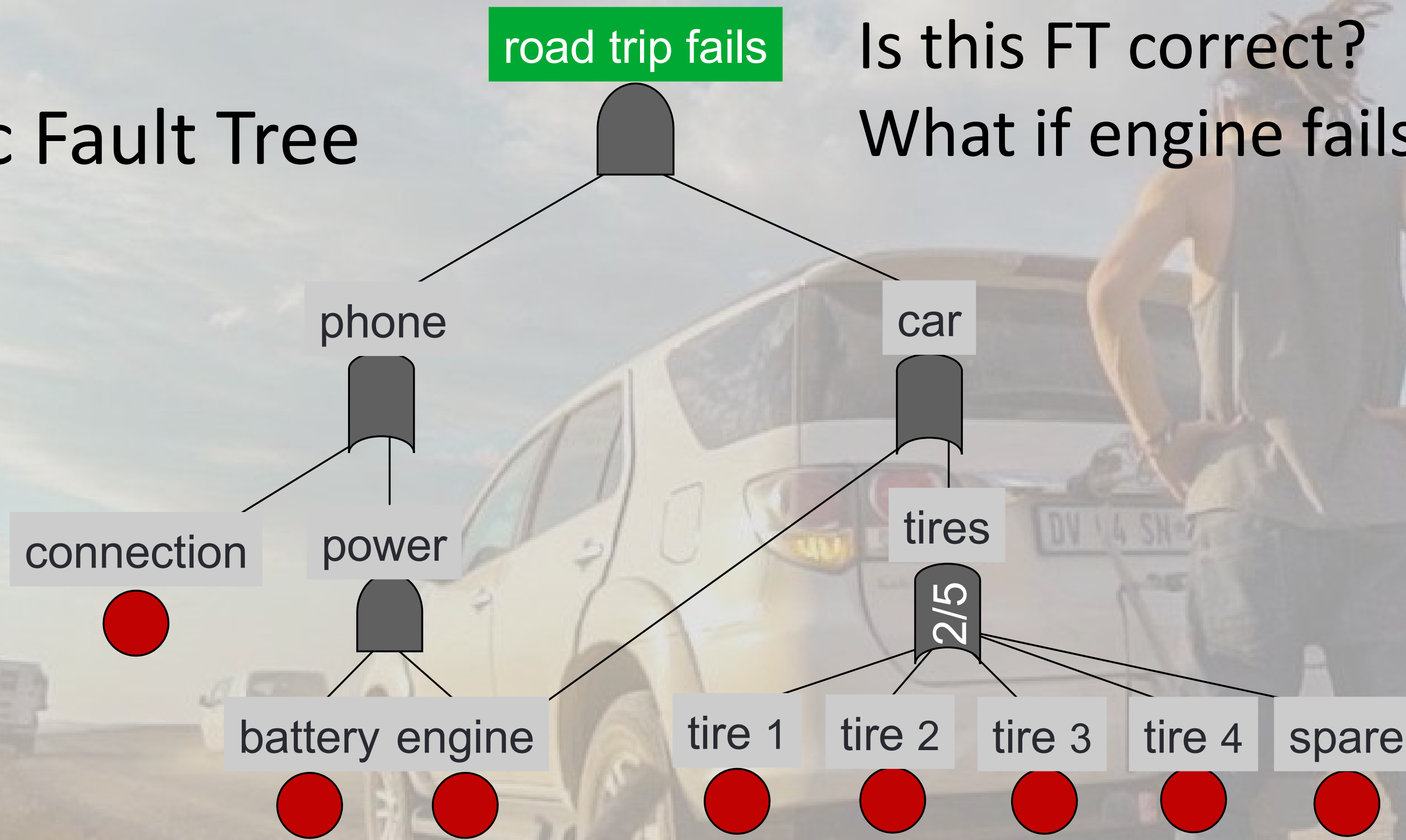
- **Cut set**
  - Set '*C*' of Basic Events that cause the Top Level Event
- **Minimal cut sets**
  - Cut set that is minimal: no proper subset of *C* is a cut set
- **Use of minimal cut sets**
  - Identify weak points
    - Too small cut sets
    - Interpretation by experts: is this acceptable?
  - Validation of Fault Trees
    - If all BEs in *C* fail, should the system fail?

Validating our road trip FT

Static Fault Tree

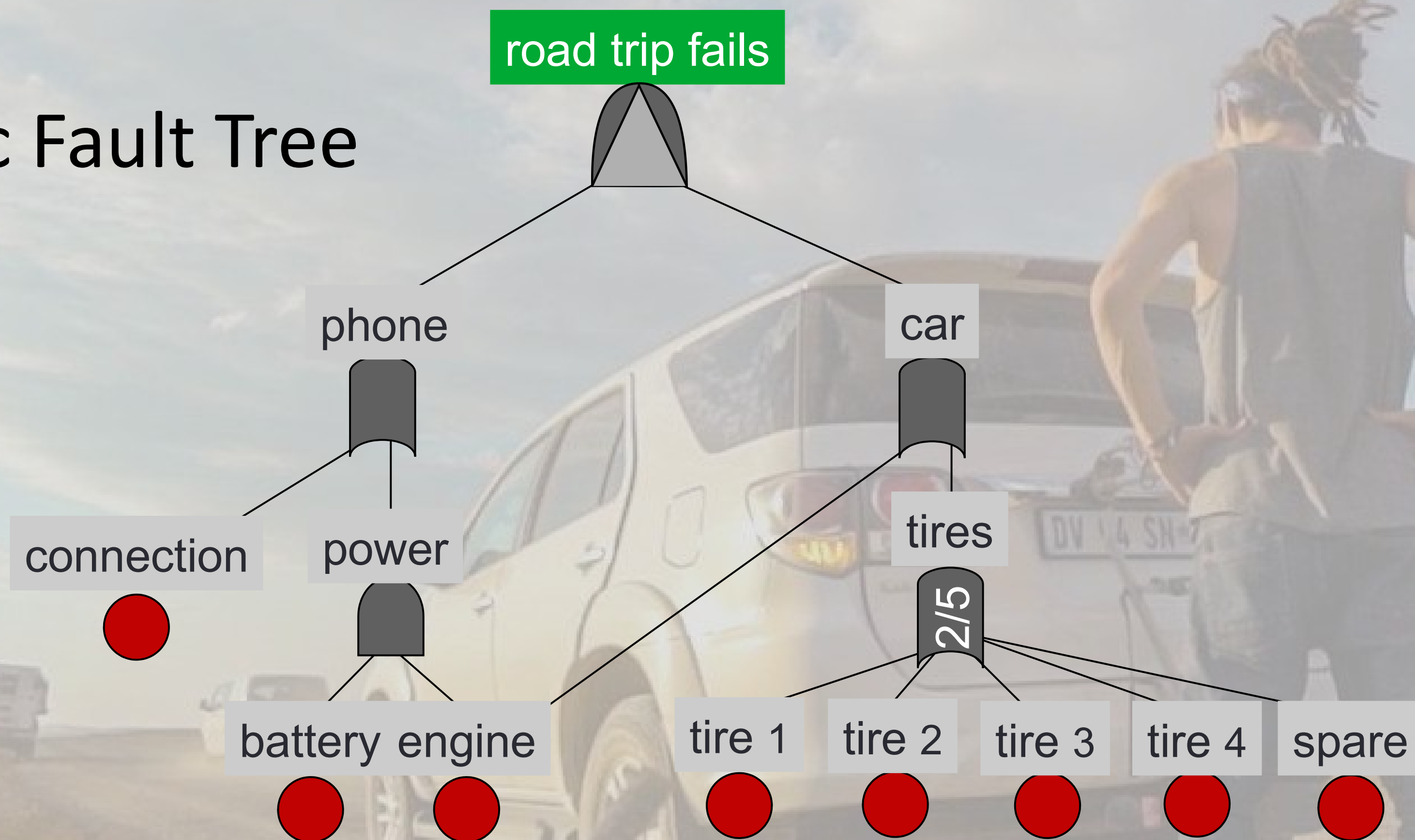
Is this FT correct?

What if engine fails **first**?



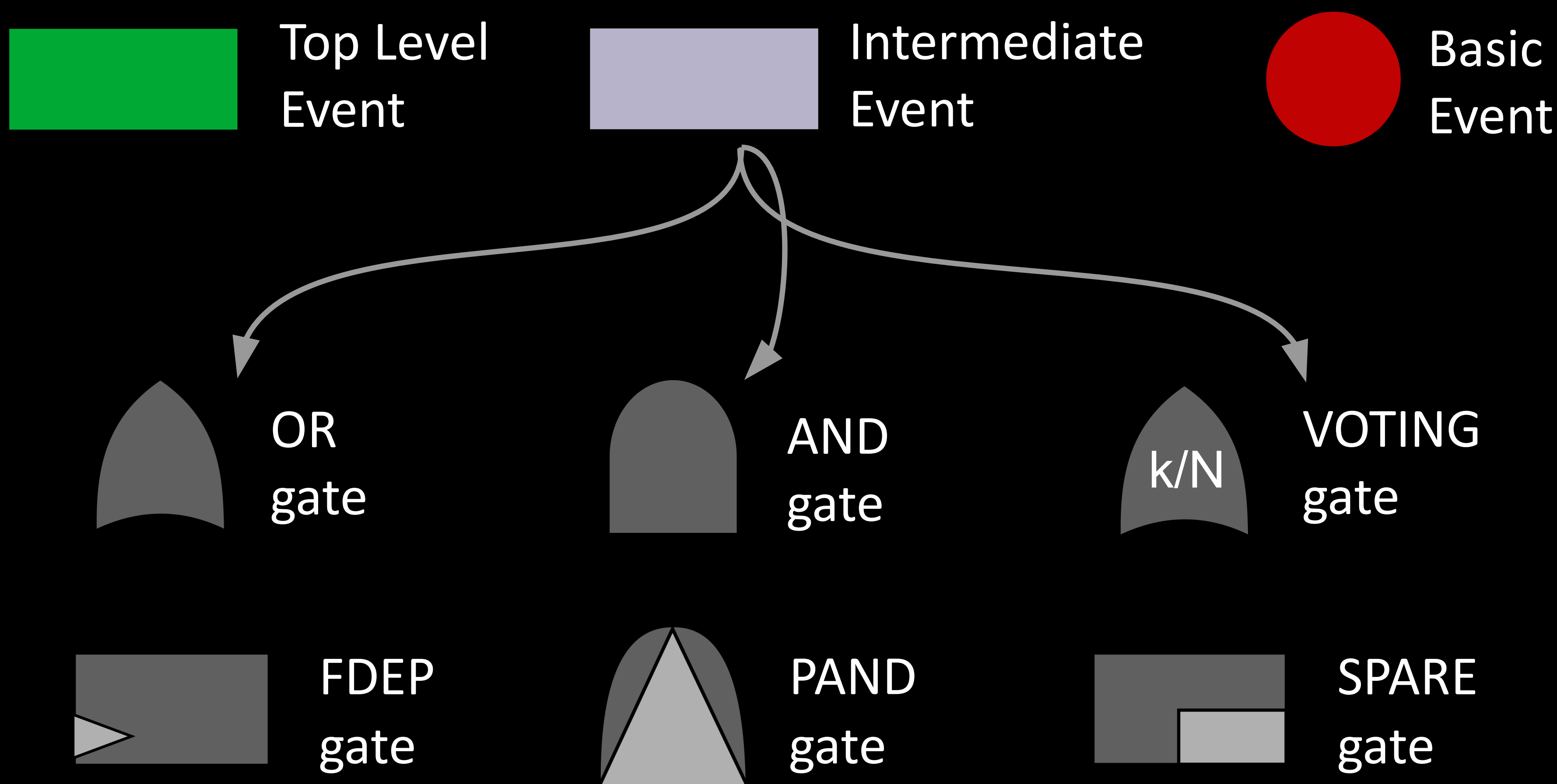
Validating our road trip FT

Dynamic Fault Tree



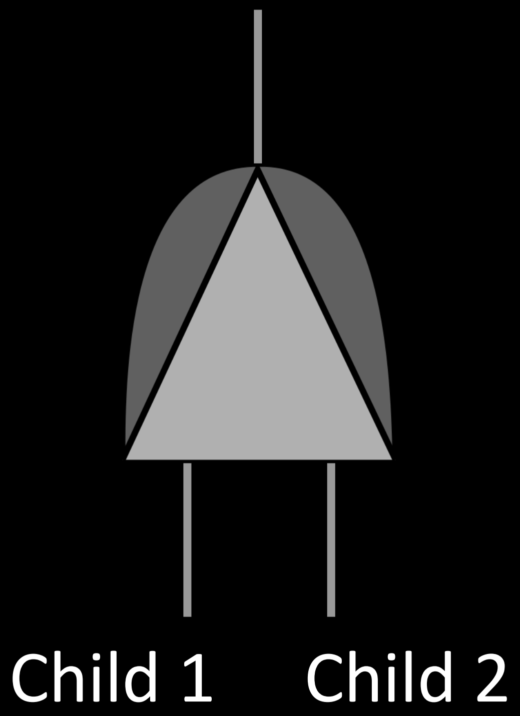
Dynamic Fault Trees

Static Fault Trees + dynamic gates



Dynamic Fault Trees

Priority AND gate (PAND)

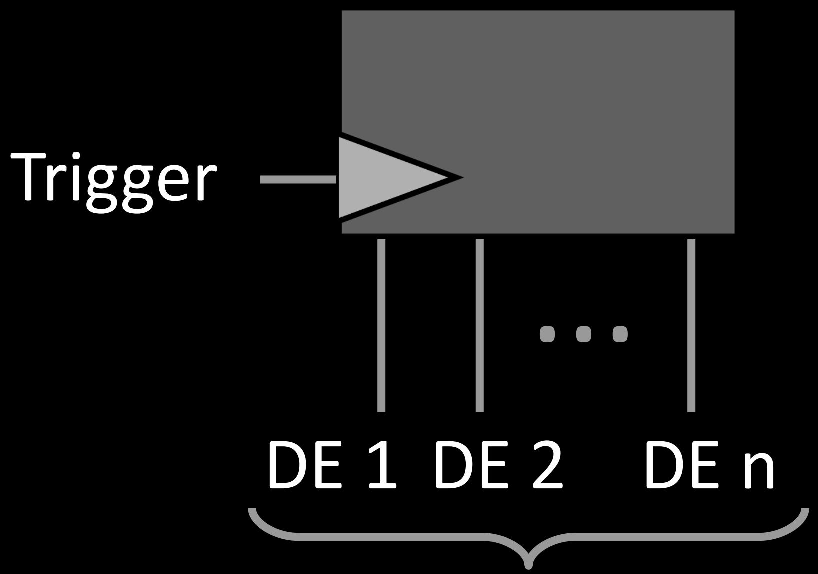


Fails when children fail from left to right

Dynamic Fault Trees

Fail-dependency gate (FDEP)

To model common-cause failures.
During a fire, the smoke (a) compromises vision
(b) compromises breathing



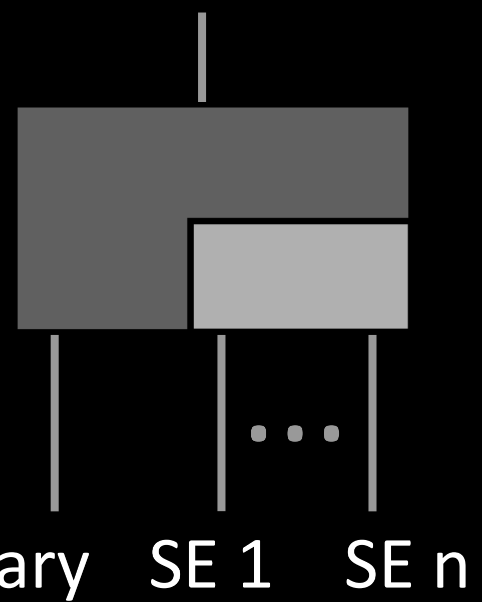
When trigger event fails, all dependent events fail

Dependent Events (usually Basic Events)

Dynamic Fault Trees

Spare gate (SPARE)

To model dormant components ("cold/warm spares") that fail less often while they are not in use



When primary fails,
Spares Elements replace it

Dynamic Fault Trees

Cold spare: car tire

S

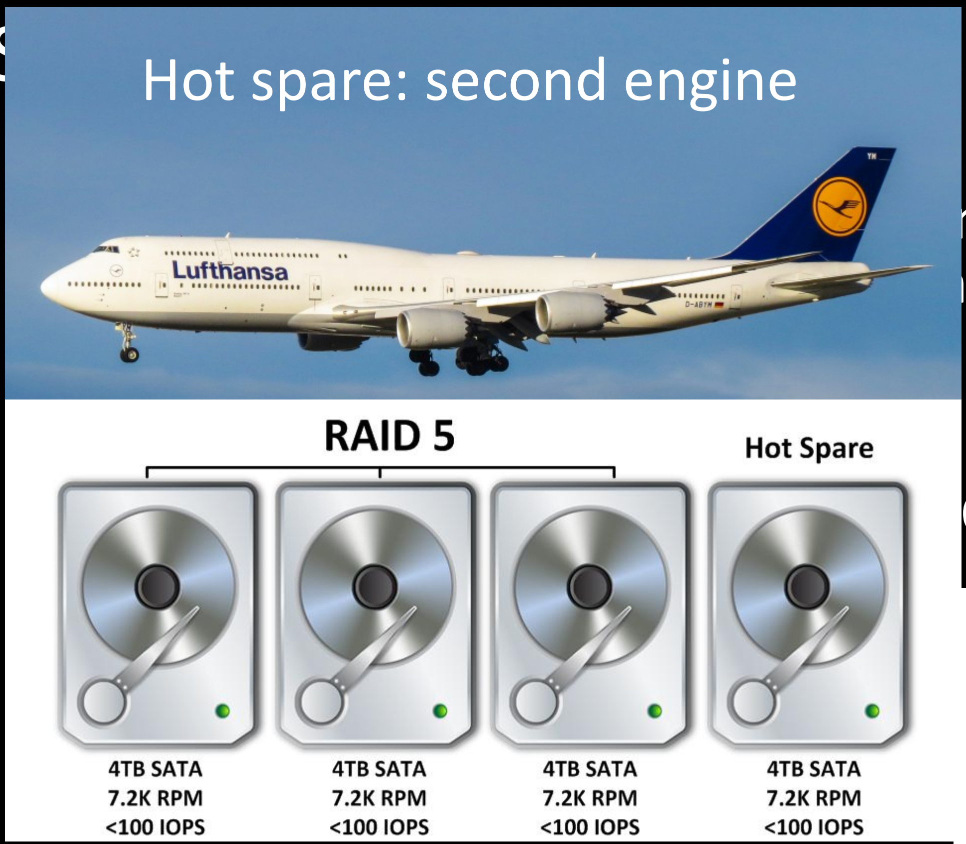
nents ( )

