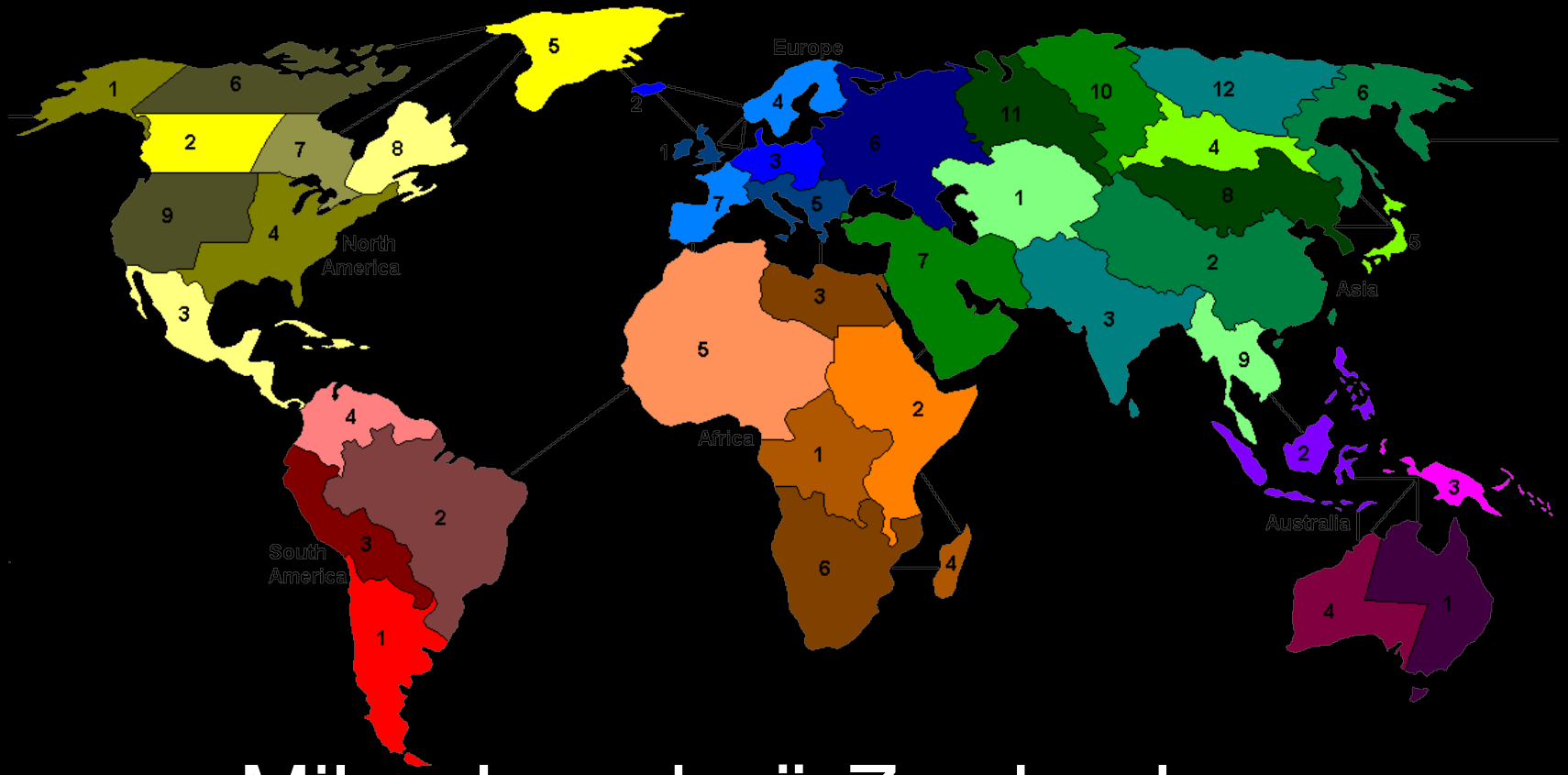
Lecture 3: Dynamic fault trees



Milan Lopuhaä-Zwakenberg

Formal Methods & Tools

System (un)reliability

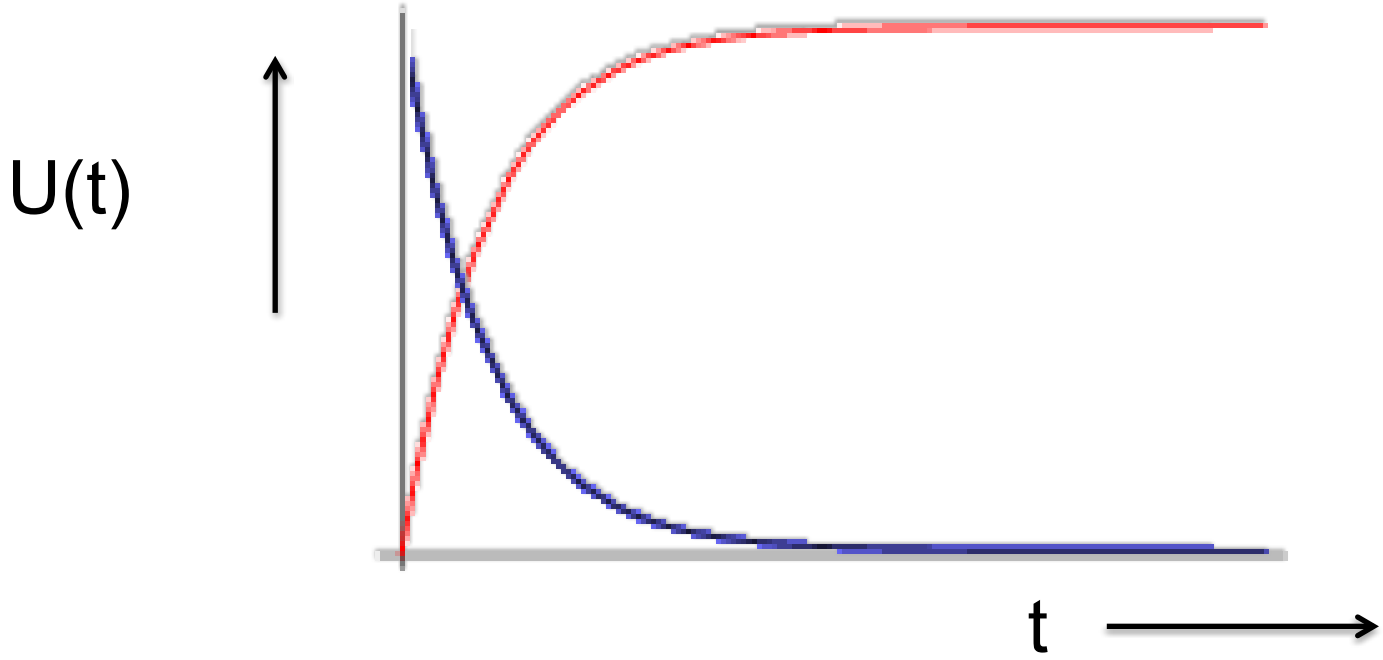
- Unreliability

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

- Reliability / Survivor function

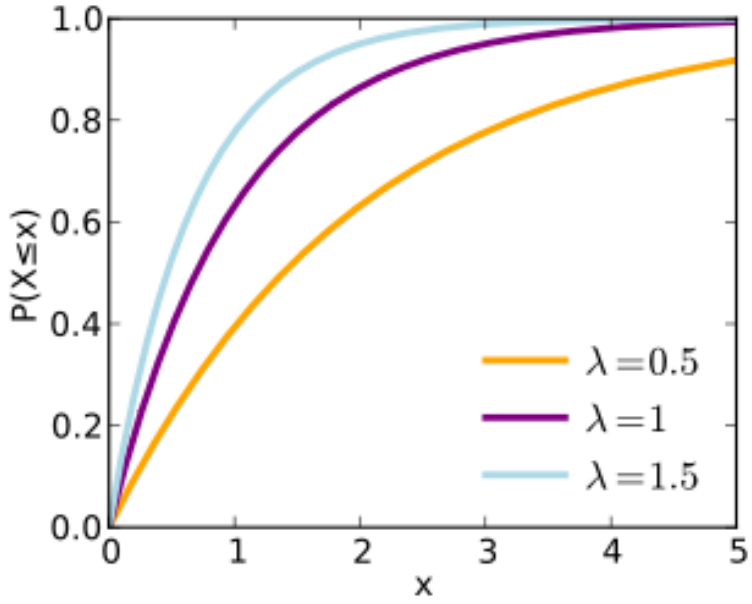
  R(t) = **P**[no failure until time *t*]

  = 1- U(t)



Exponential distribution: cumulative density function

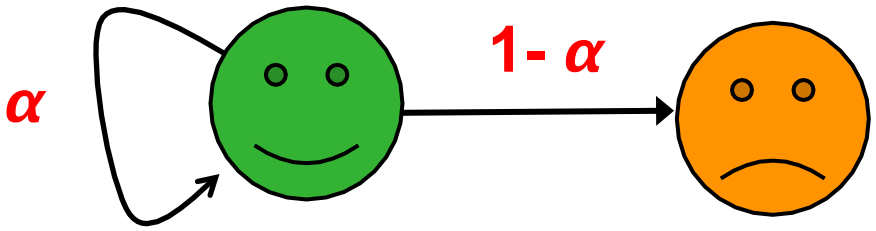
- Unreliability, CDF
  - **P**[fail before t] = **P**[$X \le t$] = $1 - e^{-\lambda t}$
  - X: random variable denoting failure time
- Parameter: λ
  - Failure rate, $\lambda > 0$
  - λ = expected number of fails per time unit
  - **E**[X] = $1/\lambda$
- Reliability / survivors function, CDF
  - **P**[fail after t] =
