Better railway engineering through statistical model checking

Enno Ruijters and Mariëlle Stoelinga

10 October 2016

UNIVERSITY OF TWENTE.

ProRail

NedTrain

Outline

1. Introduction
   - Maintenance
   - Fault Trees
   - Model checking
2. Fault maintenance trees
   - Modeling
   - Analysis
3. Case study
   - Electrically insulated joint
   - Pneumatic compressor
4. Conclusions

Do you think flying is safe?

Do you think flying is safe?

In an airplane unmaintained for a decade?

Dependability

- Dependability of many systems is critical.
    - Airplanes

Dependability

- Dependability of many systems is critical.
  - Airplanes
  - Nuclear power stations

Dependability

- Dependability of many systems is critical.
  - Airplanes
  - Nuclear power stations
  - Medical devices

Dependability

- Dependability of many systems is critical.
  - Airplanes
  - Nuclear power stations
  - Medical devices
- Traditional focus on design for dependability.

Dependability

- Dependability of many systems is critical.
  - Airplanes
  - Nuclear power stations
  - Medical devices
- Traditional focus on design for dependability.
- Even very reliable systems need maintenance.

Maintenance optimization via fault trees

Maintenance

- **Crucial:** Large impact on reliability, availability, life span.

Maintenance optimization via fault trees

Maintenance

- **Crucial:** Large impact on reliability, availability, life span.
- **Costly:** Labour, equipment, down time.

Maintenance optimization via fault trees

Maintenance

- **Crucial:** Large impact on reliability, availability, life span.
- **Costly:** Labour, equipment, down time.

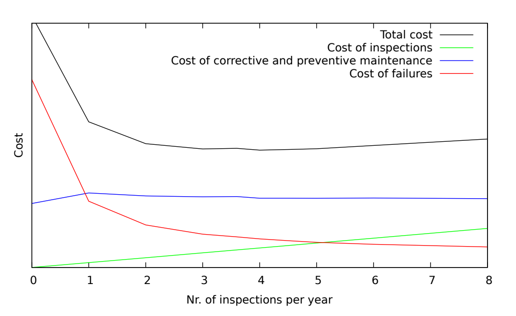
Optimize:

- Performance benefits
- Maintenance cost

Maintenance optimization via fault trees

Maintenance

- **Crucial:** Large impact on reliability, availability, life span.
- **Costly:** Labour, equipment, down time.



Optimize:

- Performance benefits
- Maintenance cost

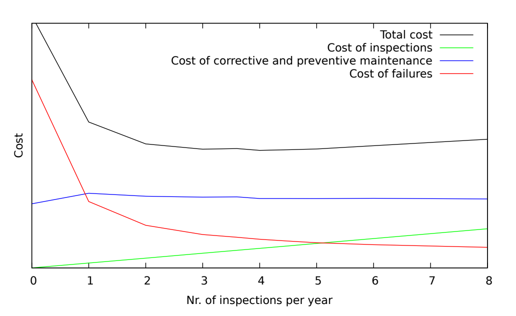
Maintenance optimization via fault trees

Maintenance

- **Crucial:** Large impact on reliability, availability, life span.
- **Costly:** Labour, equipment, down time.

Optimize:

- Performance benefits
- Maintenance cost



Support decision making to optimize maintenance plans.

Case studies

Two case studies:

Case studies

Two case studies:

EI-Joint

- Important cause of train service disruptions.
- Result: Cost-optimization of maintenance

Case studies

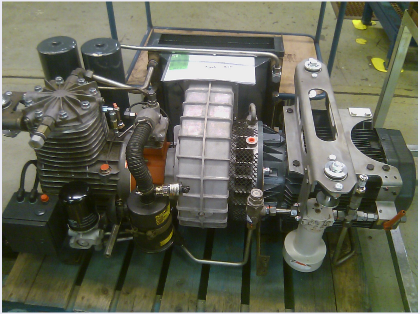
Two case studies:

EI-Joint

- Important cause of train service disruptions.
- Result: Cost-optimization of maintenance

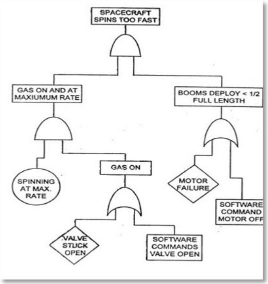
Pneumatic compressor

- Powers brakes, doors, etc., fail-safe but source of disruptions.
- Result: Reliability analysis.

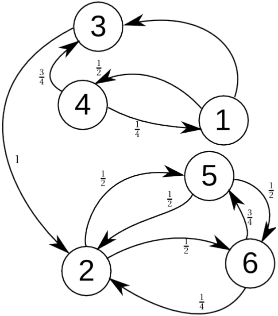


Fault maintenance trees (FMTs): 3 key ingredients

Maintenance



Fault Trees



Model Checking

FMT goals:

- What is the effect of maintenance on system performance:
  - Reliability, availability, # of failures per year?
- Can we do better (lower costs / better performance)?

Model checking brings modularity and flexibility.

Ingredient #1: maintenance

Maintenance

Types:

- Corrective maintenance:

Ingredient #1: maintenance

Maintenance

Types:

- Corrective maintenance:
- Preventive maintenance

Ingredient #1: maintenance

Maintenance

Types:

- Corrective maintenance:
- Preventive maintenance

Strategies:

- Age-based

Ingredient #1: maintenance

Maintenance

Types:

- Corrective maintenance:
- Preventive maintenance

Strategies:

- Age-based
- Use-based

Ingredient #1: maintenance

Maintenance

Types:

- Corrective maintenance:
- Preventive maintenance

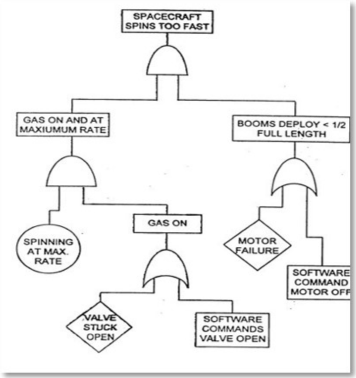
Strategies:

- Age-based
- Use-based
- Condition-based

Ingredient #2: fault trees

Industry standard tool for reliability analysis

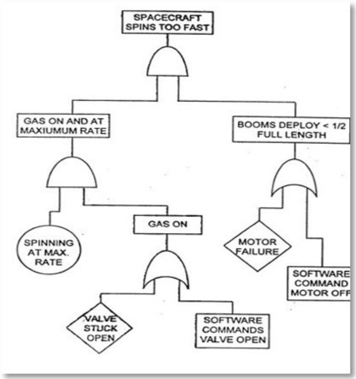
- How do component failures propagate to system failures?



Ingredient #2: fault trees

Industry standard tool for reliability analysis

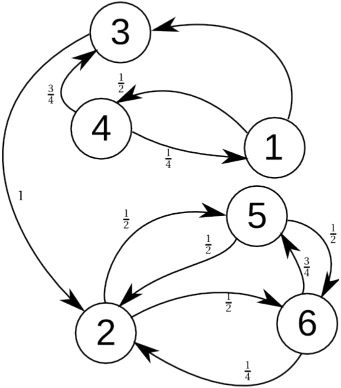
- How do component failures propagate to system failures?
- Used by NASA, ESA, Boeing, ...



