Maintenance analysis and optimization via statistical model checking:
Evaluation of a train’s pneumatic compressor

Enno Ruijters, Dennis Guck, Peter Drolenga, Margot Peters, and Mariëlle Stoelinga

25 August 2016
Outline

1 Introduction
   • Maintenance
   • Fault Trees
   • Model checking

2 Fault maintenance trees
   • Modeling
   • Analysis

3 Case study
   • System modeling
   • Analysis

4 Conclusions
Do you think flying is safe?

In an airplane unmaintained for a decade?
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.
- **Costly**: Labour, equipment, down time.

Optimize:

- Performance benefits
- Maintenance cost

Support decision making to optimize maintenance plans.
Fault maintenance trees (FMTs): 3 key ingredients

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

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?
- Used by NASA, ESA, Boeing, ...
**Ingredient #3: model checking**

**Model checking**

- Using Uppaal-SMC
- Advantages:
  - 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

1 Introduction
   • Maintenance
   • Fault Trees
   • Model checking

2 Fault maintenance trees
   • Modeling
   • Analysis

3 Case study
   • System modeling
   • Analysis

4 Conclusions
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 compressor

Train stranded due to compressor failure

No operation

1: Motor fails to start
2: De-aeration valve defective

Reduced capacity

Safety relay engaged

Oil temperature safety engaged

Compressor screws worn

Maintenance plan describes behaviour of leaves.
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.
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:

\[ s_0 \xrightarrow{\lambda_1} s_1 \xrightarrow{\lambda_2} s_2 \xrightarrow{\lambda_3} s_4 \]

\( s_0 \): New
\( s_1 \): Okay
\( s_2 \): Degraded
\( s_4 \): Failed
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.
- Failure of trigger BE accelerates degradation.
- Rates increase by factor $\gamma$.
- 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

\[ s_0 \xrightarrow{T_p} s_1 \xleftarrow{\text{start_repair?}} s_2 \xrightarrow{T_r} s_1 \]

repair!
Modelling inspections and repairs

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

![State diagram with states S0 and S1, transitions Ti, and start_repair!]
1 Introduction
   - Maintenance
   - Fault Trees
   - Model checking

2 Fault maintenance trees
   - Modeling
   - Analysis

3 Case study
   - System modeling
   - Analysis

4 Conclusions
Case study: Pneumatic compressor

- Powers brakes, doors, etc.
- Fail-safe but failures cause disruptions.
- Maintenance is essential for normal operation.
Case study

Train stranded due to compressor failure

1: Motor fails to start
2: De-aeration valve defective
...

No operation

Safety relay engaged
1

Oil temperature safety engaged
3

Reduced capacity

Compressor screws worn
13

RDEP
7

RDEP
10

RDEP
11

RDEP
9

8

12

4

5

6

2
## Failure modes

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

- Estimates from maintenance engineers, system experts.
- Experiment reports from simulation environment.
## 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)
Results are averages of 40,000 simulations.
95% Confidence window: width less than 1%.
Computation time: Approx. 6 CPU-hours.
All values scaled for confidentiality.
## Analysis results: failure causes

<table>
<thead>
<tr>
<th>All failures</th>
<th>No operation</th>
<th>Reduced capacity</th>
<th>Other no op.</th>
<th>Other red. cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>5</td>
<td>10</td>
<td>12</td>
</tr>
</tbody>
</table>

- 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 (e.g. DSN2016).
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.
- Frequency of minor service has major influence on reliability.
- Periodic overhauls do not appear very significant.
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 NedTrain.
  - Applicable in practice.

**Future work:**

- Replacing phased degradation by a continuous model.