    = 1 – **P**[fail before t]
    = 1- $(1 - e^{-\lambda * t})$
    = $e^{-\lambda * t}$
    = $(e^{-\lambda})^t$ {write $e^{-\lambda} = \boldsymbol{\alpha}$}
    = $\boldsymbol{\alpha}^t$

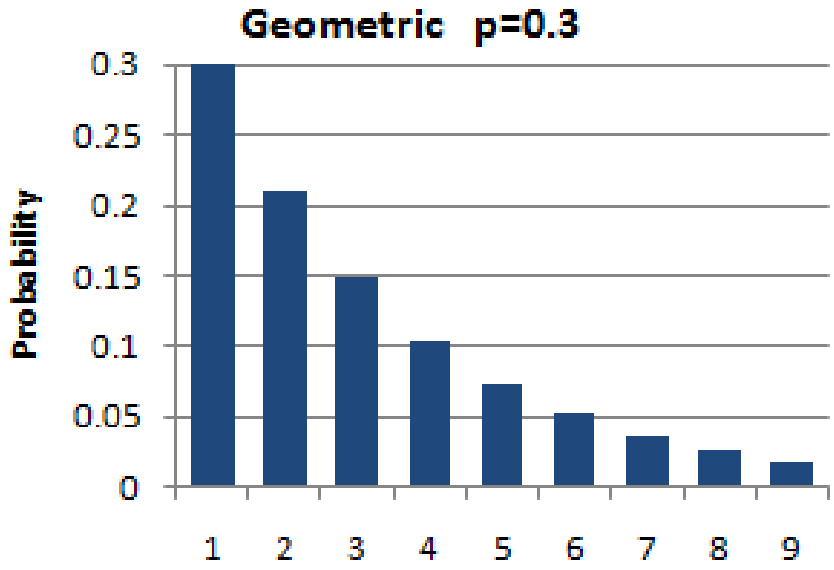


Exponential distribution: cumulative density function

Reliability / survivors function, CDF

- **P**[fail after t] = **P**[$X > t$] = α^t
- "Survive" each time unit with probability α
  - t=0: $\alpha^0 = 1$
  - t=1: α
  - t=2: α^2
  - t=3: α^3
  - …
  - t=1/2: $\alpha^{1/2}$
  - t=14.7302: $\alpha^{14.7302}$





Note: picture displays the discrete version, for fixed time steps

Exponential distribution: memoryless

- **Memoryless**
  - Makes this distribution easier
  - Crucial for use in transition systems
- $\mathbf{P}[X > t + s \mid X > s] = \mathbf{P}[X > t]$