Ingredient #3: model checking

Model checking

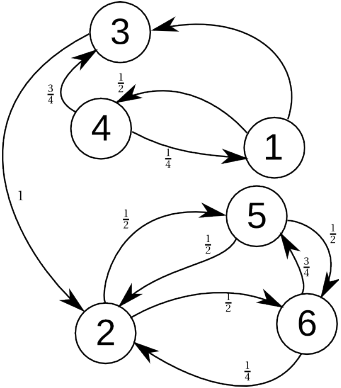
- Using Uppaal-SMC



Ingredient #3: model checking

Model checking

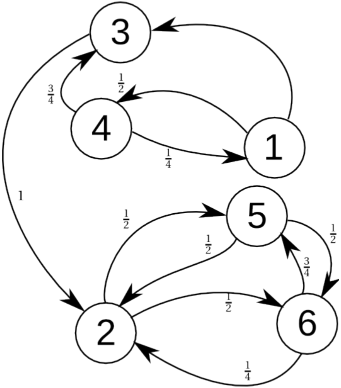
- Using Uppaal-SMC
- Advangates:
  - Ease of modelling



Ingredient #3: model checking

Model checking

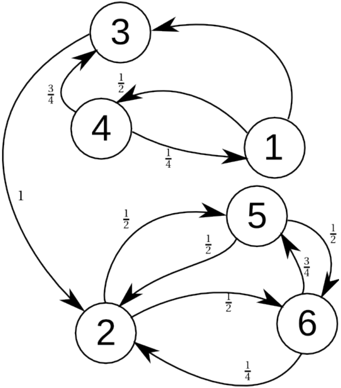
- Using Uppaal-SMC
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions



Ingredient #3: model checking

Model checking

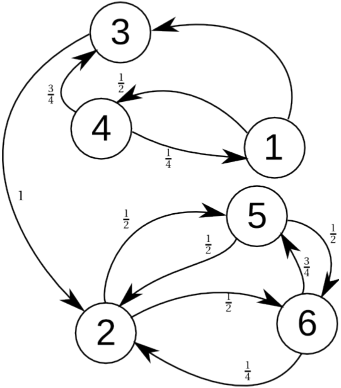
- Using Uppaal-SMC
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions
  - Choice of speed or high accuracy



Ingredient #3: model checking

Model checking

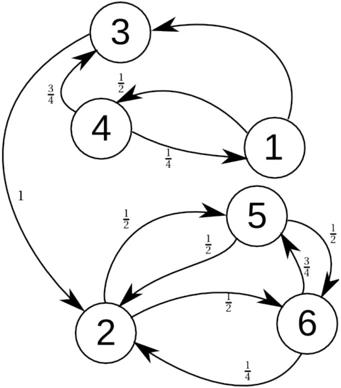
- Using Uppaal-SMC
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions
  - Choice of speed or high accuracy
- Disadvantages:
  - No guaranteed results



Ingredient #3: model checking

Model checking

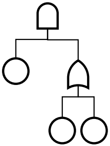
- Using Uppaal-SMC
- Advangates:
  - Ease of modelling
  - Arbitrary probability distributions
  - Choice of speed or high accuracy
- Disadvantages:
  - No guaranteed results
  - Not (currently) suitable for very rare events.



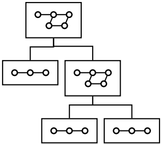
Putting it all together

Summary of our approach:

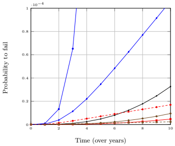
- Combine maintenance planning into fault trees.
- Compositional conversion into (P)STA.
- Analysis via statistical model checking.
- Results on system reliability, availability, etc.



(a) FMT



(b) Transformation to UPPAAL-SMC



(c) Results

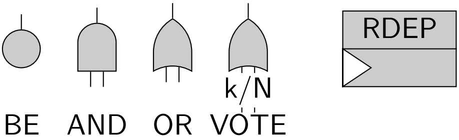
Outline

Fault trees

- Industry-standard tool for reliability analysis

Fault trees

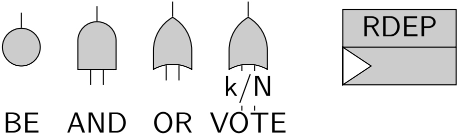
- Industry-standard tool for reliability analysis
- Describe combinations of faults leading to failures



Images of the elements in a fault (maintenance) tree

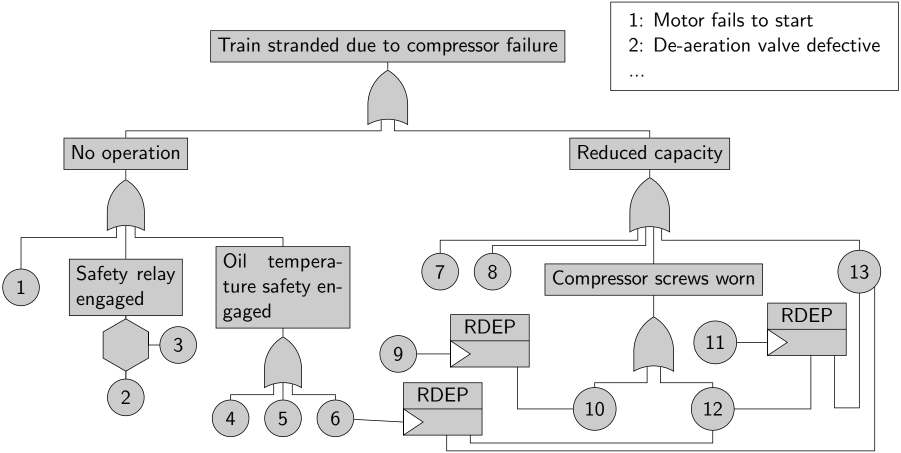
Fault trees

- Industry-standard tool for reliability analysis
- 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



Images of the elements in a fault (maintenance) tree

Fault tree of pneumatic compressor



Maintenance plan describes behaviour of leaves.

Maintenance in fault trees

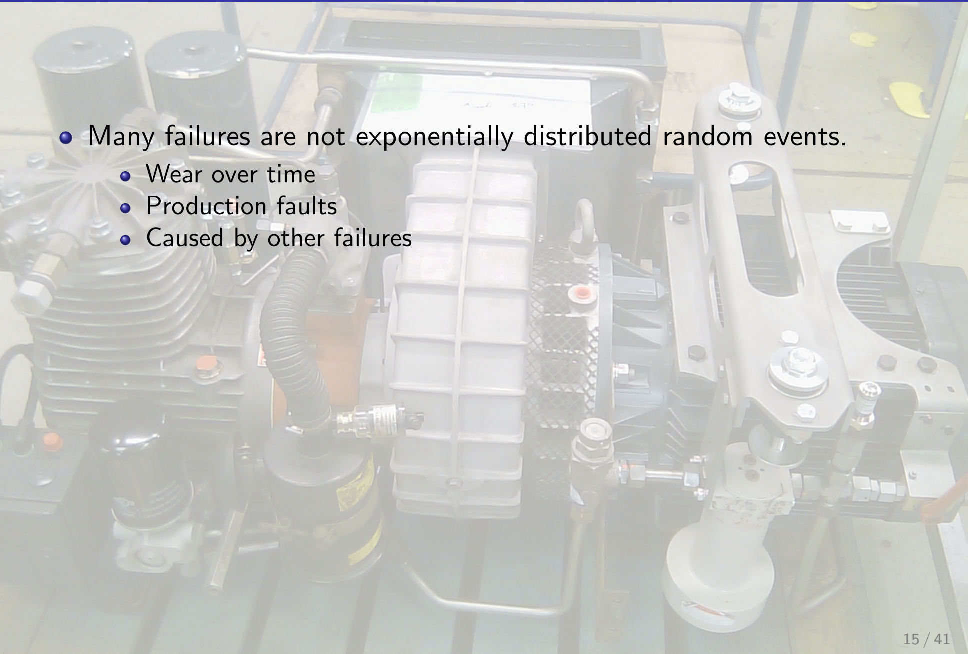
- Many failures are not exponentially distributed random events.
  - Wear over time

