Reliability-centered maintenance via fault tree analysis:
Combining fault trees, maintenance, and statistical model checking

Enno Ruijters, Dennis Guck, Mariëlle Stoelinga, Peter Drolenga, Martijn van Noort

8 March 2017

Outline

Why reliability analysis?

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

Importance of maintenance

- Even very reliable systems need maintenance

Types of maintenance

By timing:

- Preventive maintenance
  - Periodic repair/replacement
  - Inspection

Types of maintenance

By timing:

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

Types of maintenance

By timing:

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

By result:

- 'As good as new' replacement
  - example: Replace battery

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?
  - What to look for in inspections

Maintenance strategy

- What maintenance actions to do on which components?
  - What to look for in inspections
  - What actions to take (repair/replace)

Maintenance strategy

- What maintenance actions to do on which components?
  - What to look for in inspections
  - What actions to take (repair/replace)
- When to perform preventive maintenance?
  - Time-based, use-based, etc.

Maintenance strategy

- What maintenance actions to do on which components?
  - What to look for in inspections
  - What actions to take (repair/replace)
- When to perform preventive maintenance?
  - Time-based, use-based, etc.
  - Frequency of maintenance actions

Maintenance strategy

- What maintenance actions to do on which components?
  - What to look for in inspections
  - What actions to take (repair/replace)
- When to perform preventive maintenance?
  - Time-based, use-based, etc.
  - Frequency of maintenance actions
- How to react to failures?

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

Introduction to fault trees

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

Introduction to fault trees

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

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

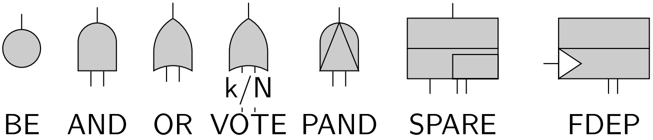
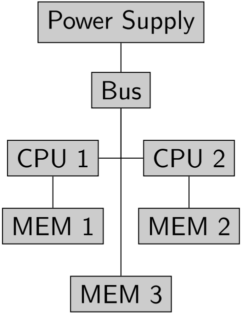
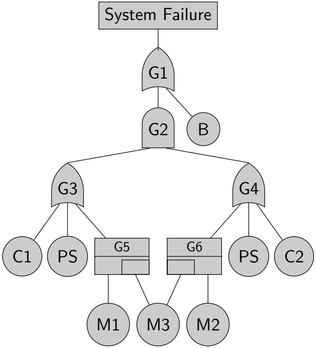


Figure: Images of the elements in a dynamic fault tree

Fault tree example

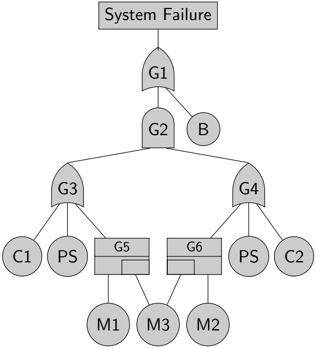




- Redundant CPUs
- 1 shared spare memory unit

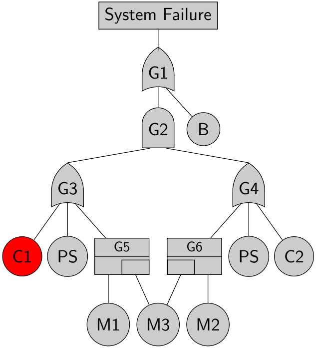
Example of fault tree failure propagation

- No failures



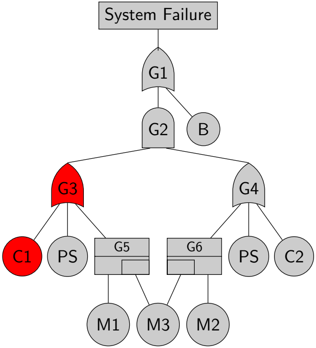
Example of fault tree failure propagation

- Failure of C1



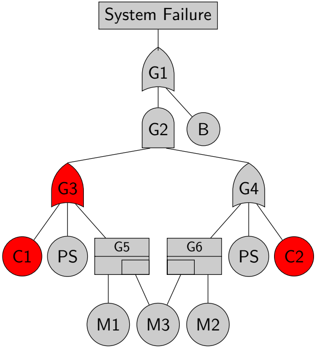
Example of fault tree failure propagation

- Failure of C1



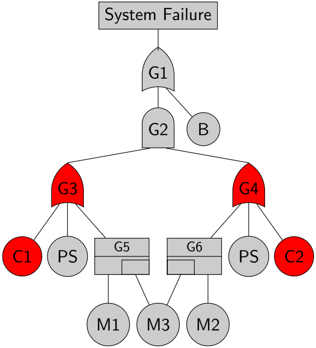
Example of fault tree failure propagation