No matter how long you have already been operational,

the probability that remain for operational for t more time units is always $\mathbf{P}[X > t]$

$$\mathbf{P}[X > t+s \mid X > s] \quad = \quad \mathbf{P}[X > t]$$

Given that you were operational for s time units,

remain operational for at least $t + s$ most units

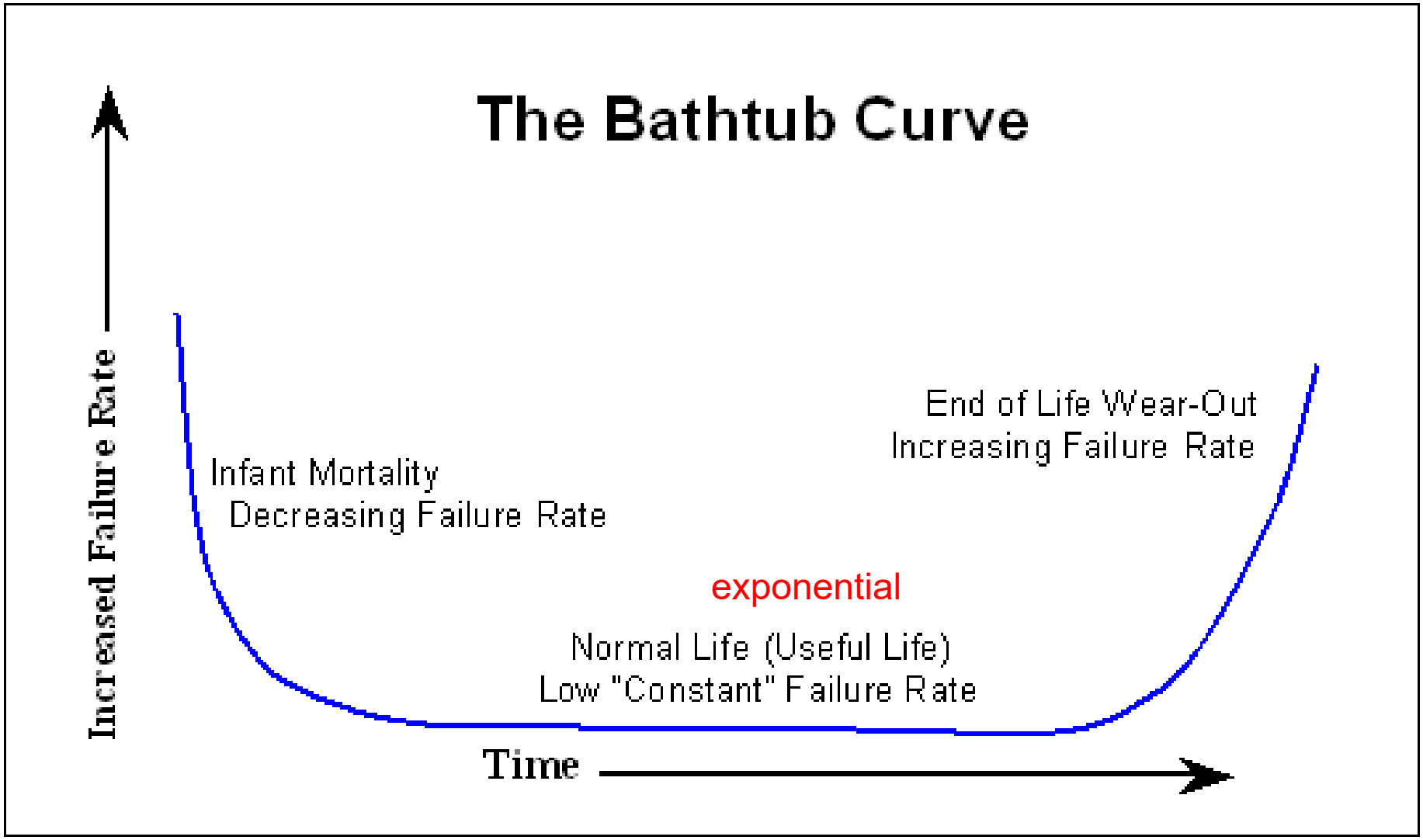
= you must remain operational

for at least t more time units

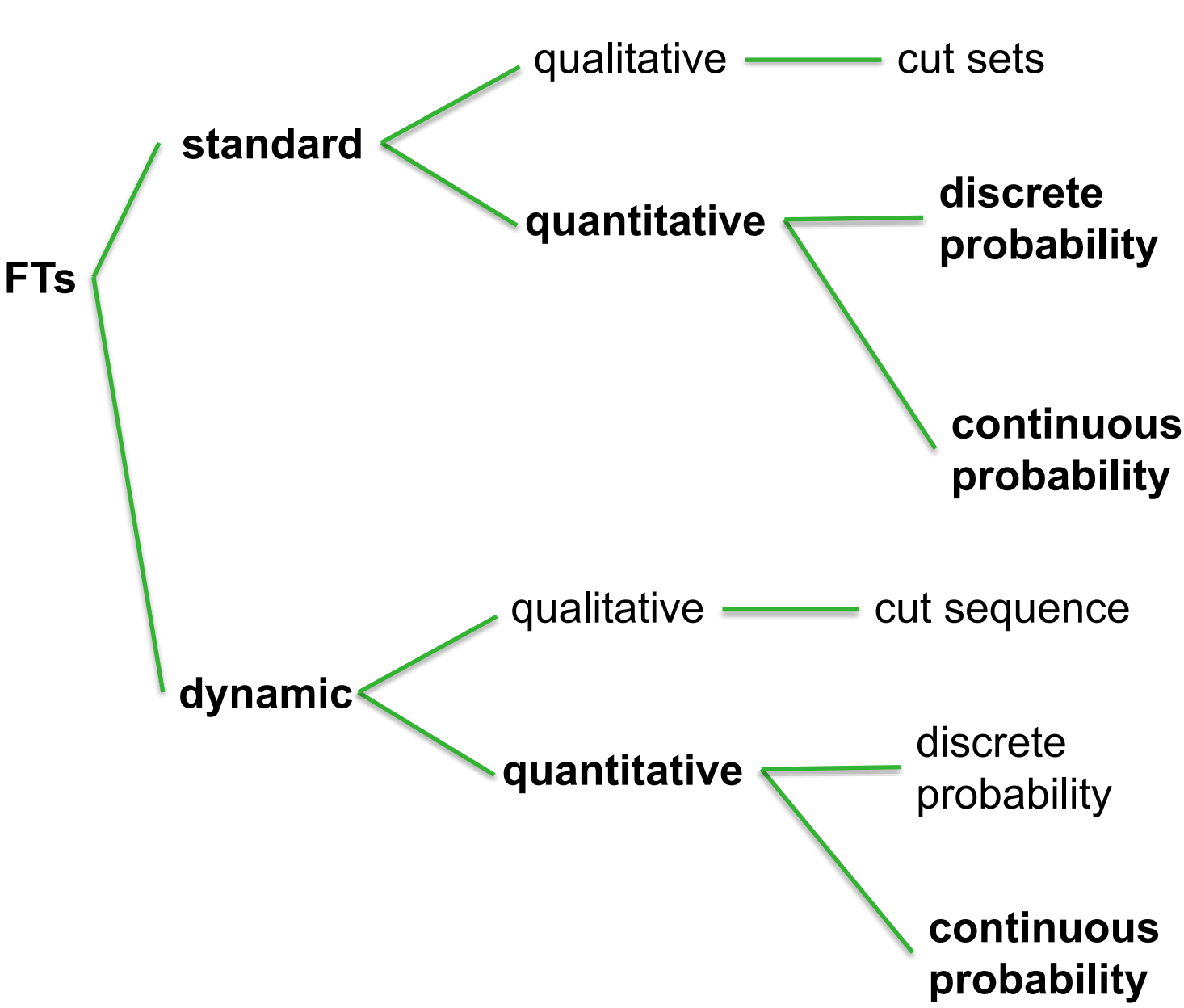
Remain operational for t more time units

