Fault Maintenance Trees:
Combining fault trees, maintenance, and stochastic model checking

Enno Ruijters

December 7, 2015

Outline

Outline

Introduction to fault trees

- Developed in 1961 by Nuclear Regulatory Agency
- Question: How reliable is your system?
- Now used by:

Introduction to fault trees

- Developed in 1961 by Nuclear Regulatory Agency
- Question: How reliable is your system?
- Now used by:


esa
ProRail


Honeywell

Why fault trees?

- Some things really should not fail
- Risk assessment is sometimes mandatory

What to we want to know?

Quantitative:

- **Reliability** $\equiv$ Probability of failure within time t
  Example: Probability of containment failure within 25 year nuclear plant lifetime

What to we want to know?

Quantitative:

- **Reliability** $\equiv$ Probability of failure within time t
  Example: Probability of containment failure within 25 year nuclear plant lifetime
- **Availability** $\equiv$ Proportion of time (in $[0, \infty\rangle$ or $[0, t]$) spent not failed
  Example: Amazon EC2 cloud offers SLA of 99.95% uptime

What to we want to know?

Quantitative:

- **Reliability** $\equiv$ Probability of failure within time t
  Example: Probability of containment failure within 25 year nuclear plant lifetime
- **Availability** $\equiv$ Proportion of time (in $[0, \infty\rangle$ or $[0, t]$) spent not failed
  Example: Amazon EC2 cloud offers SLA of 99.95% uptime
- **Expected nr. of failures** $\equiv$ Expected number of times a failure occurs within some timeframe
  Example: How frequently will my car break down?

What to we want to know?

Quantitative:

- **Reliability** $\equiv$ Probability of failure within time t
  Example: Probability of containment failure within 25 year nuclear plant lifetime
- **Availability** $\equiv$ Proportion of time (in $[0, \infty\rangle$ or $[0, t]$) spent not failed
  Example: Amazon EC2 cloud offers SLA of 99.95% uptime
- **Expected nr. of failures** $\equiv$ Expected number of times a failure occurs within some timeframe
  Example: How frequently will my car break down?
- **Costs** of failures and repairs
- Others (MTBF, etc.)

Outline

Fault trees

- Describe combinations of faults leading to failures
- Root of tree: Top Event; i.e. system failure
- Leaves: Basic Events; i.e. elementary failures and faults
- Nodes: Gates; describe how faults combine

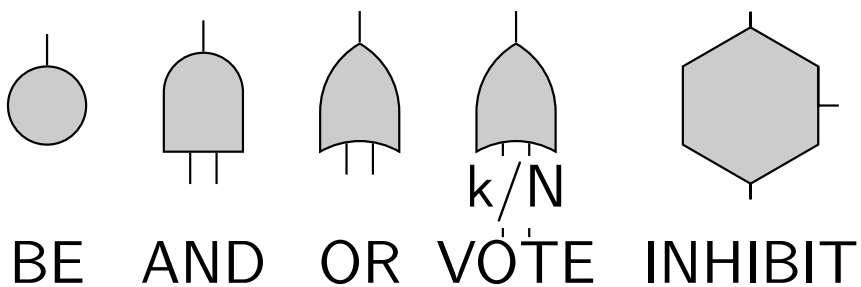
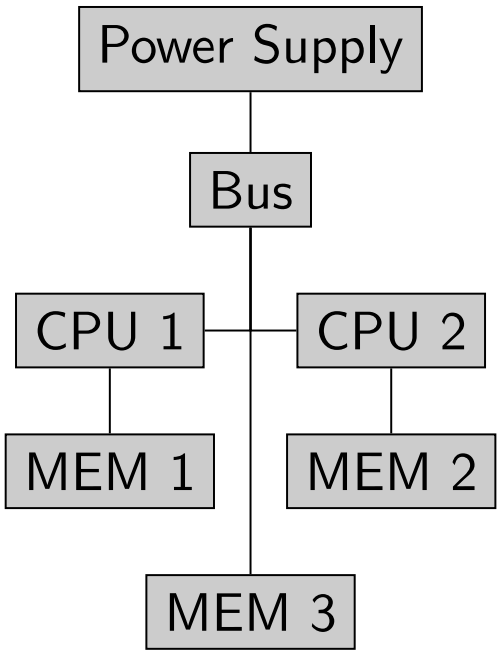
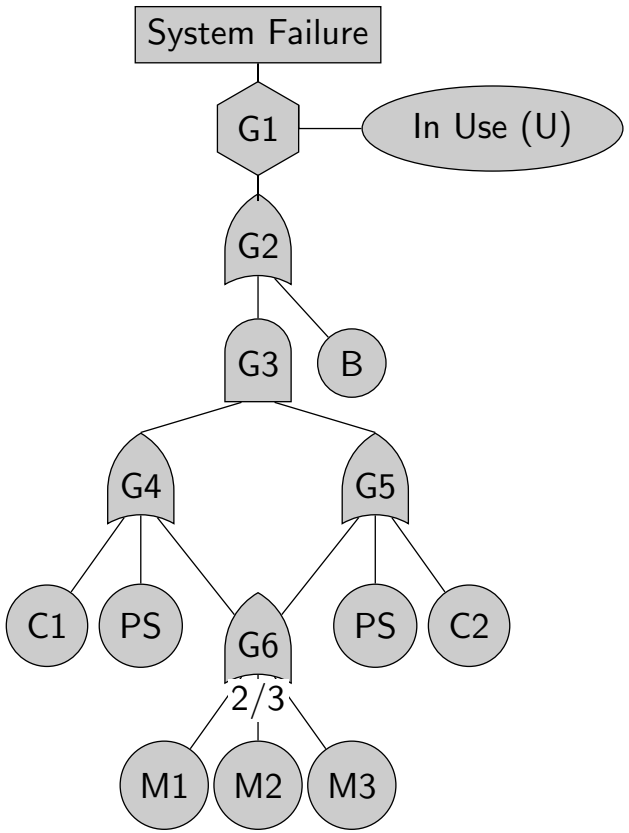


