The final publication is available at Springer via https://dx.doi.org/10.1007/978-3-319-43425-4_22.

Maintenance analysis and optimization via statistical model checking:
Evaluating a train pneumatic compressor

Enno Ruijters[1], Dennis Guck[1], Peter Drolenga[2], Margot Peters[2], and Mariëlle Stoelinga[1]
1: University of Twente, EWI-FMT, P.O. Box 217, 7500 AE Enschede, The Netherlands
e-mail: {e.j.j.ruijters, d.guck, m.i.a.stoelinga}@utwente.nl
2: NedTrain Fleet Services, P.O. Box 2167, 3500 GD Utrecht, The Netherlands
e-mail: {peter.drolenga, margot.peters}@nedtrain.nl

Abstract. Maintenance is crucial to ensuring and improving system dependability: By performing timely inspections, repairs, and renewals the lifespan and reliability of systems can be significantly improved. Good maintenance planning, however, has to balance these improvements against the downsides of maintenance, such as costs and planned downtime.
In this paper, we study the effect of different maintenance strategies on a pneumatic compressor used in trains. This compressor is critical to the operation of the train, and a failure can lead to a lengthy and expensive disruption. Within the rolling stock maintenance company NedTrain, we have modelled this compressor as a fault maintenance tree (FMT), i.e. a fault tree augmented with maintenance aspects. We show how this FMT naturally models complex maintenance plans including condition-based maintenance with regular inspections. The FMT is analysed using statistical model checking, which allows us to obtain several key performance indicators such as the system reliability, number of failures, and required unscheduled maintenance.
Our analysis demonstrates that FMTs can be used to model the compressor, a practical system used in industry, including its maintenance policy. We validate this model against experiences in the field, compute the importance of performing minor services at a reasonable frequency, and find that the currently scheduled overhaul may not be cost-effective.

1 Introduction

Maintenance of critical assets. The current trend in asset management is to use reliability-centered maintenance (RCM), with the goal of optimizing maintenance planning by maintaining critical assets more intensively than less critical ones. By focusing maintenance where it is most effective, RCM seeks to balance maintenance costs against system dependability. To achieve this balance, it is necessary to have a good understanding of the effects of a maintenance policy on the system's dependability, measured by key performance indicators like availability, reliability, mean time to failure, etc. Achieving this understanding calls for an integrated analysis of system dependability and maintenance. This paper shows a method to perform such an integral analysis, namely fault maintenance trees (FMTs), and demonstrates that this method yields useful results

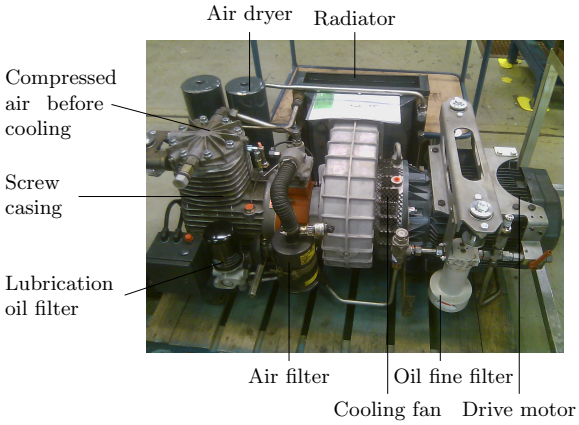


Fig. 1. *A pneumatic compressor.* Air is drawn in from the environment via the air filter and compressed by a set of screws. The compressed air is then cooled, and moisture and oil particulates are removed before the air enters the pneumatic system of the train.

on RCM strategies by studying a typical rolling stock asset (namely a pneumatic compressor, shown in Figure 1) via FMTs.

Fault trees and fault maintenance trees. Fault tree analysis (FTA) [15] is a popular methodology for dependability analysis, and is commonly used in industry. A fault tree (FT) models component failures at the leaves of the tree. Then gates (like AND and OR) show how component failures lead to system failure — indeed not every single failure causes a system failure in a system with redundancy. When the failure rates of the components are known, then FTA can compute the probability for a compound event, typically a system failure.

Traditional FTA is very useful to analyse the reliability of systems when failure rates are given. In practice, however, these failure rates are strongly affected by maintenance, which is not taken into account by fault trees. Thus, FTA is not suitable to compare the performance of different maintenance policies. Moreover, many existing approaches support only exponentially distributed failure times of components.

To overcome these limitations and to determine the effect of different maintenance strategies on system reliability and costs, fault maintenance trees (FMTs) have been developed [11] combining fault trees with arbitrary failure time distributions and *maintenance models*. The latter represent the necessary elements for modelling maintenance: degradation of components, inspections, and repairs. Moreover, FMTs introduce a new gate: the rate dependency (RDEP) gate enables the failure of one component to accelerate the degradation of other components. In this paper, we find that RDEPs are necessary to accurately model the compressor. Certain failure modes, like loss of lubricating oil, severely accelerate failures of components such as motors.