- Failure of C1
- Failure of C2



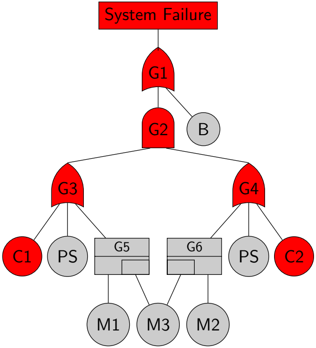
Example of fault tree failure propagation

- Failure of C1
- Failure of C2



Example of fault tree failure propagation

- Failure of C1
- Failure of C2



Fault tree analysis

Given leaf failure rates, we can perform analysis

- Obtain reliability, availability, etc.

Fault tree analysis

Given leaf failure rates, we can perform analysis

- Obtain reliability, availability, etc.

Limitations:

- External variables (e.g. temperature)

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)

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

Modelling maintenance

- BEs are timed automata with multiple states
  - Fully functional
  - Degraded
  - Failed

Modelling maintenance

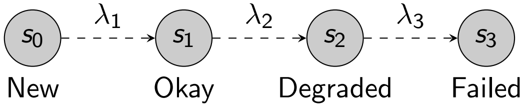
- BEs are timed automata with multiple states
    - Fully functional
    - Degraded
    - Failed
- Model non-exponential distributions

Modelling maintenance

- BEs are timed automata with multiple states
  - Fully functional
  - Degraded
  - Failed
- Model non-exponential distributions
- Inspections respond to different states

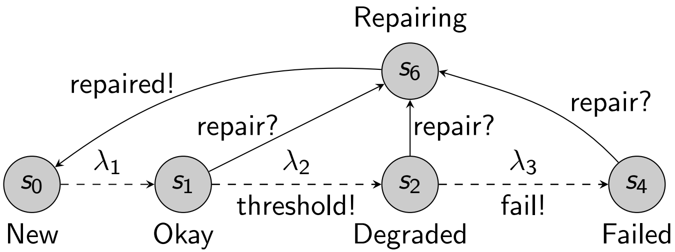
Modelling maintenance

- BEs are timed automata with 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



Rate-affecting failures

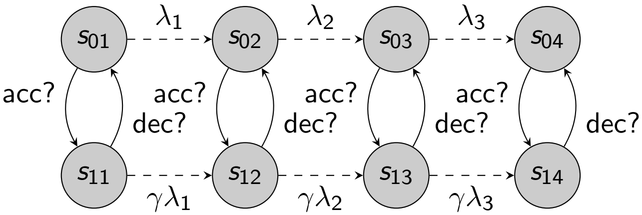
- Some failures accelerate wear of other components.

Rate-affecting failures

- Some failures accelerate wear of other components.
- New type of gate: rate dependency (RDEP).
- Failure of trigger BE accelerates degradation.
- Rates increase by factor γ.

Rate-affecting failures

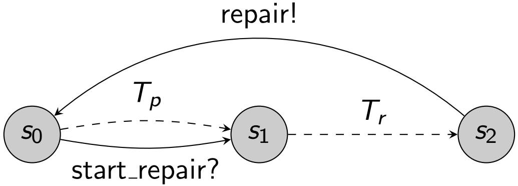
- Some failures accelerate wear of other components.
- New type of gate: rate dependency (RDEP).
- Failure of trigger BE accelerates degradation.
- Rates increase by factor γ.
- Repair of trigger BE does not repair triggered BE.



Modelling inspections and repairs

Repair module:

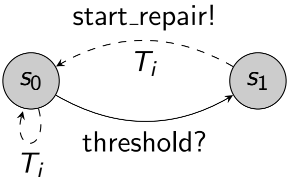
- Periodically start repairs (optional)
- Inspection may trigger repairs early



Modelling inspections and repairs

Inspection module:

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



Maintenance analysis

- Currently using statistical model checking (Uppaal-smc)
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions

Maintenance analysis

- Currently using statistical model checking (Uppaal-smc)
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions
- Disadvantages:
  - Inexact results
  - Speed