Figure: Images of the elements in a standard fault tree

Fault tree example

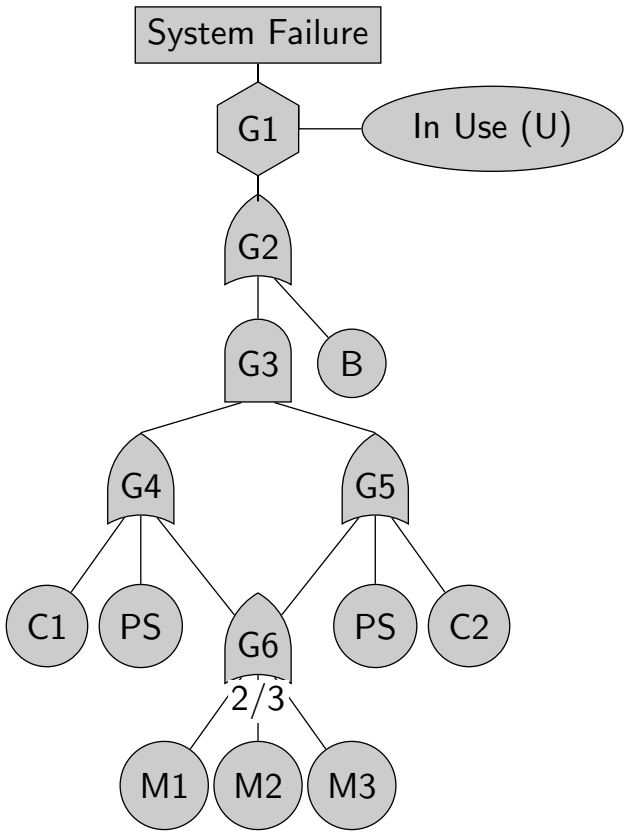




- Redundant CPUs
- 1 shared spare memory unit

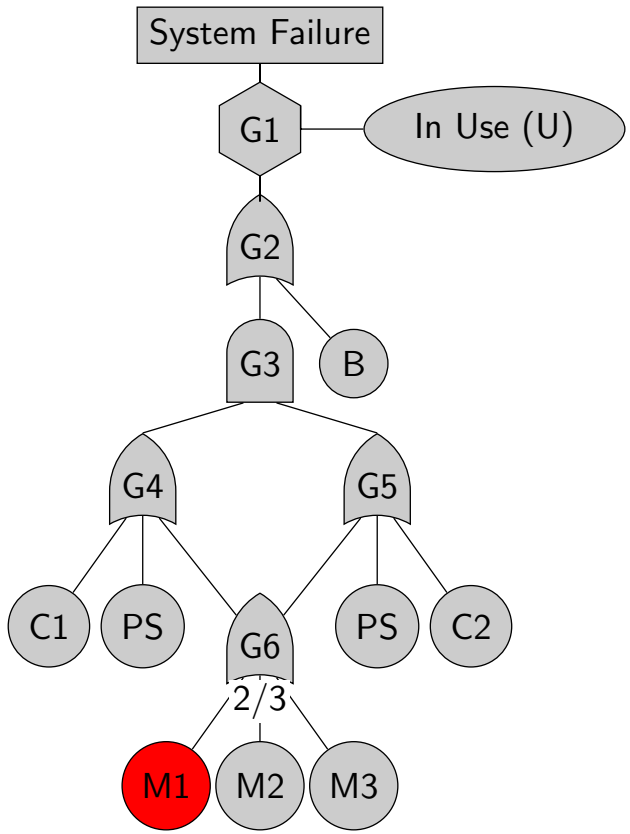
Example of fault tree failure propagation

- No failures



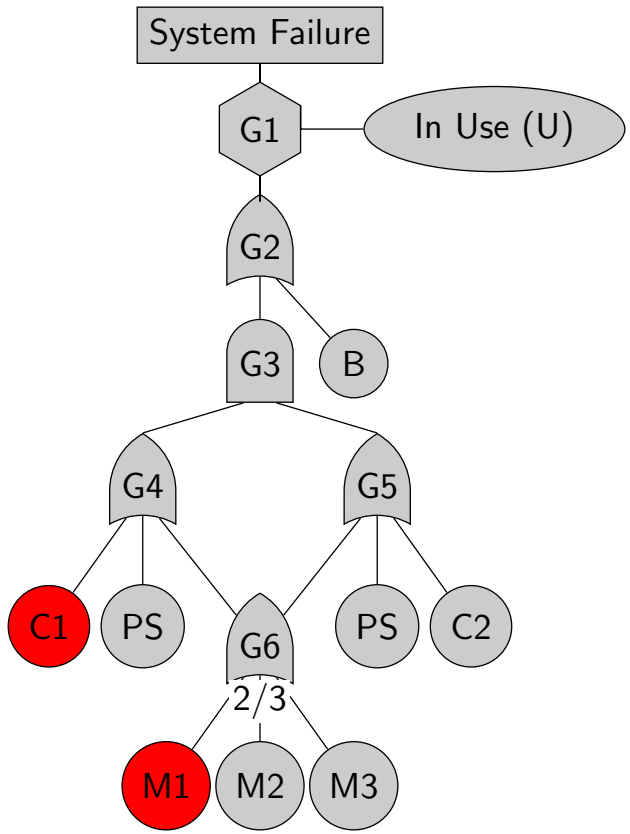
Example of fault tree failure propagation