FMT analysis via stochastic and statistical model checking. FMTs are analysed by converting each element of the FMT, i.e. leaf, gate, and maintenance element, into a priced timed automaton (PTA). These automata are then composed to yield a stochastic model of the system, which is analysed using statistical model checking (SMC) [10], a Monte Carlo simulation technique [9] to obtain numerous important dependability metrics, including system reliability, availability, MTTF, expected cost, etc.

A major advantage of our approach is that, in addition to obtaining quantitative results using SMC, we can qualitatively validate the structural correctness of our model using traditional model checking techniques in the UPPAAL tool [6].

The train-bound pneumatic compressor. Many systems on modern trains, such as the brakes and automatic doors, are controlled and powered by compressed air generated by a pneumatic compressor (shown in Figure 1). For example, when the door on a train opens, one often hears a hissing sound. This is the flow of air produced by the compressor. Since the doors and especially the brakes are safety-critical components, a loss of air pressure will leave the train stranded until it can be repaired or towed. it is thus critical to keep the compressor functioning.

The compressor generates compressed air from air in the environment. This air is filtered of dust and particulates, and pushed by motor-driven screws into a high-pressure chamber. The compressed air is then cooled and compressed moisture removed. As the screws are lubricated with oil, small droplets of oil enter the stream of air and also need to be removed. Finally, the compressed air is stored in a high-pressure reservoir to be used in the pneumatically-powered systems. Various safety elements such as pressure valves and temperature sensors ensure the compressor and the systems it powers are not damaged.

Maintenance of this compressor is required to keep it functioning correctly. The compressor contains consumable parts such as filters that need periodic replacements, and other components wear out over time. This maintenance is typical for the railway industry, with periodic replacements and inspections, and different costs for planned and unplanned maintenance. Furthermore, failure costs are high for unscheduled breakdowns during operation.

The compressor is a relevant case study for three reasons: (1) The analysis is useful for NedTrain's internal operations for logistics and maintenance engineering purposes; (2) The failure characteristics of the compressor are well documented through FMEAs, internal documentation and historical failure data; (3) Maintenance on the compressor is performed relatively independent of the rest of the train, as a defective compressor can be replaced by a functioning one from stock. This gives more freedom to optimize the maintenance program.

Modelling and analysis. We have conducted a reliability analysis of a particular model of pneumatic compressor. We analyse the dependability of these compressors, computing the reliability, expected number of failures, and expected number of required unscheduled maintenance events. In particular, we investigate the current maintenance strategy, as well as potentially better strategies. We consider (1) variations in maintenance intervals, and (2) the usefulness of periodic overhauls.

This analysis was conducted together with NedTrain, the company that performs rolling stock maintenance for the Dutch Railways and other train operators. NedTrain is responsible for the maintenance of over 800 trains.

Our analysis finds that performing periodic servicing of the compressor has a major effect on its reliability. The periodic minor overhaul, on the other hand, does not appear to have a strong influence.

Contributions. An important contribution is the demonstration that our method can easily be extended to include system-specific constructs for modelling unusual aspects of the degradation behaviour. Specifically, we included events whose failure rate depends on the state of several other components, and maintenance actions depending on the state of components that are not relevant for the system failure.

Last but not least, we conclude that FMTs are a useful framework to investigate maintenance optimization problems from industrial practice: FMTs are a convenient model, have sufficient expressive power to capture complex maintenance aspects, and are able to produce predictive analysis results.

1.1 Related work

A large number of analysis techniques and extensions for fault trees exist, for an overview we refer the reader to [12]. Current FTA techniques support simple repair strategies by either equipping leaves with repair times [15] or with repair boxes [3]. These techniques consider a BE to be either failed or functioning, while FMTs add support for degraded states and maintenance actions taken depending on the level of degradation.

Extending traditional fault trees, Bucci et al. [4] present a tool that can analyse FTs with non-Markovian failure distributions, which can also be used to analyse component failures due to wear over time. This method, however, does not consider maintenance to undo this wear.

An alternative extension of FTs is the Extended fault tree formalism by Buchacker et al. [5], which can model systems where some components have failure rates that depend on the status of other components. They still model failure times as exponential distributions, and do not include repairs or inspections dependent on full subtrees.

When FTA is not applicable, many techniques exist to analyse and optimize maintenance strategies without using FTA. We refer the reader to reviews such as [1] on the use of simulation techniques or [13] for techniques including analytic approximations and Bayesian reasoning.

One such approach, by Carnevali et al. [7], considers maintenance in phased systems where resources are used in a sequence of tasks, with detection and repair actions in-between these tasks.