Independent of s

Bath tub curve: degradation behaviour of systems



Overview

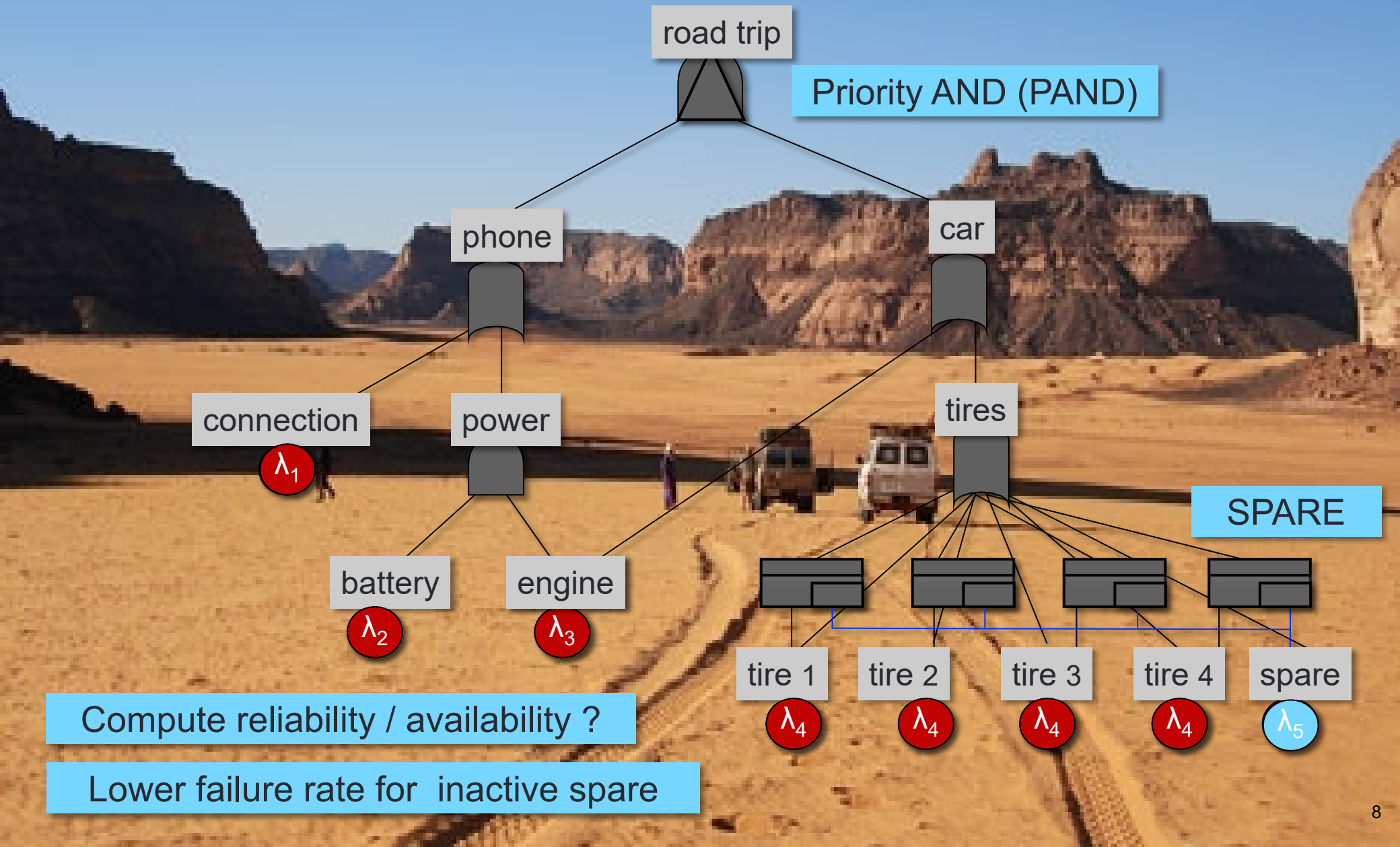


Technique
- Recursive
- BDDs

Technique
- Bottom up
- Cut sets
- BDDs

Today
- Composition
- Minimization
- Exponentials

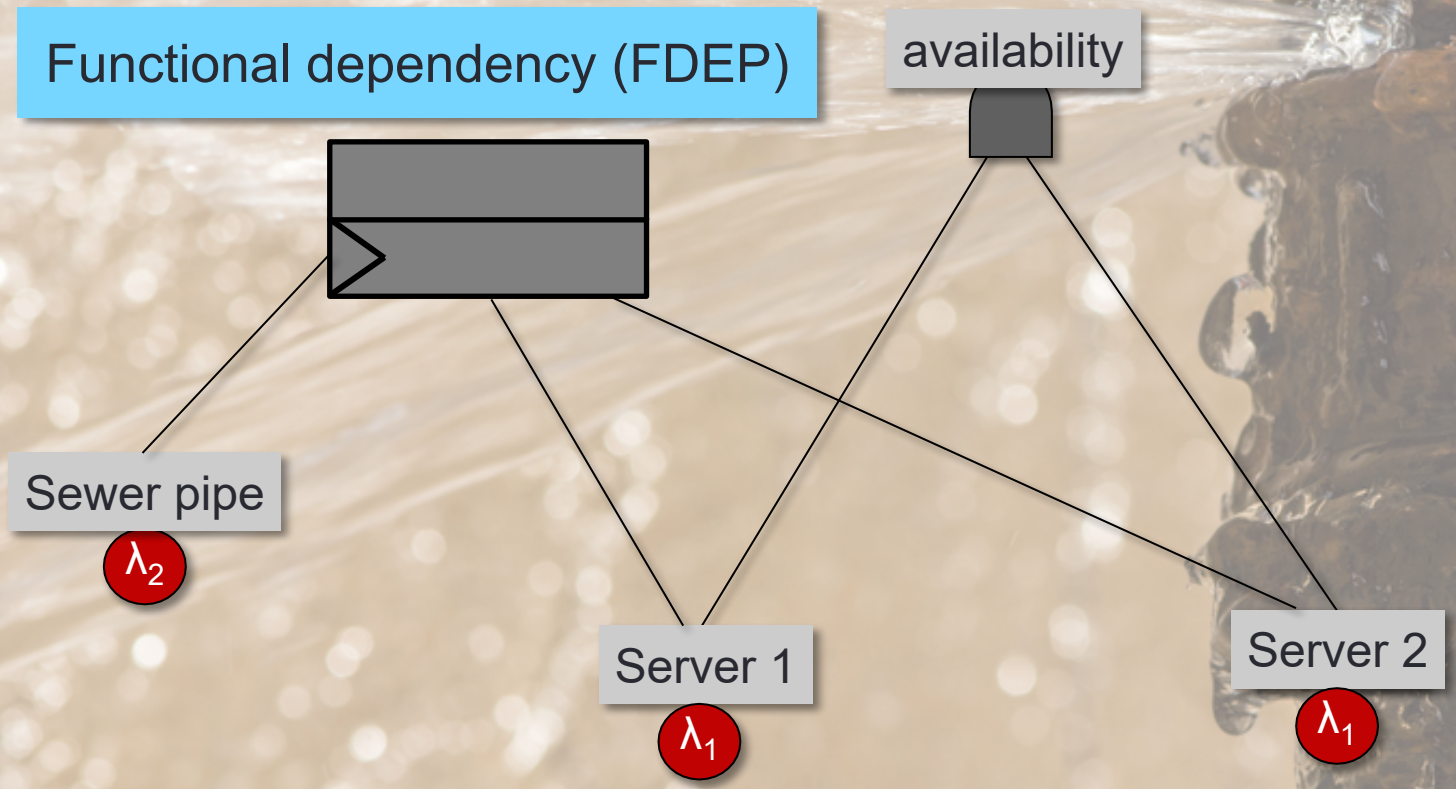
Example: Safe road trip



Compute reliability / availability ?

Lower failure rate for inactive spare

Example: server room



Dynamic Fault Tree (DFT)

Definition