- Failure of M1



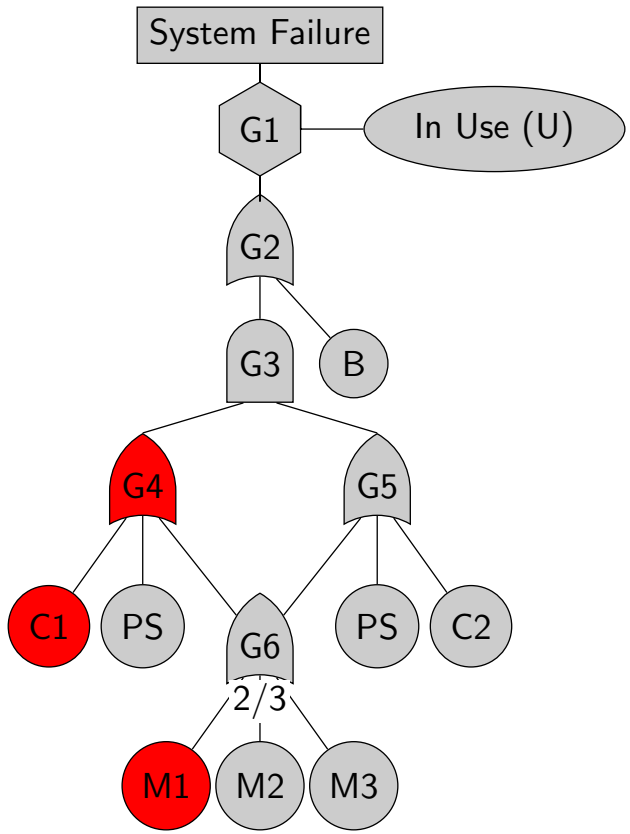
Example of fault tree failure propagation

- Failure of M1
- Failure of C1



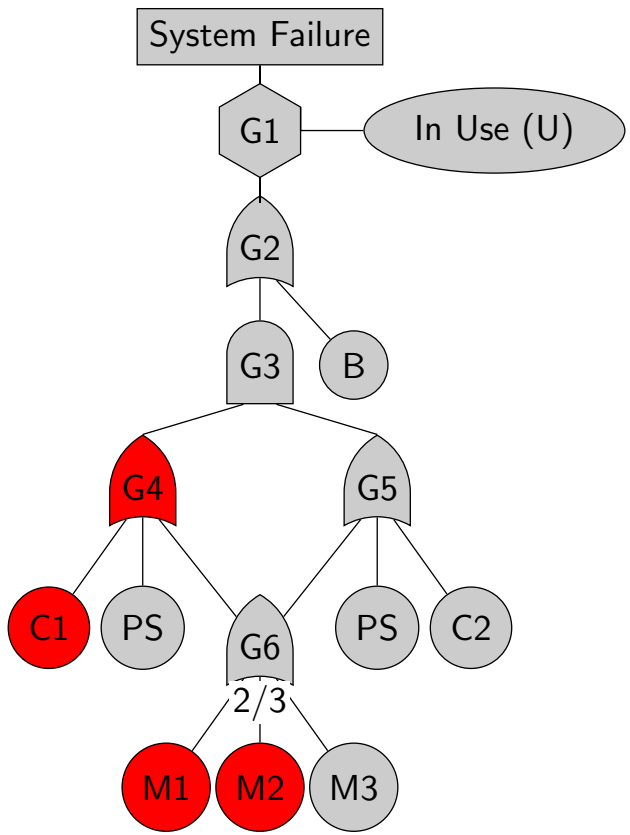
Example of fault tree failure propagation

- Failure of M1
- Failure of C1



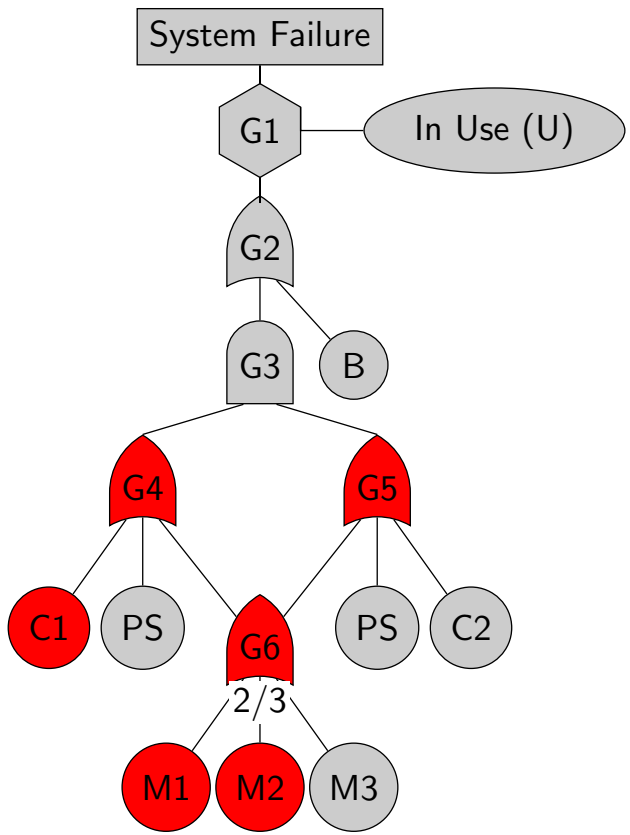
Example of fault tree failure propagation