Maintenance in fault trees

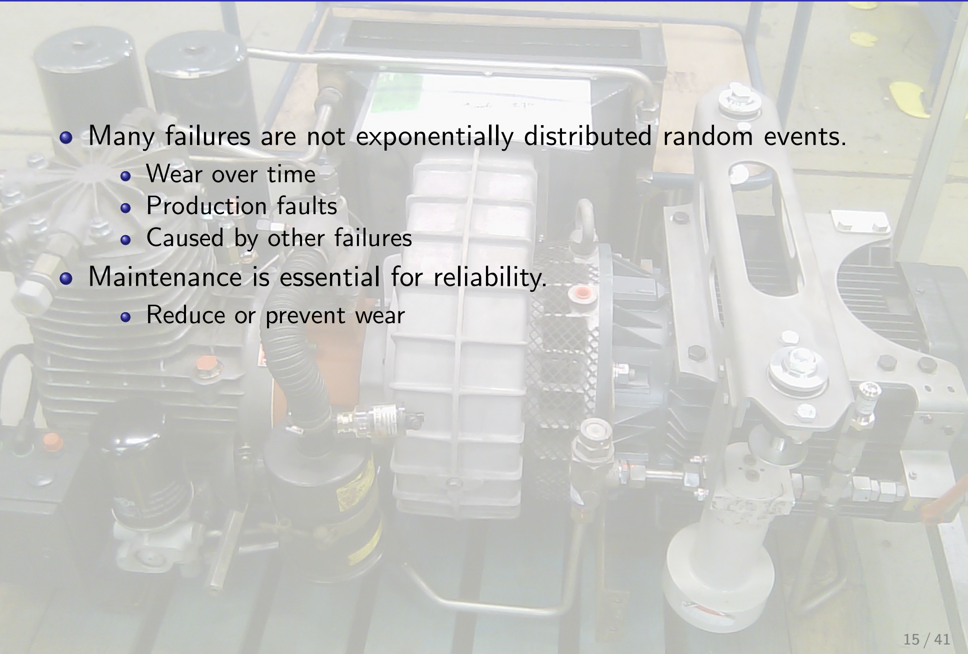
- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults

Maintenance in fault trees

- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults
  - Caused by other failures

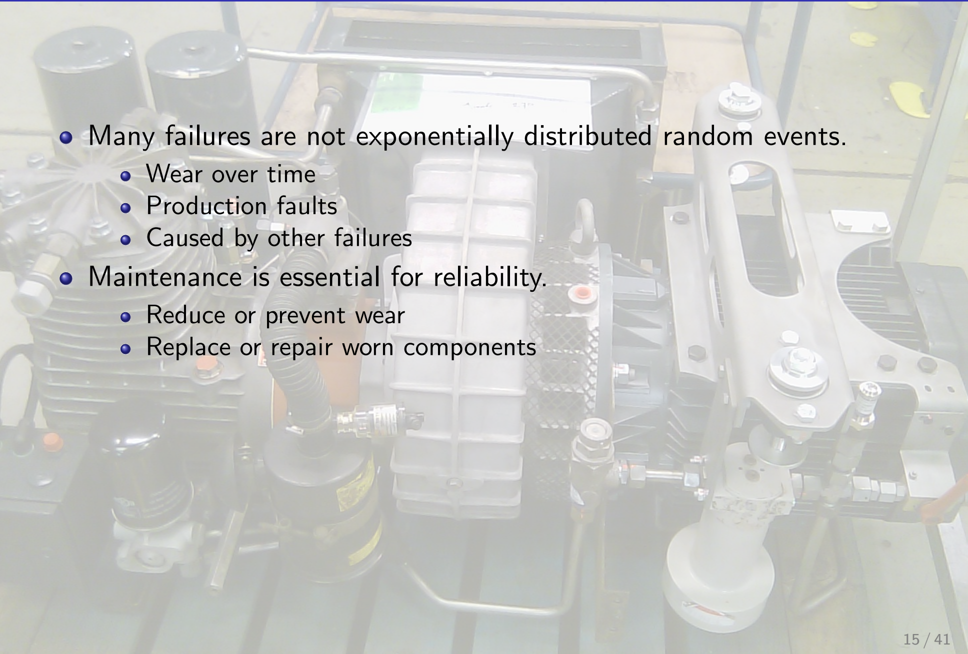


Maintenance in fault trees



- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults
  - Caused by other failures
- Maintenance is essential for reliability.
  - Reduce or prevent wear

Maintenance in fault trees



- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults
  - Caused by other failures
- Maintenance is essential for reliability.
  - Reduce or prevent wear
  - Replace or repair worn components

Maintenance in fault trees

- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults
  - Caused by other failures
- Maintenance is essential for reliability.
  - Reduce or prevent wear
  - Replace or repair worn components
  - Correct failures when they occur

Maintenance in fault trees

- Many failures are not exponentially distributed random events.
  - Wear over time
  - Production faults
  - Caused by other failures
- Maintenance is essential for reliability.
  - Reduce or prevent wear
  - Replace or repair worn components
  - Correct failures when they occur
- **Maintenance is not explicitly modeled in standard fault trees, despite its critical effect on dependability.**

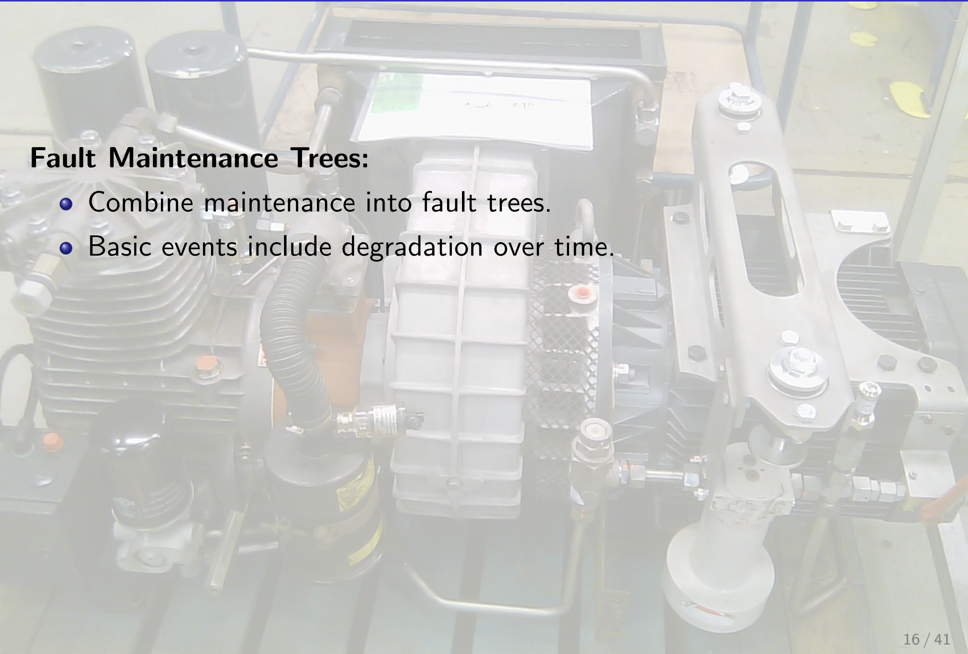
Maintenance in fault trees

Fault Maintenance Trees:

- Combine maintenance into fault trees.

Fault Maintenance Trees:

- Combine maintenance into fault trees.
- Basic events include degradation over time.