ey are

en pr

E

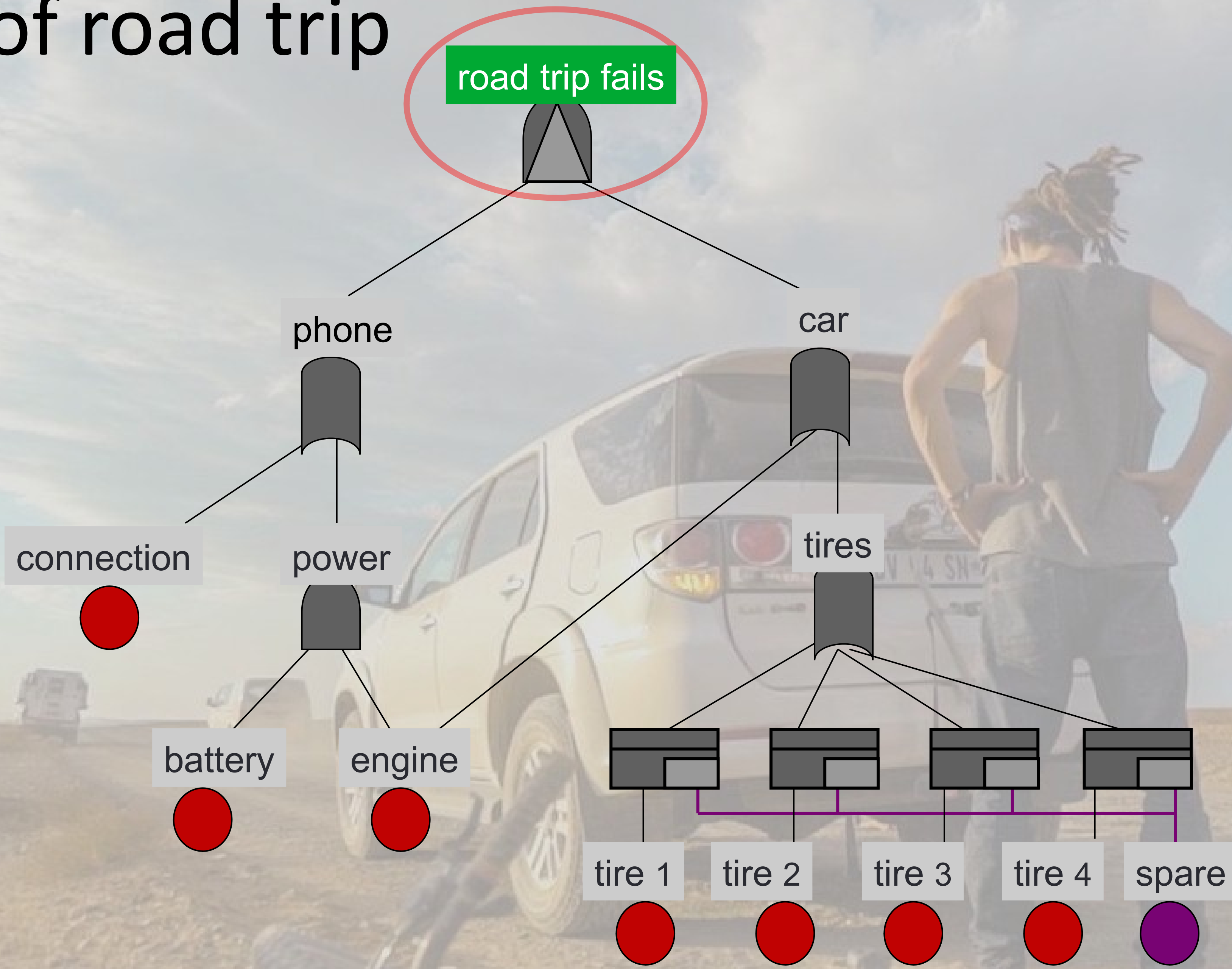
place it



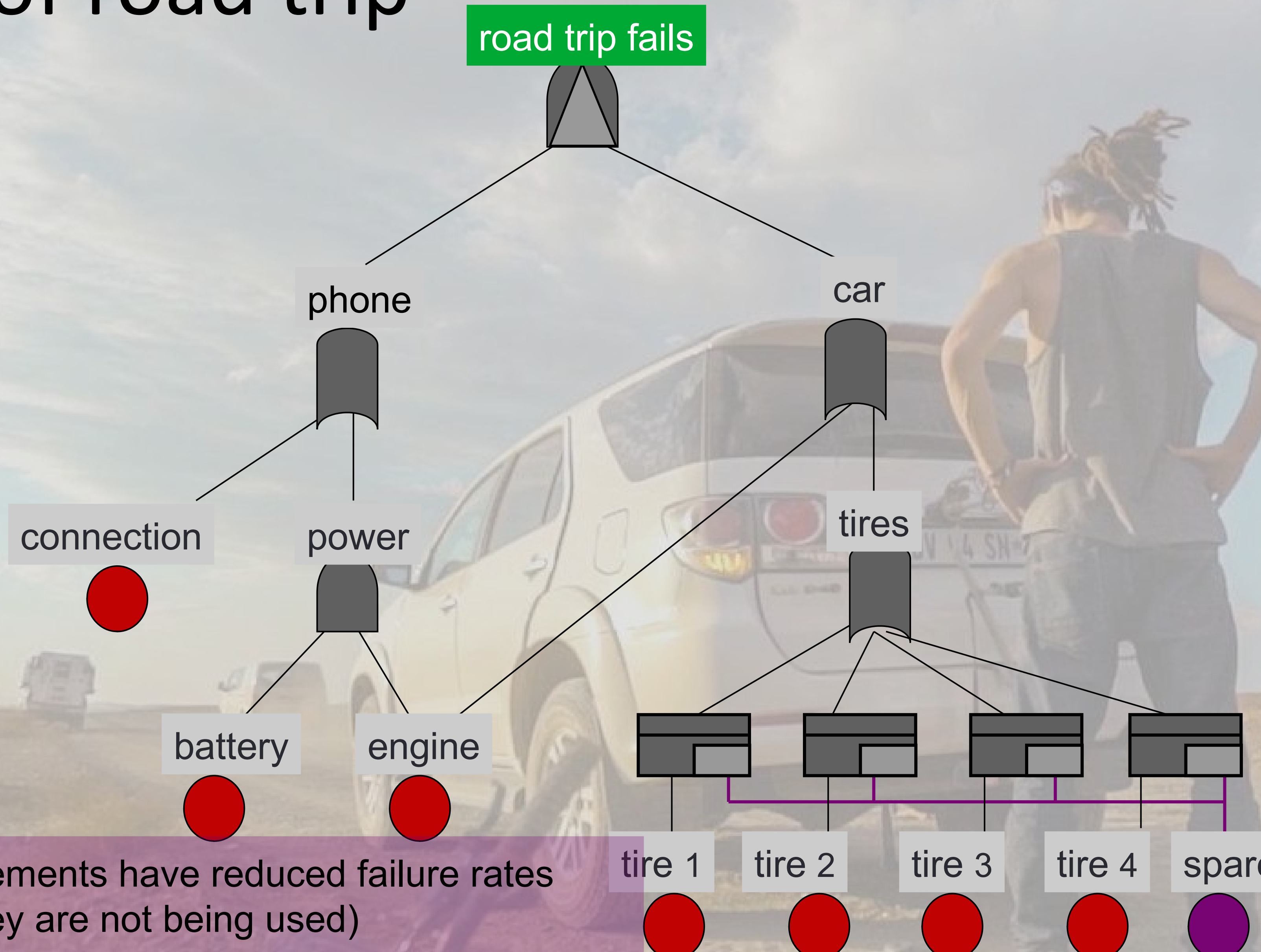
Primary SE 1 SE n

Warm spare: extra (closed) can of peas

DFT of road trip

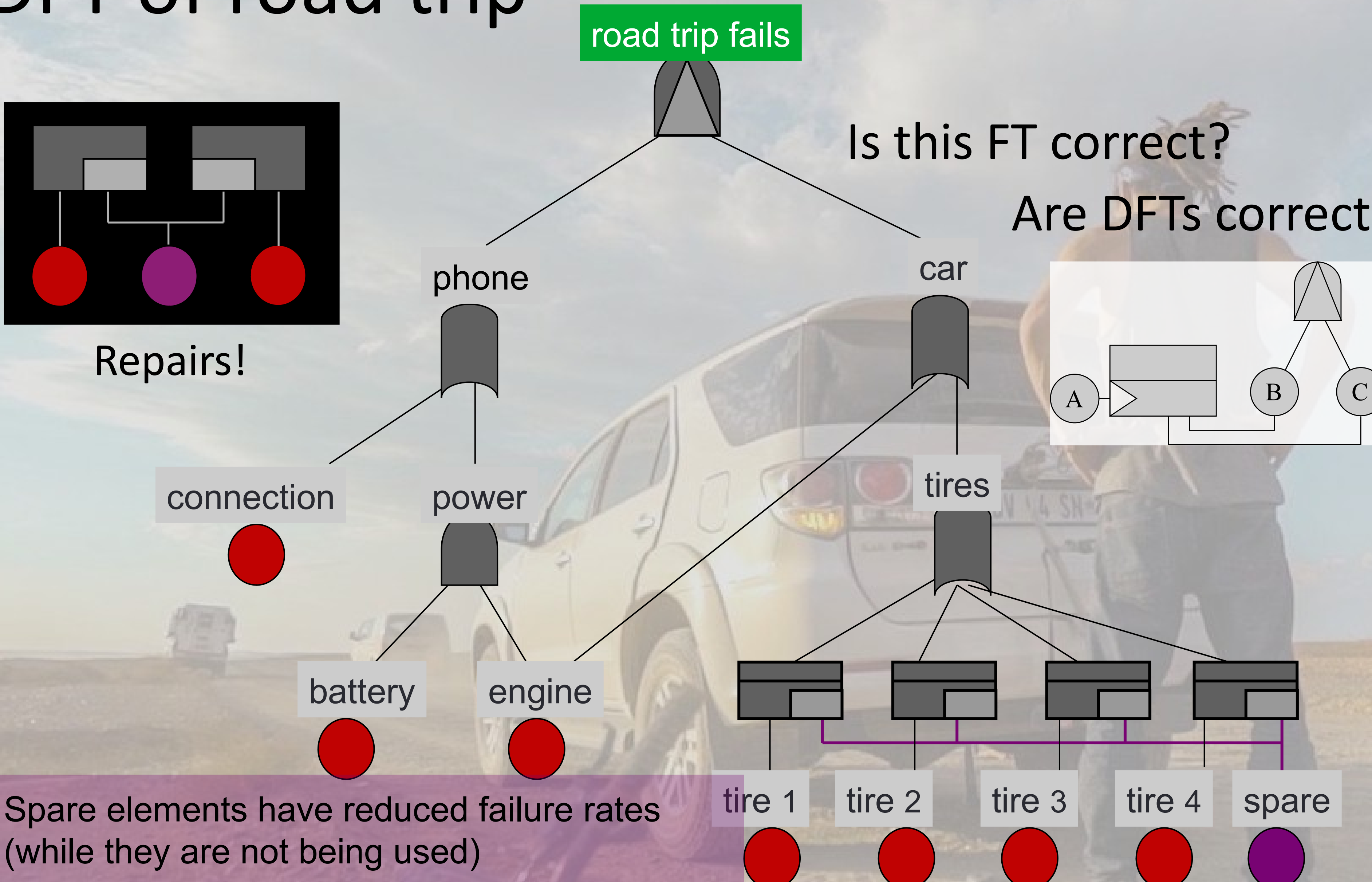


DFT of road trip



Spare elements have reduced failure rates (while they are not being used)
They can also be shared among SPARE gates

DFT of road trip



Repairs!

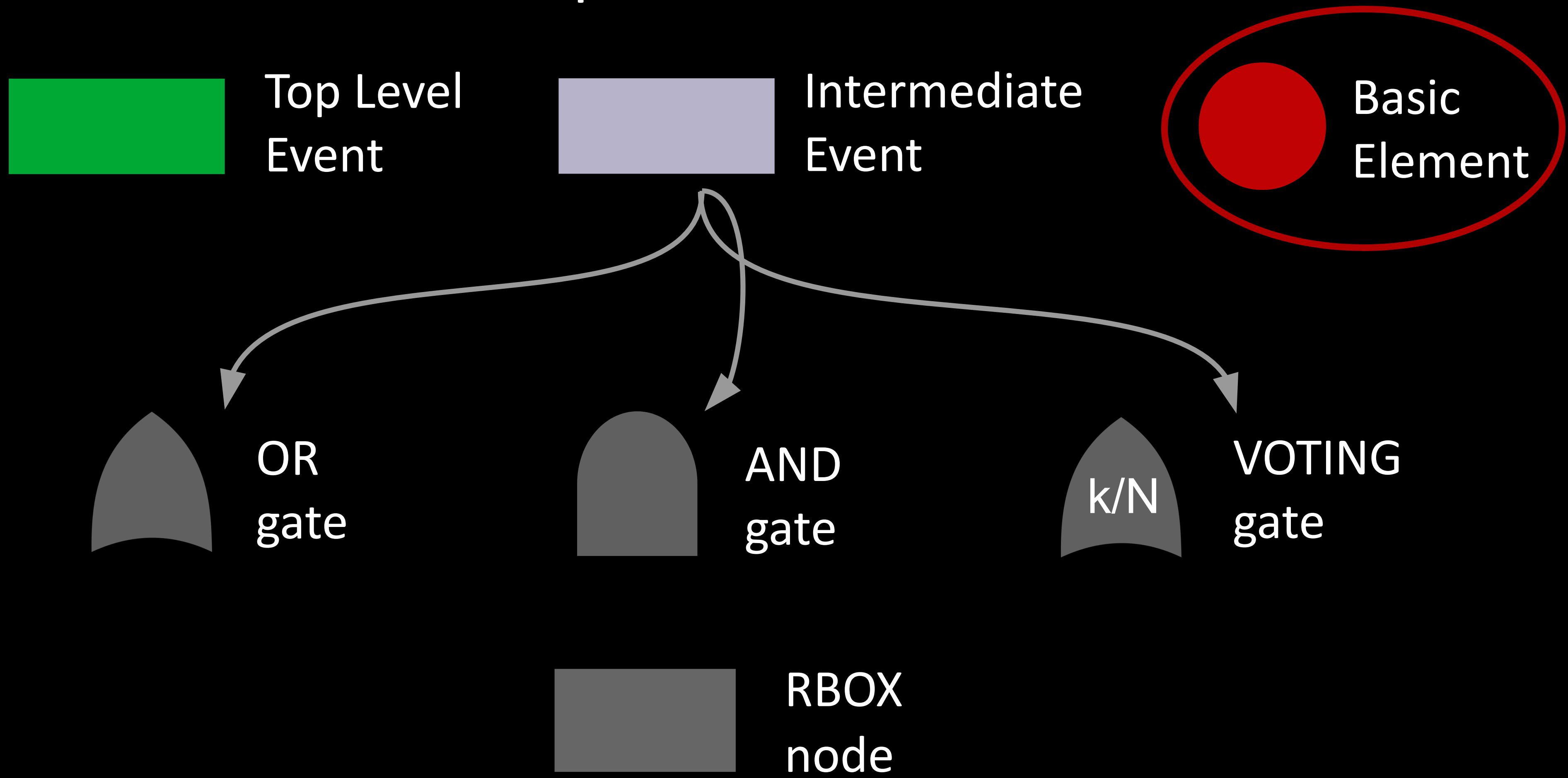
Is this FT correct?

Are DFTs correct?

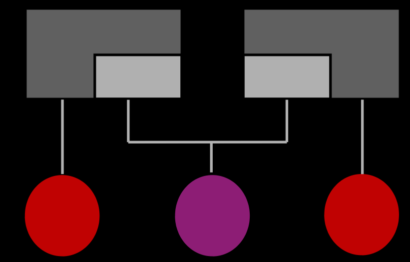
Spare elements have reduced failure rates
(while they are not being used)
They can also be shared among SPARE gates

Repairable Fault Trees

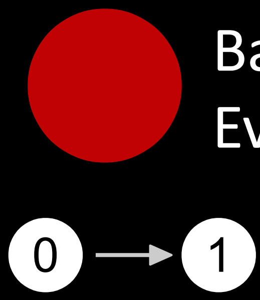
Static Fault Trees + repair boxes



Repairable Fault Trees



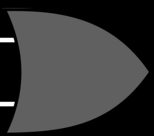
Basic Event vs. Basic Element



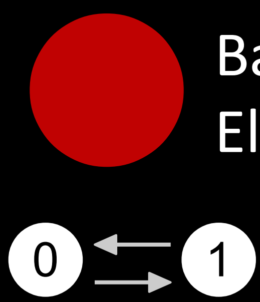
Basic Event

Models an event: **it happens once** (“CPU fried”)

Typically maps to a unique component,
but not mandatory:
- bicycle wheel skewed –
- bicycle wheel dented –



can’t ride



Basic Element

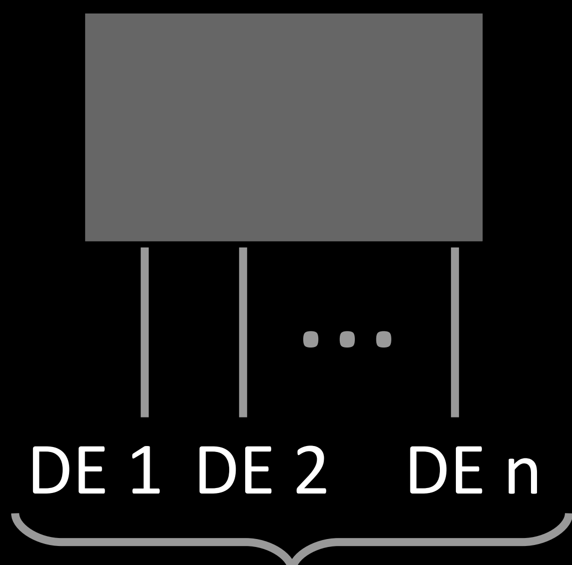
Models a basic failure point (“no AC”)

Can fail, and get repaired, and fail, etc.
Element won’t be further refined.

Repairable Fault Trees

Repair-person box (RBOX)

When dependent elements fail, the RBOX repairs one at a time

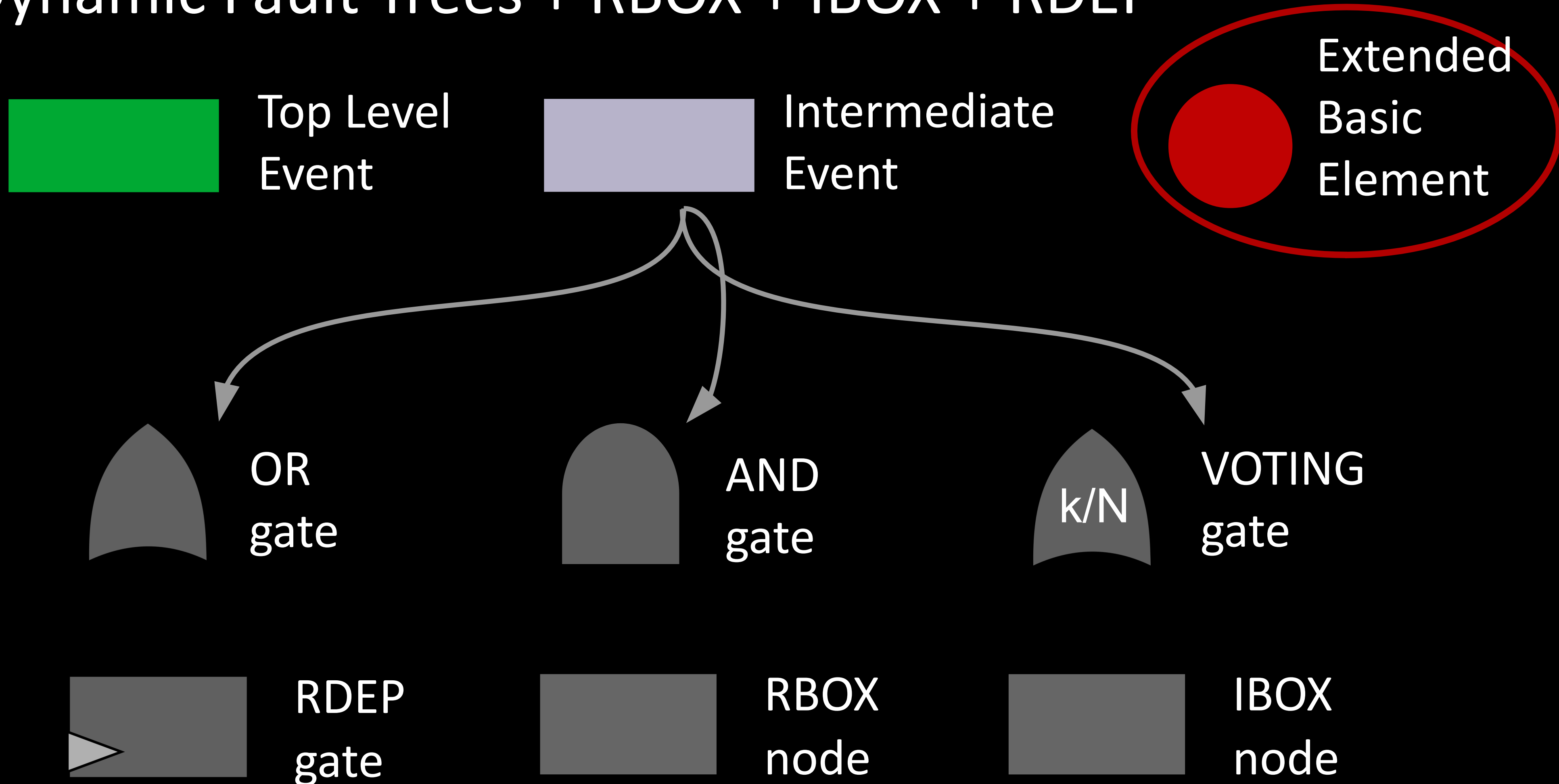


Dependent Elements (usually Basic Elements)


Time to take a break

Maintenance Fault Trees

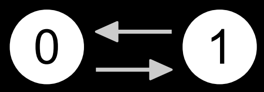
Dynamic Fault Trees + RBOX + IBOX + RDEP



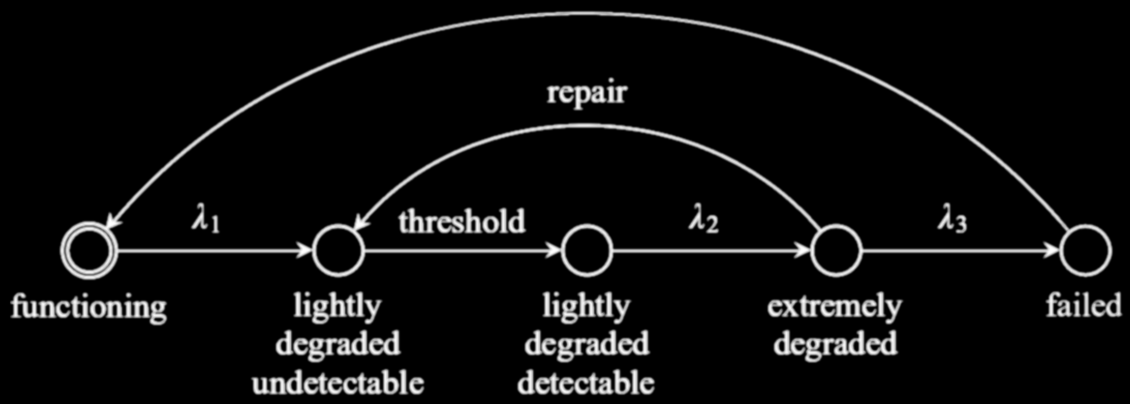
Maintenance Fault Trees

Extended Basic Element

Basic Element — Models a basic failure point that can be repaired (and fail again…)

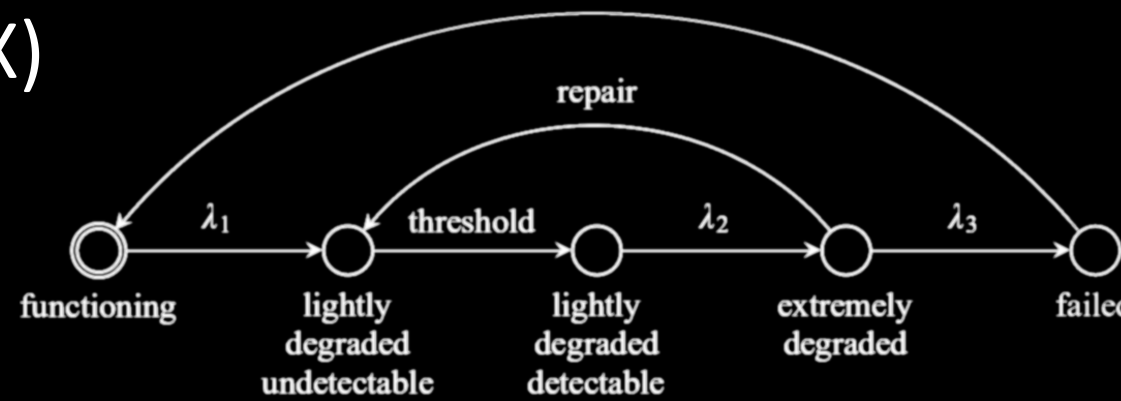


Extended Basic Element — Extends the above with (discrete) degradation

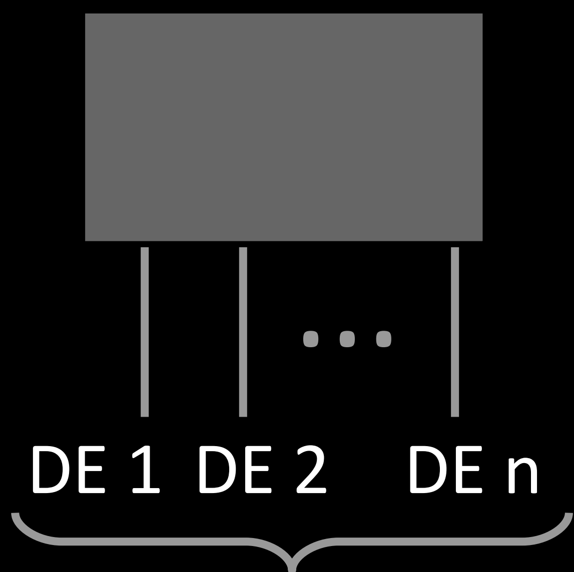


Maintenance Fault Trees

Inspection box (IBOX)



When dependent elements go beyond an inspection threshold, early repairs can be triggered