If a system consists of a single components or a group of identical components, van Noortwijk and Frangopol [14] consider in detail two models of the effects of various maintenance choices on the reliability and cost in civil infrastructure. Neither of these models consider the failure behaviour of systems of different components.

1.2 Organization of the paper

This paper begins with a description of the pneumatic compressor in Section 2 and the methodology in Section 3. The modelling of the compressor by FMTs is explained in Section 4. Then, Section 5 explains how the FMT is analysed, and provides the results of this analysis. Finally, we provide our conclusions in Section 6.

2 Case description: The pneumatic compressor

Pneumatic compressors (see Figure 1) are devices that produce compressed air. In modern trains, a pipe of compressed air runs throughout the train, and valves control the air pressure to certain installations such as the pantograph (connecting the train to the overhead power line) and automatic doors. The air pressure controls the operation of these installations, as well as providing the necessary power to operate them.

As these compressors are critical to the operation of the train, they are also a potential cause of disruptions. Various types of failures can occur, such as oil leaks and clogged filters. Inspections are performed to determine whether failures are likely to occur soon, and preventive action, such as replacing a nearly-full filter, can be taken to prevent the failure occurring in the field. Some components such as filters are also periodically replaced, since replacing them all in one service is cheaper than spreading the replacements over multiple services when inspections find a problem.

Below, we describe the operation of the compressor, its main failure modes, and the current maintenance plan.

2.1 Purpose and operation

Pneumatic systems have long been used as a control mechanism in trains. Braking systems operated by air pressure date back to 1868 [16], and are still in use today. Although electronics are starting to replace or supplement pneumatic control, modern trains still use pneumatics for emergency brakes and other applications, such as opening and closing doors automatically and raising the pantograph to connect to the overhead electrical line.

Safety-critical pneumatic systems are designed to be fail-safe: A loss of air pressure disrupts functionality, but poses no danger. Brakes, for example, are loosed by high pressure and applied when the pressure drops. A failed compressor, therefore, does not constitute a safety risk. Nonetheless, since a failed compressor leaves the train stranded, such failures cause costly and lengthy disruptions.

To provide high-pressure air for the pneumatics, modern trains use electric compressors. In addition to generating a high pressure, the compressor also clears the air of dust and debris, and removes moisture which could cause corrosion or freezing in pipes and pneumatically-powered devices.

We examine the particular model of compressor used in Dutch VIRM 1/2/3 trains. This compressor operates using rotating screws that take air from the outside and compress it into a pipe. Before reaching the screw, the air first passes through a filter to remove any dust or debris. The screw is lubricated using oil. Due to the relatively high temperatures and airflow, micro-particles of oil are carried in the airflow through the system. To remove this oil, the air passes through two additional filters. Finally, the air is cooled and passed to the pneumatic system.

Several safety features are in place to prevent damage to the compressor or pneumatic systems: Pressure-controlled valves ensure the compressed air does

not reach unsafe pressures, and a temperature switch disables the compressor if the oil temperature gets too high.

2.2 Failure modes

Compressor failures can be divided into two categories: *Complete failures* where the compressor does not operate at all, and *degraded operation* where the compressor does not generate a sufficiently high pressure. For this paper, we consider only failures that prevent the train from operating, meaning complete failure or so much degradation that immediate repair is necessary. Other forms of degraded operation can be analyzed similarly.

Table 1 lists the types of failure that can occur, together with their failure parameters: Each failure mode is characterized by the expected time to failure assuming no maintenance is performed, and the number of degradation phases we consider in our model.

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

Table 1. *Parameters of the failure modes of the compressor.* The failure times of the components follow an Erlang distribution with the indicated number of phases and total expected time to failure (in years) assuming no maintenance is performed. The values have been scaled for anonymity. Failure mode 3 is not strictly a failure, but rather an event that is required for mode 2 to lead to failures. Also failure modes 14 and 15 are not failures, but rather indicators of degradation that are used to initiate maintenance actions, as described in Section 4.

The wear of the compressor screws and the motor and bearings is complicated due to multiple causes. Particles can enter the compressor despite the filter, which causes degradation of the screws. The rate at which particles pass through the filter is significantly increased if the filter is already worn. A second mode of wear is caused by insufficient lubrication of the screws and of the motor. This can be caused by pollution of the oil, or by insufficient oil, or a combination of both.

2.3 Maintenance

The current maintenance policy followed by NedTrain consists of some specific inspections every two days, and scheduled services every three months with a larger service every nine months. A minor overhaul is performed every three years and a major overhauls every six years (for reasons of confidentiality, these times have been scaled with the same factor as the BE failure rates).

The bi-daily inspection is mostly performed at night, while the train is prepared for service. Mechanics check the on-board diagnostic system for recorded events such as overpressure, and perform an inspection to find oil leaks or excessive noise. If this inspection finds a defect, an unscheduled service is necessary to correct it.