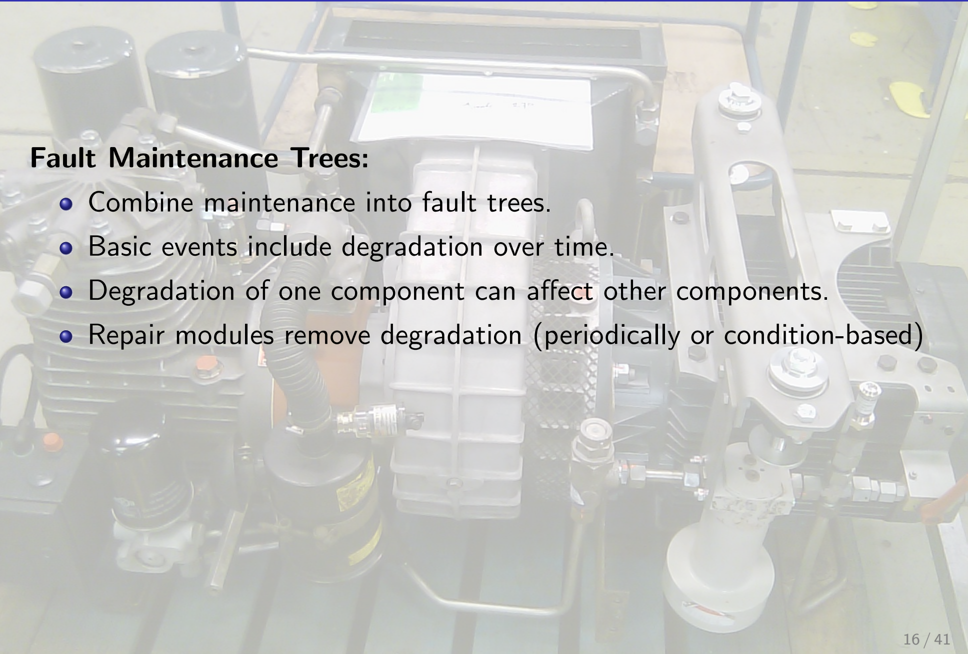


Maintenance in fault trees

Fault Maintenance Trees:

- Combine maintenance into fault trees.
- Basic events include degradation over time.
- Degradation of one component can affect other components.

Maintenance in fault trees



Fault Maintenance Trees:

- Combine maintenance into fault trees.
- Basic events include degradation over time.
- Degradation of one component can affect other components.
- Repair modules remove degradation (periodically or condition-based)

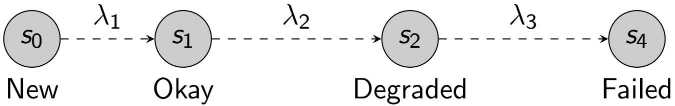
Maintenance in fault trees

Fault Maintenance Trees:

- Combine maintenance into fault trees.
- Basic events include degradation over time.
- Degradation of one component can affect other components.
- Repair modules remove degradation (periodically or condition-based)
- Inspection modules periodically check degradation and activate repairs if needed.

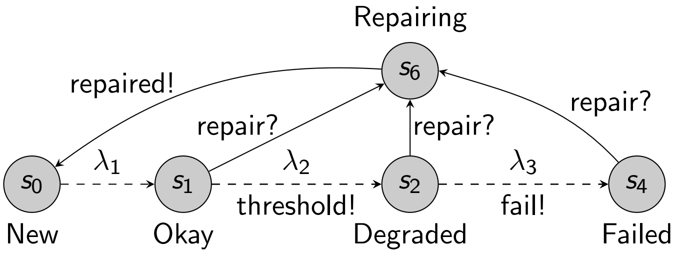
Modelling BEs

- Degradation modeled in distinct phases.
- Stochastic timed automaton:



Modelling BEs

- Timed automata with degradation stages.
- Signals for composition:
  - Maintenance threshold
  - Repair
  - Failure
- Other modules will send/receive these signals.



Rate-affecting failures

- Some failures accelerate wear of other components.

Rate-affecting failures

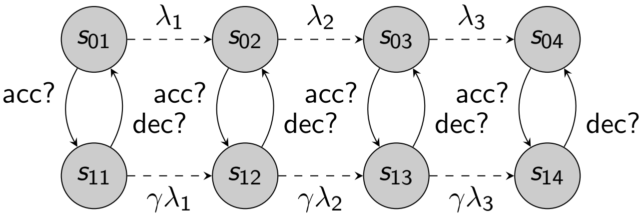
- Some failures accelerate wear of other components.
- Failure of trigger BE accelerates degradation.
- Rates increase by factor γ.

Rate-affecting failures

- Some failures 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.

Rate-affecting failures

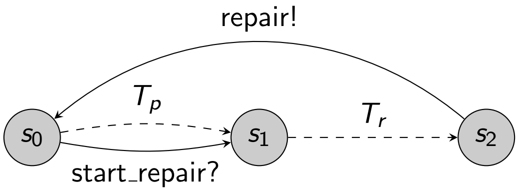
- Some failures accelerate wear of other components.
- Failure of trigger BE accelerates degradation.
- Rates increase by factor γ.
- Repair of trigger BE does not repair triggered BE.
- Timed automaton of triggered BE:



Modelling inspections and repairs

Repair module:

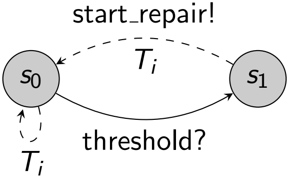
- Periodically start repairs (optional)
- Inspection may trigger repairs early



Modelling inspections and repairs

Inspection module:

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



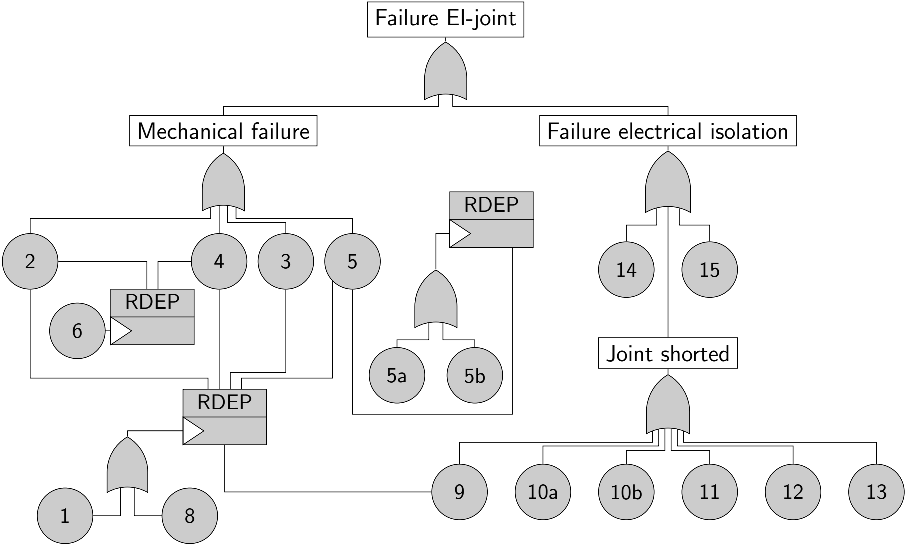
Outline

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
RDEP
5a
5b
14
15
Joint shorted
1
8
9
10a
10b
11
12
13

Modelling

Obtaining quantitative parameters:

- Follow FMEA ProRail.

Modelling

Obtaining quantitative parameters:

- Follow FMEA ProRail.
- Accelerating failure causes obtained by interviewing experts.

Modelling

Obtaining quantitative parameters:

- Follow FMEA ProRail.
- Accelerating failure causes obtained by interviewing experts.
- Failure curves obtained by fitting against historical failure data.

Modelling

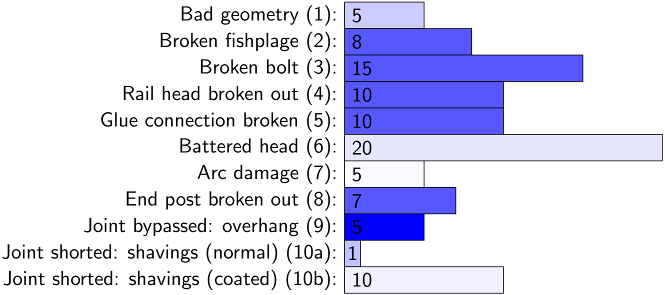
Obtaining quantitative parameters:

- Follow FMEA ProRail.
- Accelerating failure causes obtained by interviewing experts.
- Failure curves obtained by fitting against historical failure data.
- Most failures only occur in a subset of joints.
    - E.g. failures from steel shavings occur only in curved track.