- Failure of M1
- Failure of C1
- Failure of M2



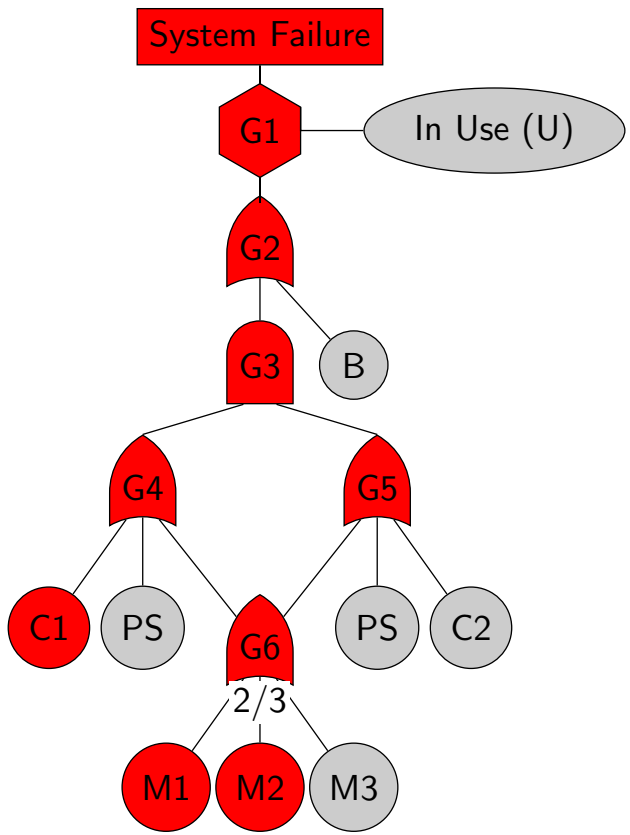
Example of fault tree failure propagation

- Failure of M1
- Failure of C1
- Failure of M2



Example of fault tree failure propagation

- Failure of M1
- Failure of C1
- Failure of M2



Fault tree analysis

Given leaf failure rates, we can perform analysis

- Obtain reliability, availability, etc.

Limitations:

- External variables (e.g. temperature)
- Use measures (e.g. total time / duration of use)
- Assumption: Failure rates are fixed

FT extensions

Extensions have been developed to model:

- Uncertainty
- Dependent events
- Repairs and repair policies
- Timing requirements
- State machines (e.g. software)
- Our current work: Maintenance

Outline

Importance of maintenance

Types of maintenance

By timing:

- Preventive maintenance
  - Periodic repair/replacement
  - Inspection
- Corrective maintenance

By result:

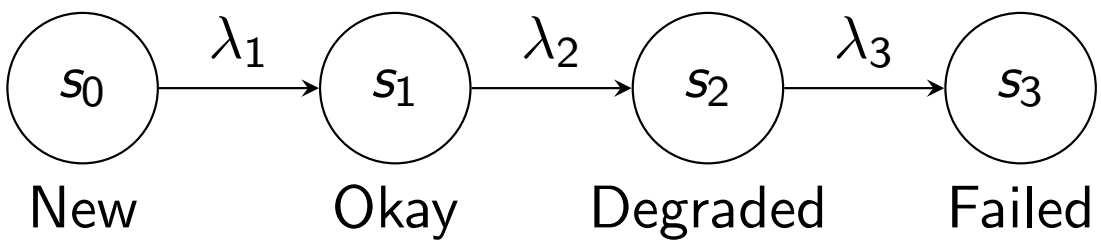
- 'As good as new' replacement
  - example: Replace battery
- Reduced failure rate
  - example: Oil change

Maintenance strategy

- What maintenance actions to do on which components?
- When to perform preventive maintenance?
  - Type of schedule (clock based, etc.)
  - Frequency
- How to react to failures?

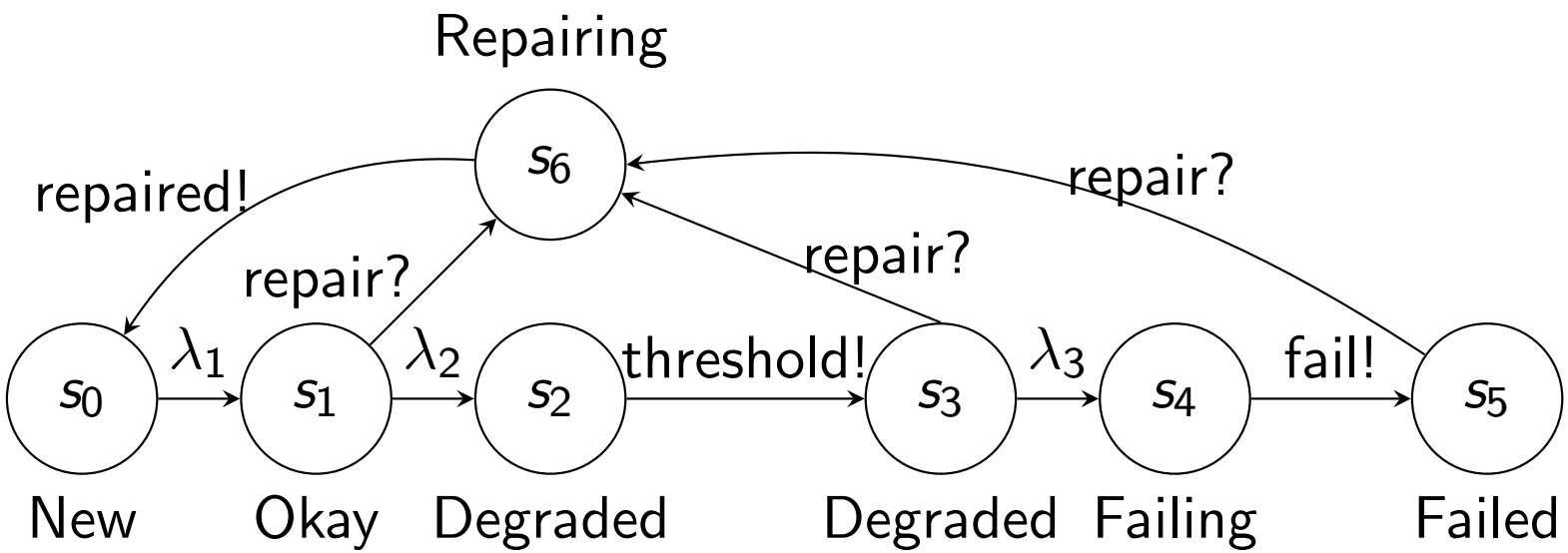
Modelling maintenance

- BEs have multiple states
  - Fully functional
  - Degraded
  - Failed
- Model non-exponential distributions
- Inspections respond to different states
- Example:



Modelling BEs

- Signals for composition:
  - Maintenance threshold
  - Repair
  - Failure
- Other models will send/receive these signals



Modelling RDEPs

- Some failure accelerate wear of other components.
- Failure of trigger BE accelerates degradation.
- Rates increase by factor γ.
- Repair of trigger BE does not repair triggered BE.

