Outline

1 Introduction

2 Fault maintenance trees

3 Case studies

4 Conclusion
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

By result:
- 'As good as new' replacement
  - example: Replace battery
- Reduced failure rate
  - example: Oil change
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
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 \([0, \infty)\) 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 $[0, \infty)$ 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 \([0, \infty)\) 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

1. Introduction
2. Fault maintenance trees
3. Case studies
4. Conclusion
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
- 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)
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:

```
  s0  s1  s2  s3
New  Okay Degraded Failed
```

\( \lambda_1, \lambda_2, \lambda_3 \)
Modelling BEs

- Signals for composition:
  - Maintenance threshold
  - Repair
  - Failure

- Other models will send/receive these signals

```
<table>
<thead>
<tr>
<th>State</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>0</td>
</tr>
<tr>
<td>Okay</td>
<td>1/10</td>
</tr>
<tr>
<td>Degraded</td>
<td>4/10</td>
</tr>
<tr>
<td>Failed</td>
<td>6/10</td>
</tr>
</tbody>
</table>
```

Diagram:
- States: New, Okay, Degraded, Failed
- Transitions: λ₁, λ₂, λ₃
- Marked states: repaired!
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 $\gamma$. 
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 $\gamma$.
- Repair of trigger BE does not repair triggered BE.
Modelling inspections and repairs

**Repair module:**
- Periodically start repairs (optional)
- Inspection may trigger repairs early

![Repair module diagram](image)
**Inspection module:**

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

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

Advantages:
- Ease of modelling
- Arbitrary probability distributions

Disadvantages:
- Inexact results
- Speed
Currently using statistical model checking (Uppaal-smc)

Advantages:
- Ease of modelling
- Arbitrary probability distributions

Disadvantages:
- Inexact results
- Speed

Past/Future: Input/Output Markov Reward Automata
Outline

1 Introduction

2 Fault maintenance trees

3 Case studies

4 Conclusion
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**: 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

Joint shorted

1 8

2

4 3 5

6

RDEP

RDEP

5a 5b

10a 10b 11 12 13

9

14 15
Failure modes EI-joint

ETTF degrading BEs:
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.

- Bad geometry (1): 5
- Broken fishplage (2): 8
- Broken bolt (3): 15
- Rail head broken out (4): 10
- Glue connection broken (5): 10
- Battered head (6): 20
- Arc damage (7): 5
- End post broken out (8): 7
- Joint bypassed: overhang (9): 5
- Joint shorted: shavings (normal) (10a): 1
- Joint shorted: shavings (coated) (10b): 10
ETTF degrading BEs:

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

- Bad geometry (1): 5
- Broken fishplage (2): 8
- Broken bolt (3): 15
- Rail head broken out (4): 10
- Glue connection broken (5): 10
- Battered head (6): 20
- Arc damage (7): 5
- End post broken out (8): 7
- Joint bypassed: overhang (9): 5
- Joint shorted: shavings (normal) (10a): 1
- Joint shorted: shavings (coated) (10b): 10
Failure modes El-joint

ETTF degrading BEs:
Red zone indicates detectable by inspection, color indicates percentage of susceptible joints.

- Bad geometry (1): 5
- Broken fishplage (2): 8
- Broken bolt (3): 15
- Rail head broken out (4): 10
- Glue connection broken (5): 10
- Battered head (6): 20
- Arc damage (7): 5
- End post broken out (8): 7
- Joint bypassed: overhang (9): 5
- Joint shorted: shavings (normal) (10a): 1
- Joint shorted: shavings (coated) (10b): 10
**Failure modes EL-joint**

**ETTF degrading BEs:**

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

- **Bad geometry (1):** 5%
- **Broken fishplage (2):** 8%
- **Broken bolt (3):** 15%
- **Rail head broken out (4):** 10%
- **Glue connection broken (5):** 10%
- **Battered head (6):** 20%
- **Arc damage (7):** 5%
- **End post broken out (8):** 7%
- **Joint bypassed: overhang (9):** 15%
- **Joint shorted: shavings (normal) (10a):** 1%
- **Joint shorted: shavings (coated) (10b):** 10%

**ETTF exponential failures (logarithmic scale):**

- **Joint shorted: splinters (11):** 200
- **Joint shorted: foreign object (12):** 250
- **Joint shorted: shavings (grinding) (13):** 5000
- **Damage due to maintenance (14):** 5000
- **Internal low resistance (15):** 2500
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

All failures

Physical

Electrical

Other mech.