Failure modes EI-joint

ETTF degrading BEs:

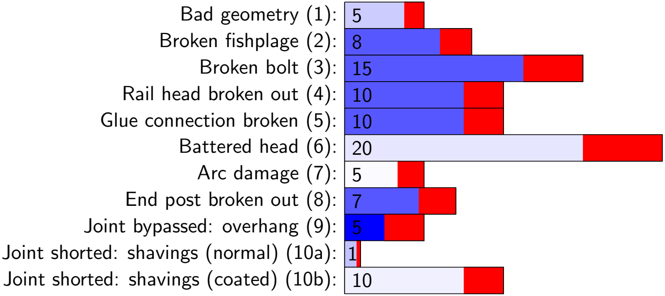
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



Failure modes EI-joint

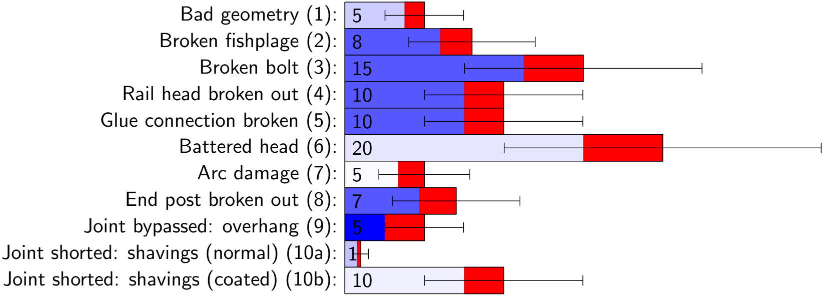
ETTF degrading BEs:

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



ETTF degrading BEs:

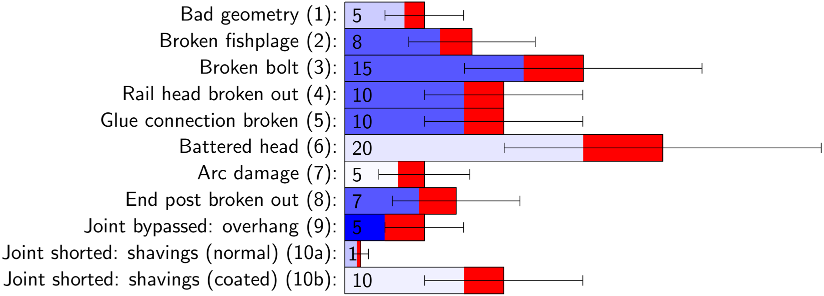
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.



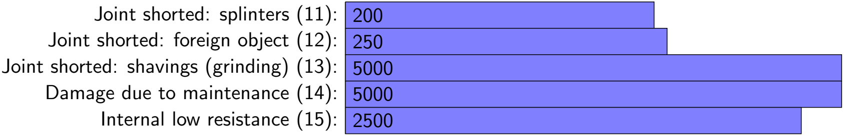
Failure modes EI-joint

ETTF degrading BEs:

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



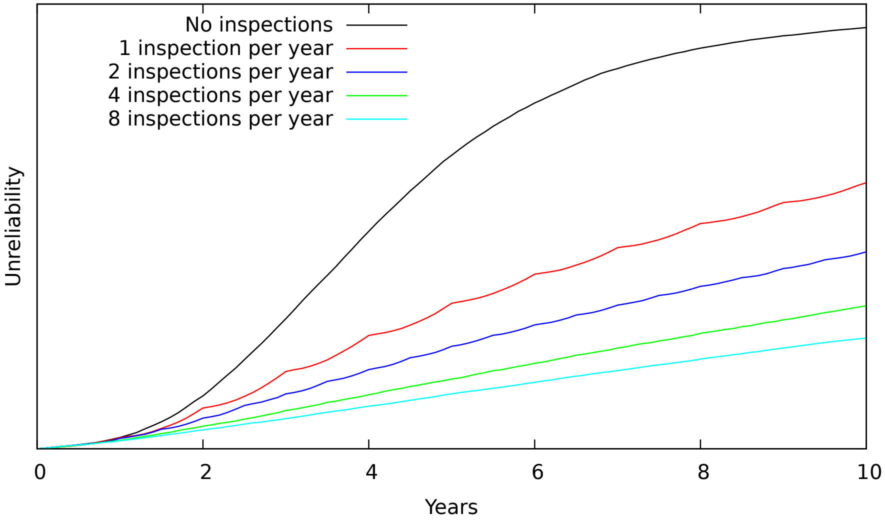
ETTF exponential failures (logarithmic scale):