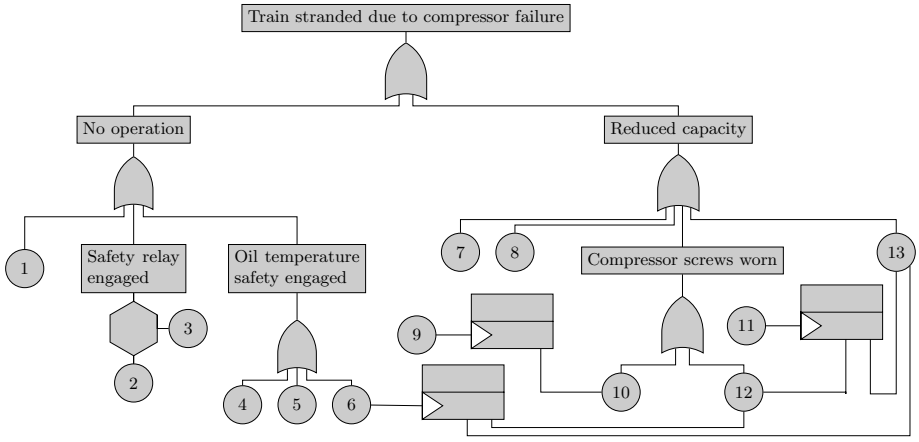


Fig. 2. *Fault Tree describing the major failure modes of the compressor.* The numbers in the basic events correspond to the numbers of the failures modes in Table 1. Failure modes 14 and 15 are not shown, as they do not contribute to the top event.

During the scheduled services, consumable parts such as filters are replaced, and components of the compressor are inspected for signs of wear. Some functional tests of the overall performance of the compressor are also performed, such as measuring the time needed to pressurize the pneumatic system for the entire train starting from atmospheric pressure.

Every three years, the compressor is removed from the train and shipped to NedTrain's component workshop for an overhaul. Minor and major overhauls are alternated. During an overhaul, the compressor is disassembled and all components are examined and replaced if needed. During a minor overhaul components with a small amount of wear are reused. During a major overhaul, all worn components are replaced, and the compressor is considered as good as new afterwards.

Each maintenance action can also lead to more intensive services if problems are found that cannot be corrected during the scheduled service. For example, if a minor service inspection finds that the compressor is not producing sufficient pressure but cannot find the cause, the compressor can be sent in for an overhaul.

3 Methodology

To analyse and optimize the maintenance strategy for the compressor, we have modelled the compressor in terms of fault maintenance trees. Below, we briefly describe the main ingredients of this framework: fault trees, maintenance models, analysis methods, and metrics.

3.1 Fault Trees

Fault trees (FTs) are a graphical method for performing reliability and safety analysis, widely used in industry. An FT models how component failures propagate through a system to lead to system failure, and allows a wide range of qualitative and quantitative properties to be analyzed [15] [12].

FTs are directed acyclic graphs in which the leaves are called *basic events* (BEs) and describe component failures, and internal nodes are called *gates* and describe what combinations of basic events cause compound failures. The gate at the root of the tree is called the *top level event* and typically denotes a system failure or other undesired event.

The gates of standard fault trees are AND-, OR-, and VOT(k)-gates, which fail when all, any, or at least k of their children fail, respectively. The leaves of a traditional continuous-time FT are equipped with exponential failure rates, describing the progression of failure probabilities over time.

Classic fault tree analysis includes techniques to compute the reliability and availability of the system, to find the biggest contributors to system unreliability, and to compute the sensitivity of these metrics to the parameters of the BEs [12].

3.2 Fault maintenance trees

Fault maintenance trees (FMTs) [11] are an extension of FTs that can model several additional contributors to system reliability, such as maintenance through inspections and repairs, degradation of components over time, and situations where one failure causes accelerated wear of another component. The FMT modelling the compressor is shown in Figure 2.

Extended basic events. The BEs in an FMT are more expressive than in standard BEs: Standard BEs generally model only exponential or Weibull distributions of failure times, while FMTs support failures that occur when a component gradually wears out, and where the effect of this wear can be reversed by maintenance actions.

BEs represent the components' failure behaviour over time. A BE can be equipped with multiple phases, representing different stages of degradation. A threshold specifies at which phase an inspection should trigger a maintenance action. The transition time into a next phase can be described by an arbitrary probability distribution, but usually follows an exponential distribution, in which case the total failure behaviour of a BE is described by an Erlang distribution.

RDEP gates. FMTs support all the gates of static and dynamic FTs [8]. Additionally, they include a rate dependency (RDEP) gate, representing dependencies between components leading to accelerated wear. This gate has one input event, and one or more dependent children. When the input event occurs, the failure behaviours of the dependent children are all accelerated by a factor γ, independently specified for each child. When the input is repaired, degradation of the children returns to their normal rates.