Other elec.
Analysis results: unreliability

Unreliability vs. Years for different inspection frequencies:
- No inspections
- 1 inspection per year
- 2 inspections per year
- 4 inspections per year
- 8 inspections per year
Analysis results: costs

- Total cost
- Cost of inspections
- Cost of corrective and preventive maintenance
- Cost of failures
Analysis results: inspection rate

Cost

Nr. of inspections per year

Total cost
Cost of inspections
Cost of corrective and preventive maintenance
Cost of failures
## Analysis results: other strategies

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Failure rate</th>
<th>Total cost</th>
<th>Maint. cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>1</td>
<td>1</td>
<td>0.76</td>
</tr>
<tr>
<td>Periodic replacement (5 yrs)</td>
<td>0.88</td>
<td>1.85</td>
<td>1.64</td>
</tr>
<tr>
<td>Periodic replacement (20 yrs)</td>
<td>0.98</td>
<td>1.17</td>
<td>0.94</td>
</tr>
<tr>
<td>Reduced maint. threshold</td>
<td>0.48</td>
<td>1.18</td>
<td>1.06</td>
</tr>
</tbody>
</table>

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

Train stranded due to compressor failure

No operation

Safety relay engaged

Oil temperature safety engaged

Reduced capacity

Compressor screws worn

1. Train stranded due to compressor failure
2. Safety relay engaged
3. Oil temperature safety engaged
4. Reduced capacity
5. Compressor screws worn
6. 40 / 50
### Failure modes

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>MTTF (years, logarithmic)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motor does not start when asked (1)</td>
<td>16.6</td>
</tr>
<tr>
<td>De-aeration valve defective (2)</td>
<td>200</td>
</tr>
<tr>
<td>Two starts in short time (3)</td>
<td>0.001</td>
</tr>
<tr>
<td>Radiator obstructed (4)</td>
<td>5.5</td>
</tr>
<tr>
<td>Oil thermostat defective (5)</td>
<td>16.6</td>
</tr>
<tr>
<td>Low oil level (6)</td>
<td>5.5</td>
</tr>
<tr>
<td>Pressure valve leakage (7)</td>
<td>3.3</td>
</tr>
<tr>
<td>Air filter obstructed (8)</td>
<td>500</td>
</tr>
<tr>
<td>Degraded air filter (9)</td>
<td>5</td>
</tr>
<tr>
<td>Particle-induced damage (10)</td>
<td>120</td>
</tr>
<tr>
<td>Oil pollution (11)</td>
<td>5.5</td>
</tr>
<tr>
<td>Lubrication-induced wear (12)</td>
<td>120</td>
</tr>
<tr>
<td>Motor/bearings degraded (13)</td>
<td>120</td>
</tr>
<tr>
<td>Oil fine filter full (14)</td>
<td>30</td>
</tr>
<tr>
<td>Degraded capacity (15)</td>
<td>10</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>MTTF (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motor does not start when asked (1)</td>
<td>16.6</td>
</tr>
<tr>
<td>De-aeration valve defective (2)</td>
<td>200</td>
</tr>
<tr>
<td>Two starts in short time (3)</td>
<td>0.001</td>
</tr>
<tr>
<td>Radiator obstructed (4)</td>
<td>5.5</td>
</tr>
<tr>
<td>Oil thermostat defective (5)</td>
<td>16.6</td>
</tr>
<tr>
<td>Low oil level (6)</td>
<td>5.5</td>
</tr>
<tr>
<td>Pressure valve leakage (7)</td>
<td>3.3</td>
</tr>
<tr>
<td>Air filter obstructed (8)</td>
<td>500</td>
</tr>
<tr>
<td>Degraded air filter (9)</td>
<td>5</td>
</tr>
<tr>
<td>Particle-induced damage (10)</td>
<td>120</td>
</tr>
<tr>
<td>Oil pollution (11)</td>
<td>5.5</td>
</tr>
<tr>
<td>Lubrication-induced wear (12)</td>
<td>120</td>
</tr>
<tr>
<td>Motor/bearings degraded (13)</td>
<td>120</td>
</tr>
<tr>
<td>Oil fine filter full (14)</td>
<td>30</td>
</tr>
<tr>
<td>Degraded capacity (15)</td>
<td>10</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>BE</th>
<th>Phase</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>S1</td>
<td>1</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>BE</th>
<th>Phase</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Any</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>S1</td>
<td>2</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>BE</th>
<th>Phase</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Any</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>S1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>S1</td>
<td>O2</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>BE</th>
<th>Phase</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Any</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>S1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>S1</td>
<td>O2</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Any</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Any</td>
<td>O1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>I1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td>S1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td>O1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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)
Current maintenance policy:

![Graph showing Total failures and Unplanned maintenance events over years.](image-url)
Results compressor case

Current maintenance policy:

- All failures
- No operation
- Reduced capacity

<table>
<thead>
<tr>
<th></th>
<th>Other no op.</th>
<th>Other reduced cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>13</td>
</tr>
</tbody>
</table>
Results compressor case

Effect of service frequency:

- Every 6 months
- Every 3 months
- Every 1.5 months

Expected number of failures vs. Years
Results compressor case

Effect of minor overhaul:

![Graph showing expected number of failures over years for normal policy and no minor overhauls.]

- **Expected number of failures**
- **Years**
- **Normal policy**
  - Line color: red
- **No minor overhauls**
  - Line style: dashed
Conclusions compressor

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