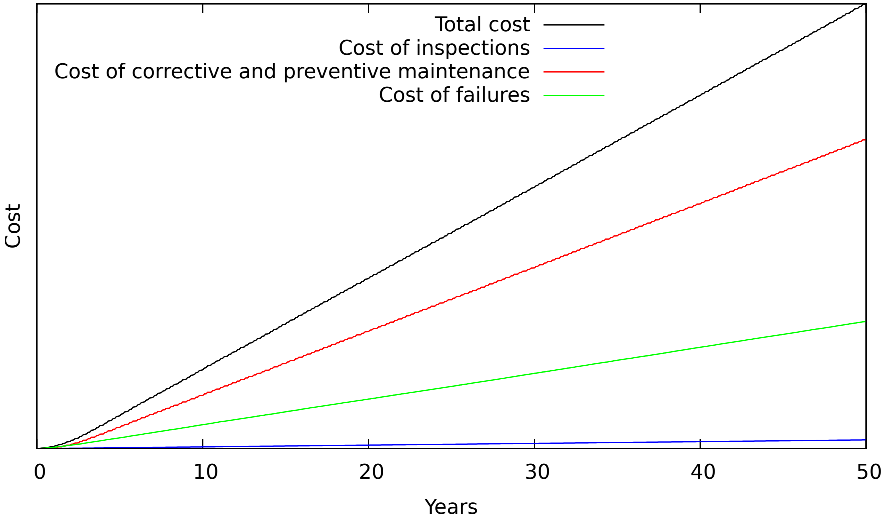
Analysis results

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

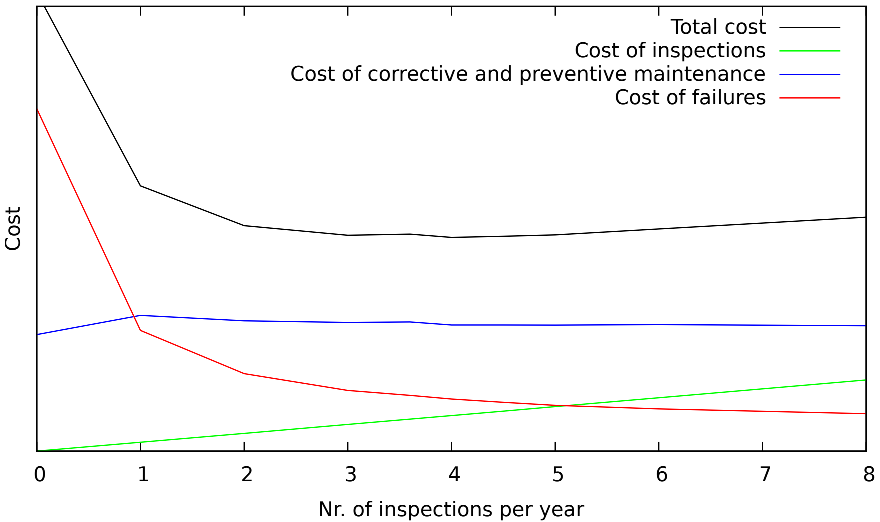
Analysis results: unreliability



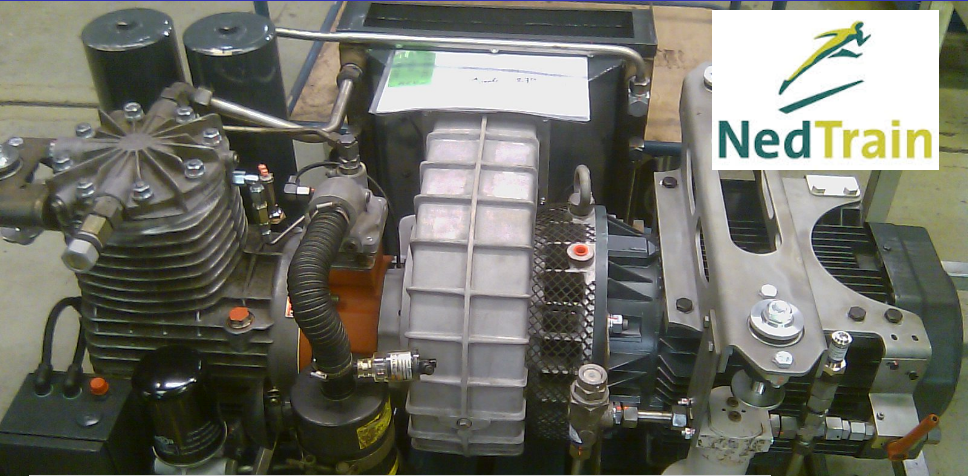
Analysis results: costs



Analysis results: inspection rate

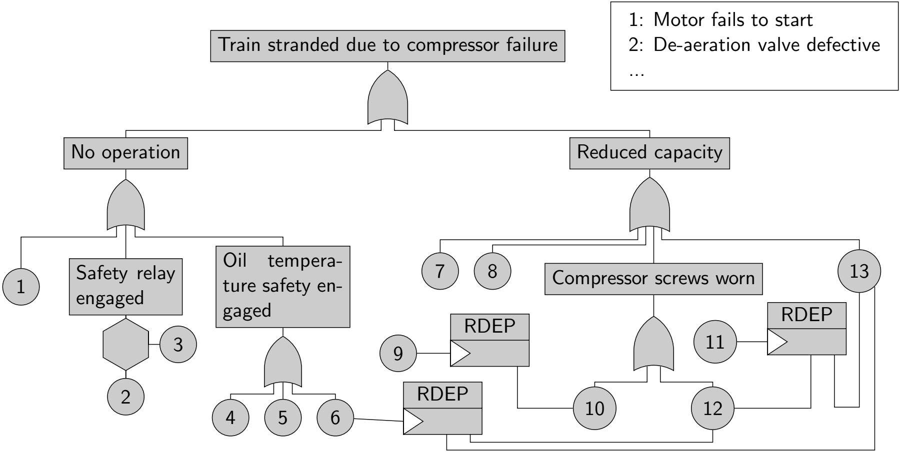


Case study: Pneumatic compressor

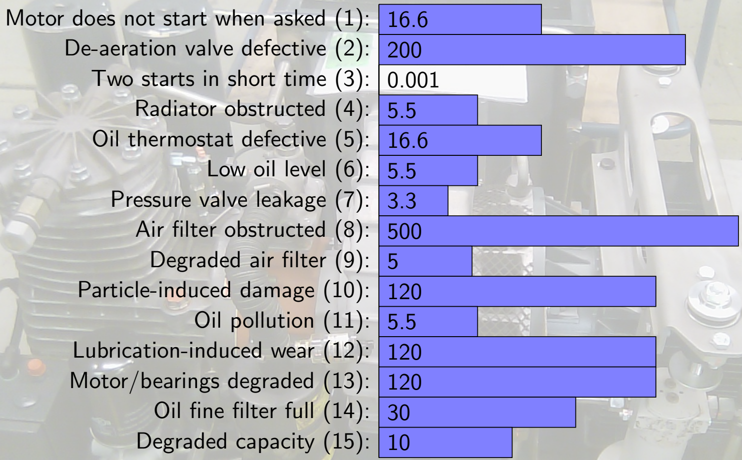


- Powers brakes, doors, etc.
- Fail-safe but failures cause disruptions.
- Maintenance is essential for normal operation.
- **Result:** Analysis of maintenance effectiveness.

Case study

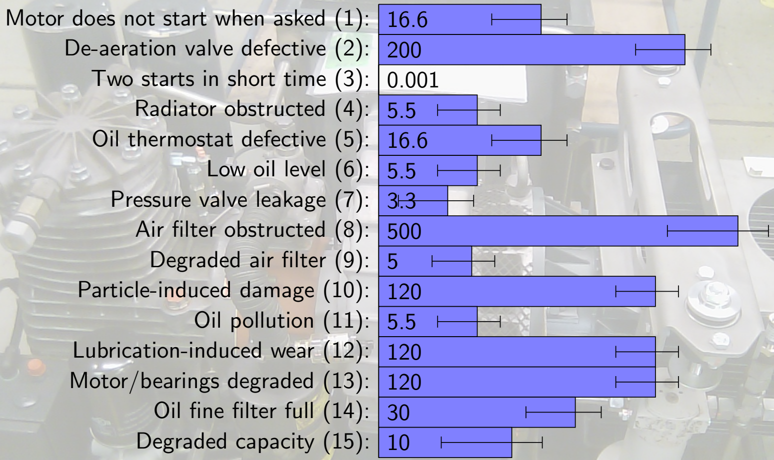

Train stranded due to compressor failure
No operation
Reduced capacity
Safety relay engaged
Oil temperature safety engaged
Compressor screws worn
RDEP
RDEP
RDEP
1
2
3
4
5
6
7
8
9
10
11
12
13
1: Motor fails to start
2: De-aeration valve defective
...

Failure modes



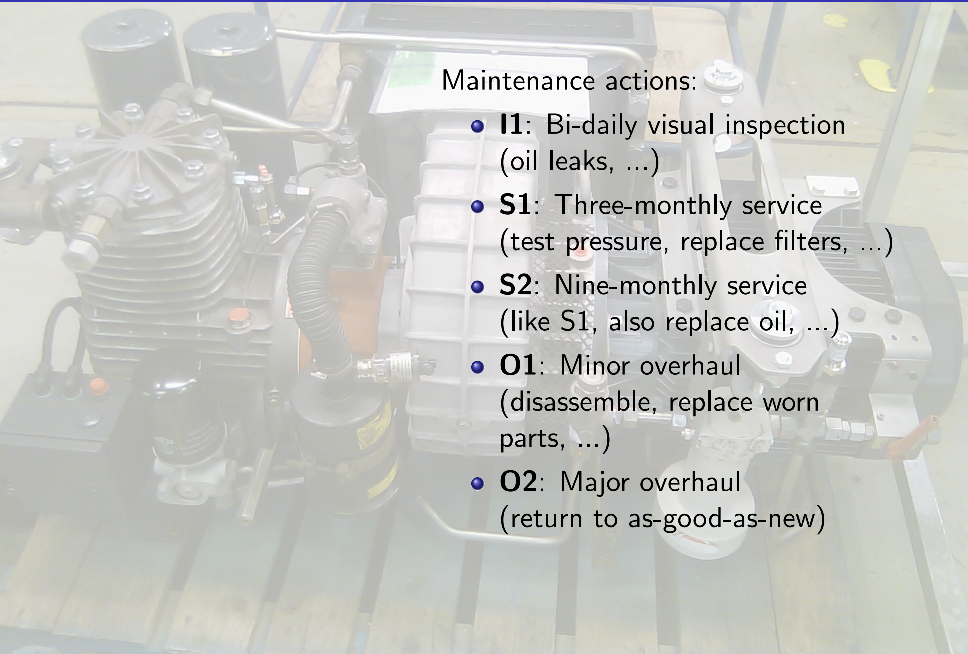
- Bars show MTTF (years, logarithmic), whiskers show std. deviation
- Estimates from maintenance engineers, system experts.
- Experiment reports from simulation environment.