Maintenance analysis

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

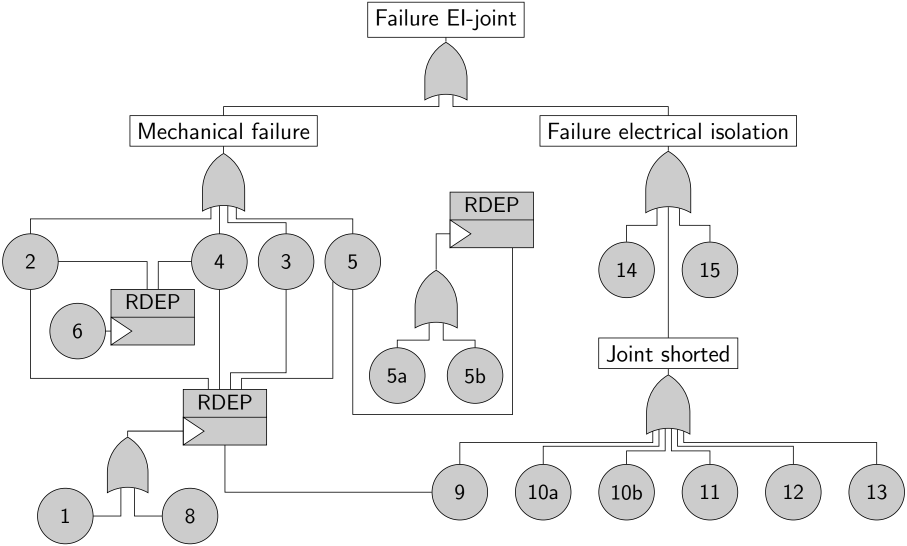
Outline

Case study: Electrically insulated joint

Case study: Electrically insulated joint

- Collaboration with ProRail (Dutch railway asset management company).
- Electrically separates section of track.
- Important cause of train service disruptions.
- **Result:** Cost-optimal maintenance strategy.

Case study

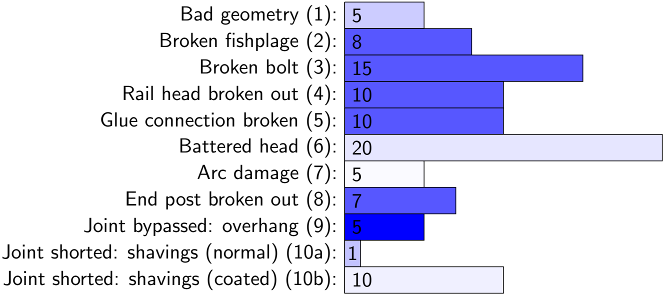


Failure El-joint
Mechanical failure
Failure electrical isolation
2
4
3
5
RDEP
6
RDEP
5a
5b
14
15
Joint shorted
RDEP
1
8
9
10a
10b
11
12
13

Failure modes EI-joint

ETTF degrading BEs:

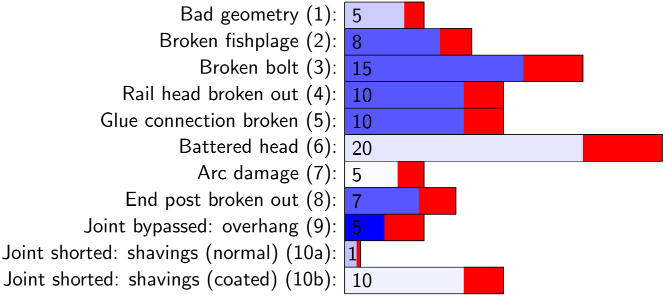
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



Failure modes EI-joint

ETTF degrading BEs:

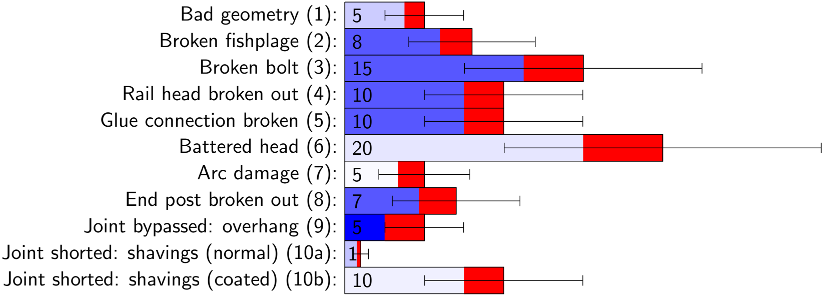
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



Failure modes EI-joint

ETTF degrading BEs:

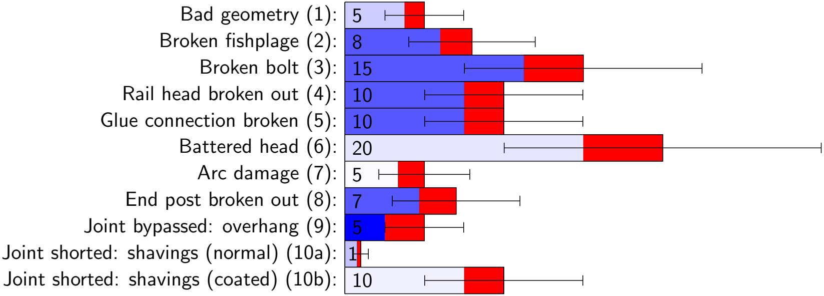
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