- Fault tree + PAND, SPARE, FDEP gates

Qualitative analysis

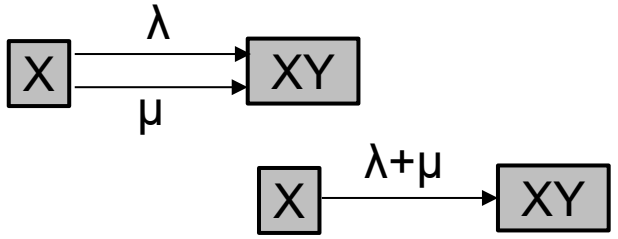
- *Cut sequence* instead of *cut set*
- (*connection, spare, tire 1*) is a cut sequence
- (*spare, tire 1, connection*) is not
- (*battery*, *engine*) might be, depending on your definition

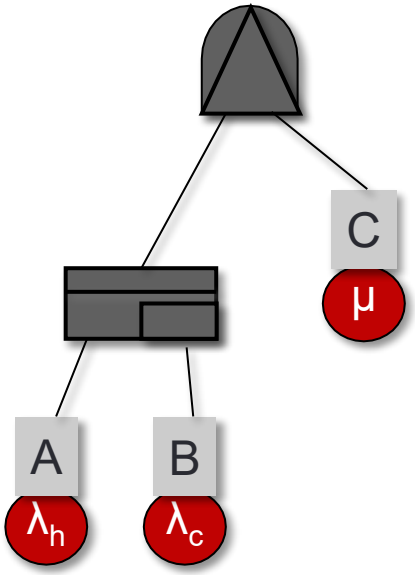
Quantitative analysis

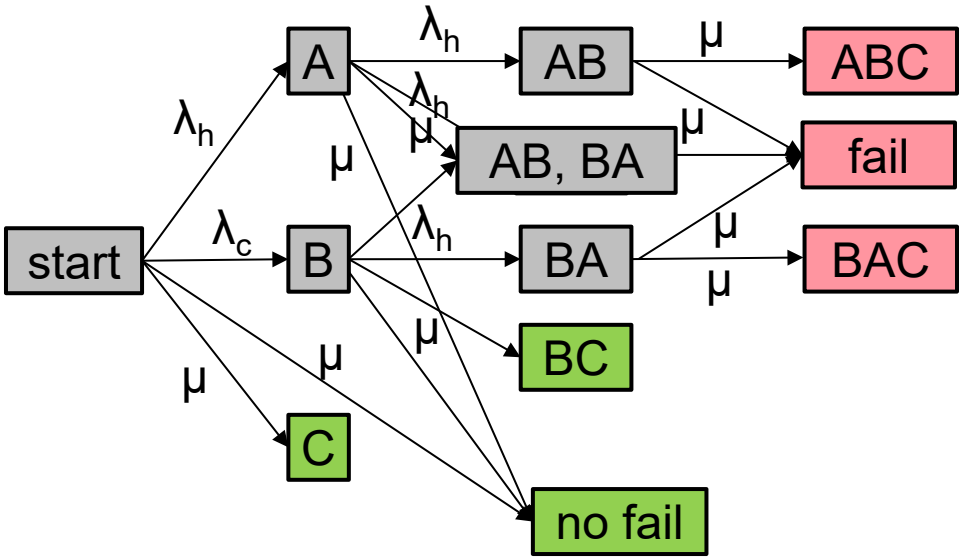
- What is U(*t*) = failure probability at time *t*?
- BDDs do not work!