Failure modes



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

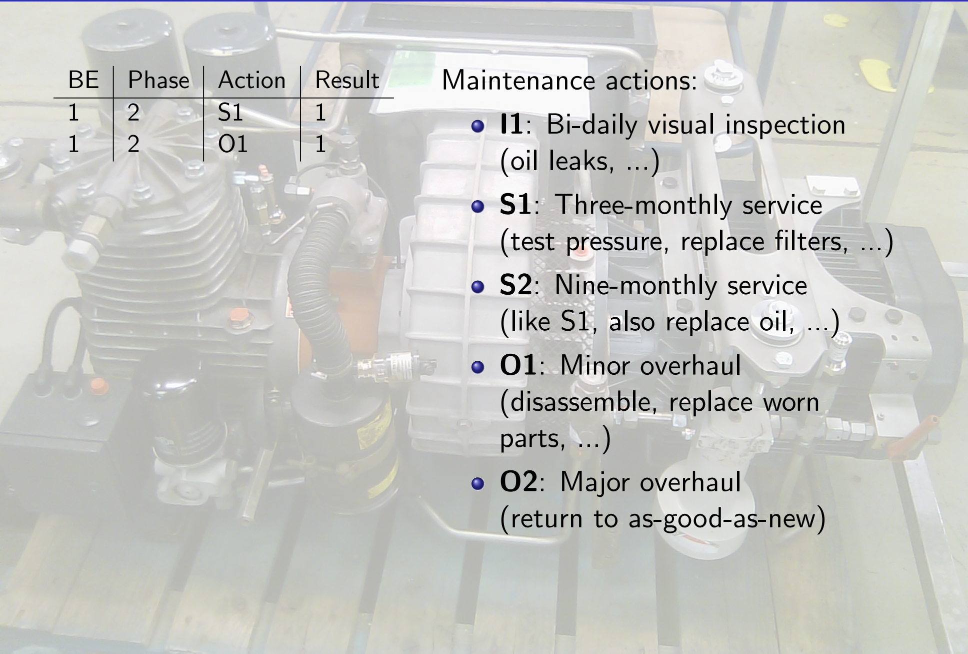
Maintenance plan



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
1	2	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)

Maintenance plan

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

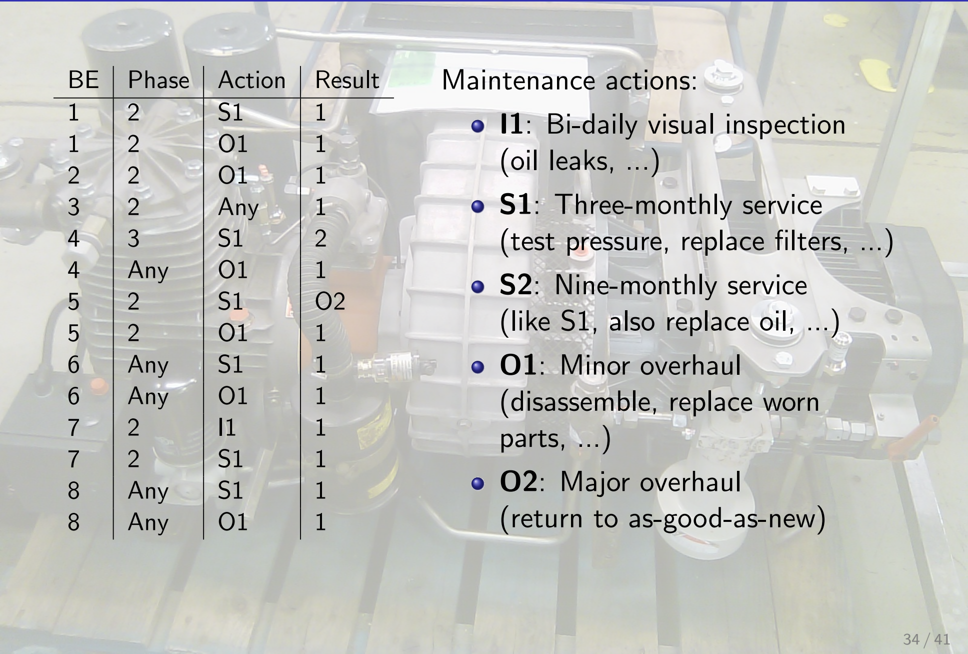
Maintenance plan

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

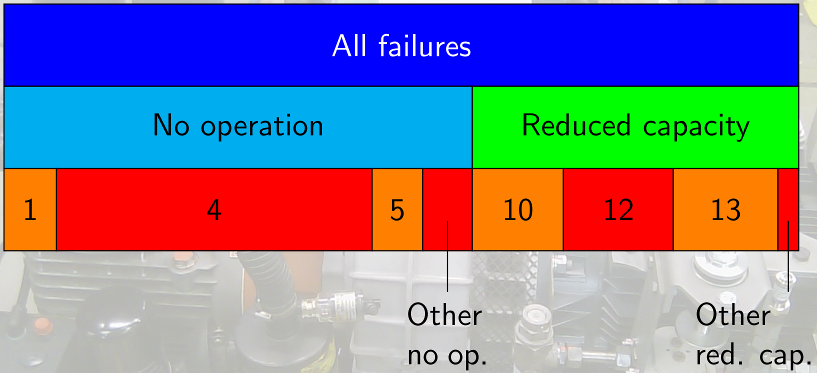


BE	Phase	Action	Result
1	2	S1	1
1	2	O1	1
2	2	O1	1
3	2	Any	1
4	3	S1	2
4	Any	O1	1
5	2	S1	O2
5	2	O1	1
6	Any	S1	1
6	Any	O1	1
7	2	I1	1
7	2	S1	1
8	Any	S1	1
8	Any	O1	1

Maintenance actions:

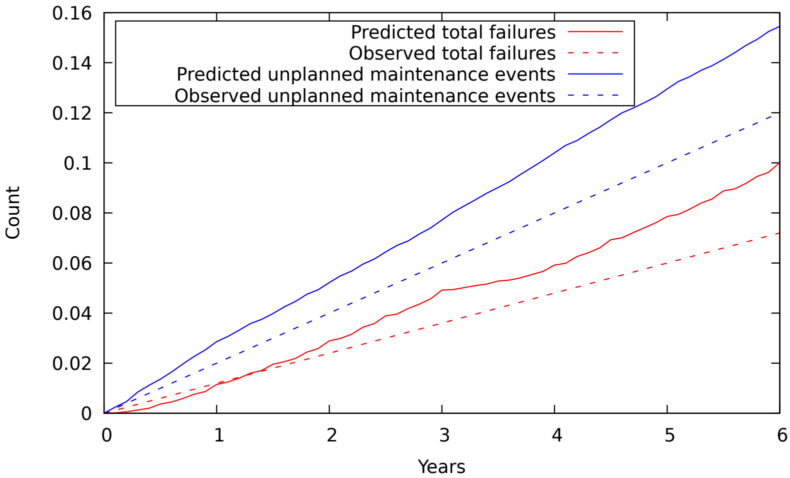
- **I1**: Bi-daily visual inspection (oil leaks, ...)
- **S1**: Three-monthly service (test pressure, replace filters, ...)
- **S2**: Nine-monthly service (like S1, also replace oil, ...)
- **O1**: Minor overhaul (disassemble, replace worn parts, ...)
- **O2**: Major overhaul (return to as-good-as-new)

Analysis results: failure causes



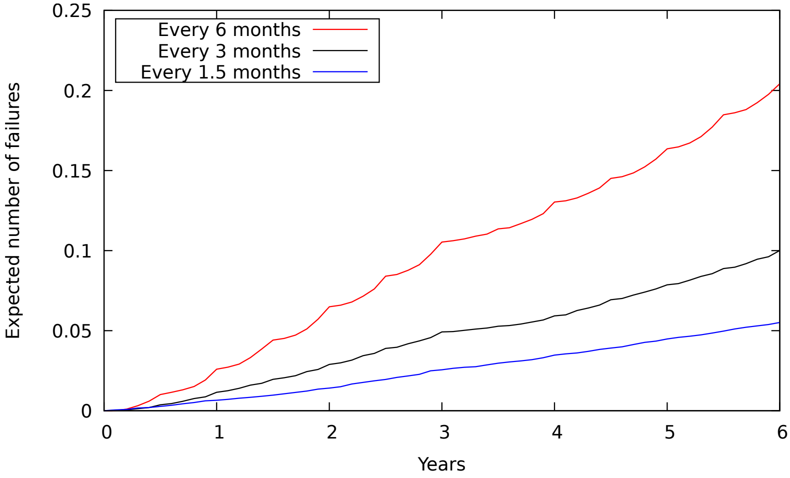
- Failure mode 4 (radiator obstructed) major cause of disruptions.
- Many failure modes rarely occur.