Modelling inspections and repairs

Repair module:

- Periodically start repairs (optional)
- Inspection may trigger repairs early

Inspection module:

- Periodically perform inspection
- If threshold reached: Start repair
- Otherwise: Do nothing

Maintenance analysis

- Currently using simulation (Uppaal-smc)
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions
- Disadvantages:
  - Inexact results
  - Speed
- Future: Input/Output Markov Reward Automata

Outline

EI-Joint

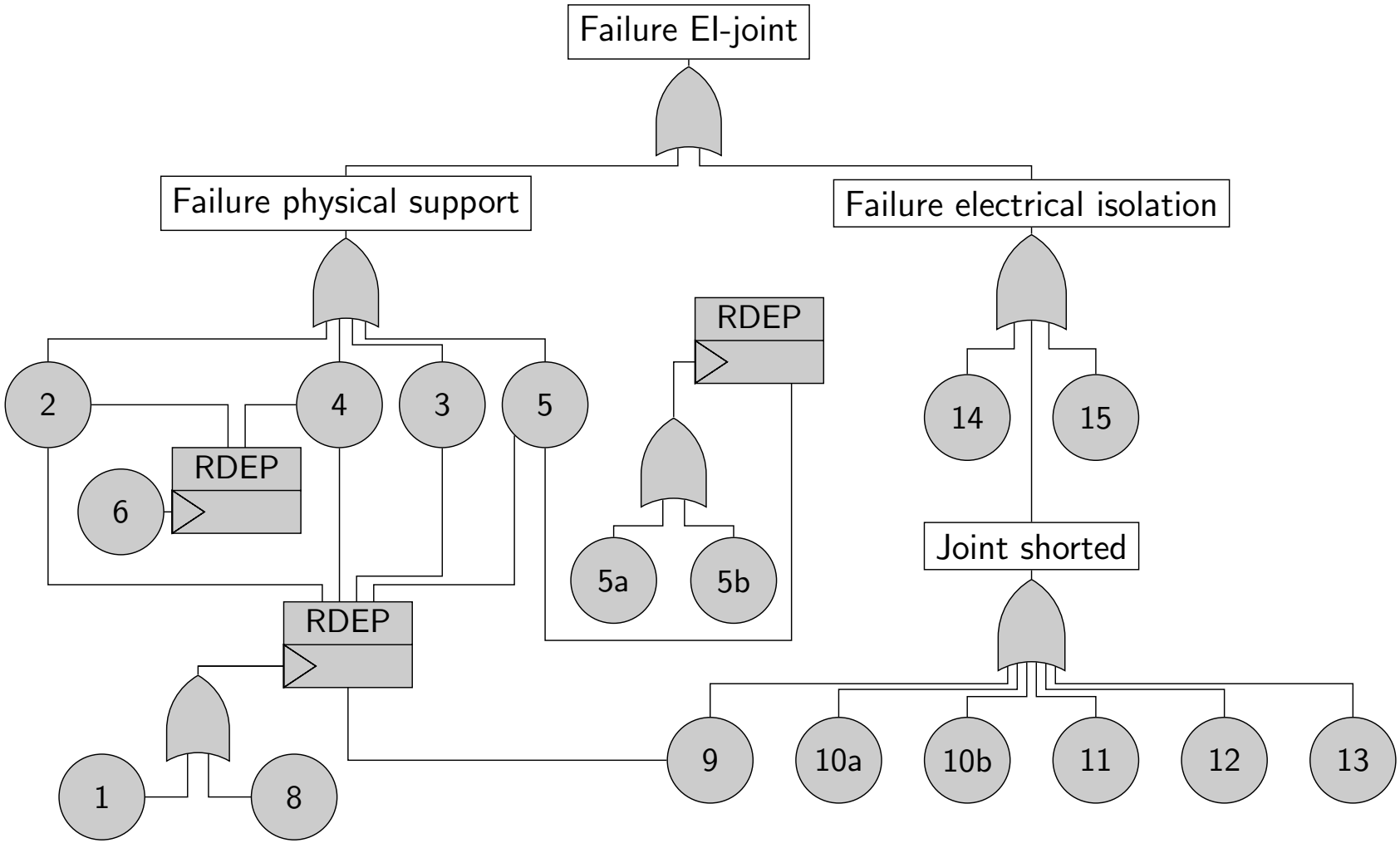
Case study: Railway component

- Data obtained from ProRail experts
- Maintenance: Periodic inspections, repairs
- Costs for inspections, repairs, and failures