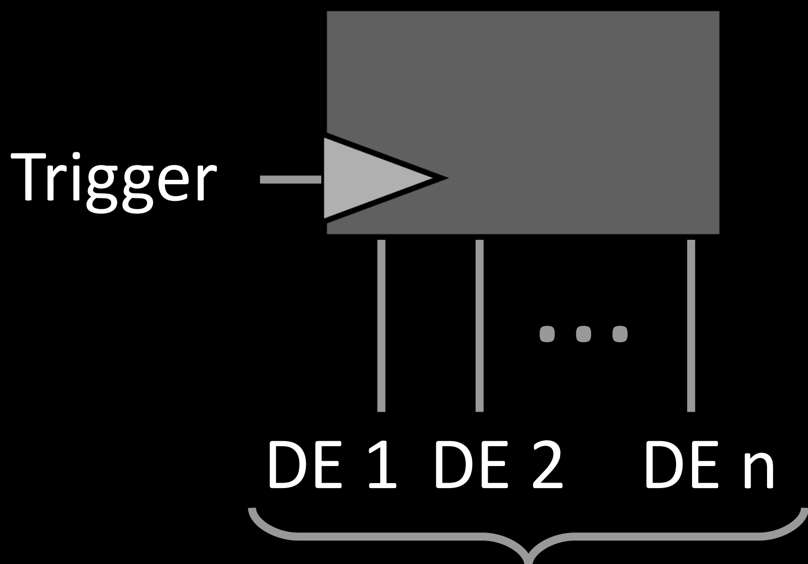


Dependent Elements (usually Extended Basic Elements)

Maintenance Fault Trees

Rate-dependency gate (RDEP)

To model common-cause performance degradators.
An oil leak (a) speeds-up bearings degradation
(b) speeds-up transmission chains degradation



Dependent Elements (usually Extended Basic Elements)

When trigger happens, the failure rate of all dependent elements increases

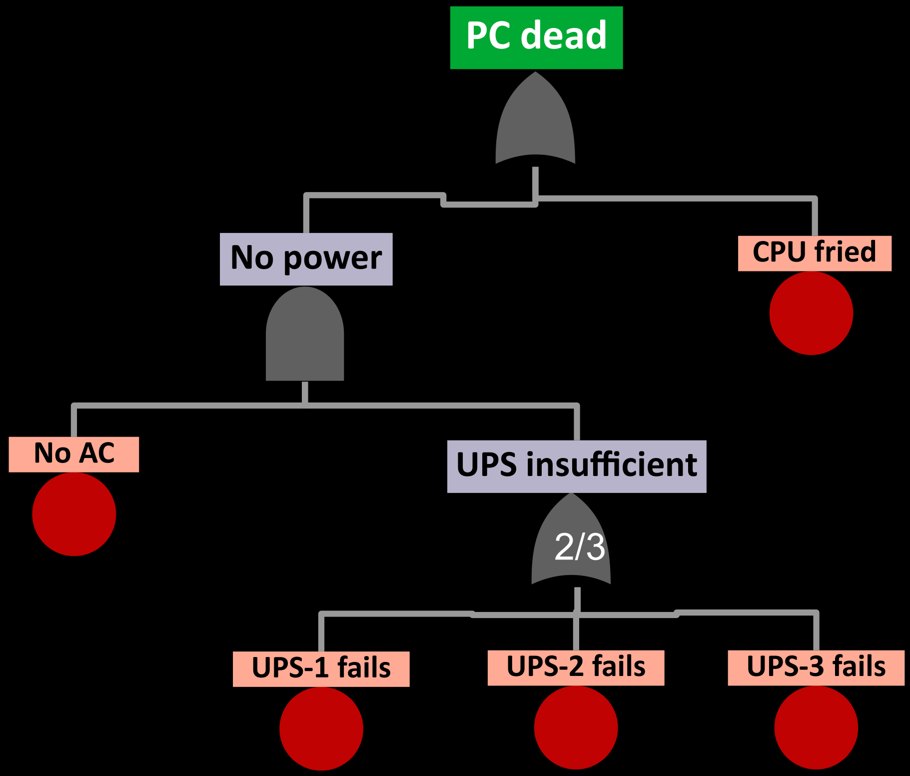
FTs in TECHNICOLOR

- Static FT
- Dynamic FT
- Repairable FT
- Maintenance FT

… what for ?

what do we want to know?

FTs in TECHNICOLOR



Reliability

How likely is my PC to die, like, ever?
What about in the first year?
And after 20 years?

Availability

How often is my PC dead?
Say in a month, how many hours?

Mean Time To Failure

How long until the next incident?

Contents

Fault Trees

What & Why

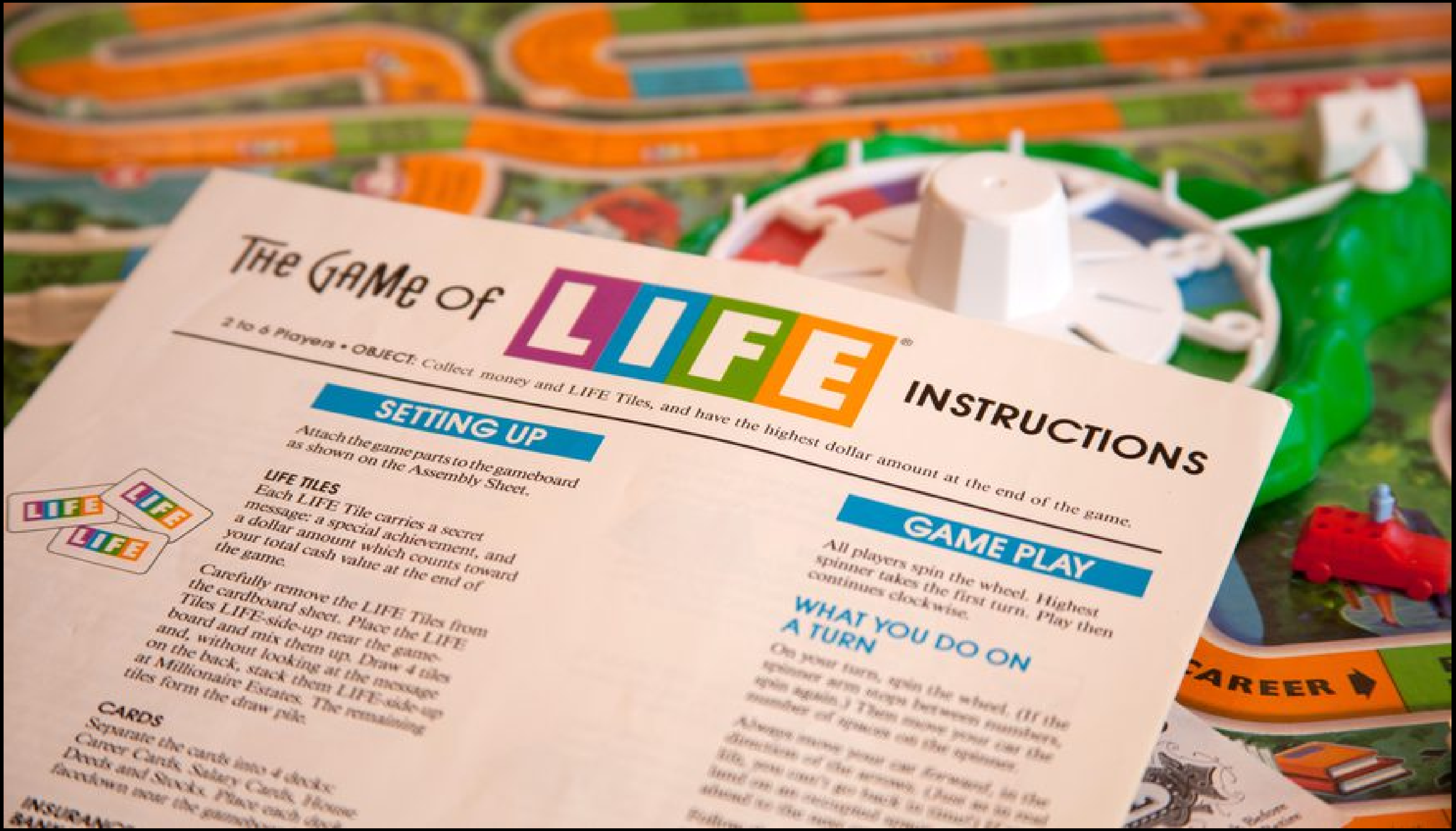
- Fault Tree Analysis
  - Discrete time
  - Continuous time

FTA in practice

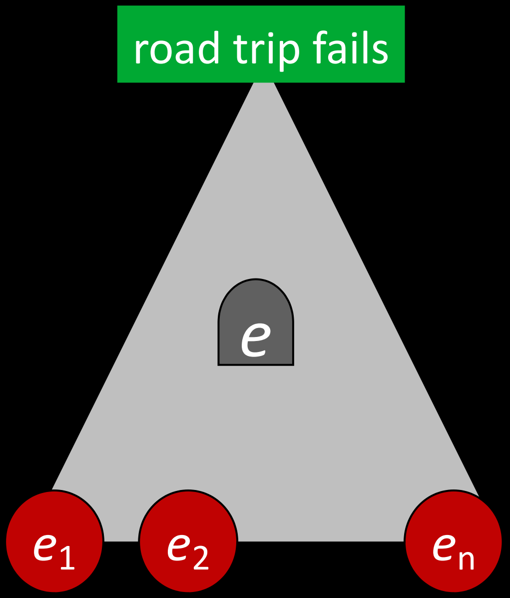
Tools & benchmarks

Concrete examples (the real deal)

How to play with FTs: semantics



Semantics model of FTs



Structure function $\Phi: \{0,1\}^{\#BEs} \rightarrow \{0,1\}$

0 = operational ; **1** = failed

Given values $e_1, \ldots e_n$, does the tree fail?

$\pi_F : P(BE) \rightarrow \{0,1\}$

If BEs $e_1, \ldots e_n$ fail, does the tree (***F***) fail?

$\pi_F : P(BE) \times Elt \rightarrow \{0,1\}$

If BEs $e_1, \ldots e_n$ fail, does ***e*** fail?

Recursive characterization

- AND-case: $\pi_F(E,e) = 1$ iff $\pi_F(E,e') = 1$ for all children *e'* of *e*
- *... etc.*

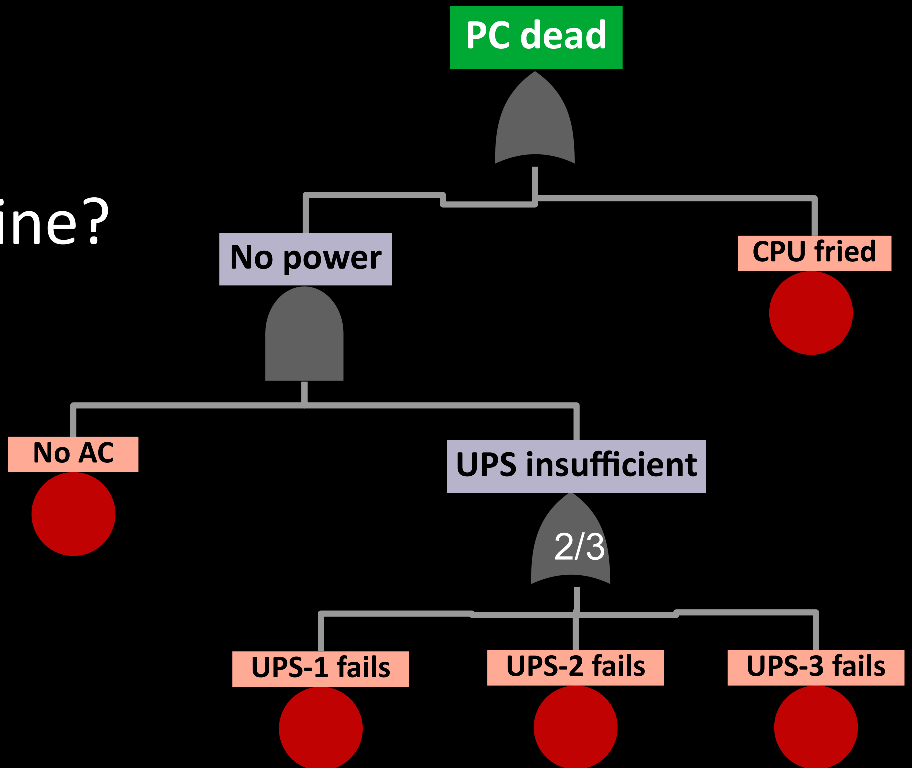
Cut set: set of Basic Events ***C*** that cause FT to fail: $\pi_F(\boldsymbol{C}) = 1$

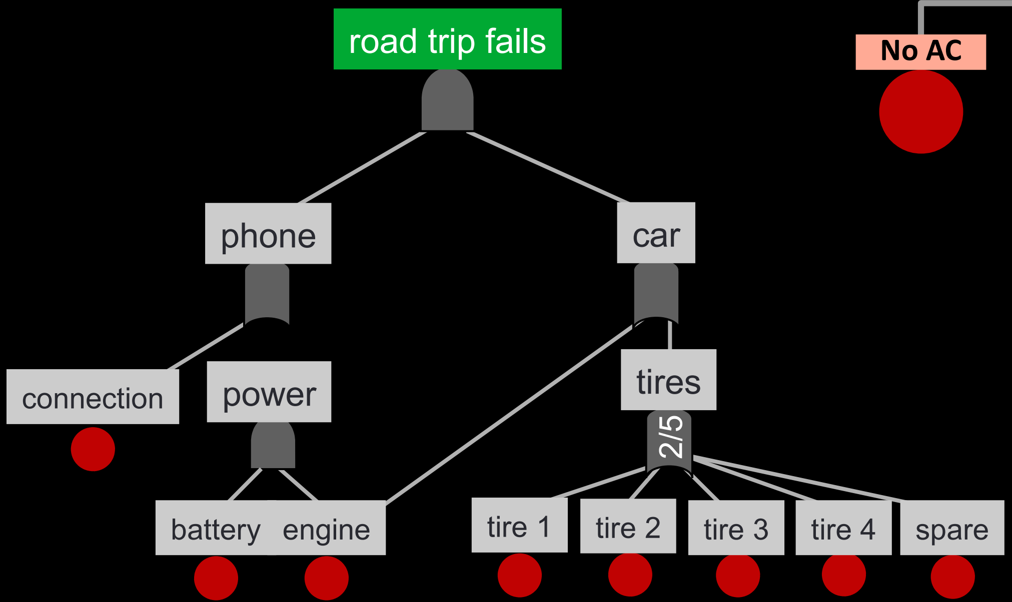
FTs are coherent:

- <u>If</u> $S \leq S'$ <u>and</u> $\pi_F(S) = 1$ <u>then</u> $\pi_F(S') = 1$
- *Non-coherent extensions exist (DFTs)*

Qualitative queries

- Can I use my PC in a blackout?
- Is my trip busted by a broken engine?



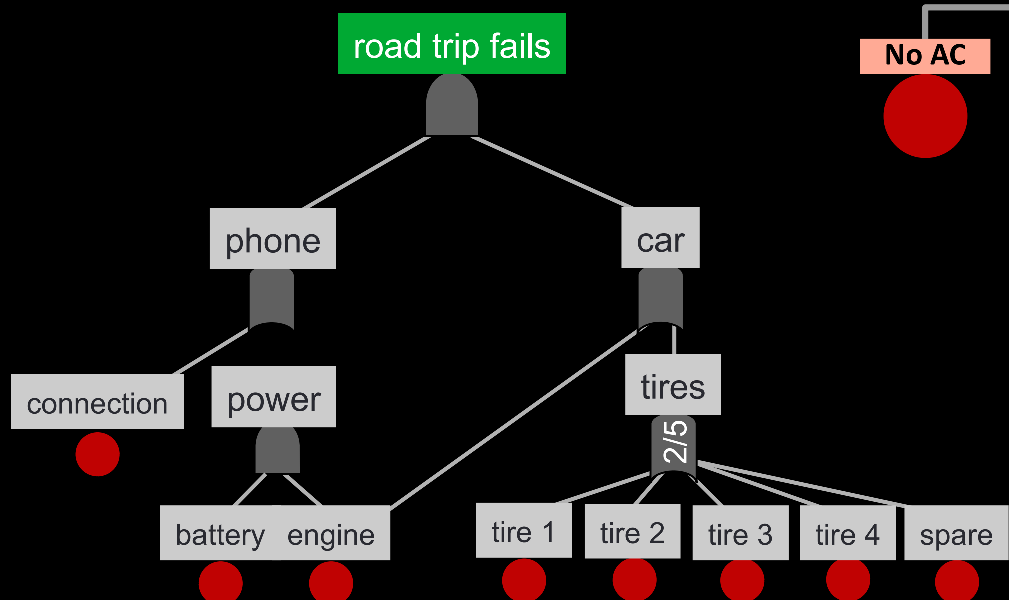


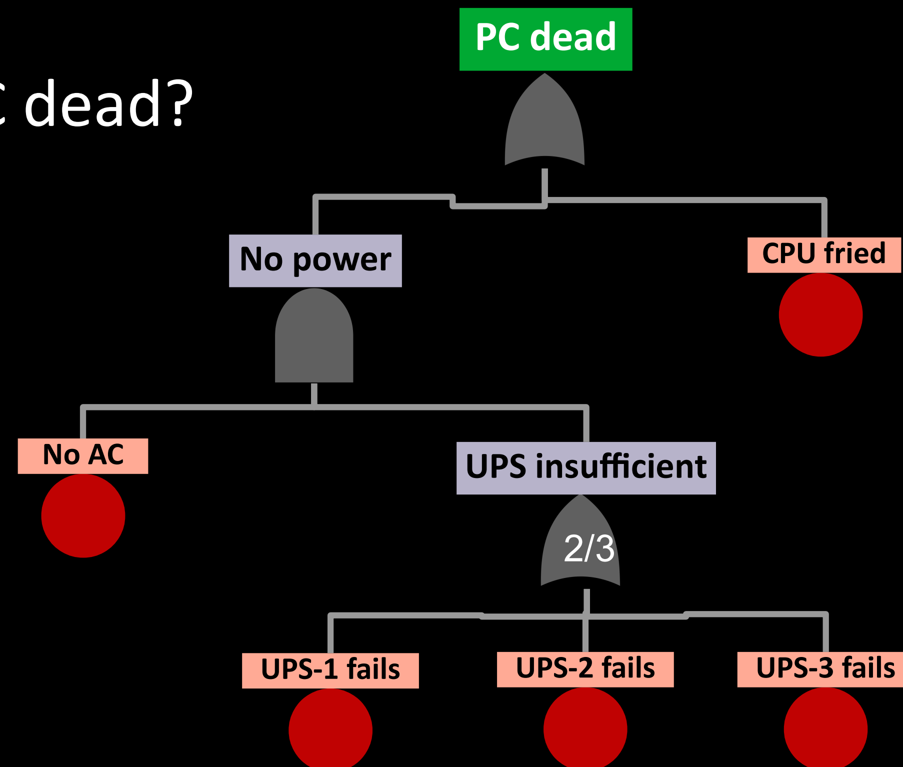
Cut set analysis!

$\pi_F : P(BE) \rightarrow \{0,1\}$

Quantitative queries

- How many hours a week is my PC dead?
- After a flat tire, how likely is my road trip to fail?