Analysis results: Current policy



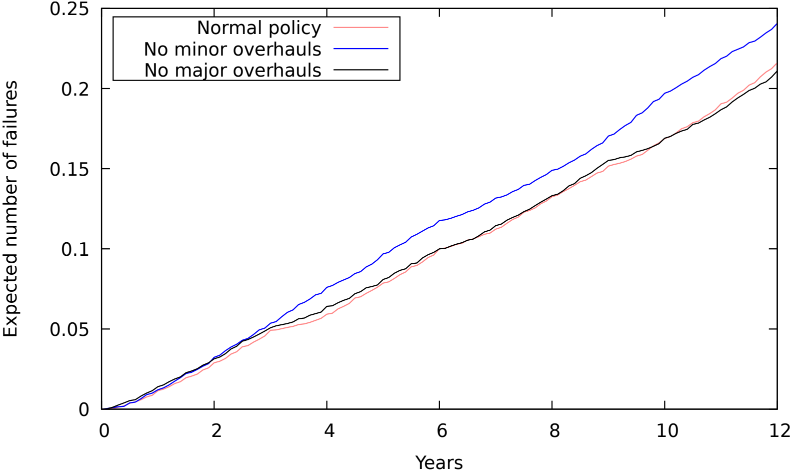
- Validation: Predictions are close to reality.

Analysis results: Varying maintenance interval



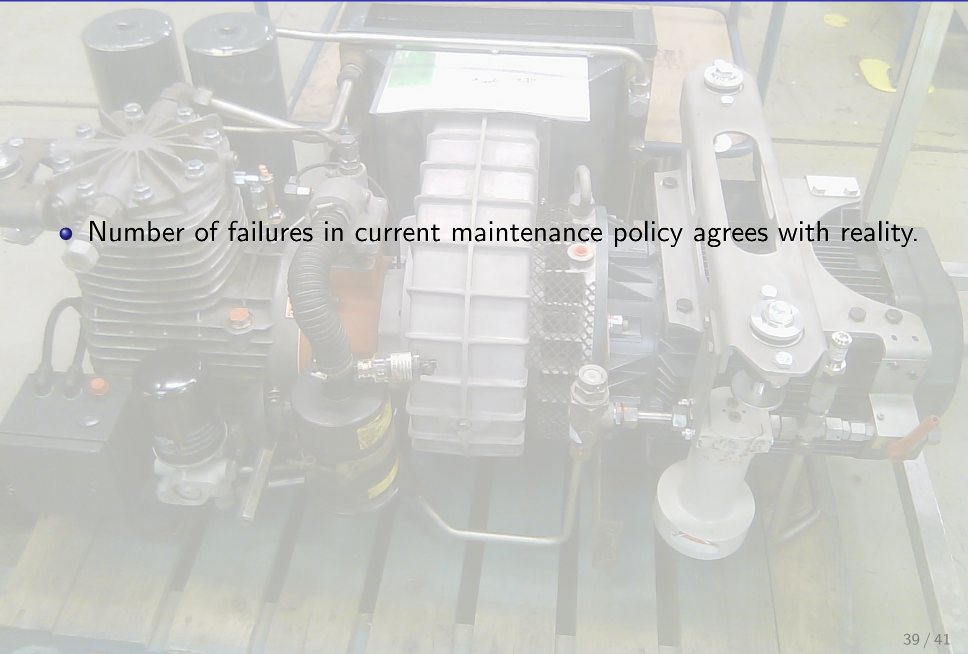
- Reliability heavily depends on maintenance interval.
- With costs, optimal inspection interval can be found.

Analysis results: Overhauls



- Scheduled overhauls do not appear to have much effect.
- Costs are confidential, but overhauls are probably not cost-effective.

Conclusions on the compressor

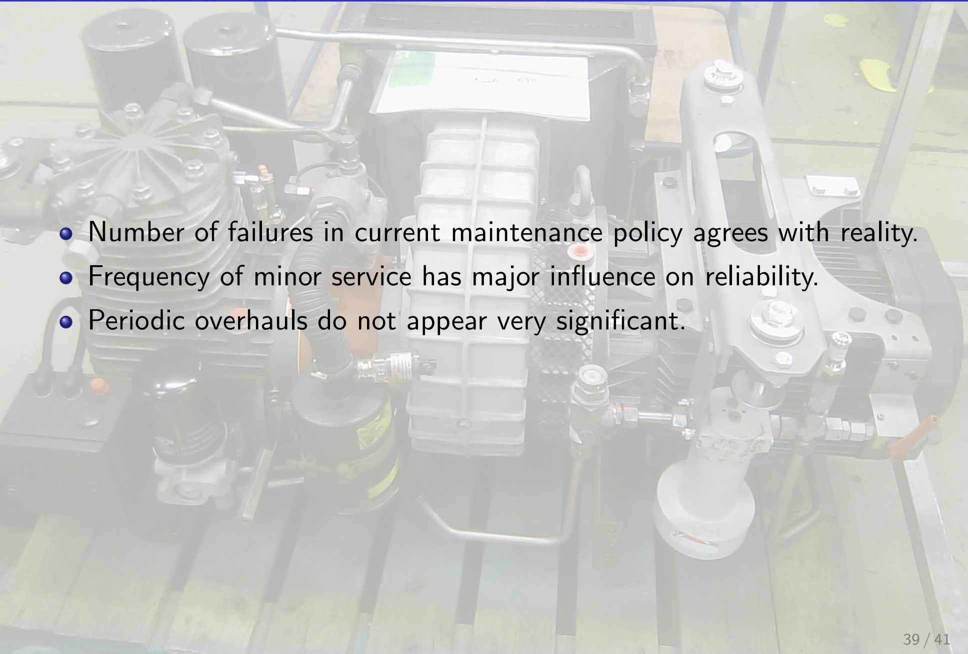


- Number of failures in current maintenance policy agrees with reality.

Conclusions on the compressor

- Number of failures in current maintenance policy agrees with reality.
- Frequency of minor service has major influence on reliability.

Conclusions on the compressor



- Number of failures in current maintenance policy agrees with reality.
- Frequency of minor service has major influence on reliability.
- Periodic overhauls do not appear very significant.

Outline

Conclusions

- FMTs integrates maintenance in fault trees.

Conclusions

- FMTs integrates maintenance in fault trees.
    - FT and maintenance plan can be separately developed.

Conclusions

- FMTs integrates maintenance in fault trees.
  - FT and maintenance plan can be separately developed.
- Useful decision support tool to compare dependability characteristics under different maintenance strategies.

Conclusions

- FMTs integrates maintenance in fault trees.
  - FT and maintenance plan can be separately developed.
- Useful decision support tool to compare dependability characteristics under different maintenance strategies.
- Demonstration FMTs in collaboration with ProRail and NedTrain.
  - Applicable in practice.

Conclusions

- FMTs integrates maintenance in fault trees.
  - FT and maintenance plan can be separately developed.
- Useful decision support tool to compare dependability characteristics under different maintenance strategies.
- Demonstration FMTs in collaboration with ProRail and NedTrain.
  - Applicable in practice.

Future work:

- Replacing phased degradation by a continuous model (SHA).