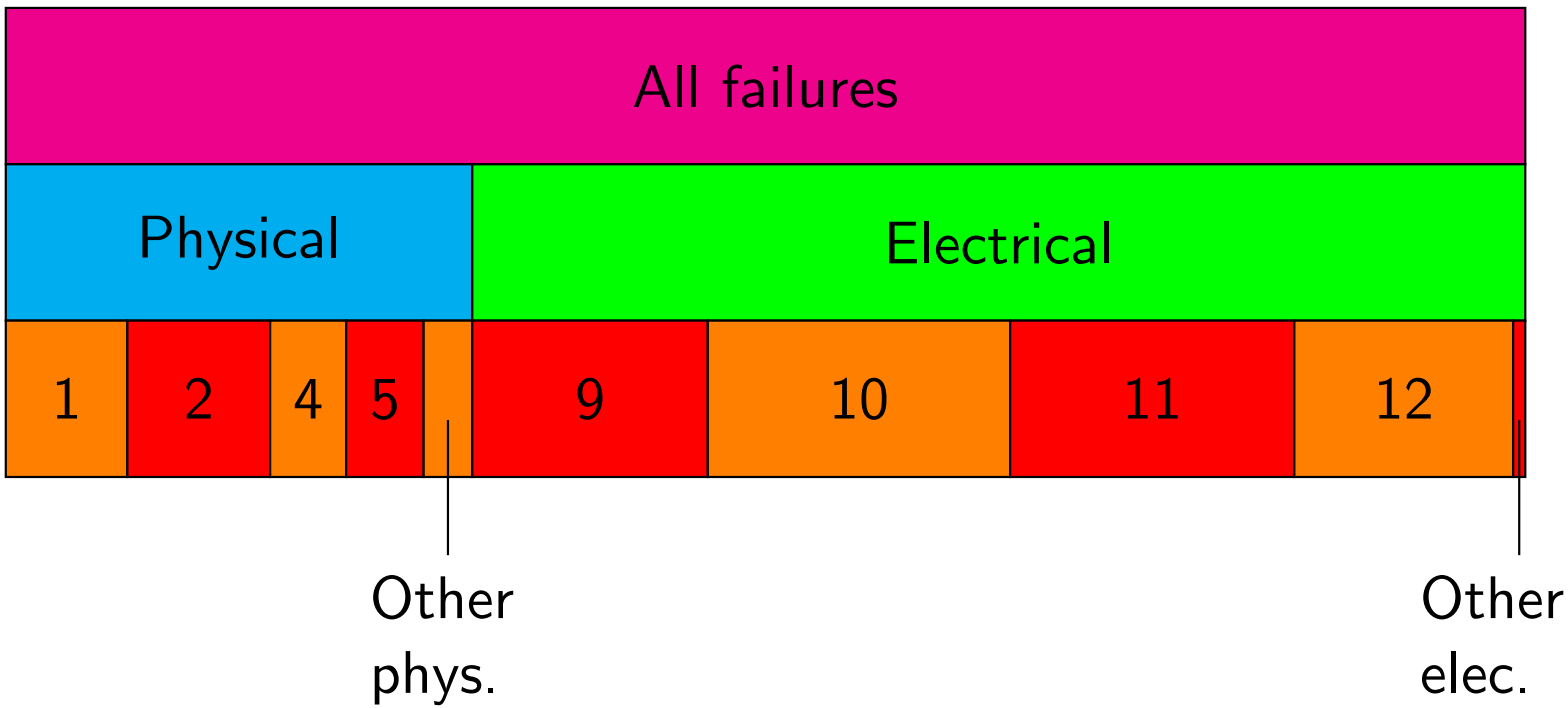
Complication: Dependent failure rates

- Some faults accelerate other failures.
- Solution: RDEP (rate-dependency) gate

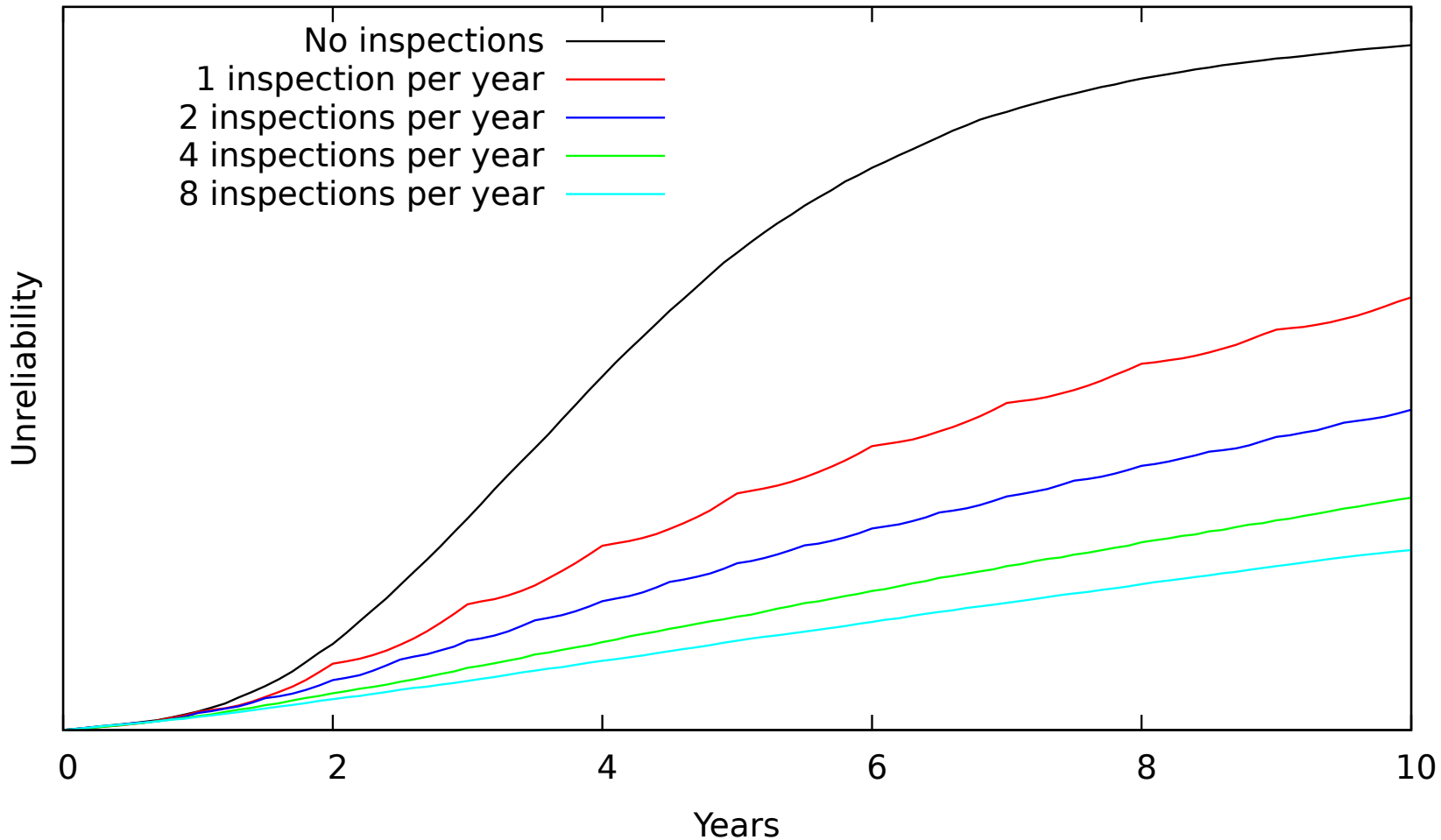
Case study


Failure El-joint
Failure physical support
Failure electrical isolation
2
4
3
5
RDEP
6
RDEP
5a
5b
RDEP
14
15
Joint shorted
1
8
9
10a
10b
11
12
13