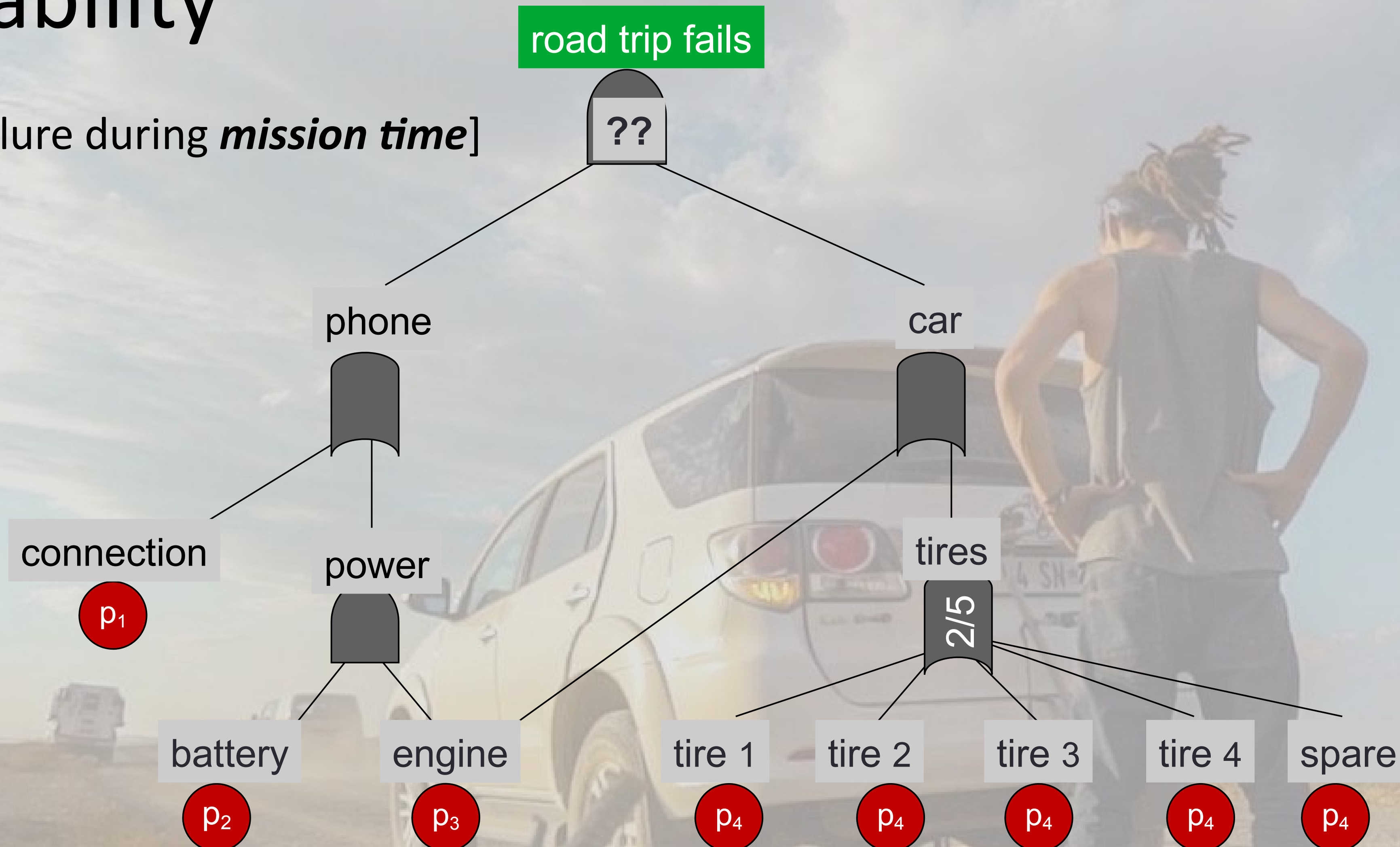


Binary outcome is insufficient

$\pi_F : P(BE) \rightarrow \{0,1\}$

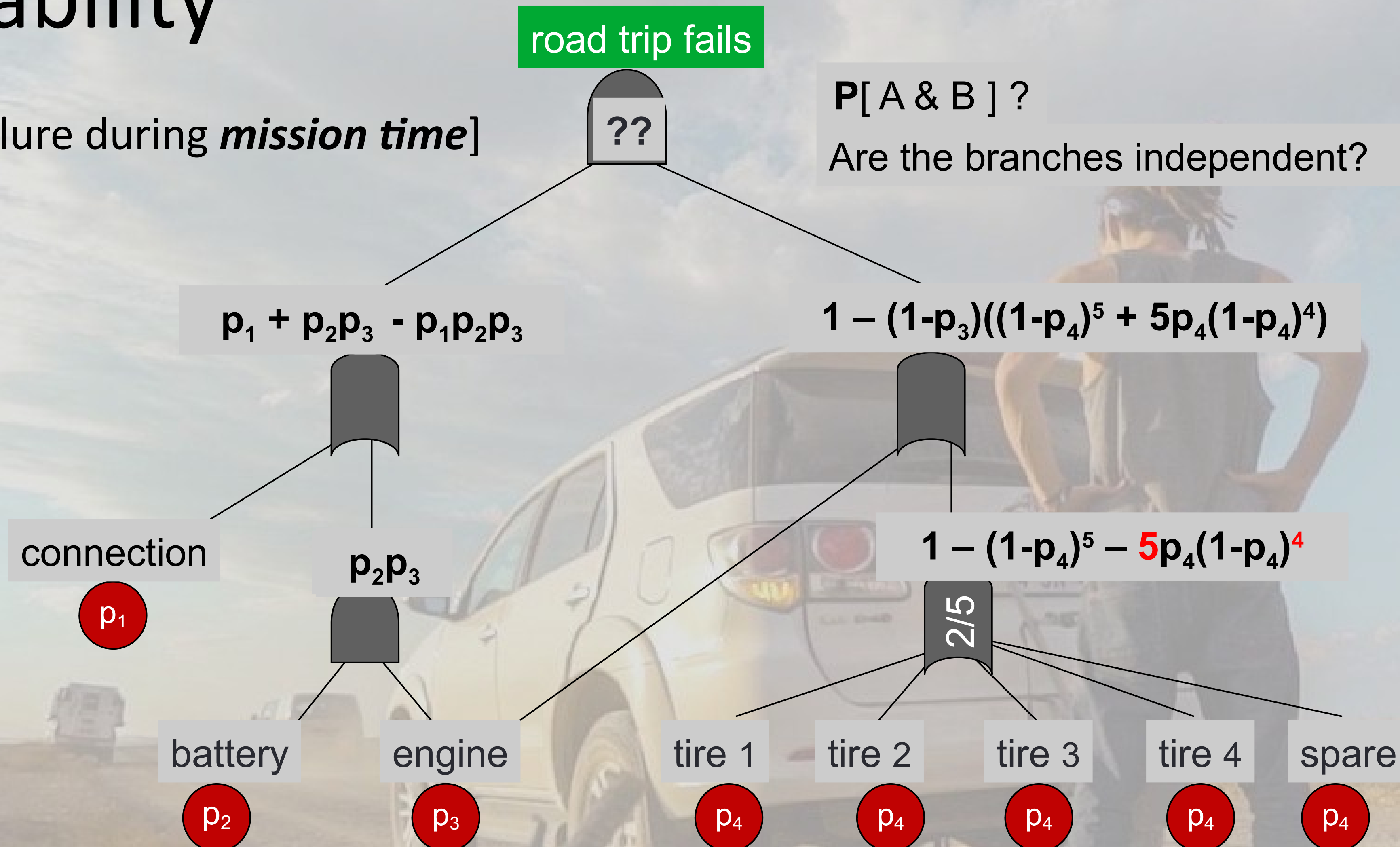
Reliability

P[no failure during ***mission time***]



Reliability

P[no failure during ***mission time***]



P[A & B] ?

Are the branches independent?

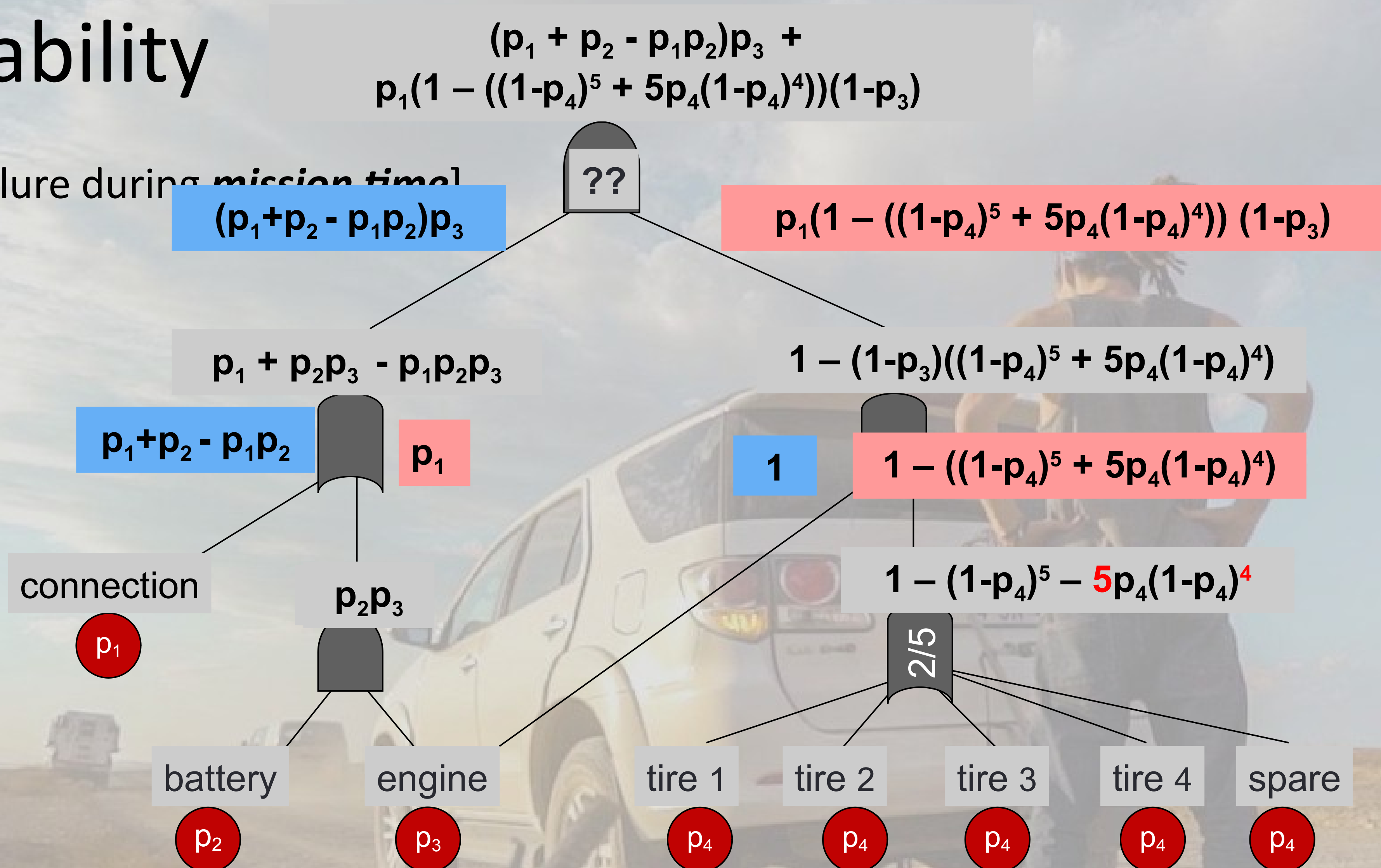
P[A & B] = **P**[A] **P**[B]
(if A,B are independent)

P[A v B] = **P**[A] + **P**[B] – P[A&B]

P[B^c] = 1 – **P**[B]

Reliability

P[no failure during *mission time*]



Case 1: engine fails; p_3=1

Case 2: engine does not fail; p_3=0

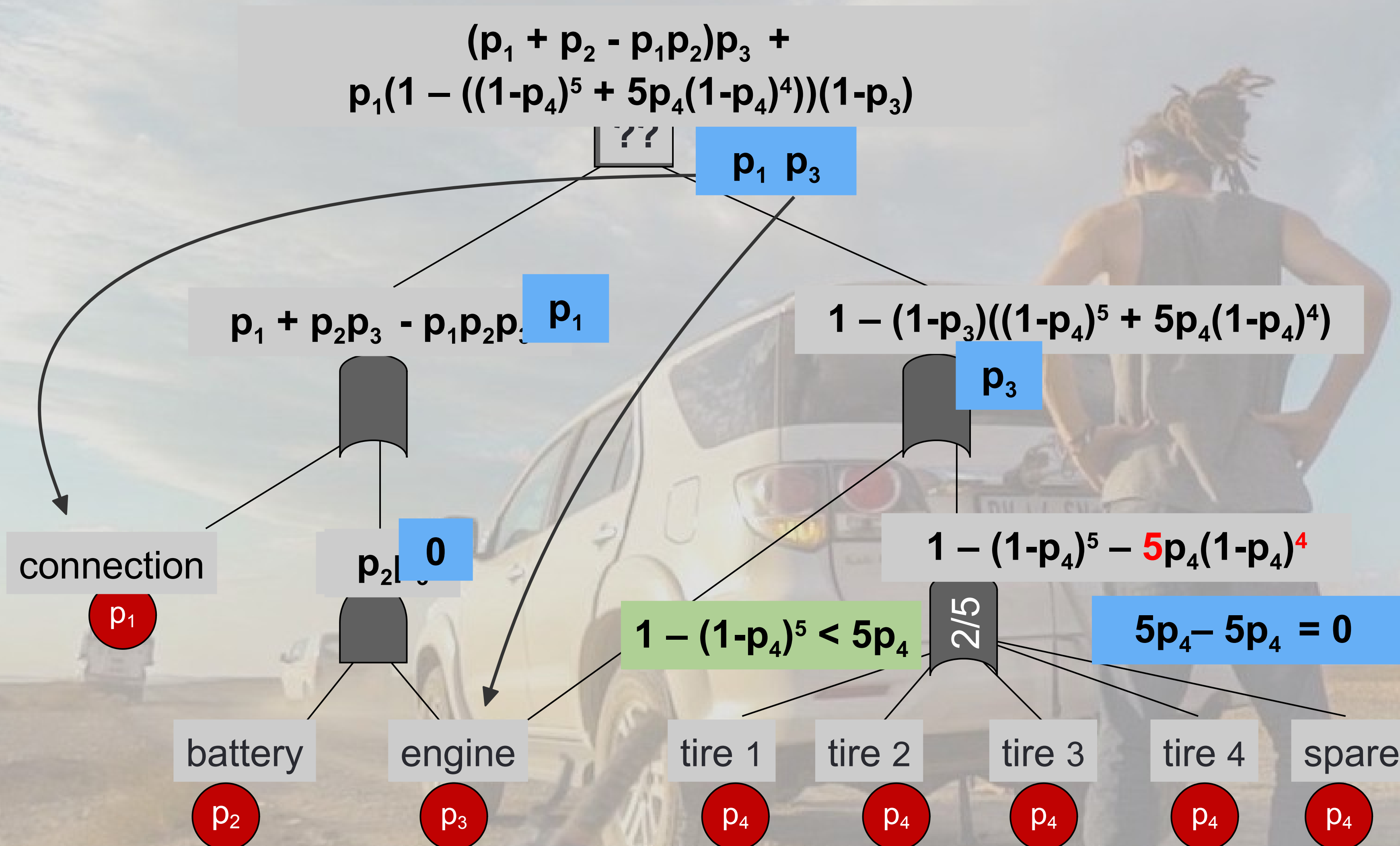
Bayes law:

P[A] = **P**[A | B] **P**[B] + **P**[A|B^c] **P**[B^c]

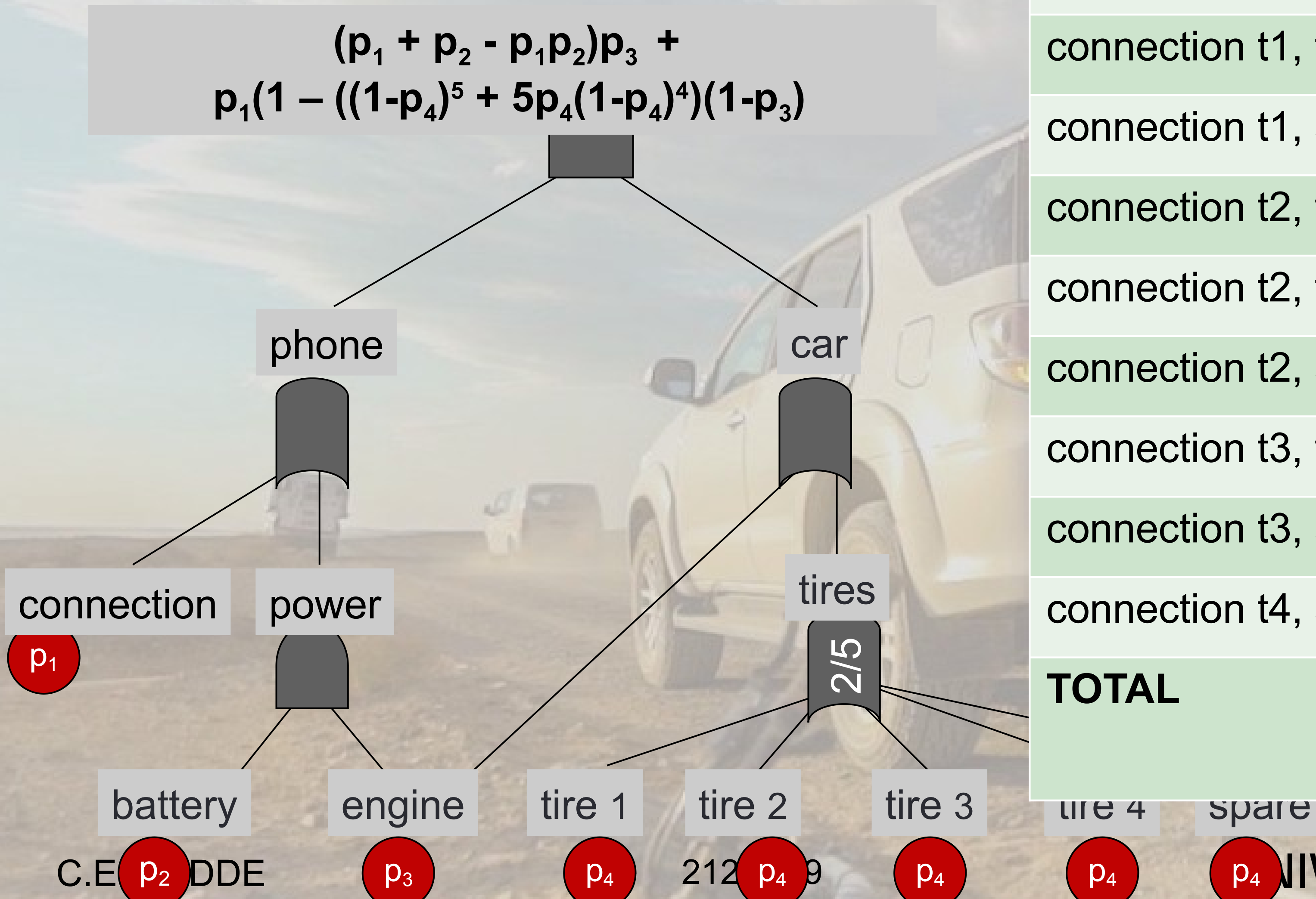
Speeding up computations

1. Disregard higher order products
2. Use minimal cut sets   (yes, for reliability also!)
3. = 1. + 2.   (do the math)
4. Binary Decision Diagrams

1. Disregard high order products



2. Use minimal cut sets



Minimal cut set	Probability
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	$p_1\, p_3 + p_2\, p_3 + 10\ p_1\, p_4^2$

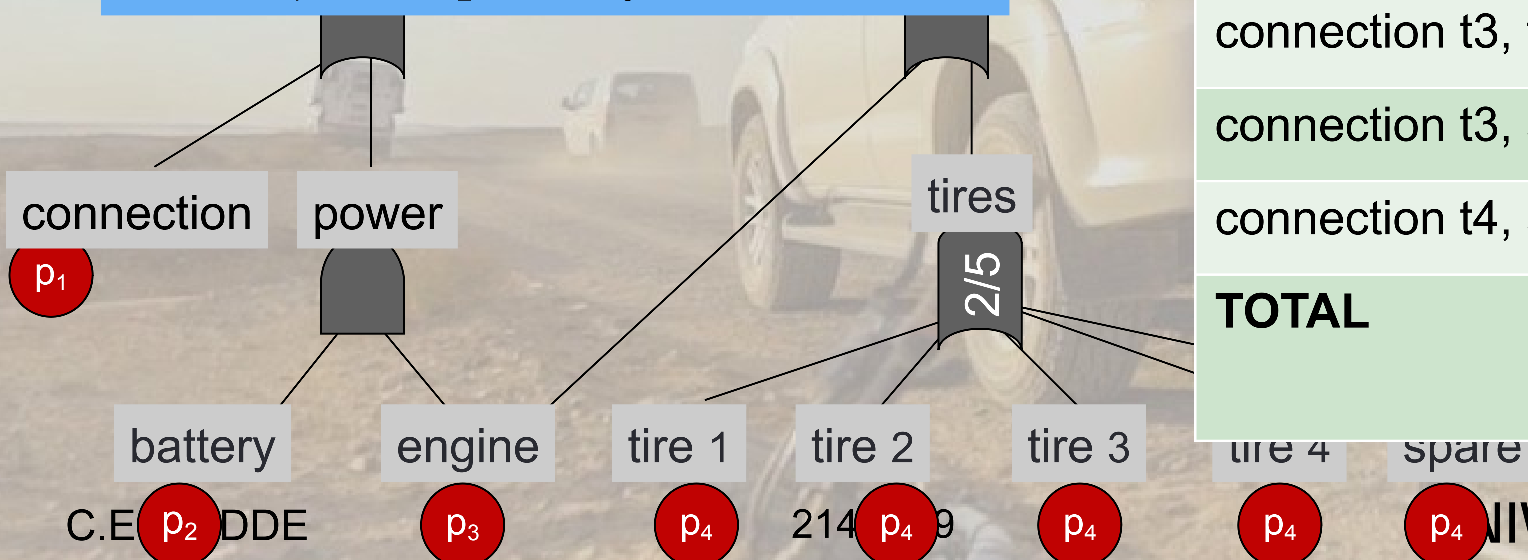
2. Use minimal cut sets

Under- or over-approximation? Why?

$$(p_1 + p_2 - p_1p_2)p_3 +$$
$$p_1(1 - ((1-p_4)^5 + 5p_4(1-p_4)^4)(1-p_3))$$

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

Minimal cut set	Probability
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	$p_1\, p_3 + p_2\, p_3 + 10\; p_1\, p_4^2$



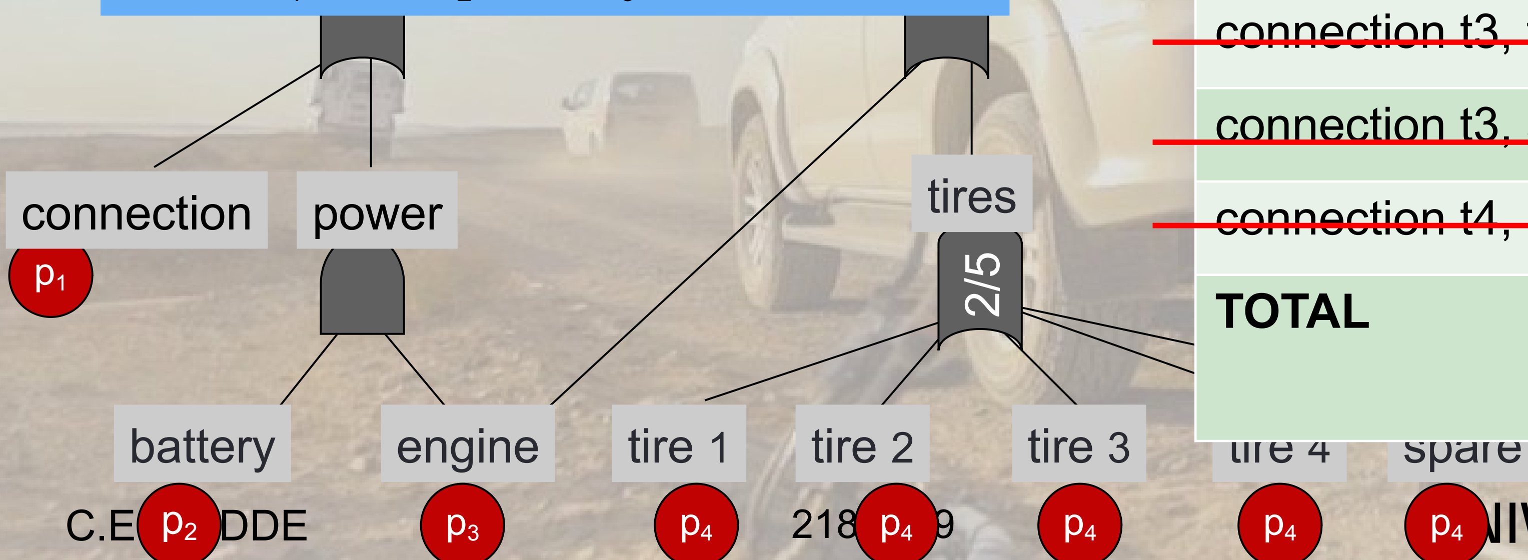
3. = 1. Disregard high order + 2. Minimal cut sets

Minimal cut set	Probability
…n, engine	$p_1\, p_3$
…ngine	$p_2\, p_3$
~~…n, t1, t2~~	$\cancel{p_1\, p_4^2}$
~~connection, t1, t3~~	$\cancel{p_1\, p_4^2}$
~~connection t1, t4~~	$\cancel{p_1\, p_4^2}$
~~connection t1, spare~~	$\cancel{p_1\, p_4^2}$
~~connection t2, t3~~	$\cancel{p_1\, p_4^2}$
~~connection t2, t4~~	$\cancel{p_1\, p_4^2}$
~~connection t2, spare~~	$\cancel{p_1\, p_4^2}$
~~connection t3, t4~~	$\cancel{p_1\, p_4^2}$
~~connection t3, spare~~	$\cancel{p_1\, p_4^2}$
~~connection t4, spare~~	$\cancel{p_1\, p_4^2}$
TOTAL	$p_1\, p_3 + p_2\, p_3 \cancel{+ 10\, p_1\, p_4^2}$