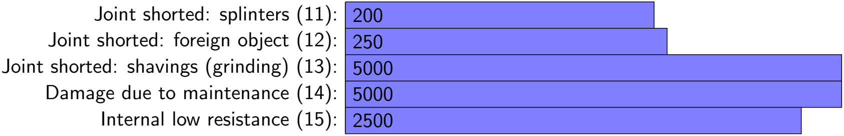
Failure modes EI-joint

ETTF degrading BEs:

Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



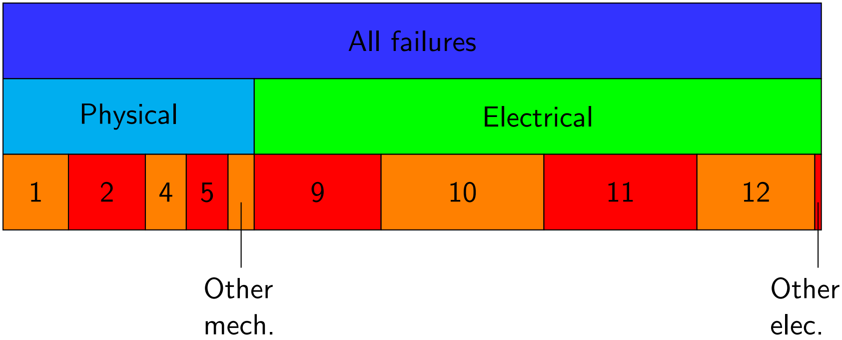
ETTF exponential failures (logarithmic scale):



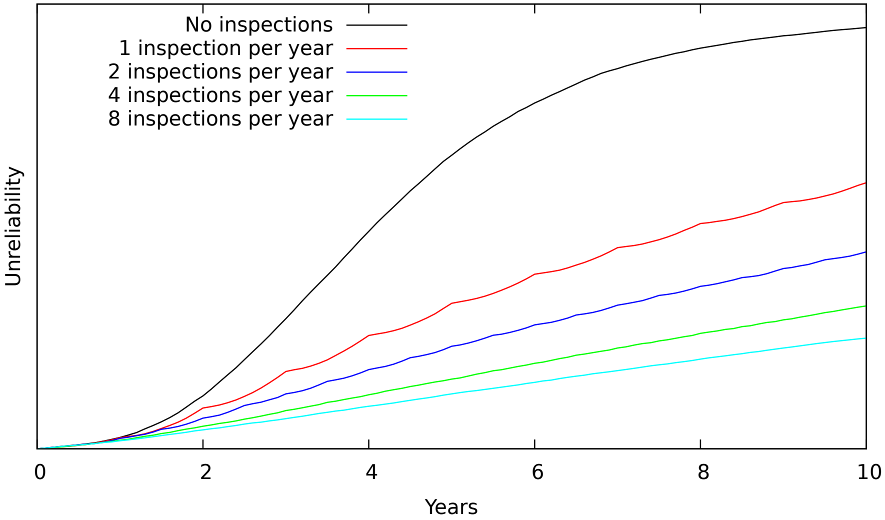
Analysis results

- Results are averages of 40,000 simulations.
- 95% Confidence window: width less than 1%.
- Computation time: Approx. 200 CPU-hours.
- Scales omitted for confidentiality.