Repair and inspection modules. Standard FTs can support relatively simple repair policies using distributions over repair times, or via repair boxes [3]. FMTs enable more advanced maintenance policies via *repair modules* (RM) and *inspection modules* (IM).

An IM describes at what frequency components are inspected as well as the so-called repair threshold. The latter is the (minimal) degradation phase where repairs will be performed. When the repair threshold is reached, the next

inspection will trigger a repair and send a repair request to the RM associated with the IM.

The RM listens for repair requests of specific IMs and initiates the repair or partial replacement of a specific set of BEs. When the RM is invoked, the BEs change their phases to a less degraded phase. Moreover, the RM can invoke a periodic renewal of components, e.g. the replacement of a tire after four years.

IMs and RMs can be combined to model more complex policies, such as periodic replacements or simultaneous repair of a group of components when one fails.

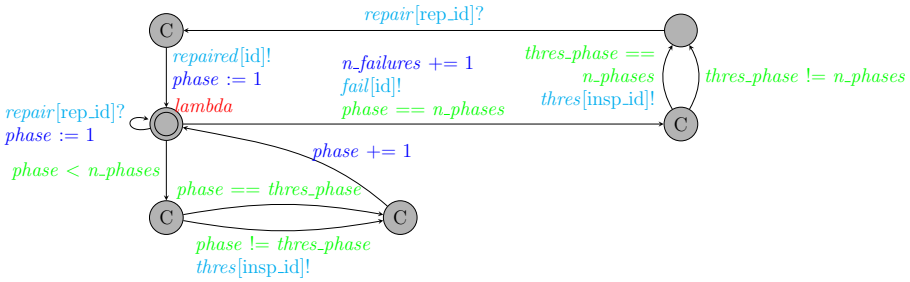


Fig. 3. *PTA of a basic event* with failure time given by an Erlang distribution with *n_phases* phases and a repair threshold at *thres_phase*. From the initial state, the PTA waits an exponentially distributed time with mean *lambda*, and moves downward if it has not yet reached the last phase in the Erlang distribution, or rightward if it has. If it is not in the final phase, it advances by one phase, and it may emit a signal *thres*[insp_id] to a listening inspection module. The BE may also receive a signal *repair*[rep_id] and return the the initial phase. Upon completing the final phase, the failure counter is incremented and a signal *fail*[id] is emitted. A threshold signal may be sent, and then the BE waits to receive a *repair*[rep_id] signal. After receiving this signal, the failed BE emits a signal *repaired*[id], and returns to the initial phase and state.

3.3 Analysis of FMTs by statistical model checking

Technically, FMTs are analysed using statistical model checking of priced timed automata (PTAs) [2]. That is, we first convert the FMTs into a network of PTAs and use the statistical model checker UPPAAL [6] to compute the requested metrics.

PTAs are an extension of timed automata with costs on locations and actions. PTAs are transition systems using real-valued clocks to specify deadlines, with enabling conditions for actions. Costs can be incurred at a fixed amount when taking a transition, or proportional to the time spent in a certain location.

Each element of the FMT (i.e. each BE, IM, RM, and gate) is assigned a unique ID, and a template of the appropriate PTA is instantiated with the specific parameters for the element.The PTAs for the basic event, repair module

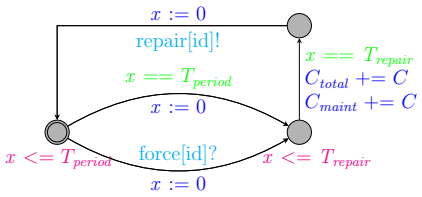


Fig. 4. *PTA for a repair module.* The PTA begins in the leftmost state with clock x initially zero. It waits until either the waiting time for a periodic repair (T_{period}) elapses, or a repair request signal (*force[id]*) is received. In either case, the module waits some time T_{repair}, incurs the C for a repair, sends a signal (*repair[id]*) to any BEs repaired by this module, and resets the timer.

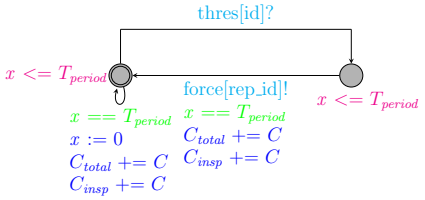


Fig. 5. *PTA for an inspection module.* The PTA begins in the leftmost state, and waits until either the time until the inspection interval (T_{period}) elapses, or a threshold signal (*thres*[id]) is received from a BE. If the time elapses before a signal is received, the inspection cost is incurred and the timer resets. If a threshold signal is received, the module waits for the scheduled inspection time, then signals its associated repair module to begin a repair (*force*[rep_id]), and resets the timer.

and the inspection module are shown in Figures 3, 4, and 5, respectively. The IDs are used to instantiate the synchronization signals.