Under- or over-approximation? Why?

$$(p_1 + p_2 - p_1p_2)p_3 \; +$$
$$p_1(1 - ((1-p_4)^5 + 5p_4(1-p_4)^4)(1-p_3))$$

$$\begin{aligned}
P[C_1 \vee C_2 \vee C_3] = \; & P[C_1] + P[C_2] + P[C_3] \\
& - P[C_1]P[C_2] - P[C_1]P[C_2] - P[C_2]P[C_2] \\
& + P[C_1]\, P[C_2]\, P[C_3] \\
\leq \; & P[C_1] + P[C_2] + P[C_3]
\end{aligned}$$



Note: p_1 , p_4 should be low

4. Binary Decision Diagrams

BDDs

- Compact representation for Boolean functions $f(x_1,x_2,\ldots,x_\mathrm{n})$
  - e.g. the structure function $\Phi\!:\!\{0,1\}^{\#\mathrm{BEs}} \to \{0,1\}$ of a Fault Tree
- Heavily used in model checking
- Based on Shannon expansion / pivotal decomposition
  - $f(x_1,x_2,\ldots,x_\mathrm{n}) = \underline{x_1}\, f(\mathbf{0},x_2,\ldots,x_\mathrm{n}) + x_1\, f(\mathbf{1},x_2,\ldots,x_\mathrm{n})$
  - works with a fixed variable ordering
  - supports (and works well with) shared subtrees

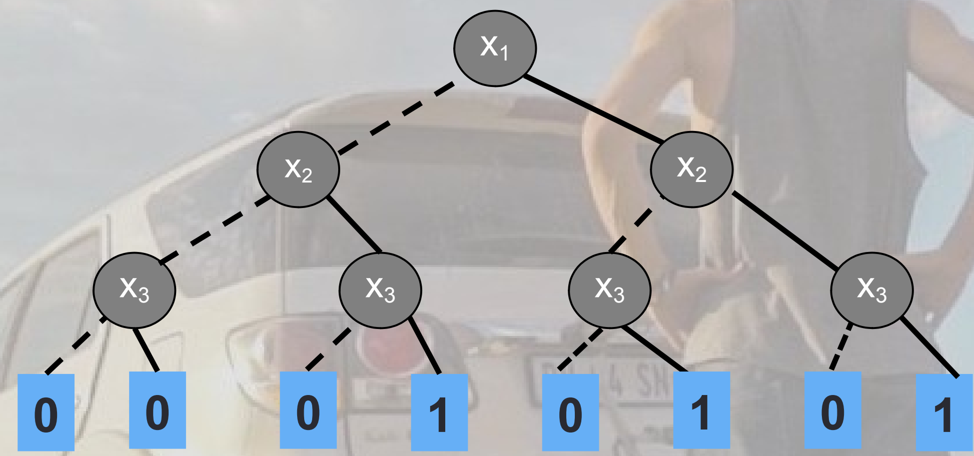
4. Binary Decision Diagrams

Boolean function: $f(x_1,x_2,x_3) = (x_1\ \underline{\text{OR}}\ x_2)\ \underline{\text{AND}}\ x_3$

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



- A vertex represents a decision:
  - follow dashed line for value **0**
  - follow solid line for value **1**
- Function value in leaves

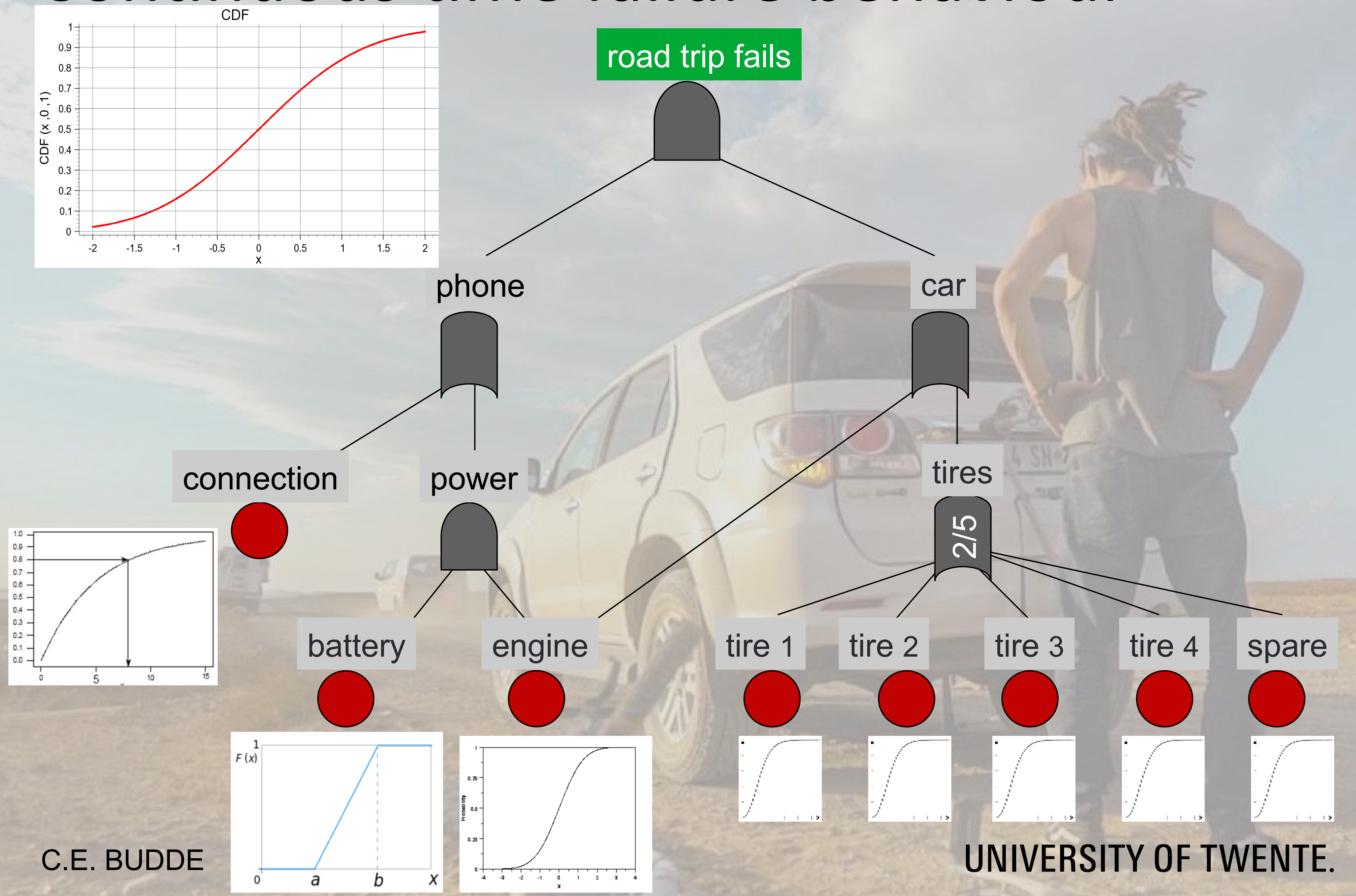

I need a break.

Contents

Fault Trees
  What & Why
- Fault Tree Analysis
  - Discrete time
  - ➢ Continuous time

FTA in practice
  Tools & benchmarks
  Concrete examples (the real deal)

Continuous time failure behaviour

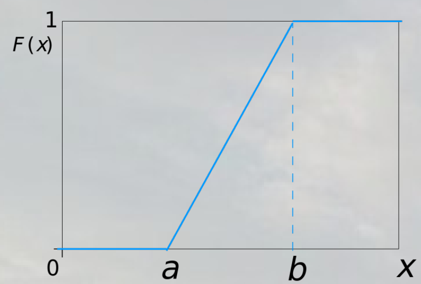


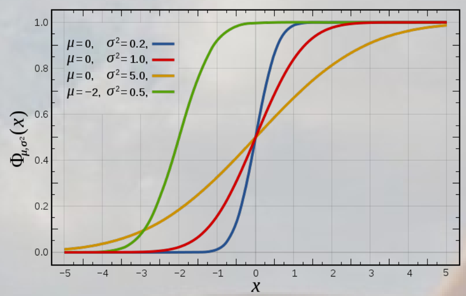
C.E. BUDDE

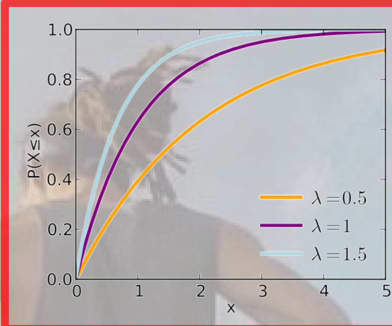
UNIVERSITY OF TWENTE.

Continuous probability distributions

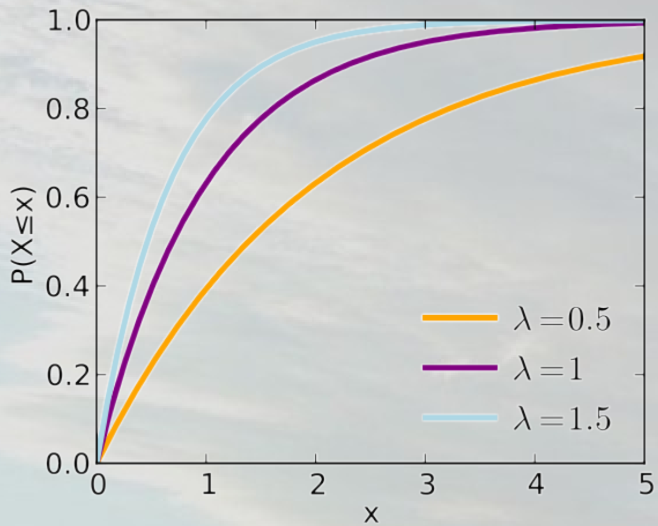
- Uniform
- Gaussian
- Exponential
  - realistic model for degradation
  - mathematically tractable
  - approximation via composed exponentials
- Weibull
  - generalized exponential
  - often used, but not discussed here







The exponential distribution

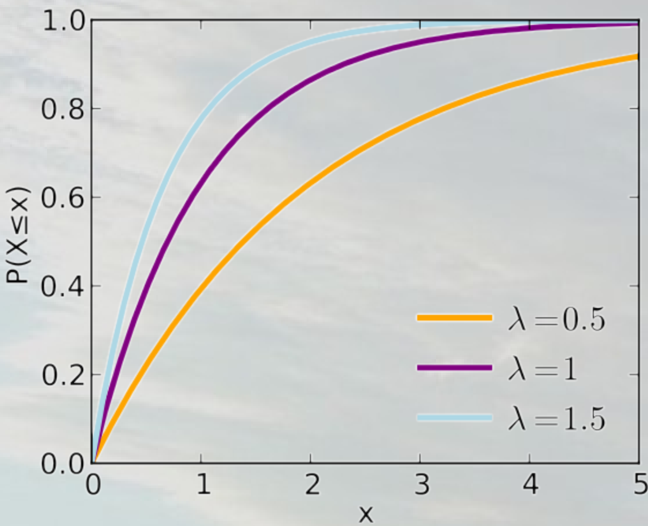


Components fail with fixed **rate** ‘λ’

λ = (Mean time to failure)$^{-1}$

If we know (on average)
when does a component fail,
we can use an exponential distribution

The exponential distribution



Components fail with fixed **rate** 'λ'
λ = (Mean time to failure)$^{-1}$

Unreliability / CDF

P[fail before x] = **P**[$X \leq x$] = $1 - e^{-\lambda x}$

Reliability

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

PDF

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

For continuous distributions
P[$X = x$] = 0
for any time point $x \in$ R

Cumulative Density Function: $F(x)$ = **P**[$X \leq x$]

P[$x \leq X \leq y$] = **P**[$X \leq y$] – **P**[$X > x$]

The exponential distribution

The exponential distribution

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

Reminder:
$\mathbf{P}[X \leq x] = 1 - e^{-\lambda x}$

The exponential distribution

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 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? $\mathbf{P}[10 < X < 25] = \mathbf{P}[X < 25] - \mathbf{P}[X < 10] = e^{-10/15} - e^{-25/15}$

   $1 - e^{-25/15} - (1 - e^{-10/15})$
2. What is the expected amount of time you have to wait?

   $\mathbf{E}[X] = 15$

The exponential distribution

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

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

$\mathbf{P}[\, X > 25 \;\mathbf{|}\; X > 15 \,]$

$= \mathbf{P}[\, X > 25 \;\&\; X > 15 \,] \,/\, \mathbf{P}[\, X > 15 \,]$

$= \mathbf{P}[\, X > 25 \,] \,/\, \mathbf{P}[\, X > 15 \,]$

$= e^{-25/15} \;/\; e^{-15/15}$

$= e^{-25/15 + 15/15}$

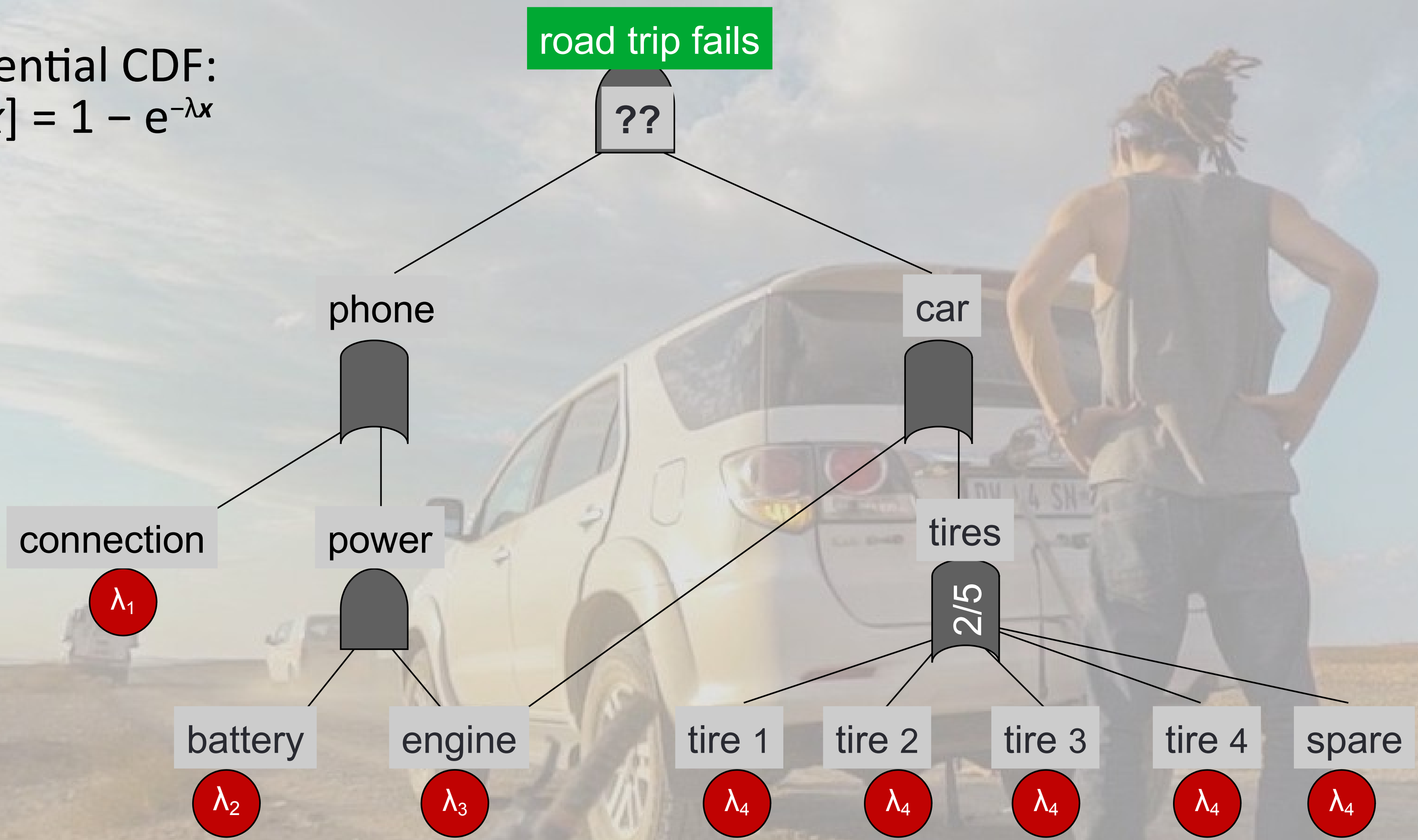
$= e^{-10/15}$

$= \mathbf{P}[\, X > 10]$

The exponential distribution has the **memoryless property:**
past waiting time has not influence on future waiting time

Reliability with continuous time

Exponential CDF:
$\mathbf{P}[X \leq x] = 1 - e^{-\lambda x}$

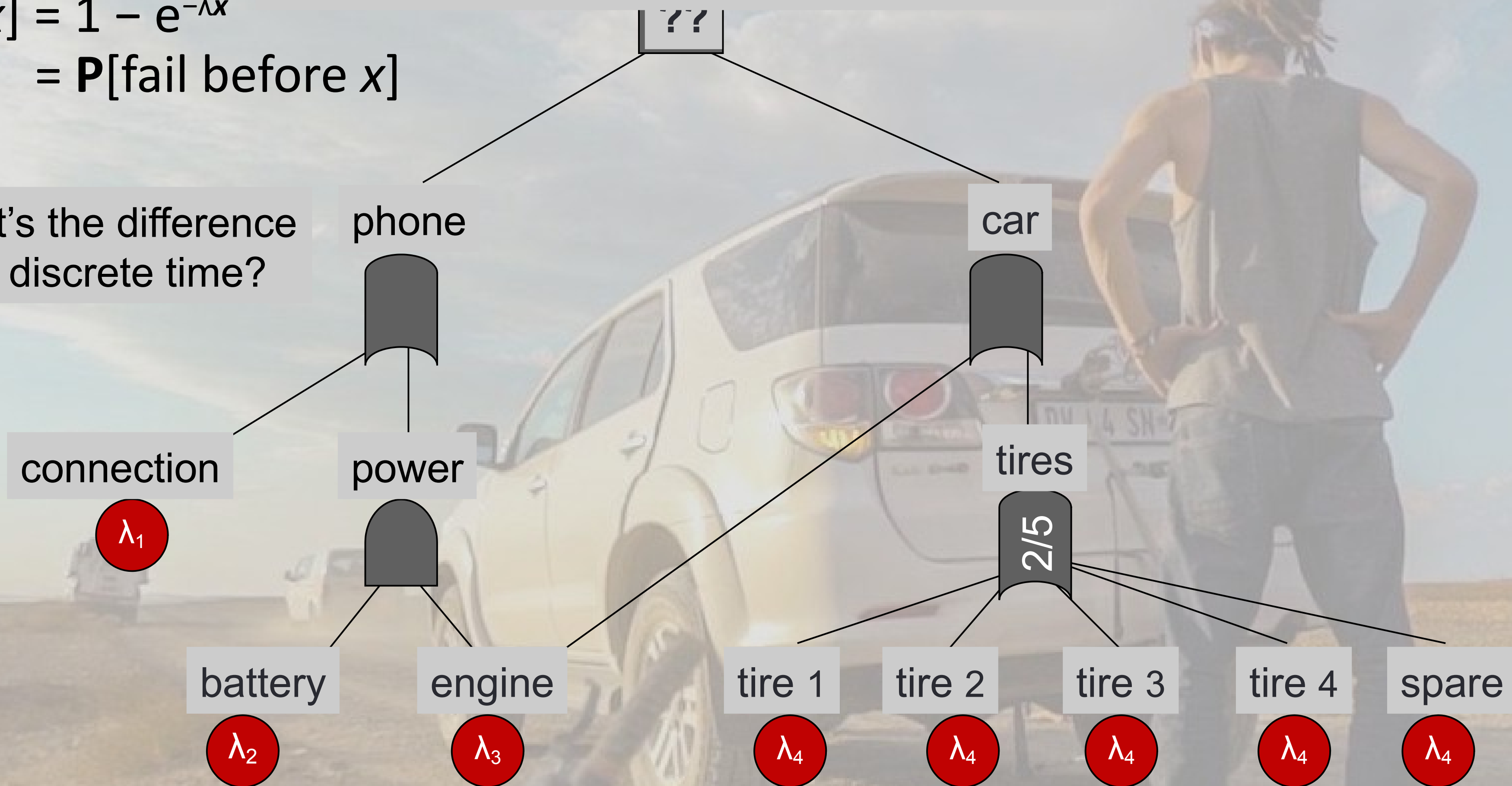


Reliability with continuous time

$$(p_1 + p_2 - p_1p_2)p_3 +$$
$$p_1(1 – ((1\text{-}p_4)^5 + 5p_4(1\text{-}p_4)^4))(1\text{-}p_3)$$

Exponential CDF:
$\mathbf{P}[X \leq x] = 1 - e^{-\lambda x}$
$= \mathbf{P}[\text{fail before } x]$

Hint: what's the difference with discrete time?