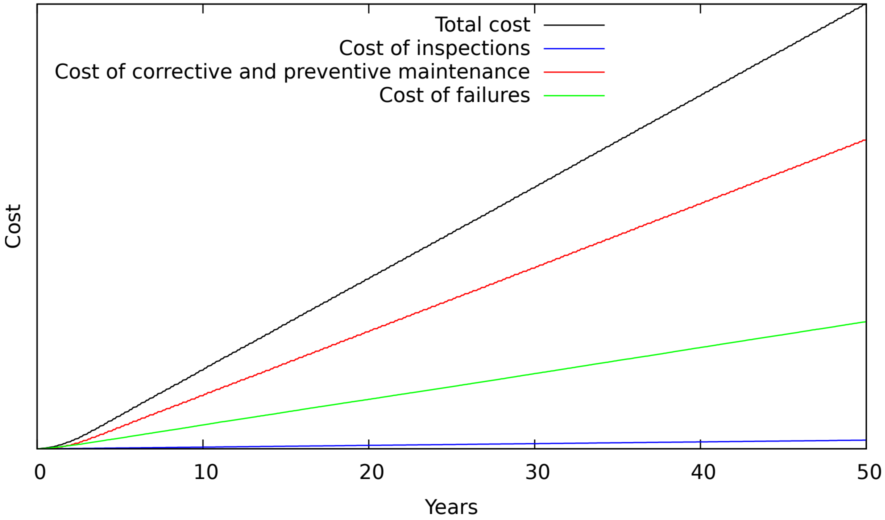
Analysis results: failure causes



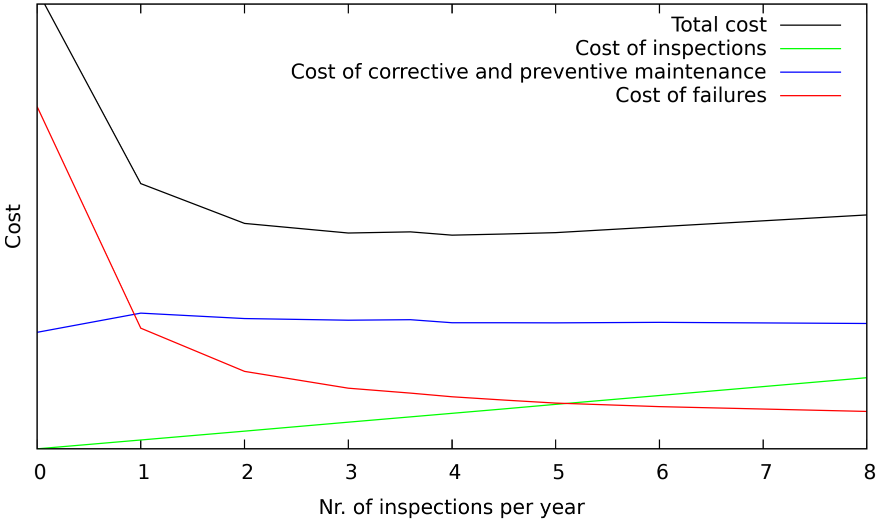
Analysis results: unreliability



Analysis results: costs



Analysis results: inspection rate



Analysis results: other strategies

Strategy	**Failure rate**	**Total cost**	**Maint. cost**
Standard	1	1	0.76
Periodic replacement (5 yrs)	0.88	1.85	1.64
Periodic replacement (20 yrs)	0.98	1.17	0.94
Reduced maint. threshold	0.48	1.18	1.06

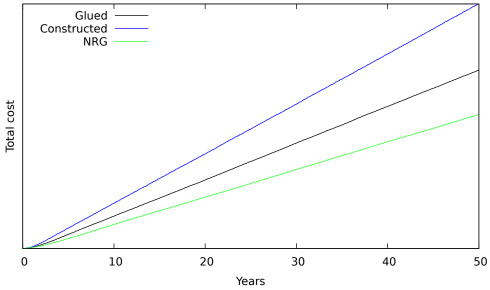
- Note: Reduced maintenance threshold may not be feasible in practice.

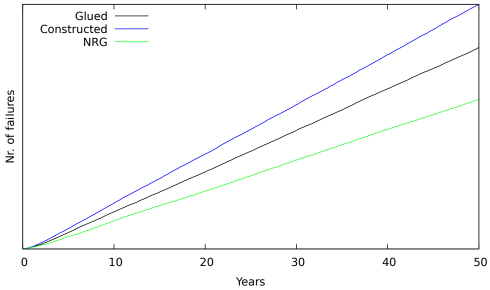
Case study: New Electrically insulated joint

Case study: New Electrically insulated joint

- New and improved joint developed for ProRail.
- Longer plates, more and repositioned bolts.
- More reliable, and more expensive.

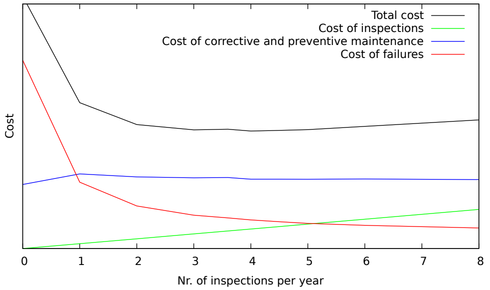
Results on new joints

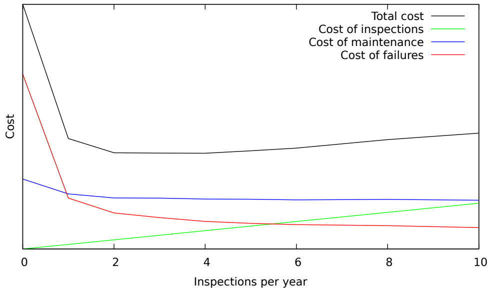




- Comparison of costs of three joint types:
    - Glued (previous case)
    - Constructed in situ
    - NRG (new)
- New joint is cost-effective under current maintenance policy.