Quantitative DFT analysis

1. **Create (continuous) Markov chain**
2. **Simplify**
   1. Merge fails, no fails, equivalent states
   2. Merge double edges
   3. Eliminate self-loops

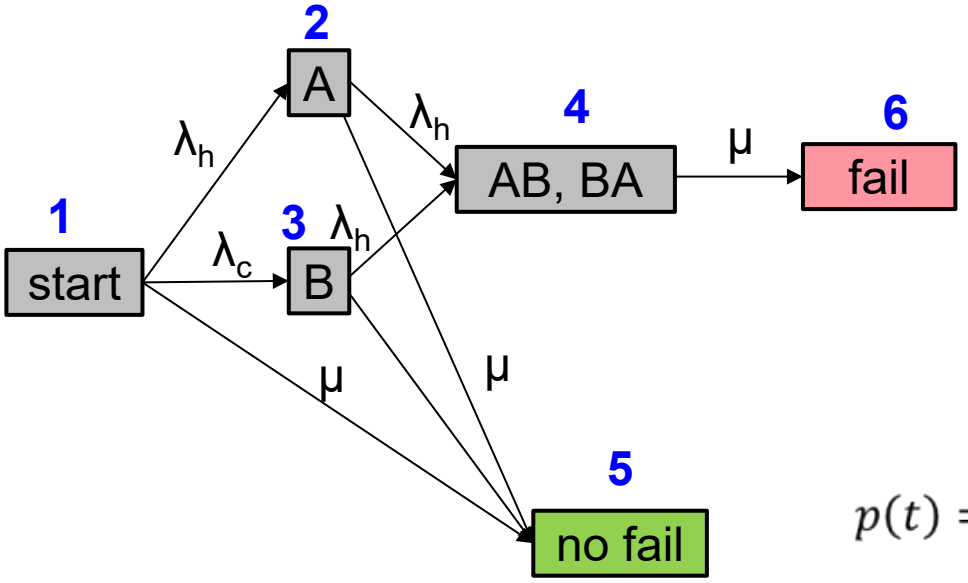


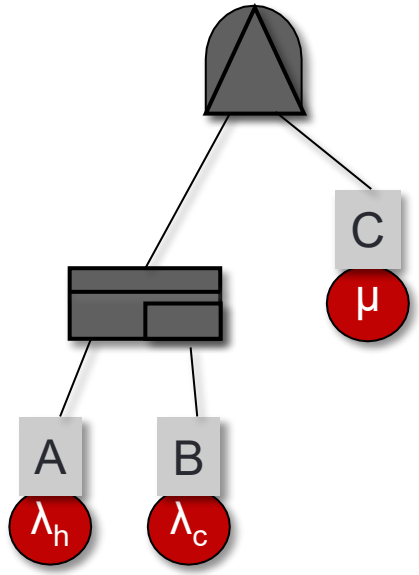




Quantitative DFT analysis

1. **Create (continuous) Markov chain**
2. **Simplify**
3. **Derive transition matrix**
4. **Compute probability vector**





$p(t)$ = probability vector of system state at time t

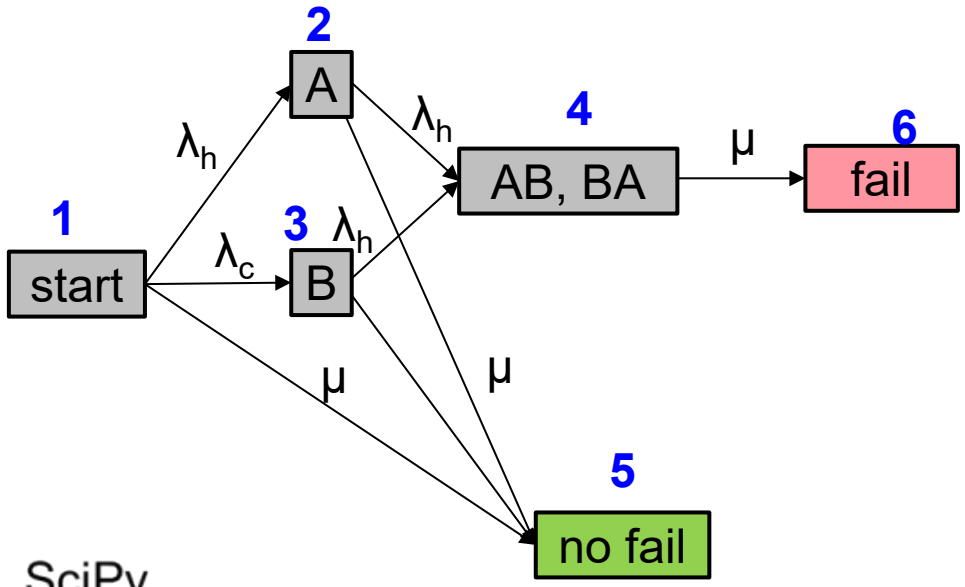
$$A = \begin{pmatrix} -\lambda_h - \lambda_c - \mu & \lambda_h & \lambda_c & 0 & \mu & 0 \\ 0 & -\lambda_h - \mu & 0 & \lambda_h & \mu & 0 \\ 0 & 0 & -\lambda_h - \mu & \lambda_h & \mu & 0 \\ 0 & 0 & 0 & -\mu & 0 & \mu \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$p(0) = (1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0)$$

$$p(t) = p(0) \cdot e^{tA}$$

Quantitative DFT analysis

1. **Create (continuous) Markov chain**
2. **Simplify**
3. **Derive transition matrix**
4. **Compute probability vector**