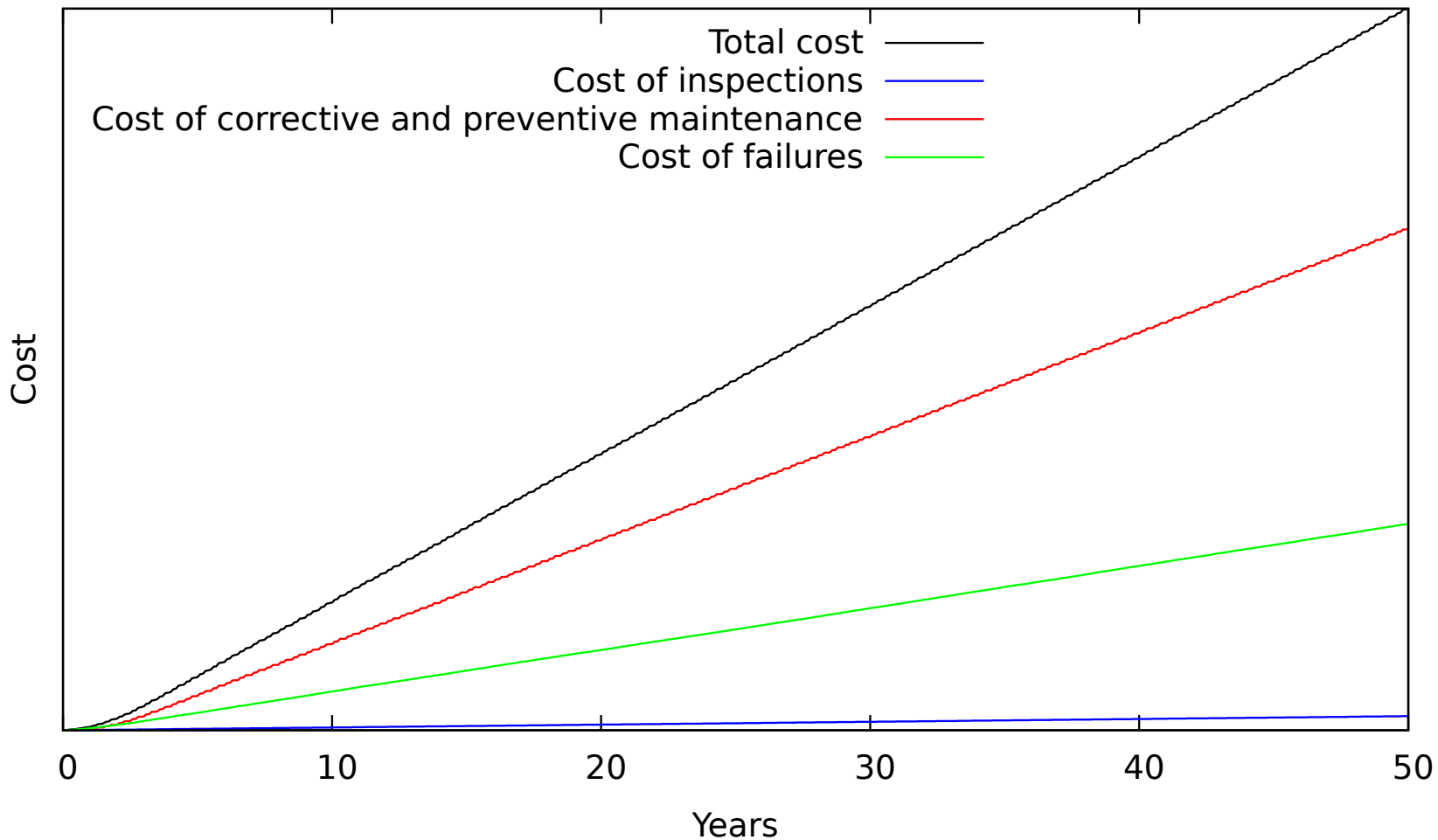
Analysis results: failure causes



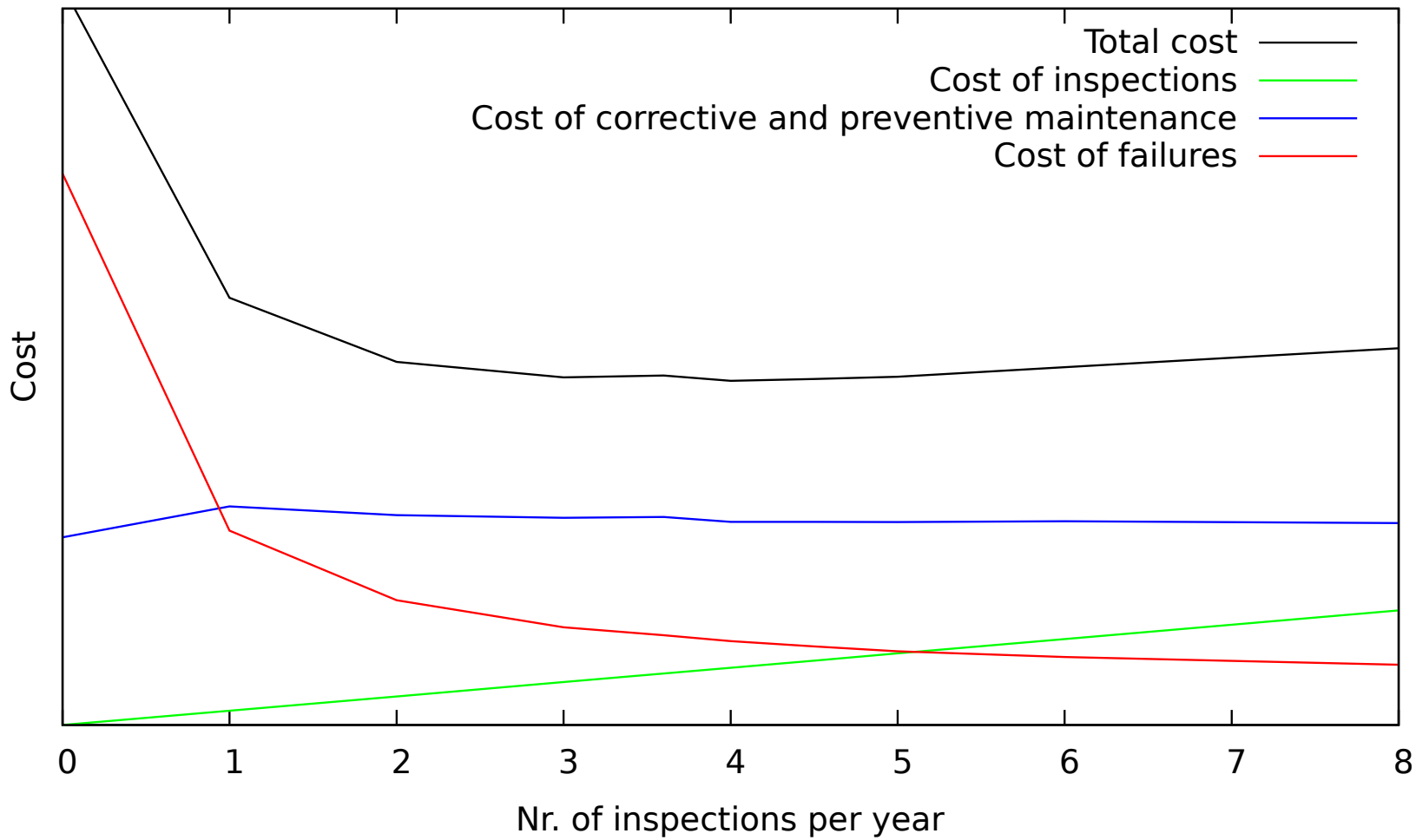
Analysis results: unreliability



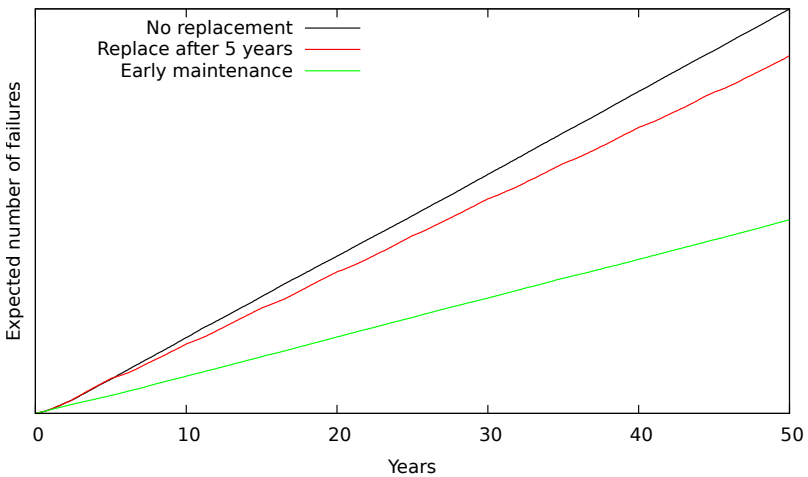
Analysis results: costs

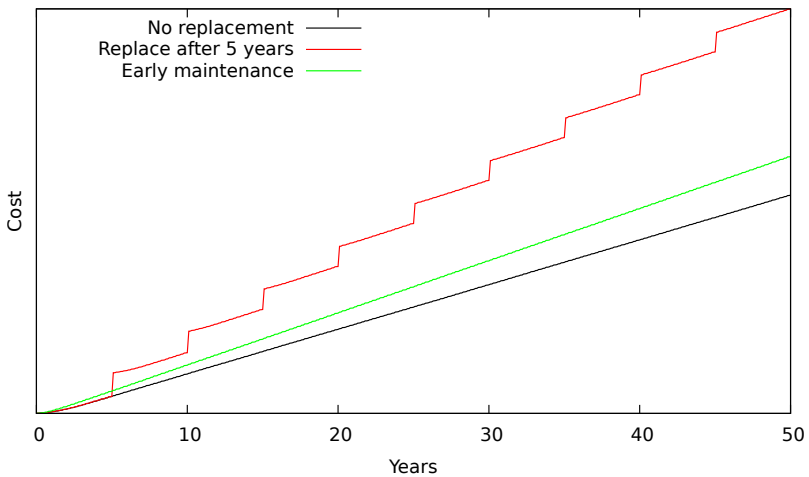


Analysis results: inspection rate



Analysis results: other strategies





Conclusions on EI-joints

- Cost-optimal inspection frequency around 4 times per year.
- Cost approximately flat from 2 to 6 inspection per year.
- More failures can be prevented, but not cost-effectively.

Outline

Conclusions

- Our method integrates maintenance in fault trees.
- We can compute quantitative metrics to compare maintenance strategies.
- We demonstrated our method on an industrial case study.