The PTA is then analyzed using the UPPAAL model checker. This approach has the advantage of allowing both quantitive analysis of the metrics described in Section 3.4 using statistical model checking, and qualitative analysis and validation of the structural correctness of the model using traditional model checking. The latter enables us to check properties of the model such as that every BE can be repaired, that every gate can fail, etc.

Qualitative checks require state-space exploration of the model, which leads to exponential time-complexity as the number of FMT elements increases. Fortunately, the statistical model checker does not need to generate the full state-space, and thus its computation time is relatively independent of the number of elements, but rather grows with the desired accuracy of the result.

3.4 Metrics

We analyse several aspects of the dependability of the compressor, namely the reliability, expected number of failures, and expected number of unplanned maintenance activities. These can be used to compare different maintenance policies and help in deciding which policy is better, as well as to check that the compressor population will meet its performance requirements under a given policy.

Reliability. The probability of experiencing no system failures within a given time period. We compute the probability that within a certain period, there is never a time where a set of BEs is in a failed state leading to the occurrence of the top level event of the FMT. In LTL, we annotate the state corresponding to

the failure of the top-level event as *failed*, and express the reliability within time t as $P(\diamond^{\leq t} \mathit{failed})$.

The term *unreliability* denotes the probability that at least one failure occurs in the time of interest.

Expected number of failures. We compute the expected number of occurrences of the top event within a given time window. Since the compressor can always be repaired after a failure, there can be multiple failures over time. We can also compute the number of failures of individual components or subtrees of the FMT.

Expected number of unplanned maintenance activities. We compute the expected number of times that an inspection finds a defect that is not corrected during the normal maintenance procedure. In the case of the compressor, this occurs for any failure found during the bi-daily inspection, or at certain levels of degradation of components during servicing. These cases require a repair to be scheduled in the maintenance depot or overhaul facility. During an overhaul, all repairs are considered part of planned maintenance.

4 Modelling of the compressor

The fault tree and maintenance plan described in Section 2 were constructed by the research department of NedTrain.

Based on documentation of failure characteristics and expert opinions of system engineers and mechanics, the structure of the FMT was constructed. The resulting FMT is displayed in Figure 2. As described in Section 2.2, compressor failures are divided into complete failures and reduced capacity. This division helps validate the model, since these categories of failures are easy to distinguish in a practical fault condition.

	State BE 6			
State BE 11	0	1	2	3
0	1	2	4	6
1	2	4	6	10
2	4	6	10	15
3	6	10	15	30

Table 2. *Specification of the acceleration factor of BEs 12 and 13*, depending on the states of BEs 6 and 11. The non-degraded state is state 0, the failed state is state 3.

While modeling the compressor, it was noted that several failure modes are related to each other, such as degradation of the air filter leading to increased wear of the screws. While it is possible to model these independently as 'particle-induced wear under normal condition' and 'particle-induced wear with ruptured filter' (since a degraded air filter is not by itself a cause of failure), this leads to difficulty when describing the maintenance policy. The RDEP gates offer a much more natural description of a single BE with degradation that is accelerated by another BE. For BEs 12 and 13, special variants are used that capture the simultaneous but non-linear accelerating effects of BEs 6 and 11. Table 2 specified how much the affected BEs are accelerated depending on the states of the triggering BEs.

Quantitative parameters on degradation patterns and parameters were estimated based on interviews with maintenance engineers responsible for the maintenance plan and system engineers specialized in pneumatics, as well as

experiment reports of a simulation environment where compressors can be tested.

While FMTs support arbitrary failure time distributions, determining the exact distribution of each BE was beyond the scope of this case study. Instead, we have modeled the BEs as exponential distributions or Erlang distributions with few phases, as these overestimate the number of failures in the relatively short times between maintenance actions. Due to the very high cost of failure compared to maintenance, relying on a conservative model and performing more maintenance than required is preferable to using an optimistic models and experiencing more failures in the field.

While describing the maintenance policy, we found two properties of the system that are used in maintenance scheduling (BEs 14 and 15), which are in fact complex properties influenced by the degradation of most basic events. Since the exact effect is too complex to include in the model, we instead treat these as basic events that do not contribute to the top level event but are included in the maintenance policy.

Another behaviour that was not included in the model is the low oil level, which can be accelerated by oil leaks in several components. Since it is unlikely that multiple such leaks occur at the same time, we instead chose to model the oil pressure as a single BE.

The parameters of the BEs are listed in Table 1. The failure rates were obtained by consultation with experts within NedTrain, specifically system engineers and mechanics, to include both theoretical estimates and practical information. The estimates were further informed by experiments conducted at the overhaul facility operating a compressor in a simulated environment.

4.1 Maintenance modelling

We compare the dependability and costs of compressors subject to different maintenance policies. This allows us both to validate the model against actual recorded failures, and to offer suggestions for improvements in the policy that lead to cost savings or increased dependability.