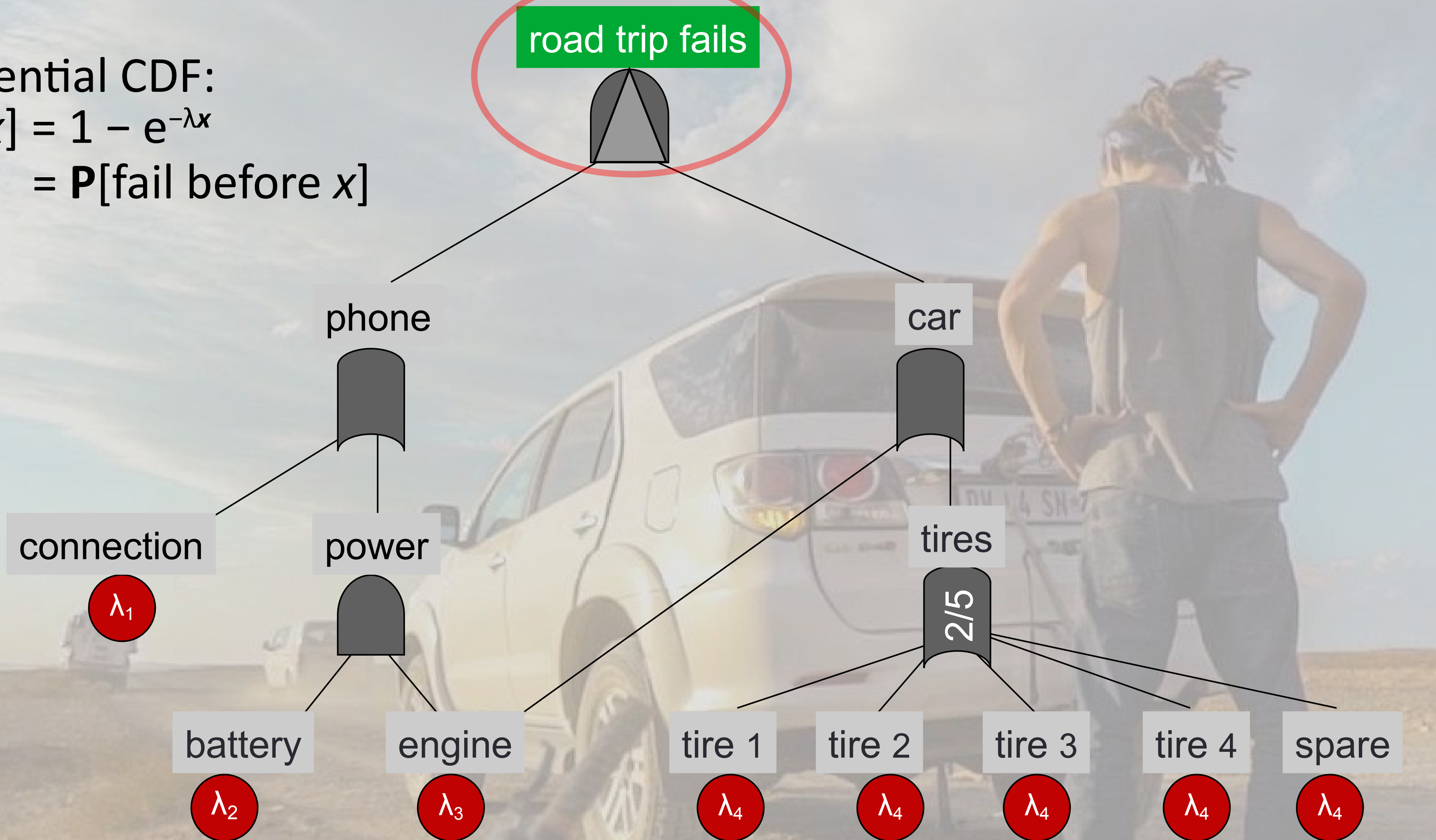
$$((1\text{-}e^{-\lambda 1x}) + (1\text{-}e^{-\lambda 2x}) - (1\text{-}e^{-\lambda 1x})\,(1\text{-}e^{-\lambda 2x}))\,(1\text{-}e^{-\lambda 3x}) +$$
$$(1\text{-}e^{-\lambda 1x})(1 – (e^{-\lambda 4x})^5 + 5(e^{-\lambda 4x})\,e^{-\lambda 4x4})e^{-\lambda 3x}$$

Reliability with continuous time

Exponential CDF:

$\mathbf{P}[X \leq x] = 1 - e^{-\lambda x}$

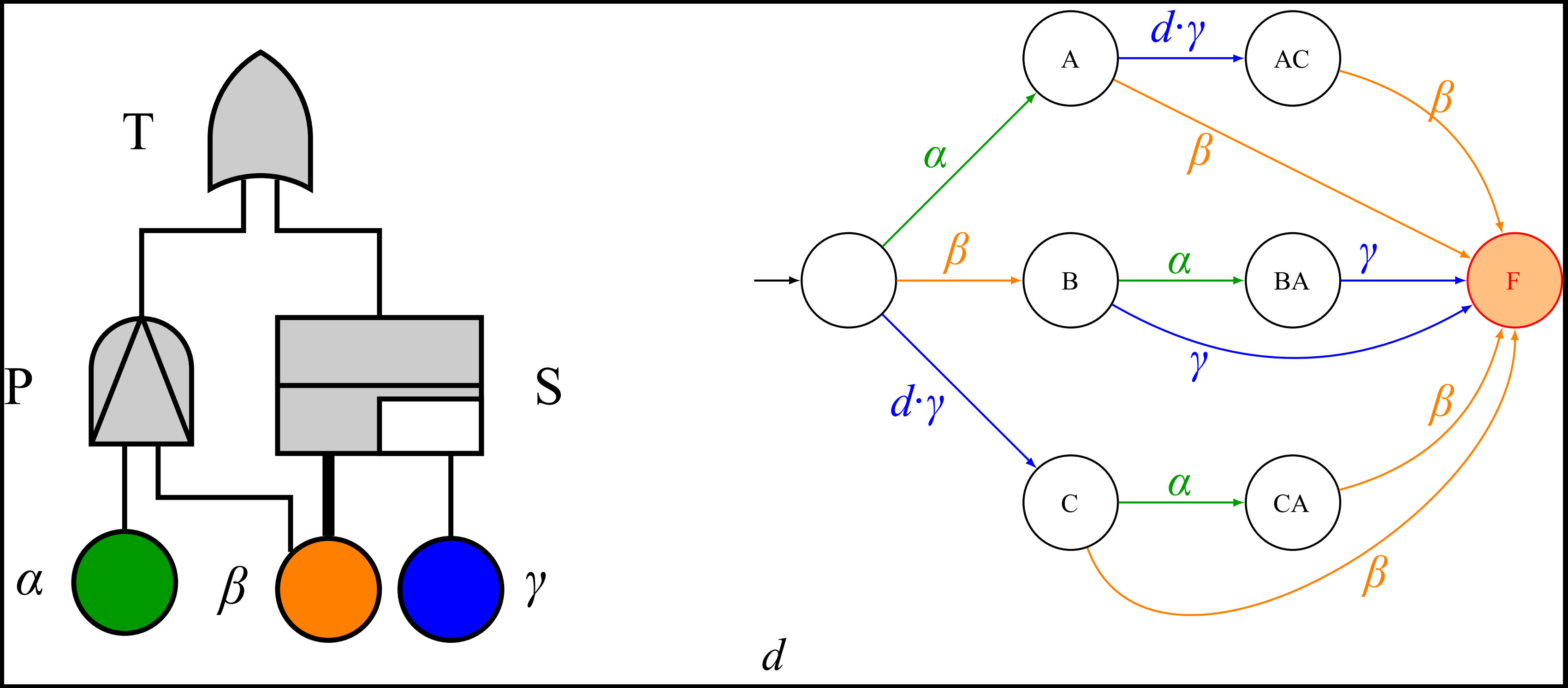
$= \mathbf{P}[\text{fail before } x]$



$$((1\text{-}e^{-\lambda 1x}) + (1\text{-}e^{-\lambda 2x}) - (1\text{-}e^{-\lambda 1x})\,(1\text{-}e^{-\lambda 2x}))\,(1\text{-}e^{-\lambda 3x}) +$$
$$(1\text{-}e^{-\lambda 1x})(1 - (e^{-\lambda 4x})^5 + 5(e^{-\lambda 4x})\, e^{-\lambda 4x4})e^{-\lambda 3x}$$

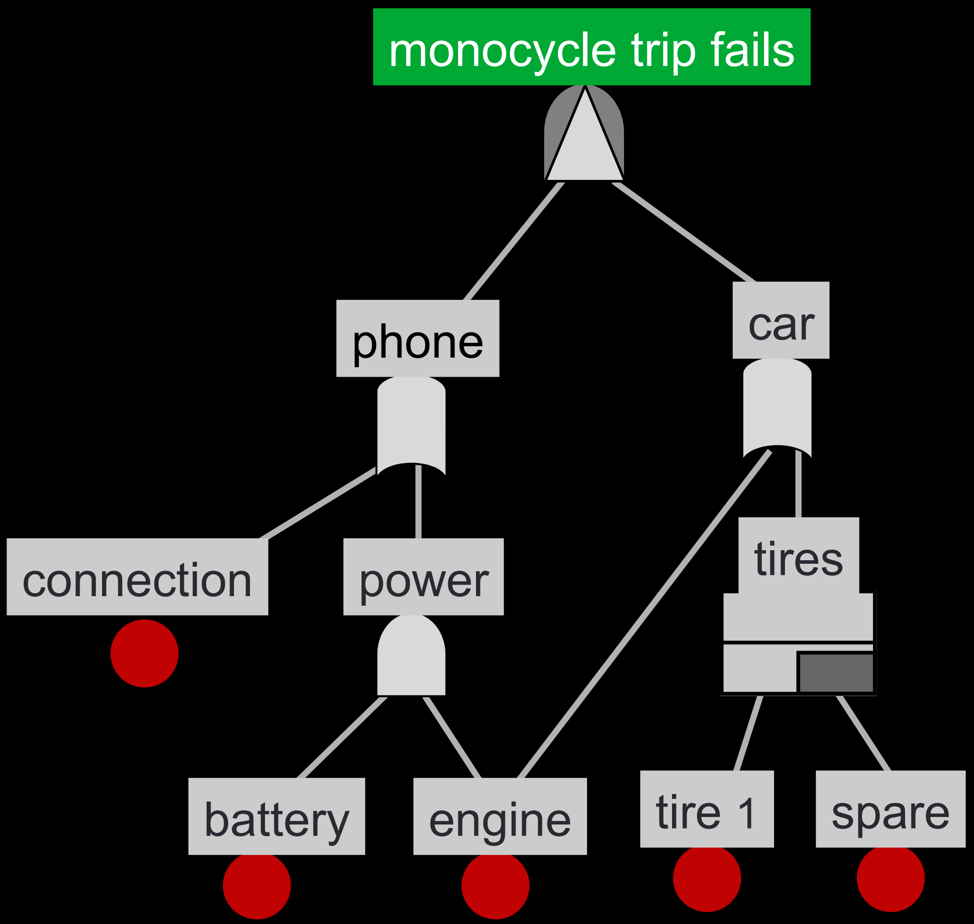
Quantitative analyses for DFTs

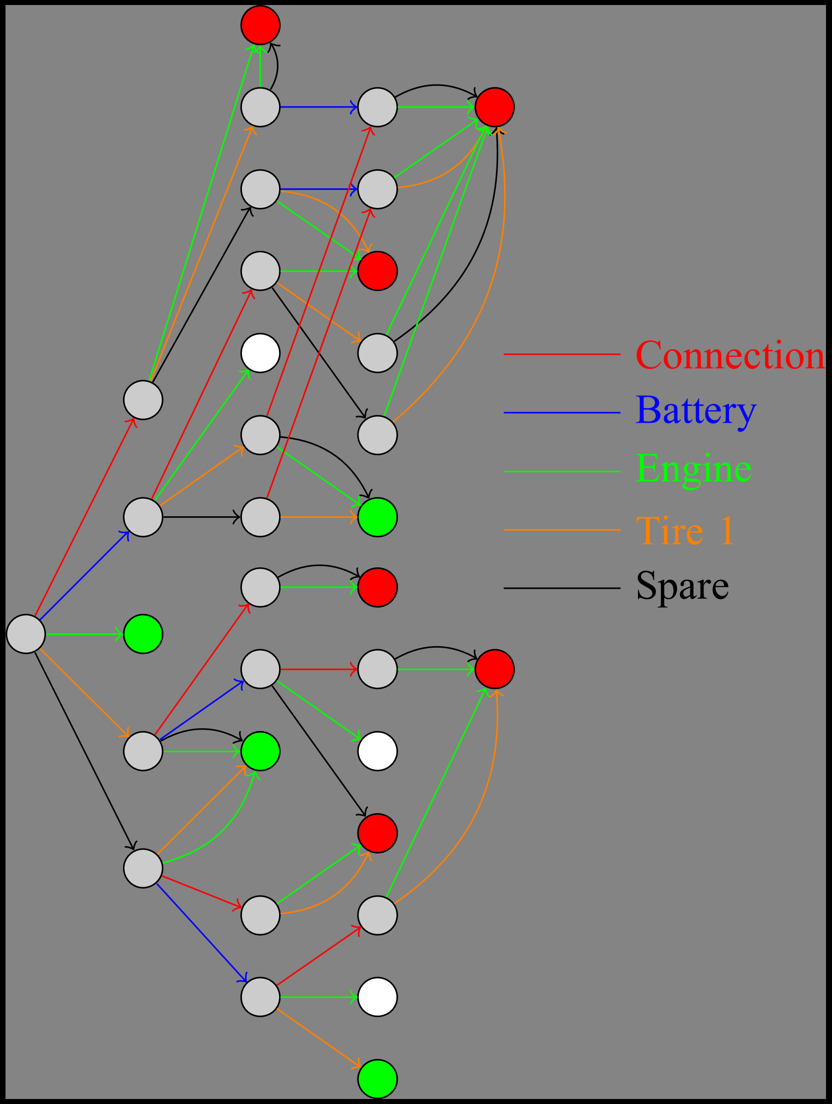
Original method: Markov chains



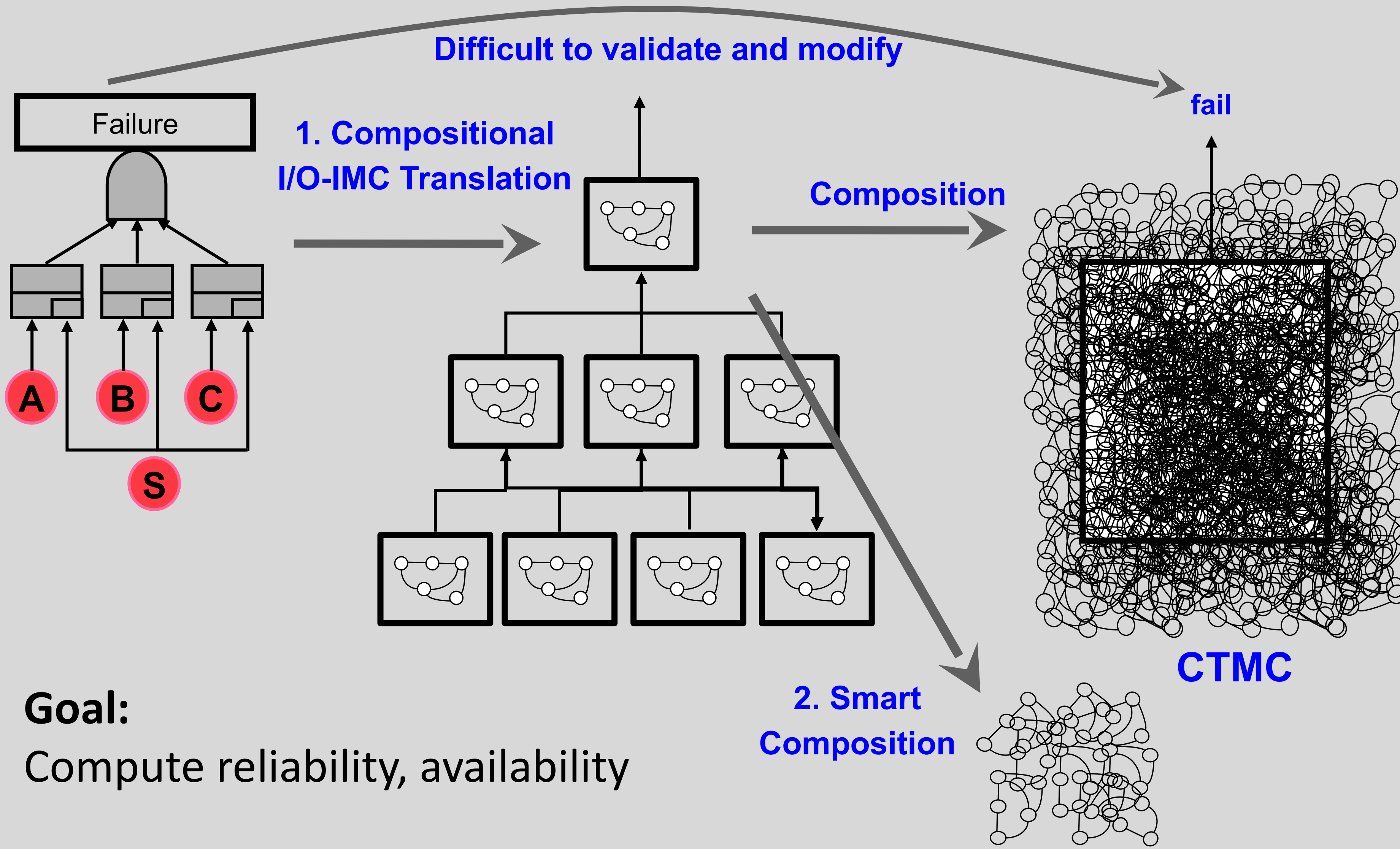
Quantitative analyses for DFTs

Draw the Markov chain for this simplified DFT.



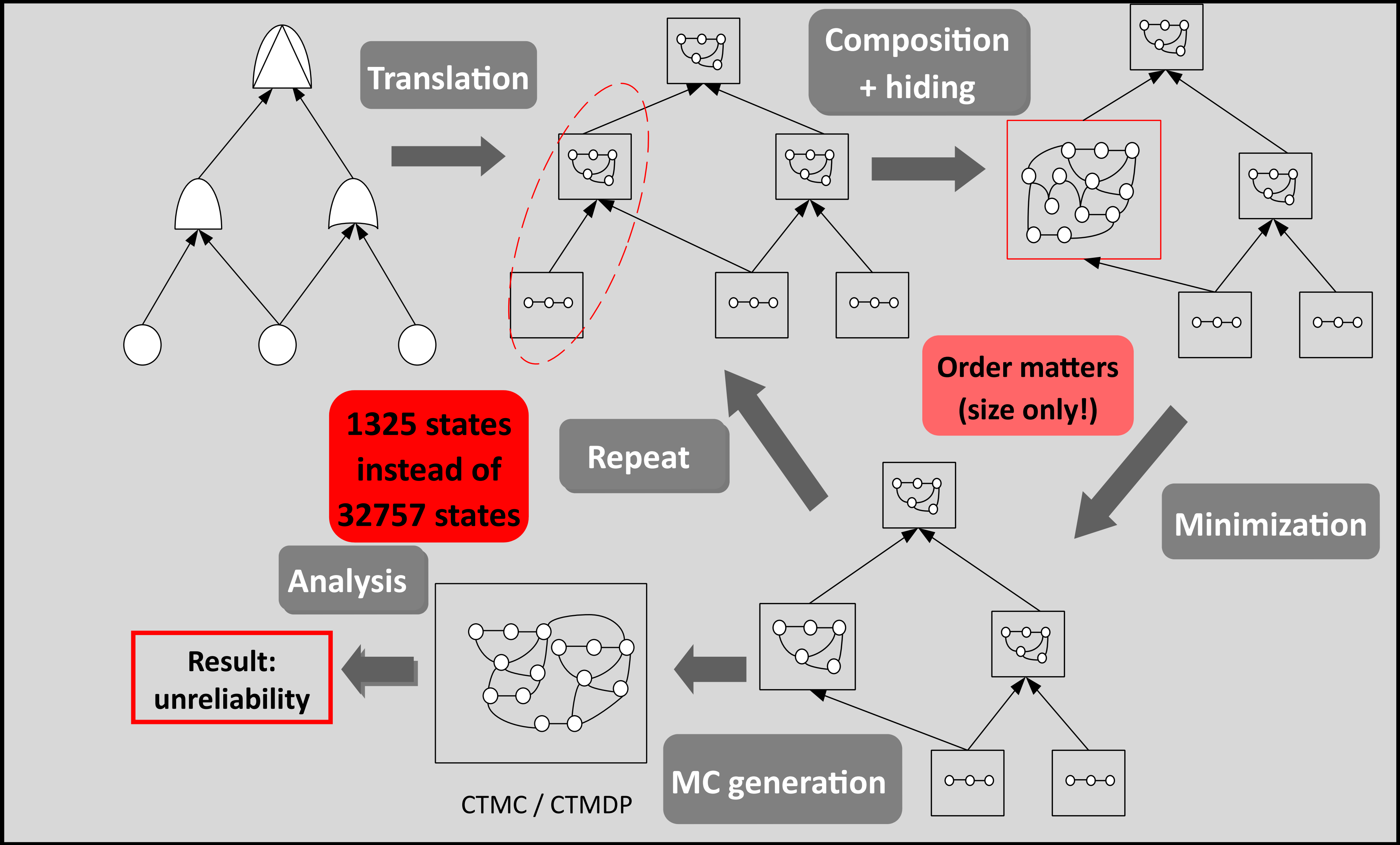


Quantitative analyses for DFTs



Goal:
Compute reliability, availability

Quantitative analyses for DFTs



Contents

- Fault Trees
  - What & Why
- Fault Tree Analysis
  - Discrete time
  - Continuous time
- FTA in practice
  - Tools & benchmarks
  - Concrete examples (the real deal)

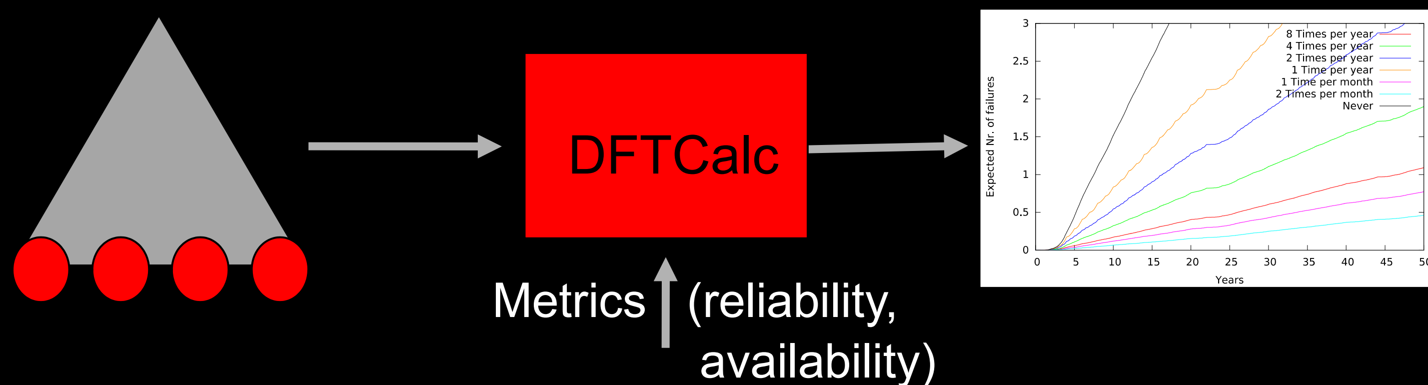
Software tools for FTA

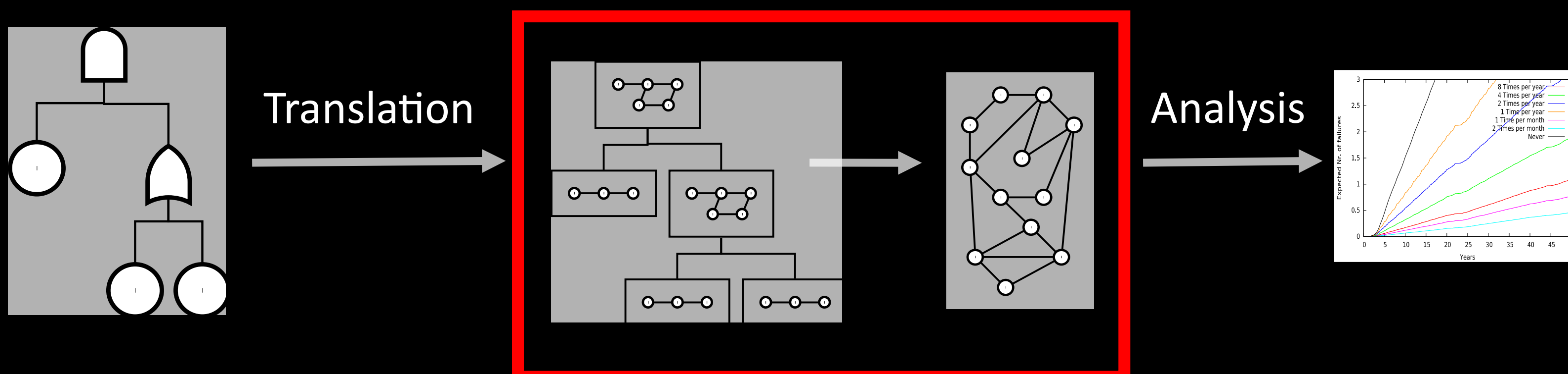
DFTCalc

- Developed in the University of Twente

Software tools for FTA

DFTCalc





Galileo input format:

```
toplevel “TLE”;
“TLE” or “G1” “G2”;
“G1” wsp “B1” “B2” “S”;
“B1” lambda=1.23e-2;
…
```