Results on new joints



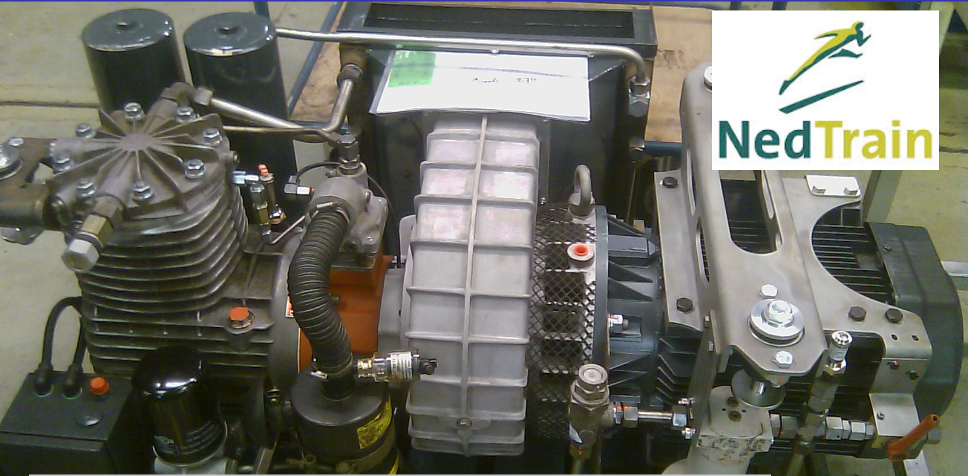


- Costs versus inspections of the two joint types.
- NRG joints require less maintenance for optimal costs.

Conclusions on EI-joints

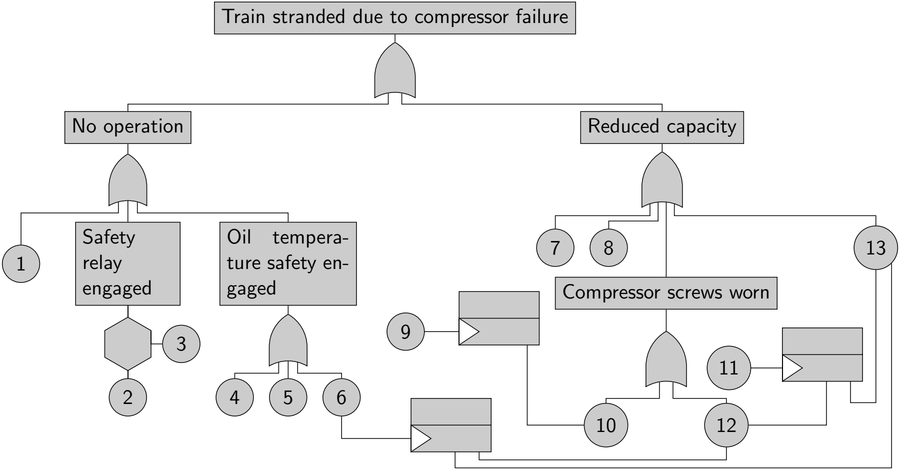
- Cost-optimal inspection frequency around 4 times per year.
- Cost approximately flat from 2 to 6 inspection per year.
- More failures can be prevented, but not cost-effectively.
- New NRG-Joint is cost-effective, and requires less maintenance.

Case study: Pneumatic compressor

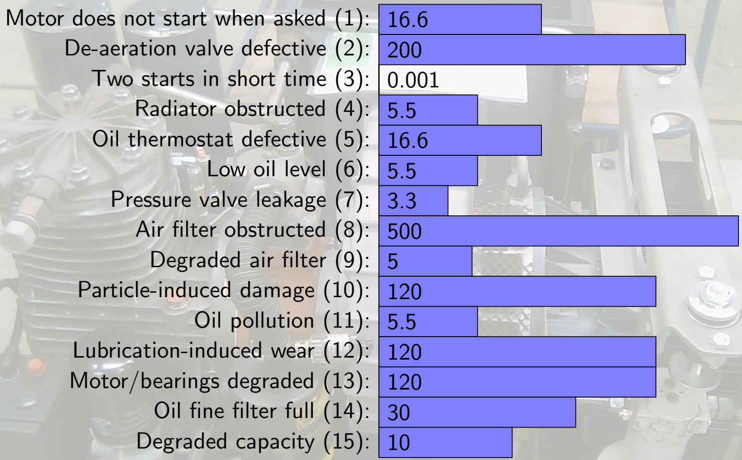


- Powers brakes, doors, etc.
- Fail-safe but failures cause disruptions.
- Maintenance is essential for normal operation.
- **Result:** Analysis of maintenance effectiveness.