BE	Phase	Maintenance action	Result phase
1	2	M1	1
1	2	O1	1
2	2	O1	1
3	2	Any	1
4	3	M1	2
4	Any	O1	1
5	2	M1	O2
5	2	O1	1
6	Any	M1	1
6	Any	O1	1
7	2	I1	1
7	2	M1	1
8	Any	M1	1
8	Any	O1	1
9	Any	M1	1
9	Any	O1	1
11	3 or 4	M1	1
11	Any	M2	1
11	Any	O1	1
13	2 or 3	M1	1
13	2 or 3	O1	1
14	2	M1	1
14	3	M1	O2
14	Any	O1	1
15	2	M1	O2
15	Any	O1	1

Legend

I1	bi-daily inspection
M1	three-monthly maintenance
M2	nine-monthly maintenance
O1	minor overhaul
O2	major overhaul

Table 3. *Maintenance description for the compressor.* Given a BE, a phase of degradation, and a maintenance action, the table lists the effect of that action on the degradation of the BE. I.e. the last column lists the phase to which the BE moves when the given action is performed while the BE is in the listed phase. If the top event occurs, and after some maintenance actions denoted with result 'O2', a large overhaul is immediately performed resetting all components to their undegraded state.

NedTrain has specified the current maintenance policy, which is based on a balance between performance, risks, and costs. The specification of this policy consists of the frequency with which each maintenance action must be performed, and for each BE and degradation level the effect of the action.

In the FMT, inspection modules describe the inspection rates and the threshold at which corrective action is performed. Different BEs have different thresholds, depending on the visibility of the degradation of a component and the importance of correction.

Most maintenance actions return various components to the undegraded state if they are found in a certain degraded state. This is modelled using separate inspection and repair modules for the different BEs. For example, as shown in Table 3, an inspection module inspects BE 11 every month checking whether it has reached phase 3 and if so, repairs it. Some repair actions, in particular the major overhaul, are initiated when other maintenance actions find excess wear. In this case, the BE is modified to have multiple inspection thresholds for different inspection modules.

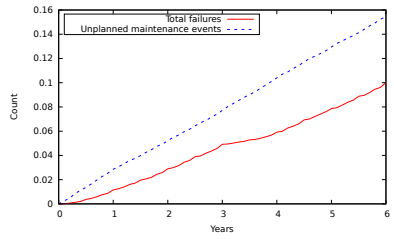
The current model makes a few assumptions: First, we assume that all maintenance is carried out exactly on schedule. In practice, maintenance actions with scheduled intervals greater than one month are sometimes performed in the last 10 - 20% of the interval, to optimise allocation of resources. Since the fluctuations in inspection times are small compared to the inspection interval and do not occur often, we expect this assumption not to significantly distort the results.

We also assume that inspections are perfect, i.e. an inspection always leads to a repair if the degradation level is past the threshold. While this may seem questionable, we argue that the actual inspections are performed well enough that this is not a significant source of error in the model. Moreover, we assume that repairs occur instantly. Since the degradation rates already factor in that the compressor is not in use all the time, we consider it reasonable to also factor in the relatively short time spent in repair.

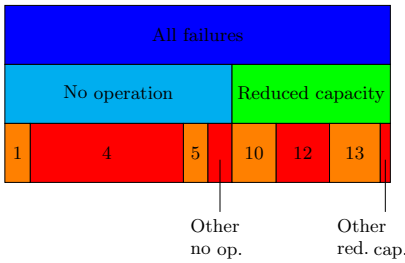
5 Analysis and results

In this section we describe the results of several experiments we conducted on the FMT of the compressor. As a first step, we have validated the FMT using the current maintenance policy against observations from the field. Therefore, we used the model as constructed, i.e. we analysed the compressor under the current policy. Since we concluded that the model is in line with our expectations based on failure data, we continued with finding possible improvements of the current policy. Therefore, the maintenance strategy within the FMT was modified by changing inspection frequencies and replacements. This led to a description of how an optimal maintenance strategy of the compressor can be constructed.

Note that the results in this section are averages of 40,000 simulation runs each. The variance between the simulation runs is low enough that a 95% confidence interval around the mean results has a width of less than 5% of the

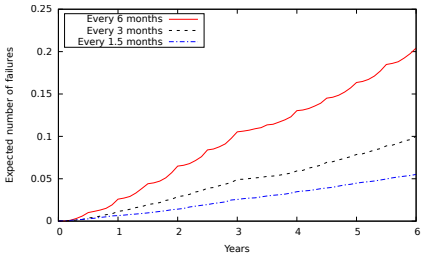


(a) Number of compressor failures and unplanned maintenance events over time. Note that each failure also causes unplanned maintenance, but these are not included here.