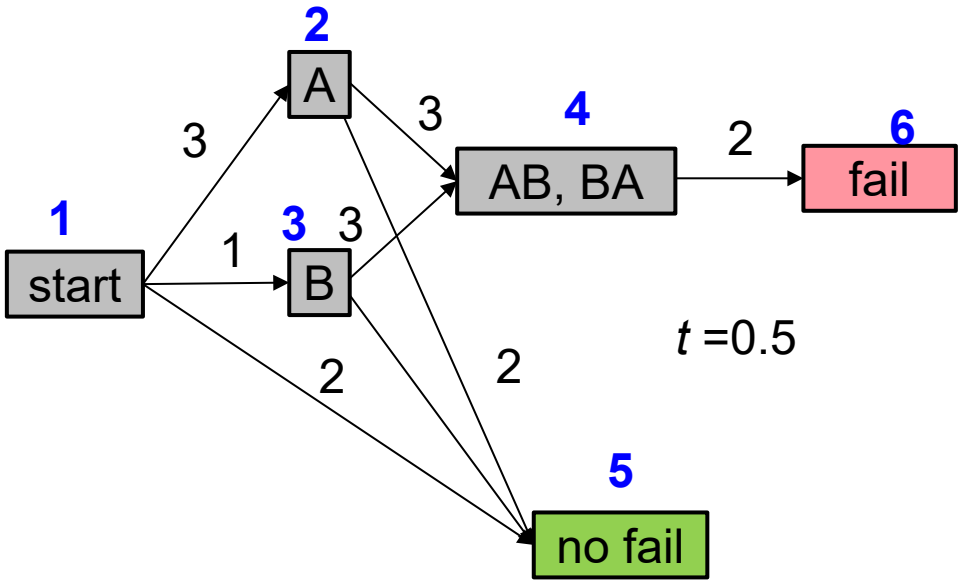
$$p(t) = p(0) \cdot \mathrm{e}^{tA}$$

$$\mathrm{e}^{X} = \sum_{k=0}^{\infty} \frac{1}{k!} X^{k}$$

- Can be computed with Wolfram alpha, SciPy,…
- Google “Matrix exponential”
- t integer: $p(t) = p(0) \cdot M^{t}$ with $M = \mathrm{e}^{A}$

Quantitative DFT analysis

1. **Create (continuous) Markov chain**
2. **Simplify**
3. **Derive transition matrix**
4. **Compute probability vector**

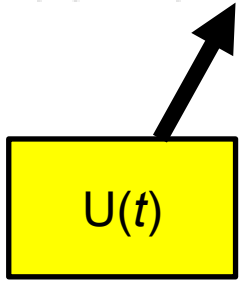


$$p(t) = p(0) \cdot e^{tA}$$

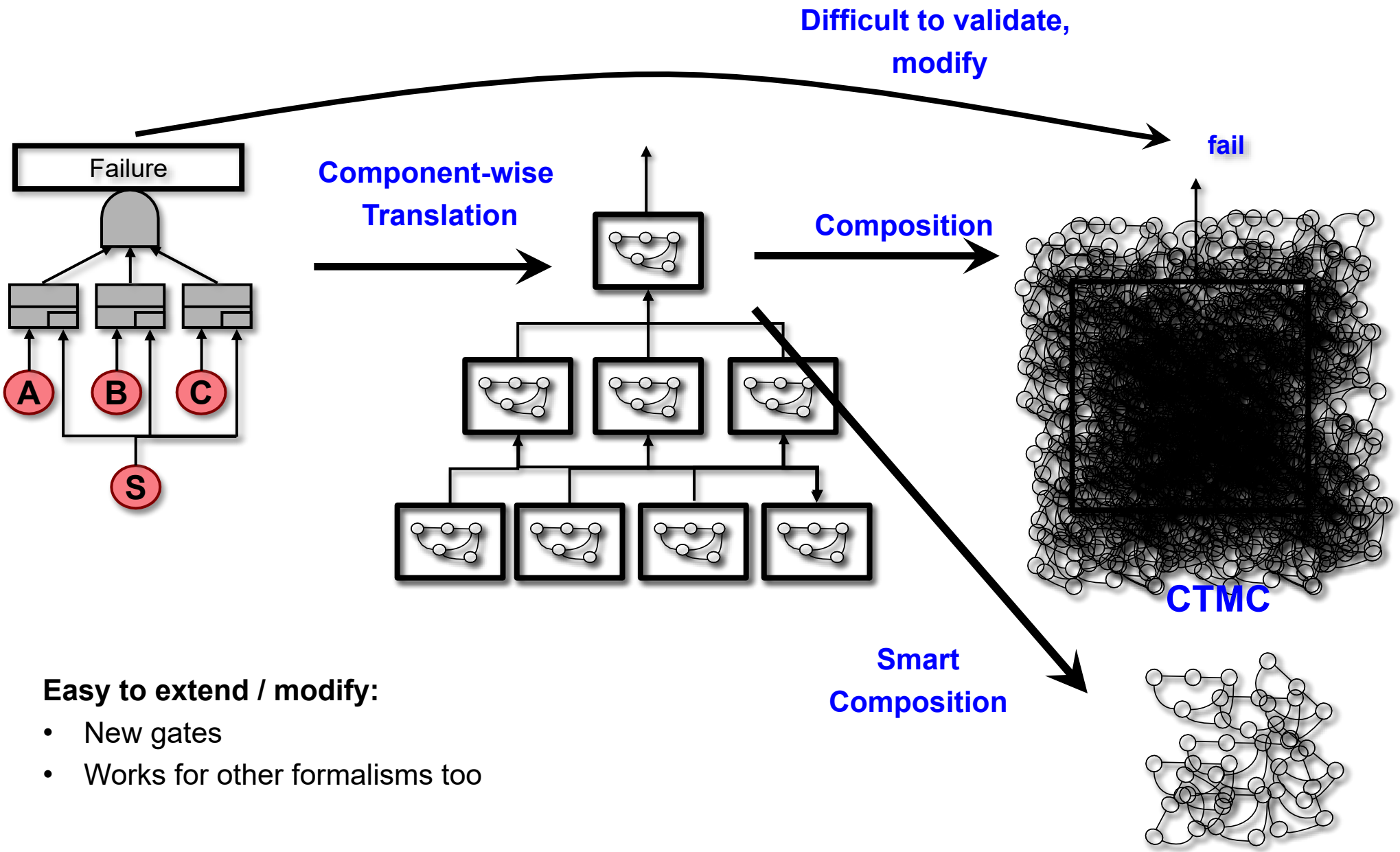
$$tA = \begin{pmatrix} -3 & 1.5 & 0.5 & 0 & 1 & 0 \\ 0 & -2.5 & 0 & 1.5 & 1 & 0 \\ 0 & 0 & -2.5 & 1.5 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$p(t) = (0.05 \quad 0.10 \quad 0.03 \quad 0.19 \quad 0.52 \quad 0.11)$$

$$\exp(tA) = \begin{pmatrix} 0.05 & 0.10 & 0.03 & 0.19 & 0.52 & 0.11 \\ 0 & 0.08 & 0 & 0.29 & 0.37 & 0.26 \\ 0 & 0 & 0.08 & 0.29 & 0.37 & 0.26 \\ 0 & 0 & 0 & 0.37 & 0 & 0.63 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$



Fault tree analysis via deep compositionality



Easy to extend / modify:

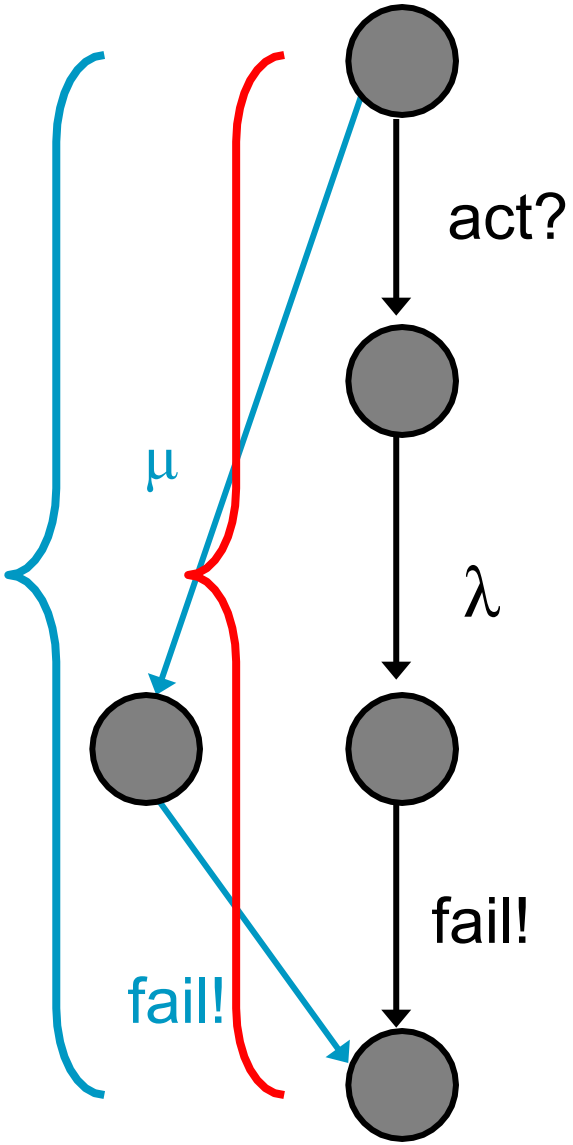
- New gates
- Works for other formalisms too

Interactive Markov Chains (I/O-IMC)

- Transition sytems + I/O + CTMC
- Markovian transitions (CTMC)
  - labeled with rates λ
  - delays governed by exponential distribution
  - **P**[transition within t sec] = $1 - e^{-\lambda t}$
- Interactive transitions (I/O)
  - labeled with actions
  - synchronization
- Action signature
  - ? - Input actions: *delayable*
  - ! - Output actions: *immediate*
  - ; - Internal actions: *immediate*

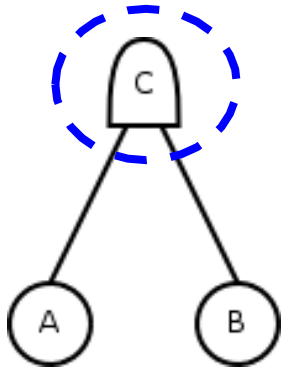
I/O-IMC for cold basic event

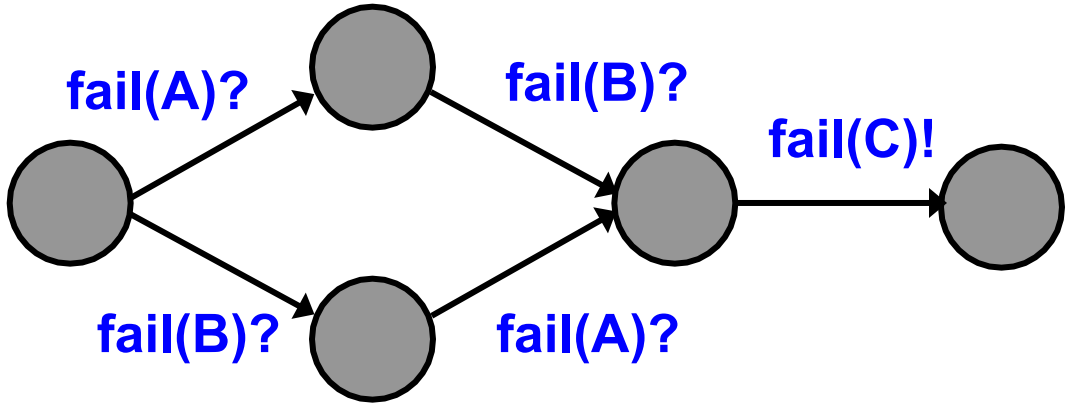
Warm BE: can fail before activation, at reduced rate



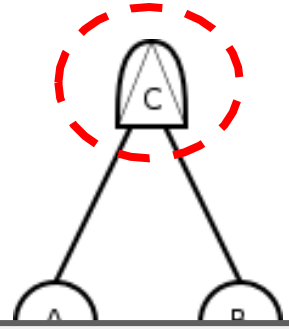
Semantics for FT gates

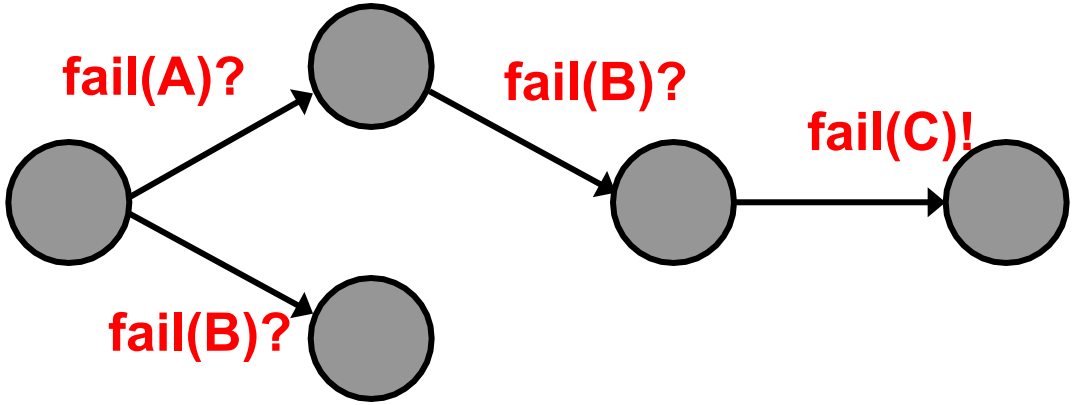
AND gate





PAND gate





Similar, but more complex for other gates

Conclusion

Dynamic fault trees

- More detailed modelling
- More complicated analysis
  - Qualitative: cut sequences
  - Quantitative: Markov Chains

Next week:

- Monday: deadline homework 3, RA group project
- Wednesday, Friday: lectures on Testing