Efficiency:

- Compositional aggregation
- Context-dependent state space generation

Software tools for FTA

Storm

- Developed in RWTH Aachen University (Germany)
- General purpose model checker
  - Very efficient (for “general” analyses)
- Supports a subset of Galileo
- Computes reliability and availability (not MTTF)

Software tools for FTA

FIG

- Developed in Universidad Nacional de Córdoba (Argentina)
- Statistical model checker
  - Specialises in Rare Event Simulation
- Supports an extended subset of Galileo
- Computes reliability and availability (not MTTF)

Commercial tools

- Fault Tree **+**
- isograph *Fault Tree Analysis Software*
- OpenFTA (defunct?)
- SCRAM

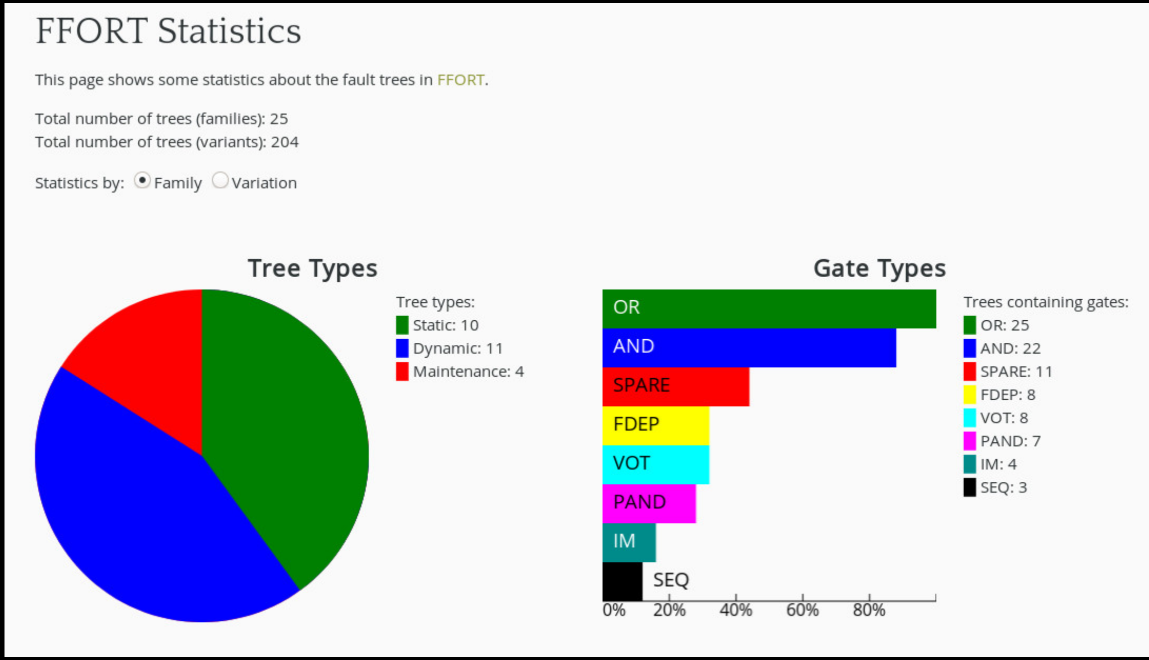
Most offer support for Static Fault Trees alone, e.g. via cut set analysis + optimisations 1. & 2.

Scale much better than academic tools!

Benchmarks

FFORT [https://dftbenchmarks.utwente.nl/]

- Over 200 fault trees, and growing
- All types (static, dynamic, etc.)



Benchmarks

FFORT [https://dftbenchmarks.utwente.nl/]

- Over 200 fault trees, and growing
- All types (static, dynamic, etc.)
- FTs from research and real world cases
- Published + reference analysis results

Examples: real FTs in action

Featuring:

- Railways
- Rockets
- Colossal gates

Example #1: Falcon 9

ONGOING COVERAGE: SPACEX FALCON 9 CRS 7 ACCIDENT

A SpaceX Falcon 9 v1.1 encountered an anomaly about two minutes into the flight of the CRS-7 mission - resulting in the complete loss of the booster and Dragon spacecraft. Photo Credit: Jared Haworth / SpaceFlight Insider

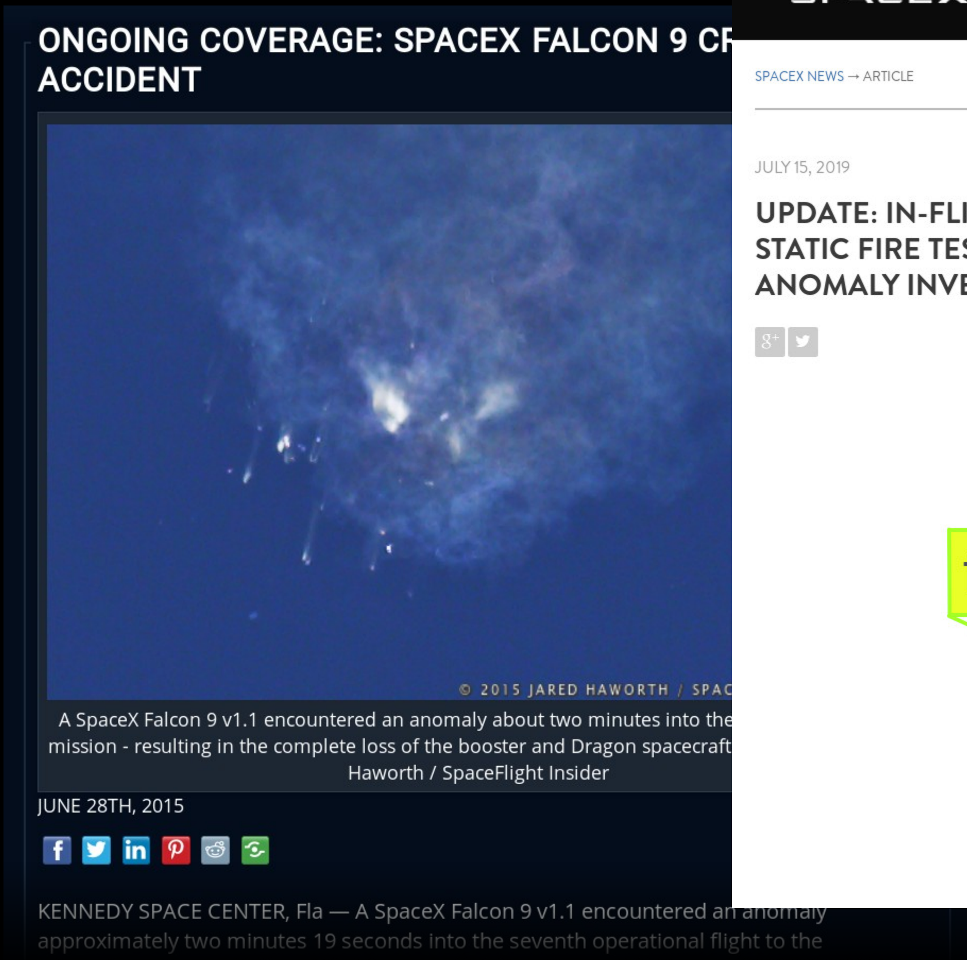
JUNE 28TH, 2015 by JASON RHIAN

KENNEDY SPACE CENTER, Fla — A SpaceX Falcon 9 v1.1 encountered an anomaly approximately two minutes 19 seconds into the seventh operational flight to the

https://www.spaceflightinsider.com/organizations/space-exploration-technologies/ongoing-coverage-spacex-falcon-9-crs-7-accident/

https://www.youtube.com/watch?v=IlduwR41WFQ&feature=youtu.be

Example #1: Falcon 9



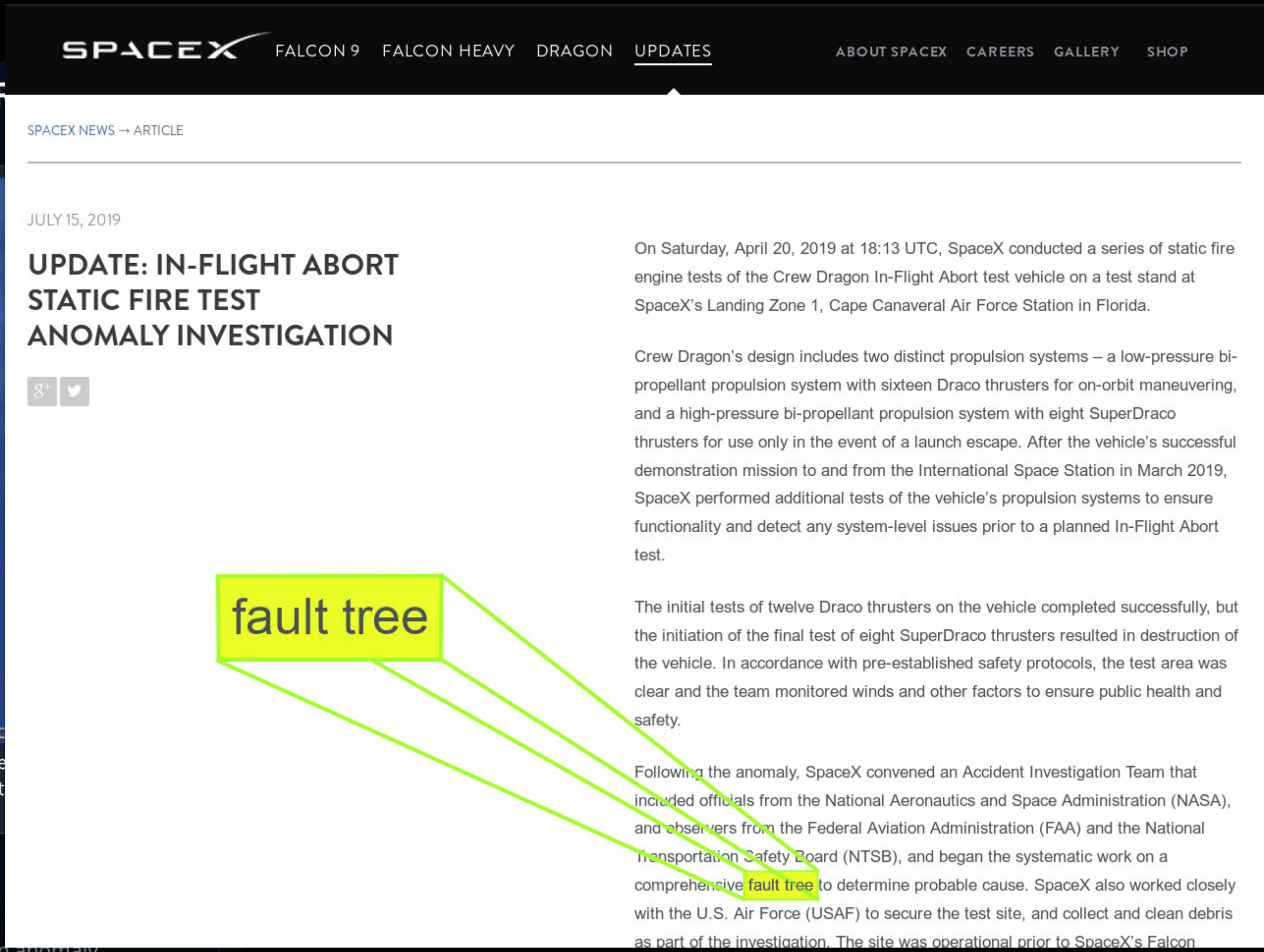
ONGOING COVERAGE: SPACEX FALCON 9 CR
ACCIDENT

© 2015 JARED HAWORTH / SPAC

A SpaceX Falcon 9 v1.1 encountered an anomaly about two minutes into the
mission - resulting in the complete loss of the booster and Dragon spacecraft
Haworth / SpaceFlight Insider

JUNE 28TH, 2015

KENNEDY SPACE CENTER, Fla — A SpaceX Falcon 9 v1.1 encountered an anomaly
approximately two minutes 19 seconds into the seventh operational flight to the



SPACEX FALCON 9 FALCON HEAVY DRAGON UPDATES ABOUT SPACEX CAREERS GALLERY SHOP

SPACEX NEWS → ARTICLE

JULY 15, 2019

UPDATE: IN-FLIGHT ABORT STATIC FIRE TEST ANOMALY INVESTIGATION

On Saturday, April 20, 2019 at 18:13 UTC, SpaceX conducted a series of static fire engine tests of the Crew Dragon In-Flight Abort test vehicle on a test stand at SpaceX's Landing Zone 1, Cape Canaveral Air Force Station in Florida.

Crew Dragon's design includes two distinct propulsion systems – a low-pressure bi-propellant propulsion system with sixteen Draco thrusters for on-orbit maneuvering, and a high-pressure bi-propellant propulsion system with eight SuperDraco thrusters for use only in the event of a launch escape. After the vehicle's successful demonstration mission to and from the International Space Station in March 2019, SpaceX performed additional tests of the vehicle's propulsion systems to ensure functionality and detect any system-level issues prior to a planned In-Flight Abort test.

The initial tests of twelve Draco thrusters on the vehicle completed successfully, but the initiation of the final test of eight SuperDraco thrusters resulted in destruction of the vehicle. In accordance with pre-established safety protocols, the test area was clear and the team monitored winds and other factors to ensure public health and safety.

Following the anomaly, SpaceX convened an Accident Investigation Team that included officials from the National Aeronautics and Space Administration (NASA), and observers from the Federal Aviation Administration (FAA) and the National Transportation Safety Board (NTSB), and began the systematic work on a comprehensive fault tree to determine probable cause. SpaceX also worked closely with the U.S. Air Force (USAF) to secure the test site, and collect and clean debris as part of the investigation. The site was operational prior to SpaceX's Falcon

https://www.spaceflightinsider.com/organizations/space-exploration-technologies/ongoing-coverage-spacex-falcon-9-crs-7-accident/

https://www.youtube.com/watch?v=IlduwR41WFQ&feature=youtu.be

Example #1: Falcon 9

Topics | Missions | Galleries | NASA TV | Follow NASA | Downloads | About | NASA Audiences | Search

Latest | **Related**

NASA Highlights Science on 18th SpaceX Resupply Mission to Space Station
a month ago

NASA to Broadcast Next Space Station Resupply Launch, Prelaunch Activities
4 months ago

NASA Invites Media to 17th SpaceX Cargo Launch to Space Station
5 months ago

NASA Highlights Science on Next Resupply Mission to International Space Station
9 months ago

NASA to Highlight Science Launching on Next Resupply Mission to Space Station
a year ago

NASA Releases Summary of SpaceX Cargo Mission Accident
a year ago

NASA Invites Media to Upcoming Space Station Cargo Launch
a year ago

March 12, 2018

NASA Releases Summary of SpaceX Cargo Mission Accident

A NASA team who independently reviewed the unsuccessful launch of SpaceX's seventh contracted commercial resupply services (CRS) mission to the International Space Station for the agency has released a public summary of its findings.

SpaceX launched a Falcon 9 rocket June 28, 2015, from Launch Complex 40 on Cape Canaveral Air Force Station in Florida. The rocket was carrying a Dragon spacecraft loaded with more than 4,300 pounds of scientific investigations, supplies and station hardware. According to the summary, about 139 seconds into flight, the rocket experienced an anomaly in the upper stage liquid oxygen tank, resulting in the loss of the mission.

The flight was launched under a commercial license from the Federal Aviation Administration (FAA), and was not considered a NASA mishap. Following SpaceX and FAA contingency protocol, the company established an accident investigation team immediately following the mishap. NASA was among the participants invited to join the team, and served as non-voting member.

With SpaceX scheduled to launch the Jason-3 satellite on a Falcon 9 rocket under a NASA launch services contract after the accident, the agency had the right to accept/reject any finding, root cause, and corrective action from SpaceX's board. In addition to observing the SpaceX-led investigation, NASA stood up its own independent review team Aug. 3, 2015, to evaluate the launch events.

As part of its review, the NASA team performed an independent analysis of the rocket's telemetry, and developed a detailed timeline to the millisecond level of the launch events. Among their research, the team analyzed various Falcon 9 systems, the SpaceX fault tree, and conducted multiple engineering boards.

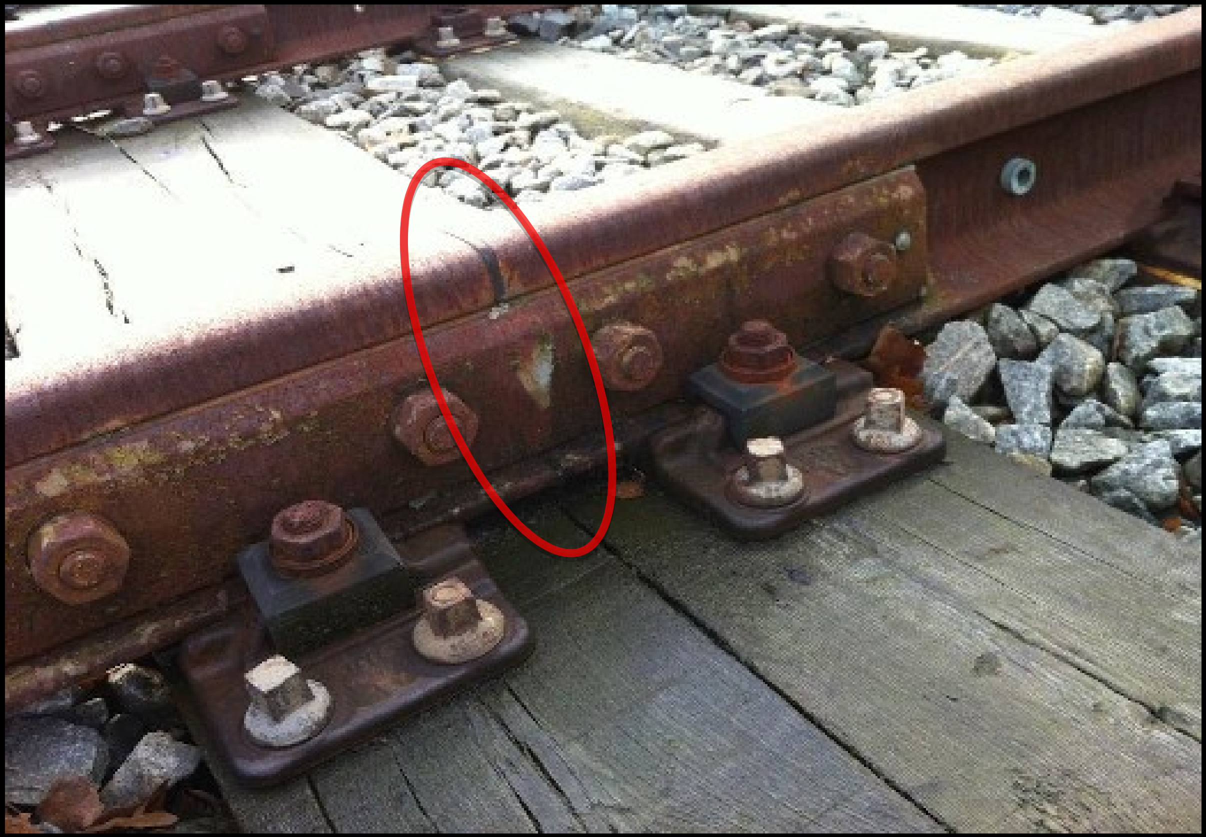
Based on their detailed review and analysis of telemetry data, photos and video capturing the launch and failure, the NASA review team determined the direct or proximate cause of the Falcon 9 launch vehicle failure was the rupture of the stage 2 liquid oxygen tank. The primary failure scenario was likely a composite overwrapped pressure vessel within the stage 2 liquid oxygen tank became liberated, hitting the tank dome, causing it to rupture. The public summary includes additional details about the team's findings and recommendations.