FMT Pneumatic compressor

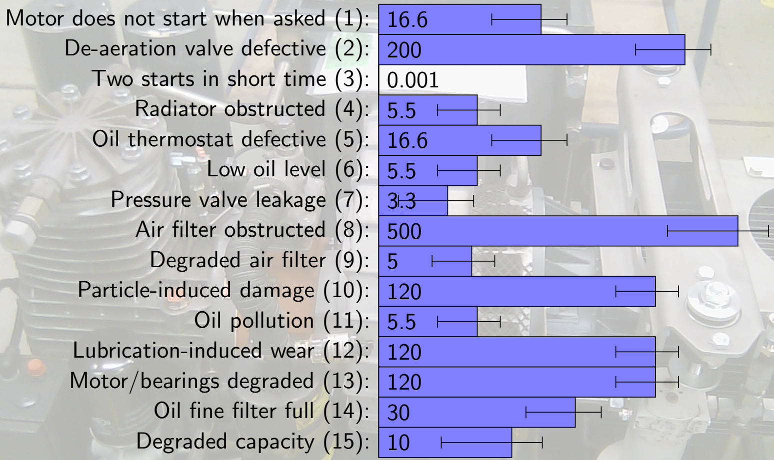


Failure modes



- Bars show MTTF (years, logarithmic), whiskers show std. deviation
- Estimates from maintenance engineers, system experts.
- Experiment reports from simulation environment.

Failure modes



- Bars show MTTF (years, logarithmic), whiskers show std. deviation
- Estimates from maintenance engineers, system experts.
- Experiment reports from simulation environment.

Maintenance plan

Maintenance actions:

- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

Maintenance plan

BE	Phase	Action	Result
1	2	S1	1

Maintenance actions:

- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

Maintenance plan

BE	Phase	Action	Result
1	2	S1	1
1	2	O1	1
2	2	O1	1
3	2	Any	1
4	3	S1	2

Maintenance actions:

- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

Maintenance plan

BE	Phase	Action	Result
1	2	S1	1
1	2	O1	1
2	2	O1	1
3	2	Any	1
4	3	S1	2
4	Any	O1	1
5	2	S1	O2

Maintenance actions:

- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

Maintenance plan

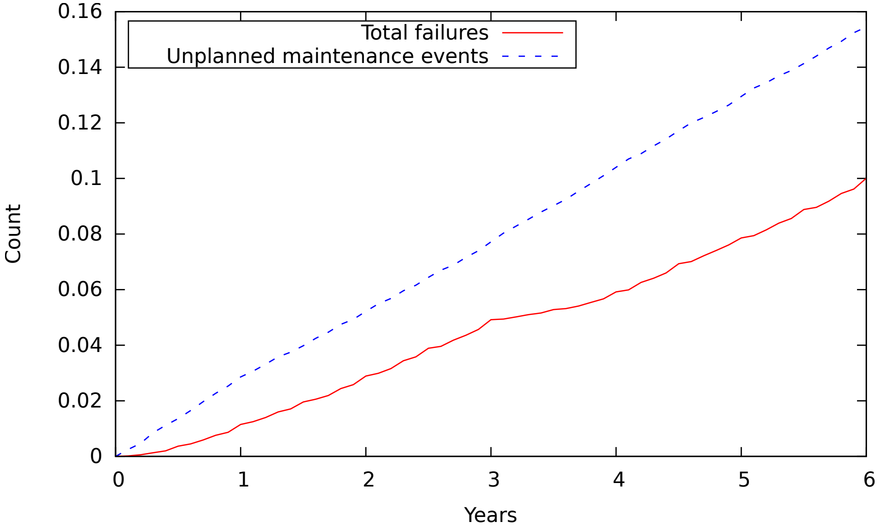
BE	Phase	Action	Result
1	2	S1	1
1	2	O1	1
2	2	O1	1
3	2	Any	1
4	3	S1	2
4	Any	O1	1
5	2	S1	O2
5	2	O1	1
6	Any	S1	1
6	Any	O1	1
7	2	I1	1
7	2	S1	1
8	Any	S1	1
8	Any	O1	1

Maintenance actions:

- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

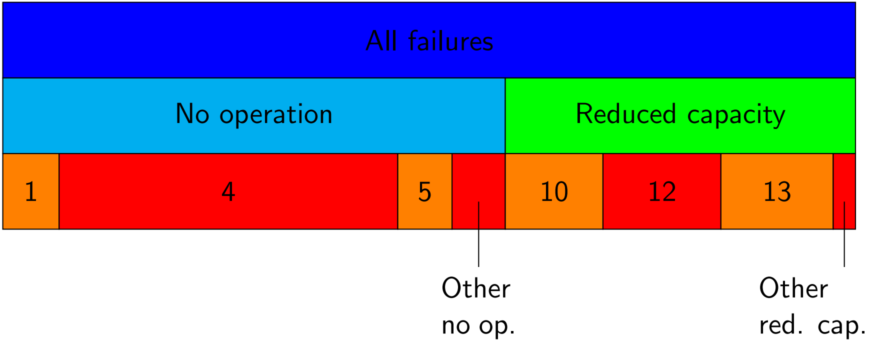
Results compressor case

Current maintenance policy:



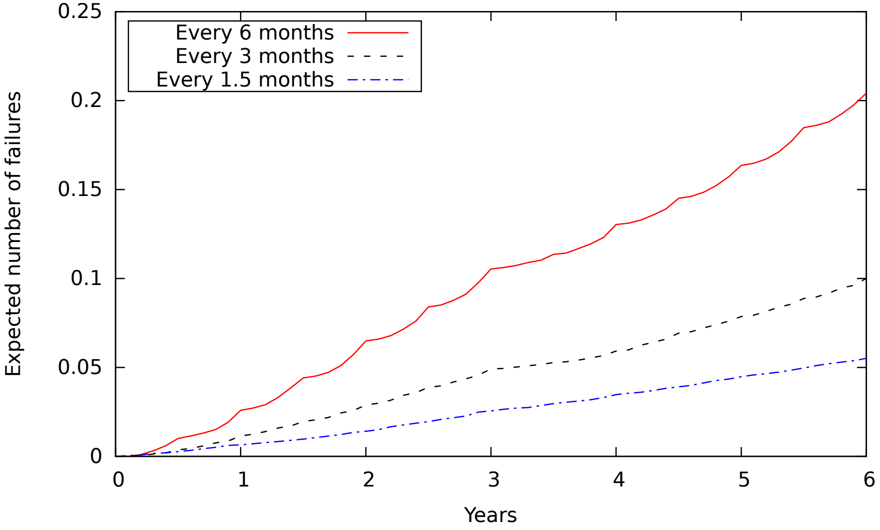
Results compressor case

Current maintenance policy:



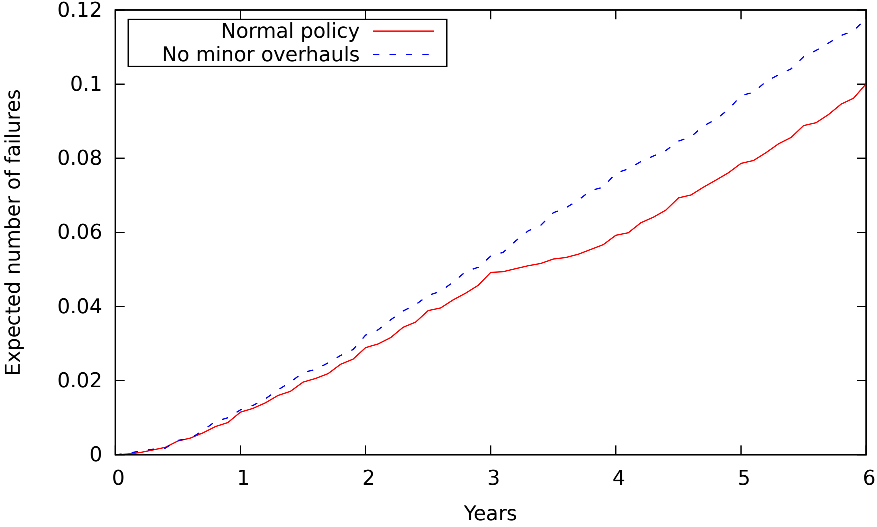
Results compressor case

Effect of service frequency:



Results compressor case

Effect of minor overhaul:



Conclusions compressor

- Results for current policy are close to reality.
- Service frequency is important parameter for reliability.
- Minor overhaul may not be cost-effective.

Outline

Conclusions

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

Ongoing work

- Automated translation from FMT to Uppaal.
- Model reduction to make analysis using I/O-MRA feasible.