Example #1: Falcon 9

https://www.spaceflightinsider.com/organizations/space-exploration-technologies/ongoing-coverage-spacex-falcon-9-crs-7-accident/

https://www.youtube.com/watch?v=IlduwR41WFQ&feature=youtu.be

Example #2: Electrically Insulated Joint



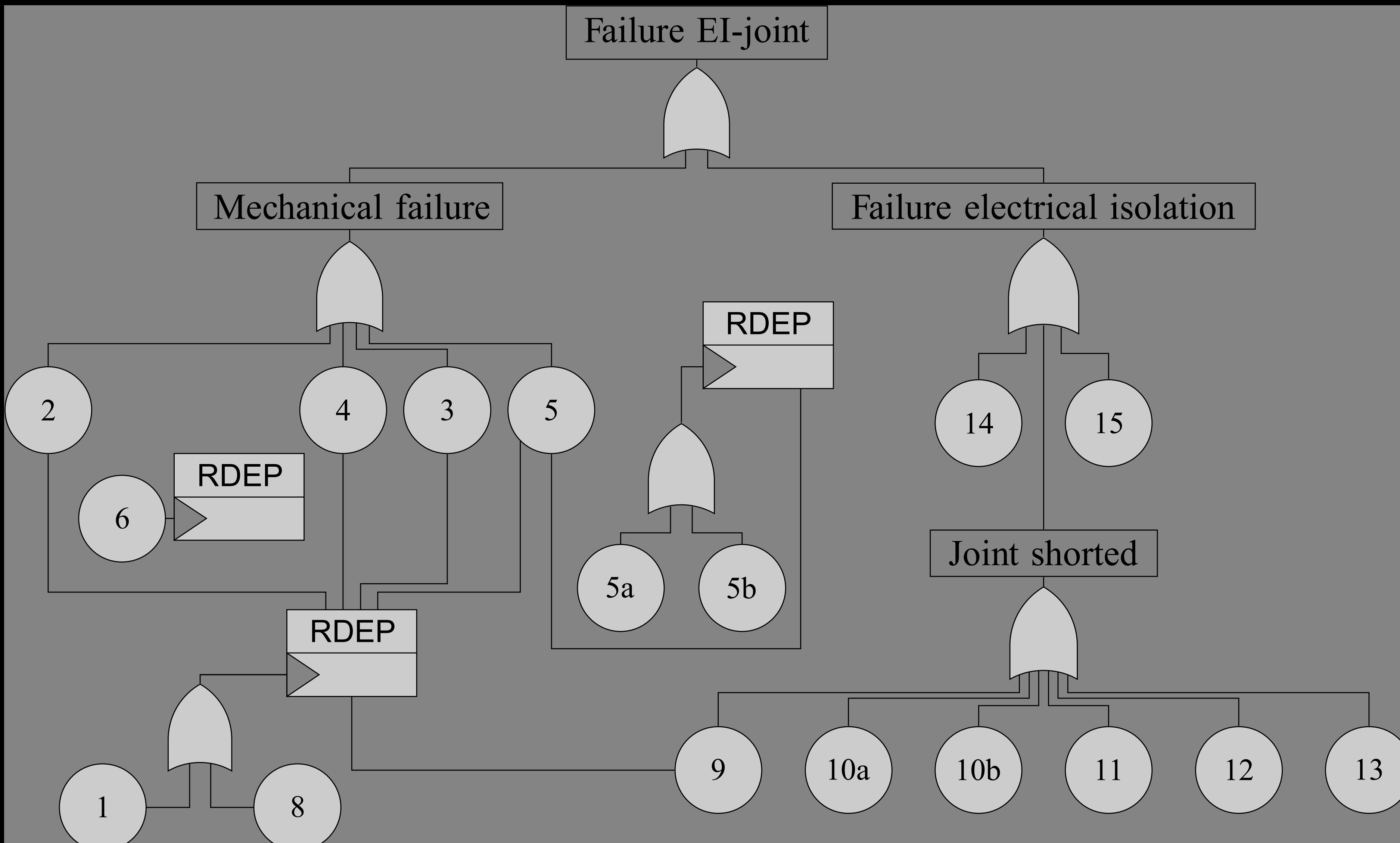
ProRail

Electrically separates tracks, to measure train distance

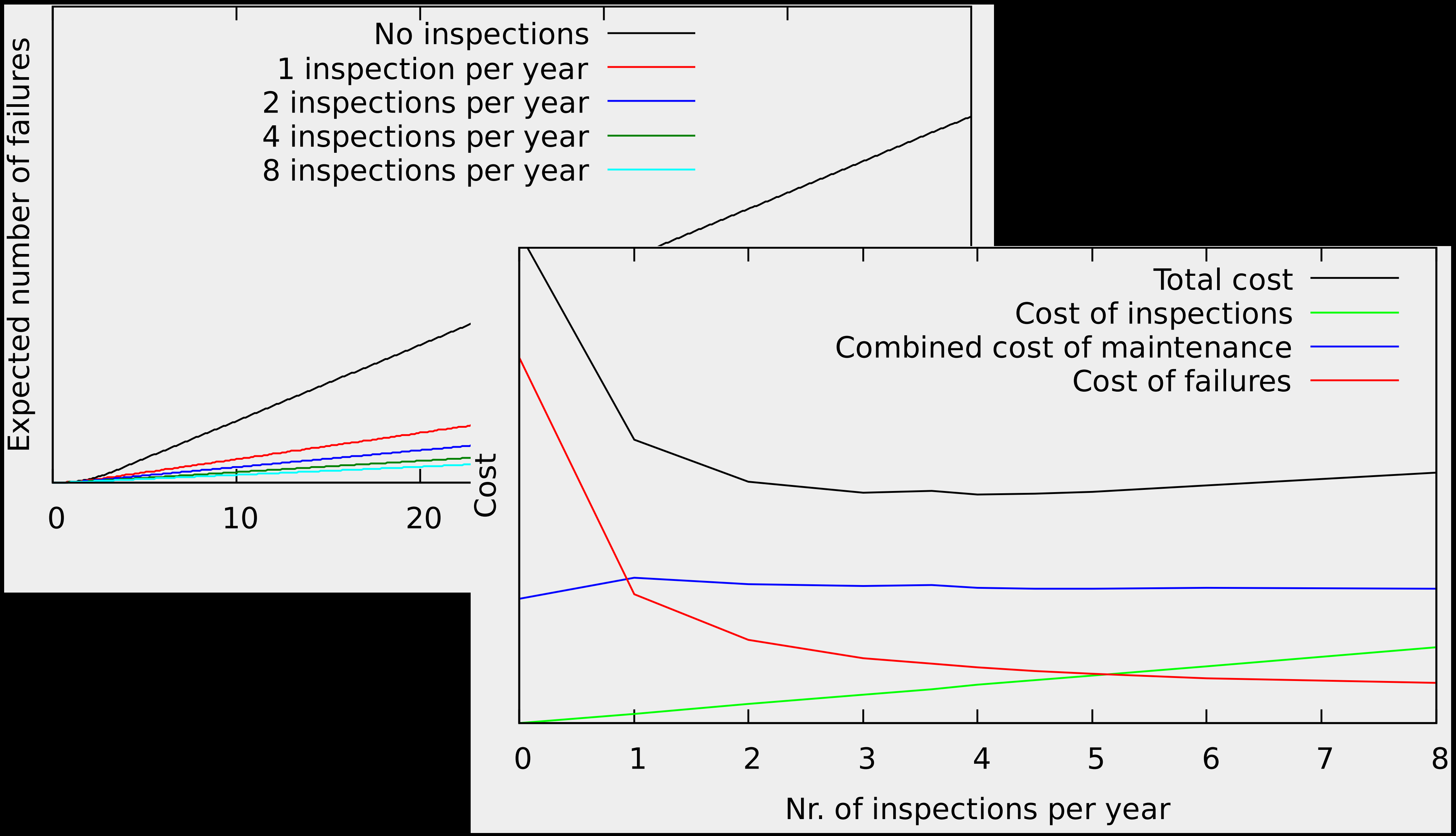
In total: 45.000 EIJs in the Netherlands

Important cause of train disruptions

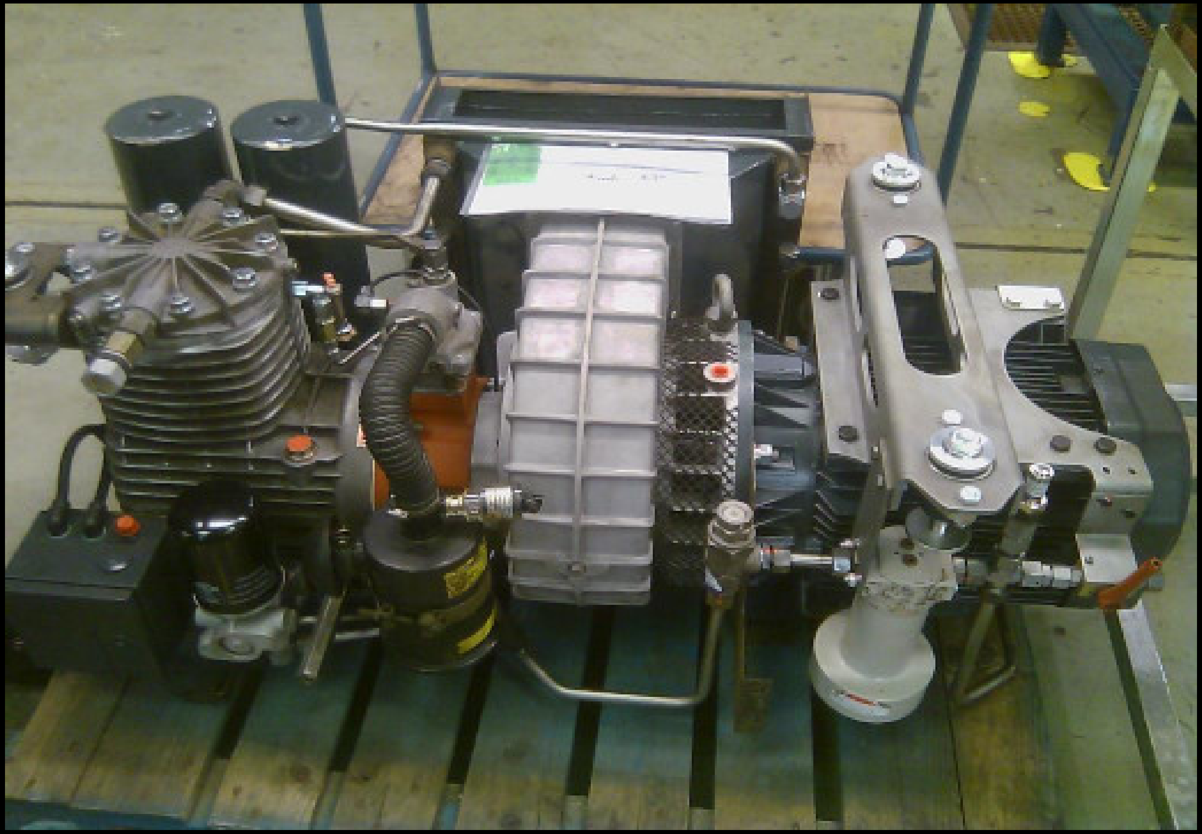
Example #2: Electrically Insulated Joint



Example #2: Electrically Insulated Joint



Example #3: Pneumatic Compressor

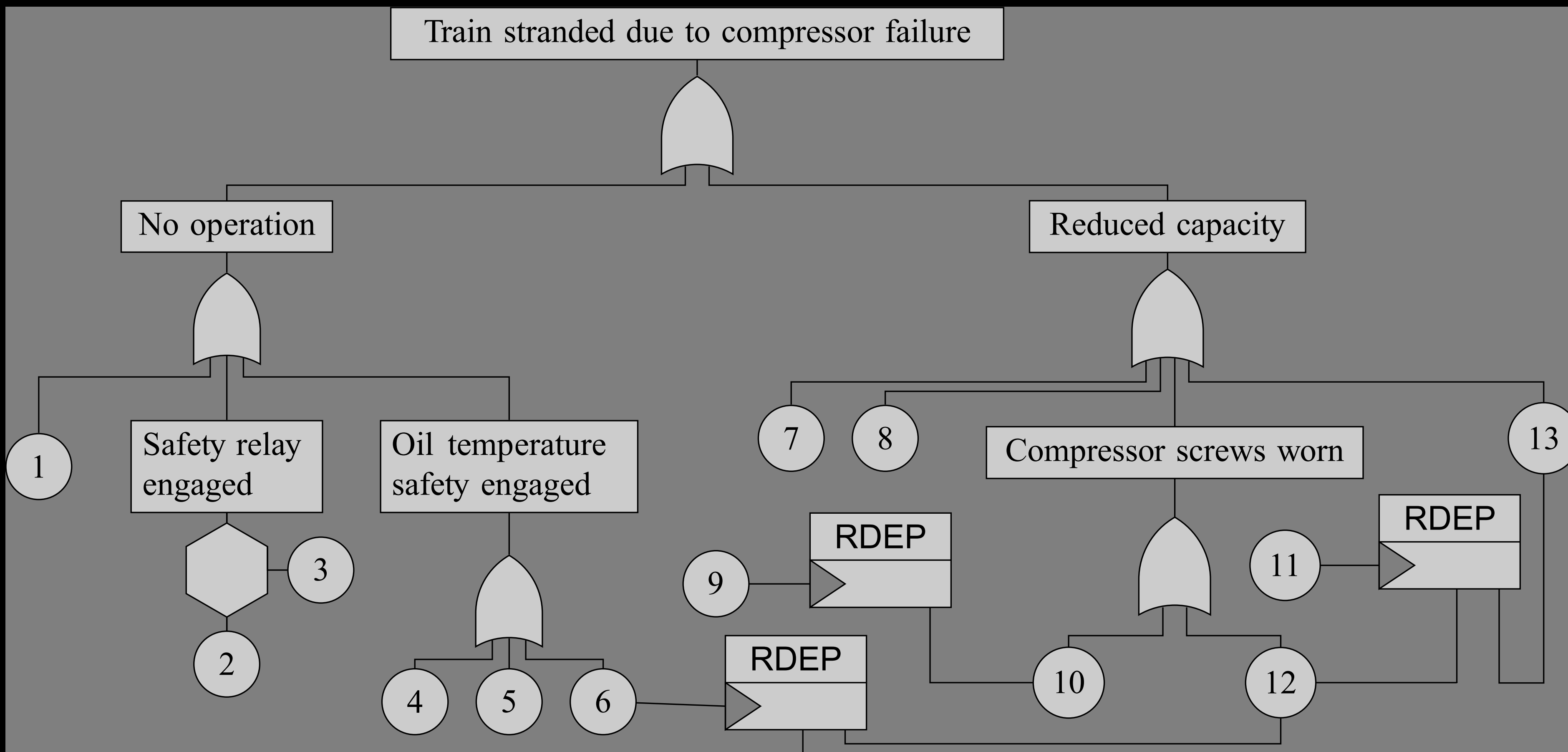


Powers the breaks of a train, its doors, etc.

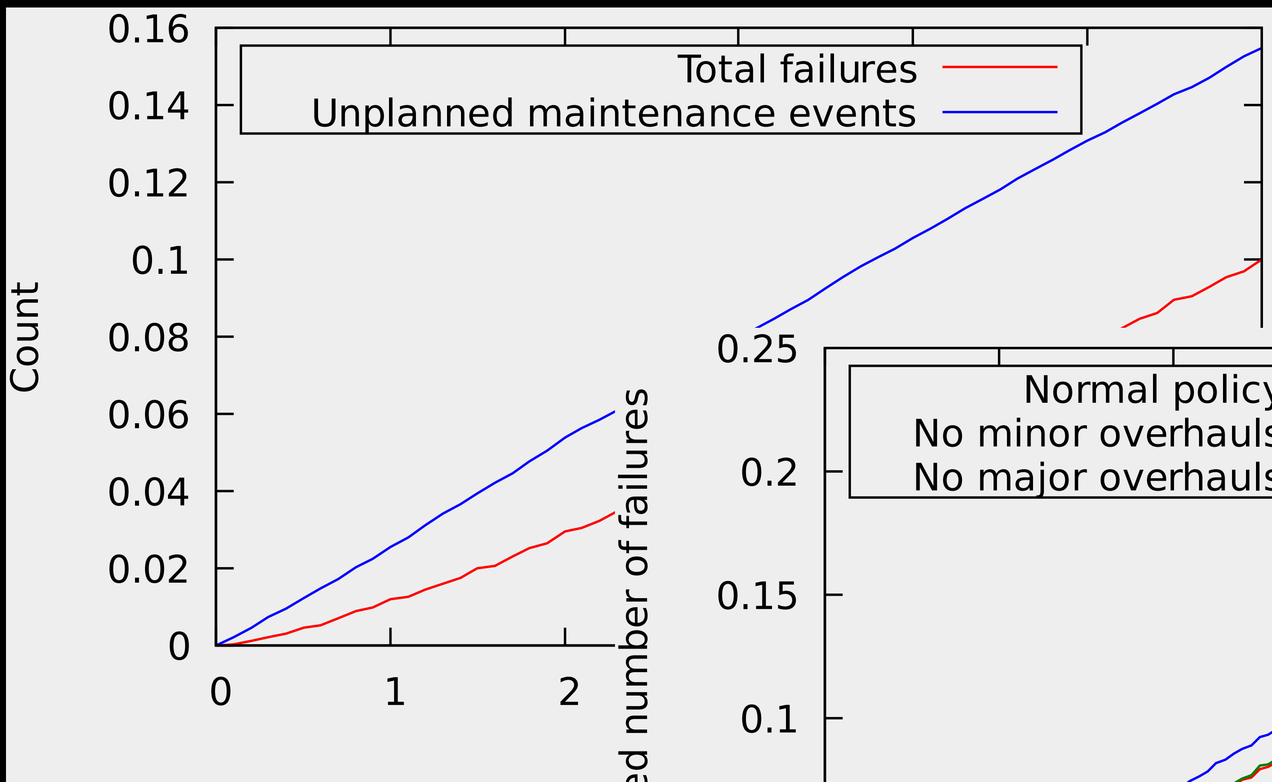
Failures can strand a train on a rail, causing disruptions

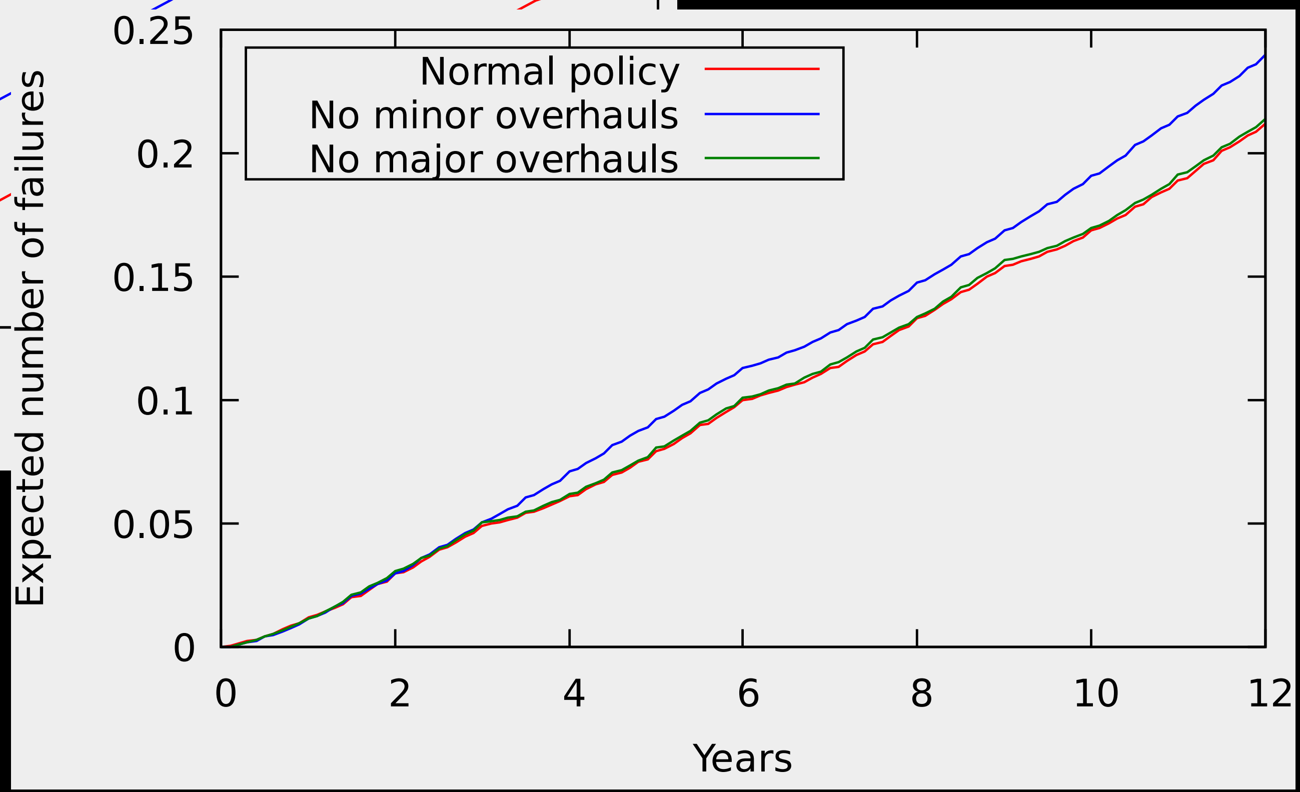
Normal operation requires regular maintenance

Example #3: Pneumatic Compressor



Example #3: Pneumatic Compressor





Example #4: Oosterscheldekering

The existing FT has several thousands of gates

The leaves include SPARE handling (hot & cold)

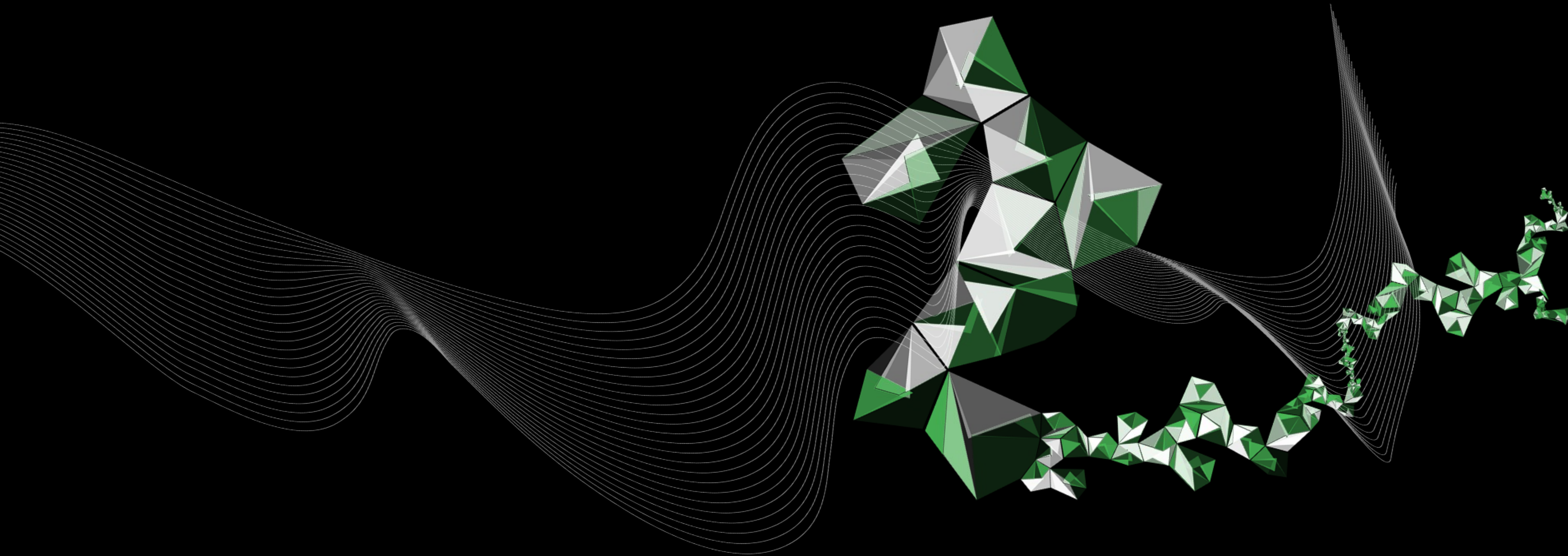
One of the largest formally verified systems in the world

Is keeping us dry NOW!

delta π performance improvement

NRG

Risk Management



Risk Assessment Techniques #1

Fault Tree Analysis

Carlos E. Budde

Thanks to Dr. Enno Ruijters

https://youtu.be/eebfMFzJHNs