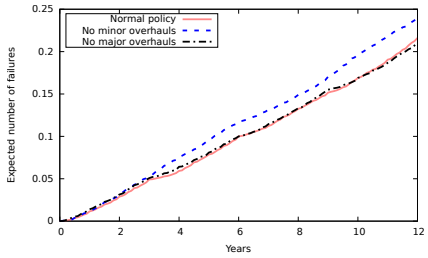


(b) Breakdown of the failures of the compressor by cause. The numbers in the bottom row correspond to the failure causes in Table 1.

Fig. 6. *Results for the compressor under the current maintenance policy.*



(a) Effect of different frequencies of the small service.



(b) Effect of the minor and major overhauls.

Fig. 7. *Expected number of failures for variations on the maintenance policy.*

indicated value, both with the original and the anonymized values. The analysis required approx. 6 CPU-hours per model on an Intel Opteron 4386.

First, we estimate the total failure rate of the compressor over time. We consider NedTrain's fleet of 239 compressors since this model of train began operation in 1994 until 2015. Although a direct comparison with the model is not possible due to long periods of time when compressors are kept unused in a warehouse, the model's prediction is in agreement with NedTrain's estimate of the operational failure rate to within 50%.

Failure cause	**Failure rate**
Motor does not start when asked	0.41
De-aeration valve defective	0.025
Radiator obstructed	2.48
Oil thermostat defective	0.40
Low oil level	0.34
Pressure valve leakage	0.22
Air filter obstructed	0
Particle-induced rupture	0.71
Lubrication-induced wear	0.86
Motor/bearings degraded	0.82

Table 4. *Listing of the expected failure rates of different causes of compressor failures.* Values are yearly occurrences in a population of 233 compressors.

A graph of the cumulative number of failures over time is shown in Figure 6a. We observe that the unplanned maintenance events increase almost linearly with time, as they are mostly caused by failures that are not

wear-related, and thus occur with exponentially distributed failure times. We only consider the interval between two major overhauls, since the compressor is expected to be as good as new after a major overhaul.

Other maintenance policies. To examine the leading causes of failures, the expected number of occurrences of each failure mode per year was estimated. Table 4 shows the annual number of expected failures, averaged over the six-year period between major overhauls. A graphical breakdown of the causes of failures is displayed in Figure 6b. We see that the failure mode 'radiator obstructed' is by far the leading cause of failure. The current maintenance policy for the radiator is to remove large obstructions when found during visual inspections, and more thoroughly clean it during larger maintenance operations. Our analysis suggests that more frequent cleaning may cheaply reduce failures, although we note that these failures are also usually quickly and cheaply resolved when they do occur.

Next, we consider two possible variations to the maintenance policy: Figure 7a shows the number of failures over time for different frequencies of the minor service. We find that this service has a significant effect on the expected failure rate. It is therefore useful to carefully examine the costs associated with this service, to find an optimal balance between servicing and failure costs.

We also consider the possibility of omitting the minor overhaul after three years, and of omitting the major overhaul after twelve years (instead performing a minor overhaul at this time). The effects of which are graphed in Figure 7b. After six years, the minor overhaul has prevented approx. 0.02 failures per compressor. This suggests that the overhaul may not be cost-effective, although this depends strongly on the relative costs of the overhaul and the failure. Furthermore, the effects of replacing the major overhaul by a minor one are too small to be measured by our approach, offering a further possibility for cost savings. We do note, that although we have no indications that the degradation behaviour will be noticeably different after six years, we do not have the data to prove that nonlinear effects such as metal fatigue will not cause more unexpected failures.

6 Conclusion

We have modelled and analysed several maintenance policies for the compressor via fault maintenance trees. We conclude that FMTs are a useful tool for maintenance analysis and optimization. In particular, the modelling process is not too difficult, and the analysis provides useful insights. Obtaining correct failure rates and degradation data from the field required additional effort, but was also feasible in practice.

We obtain dependability estimates for the compressor, which maintenance planners can use in combination with known costs of maintenance and effects of failures to determine which plan results in the lowest cost with optimal effectiveness.

Future work includes the extension of FMTs with continuous degradation phases, models that take into account specific conditions and usage scenarios that influence degradation. We would further like to explore how to convert the per-compressor failure estimates into per-train estimates, given that compressors are

commonly swapped between trains or left in storage for extended periods of time. Finally, we would like to extend FMTs to include imperfect maintenance, such as inspections that have some probability of not detecting a degraded component.

Acknowledgements

This work has been supported by STW and ProRail under the project ArRangeer (122238), the EU FP7 project TREsPASS (318003), and the NWO project BEAT (612.001.303).

References

1. A. Alrabghi and A. Tiwari. State of the art in simulation-based optimisation for maintenance systems. *Computers & Industrial Engineering*, 82:167 – 182, 2015.
2. G. Behrmann, K. G. Larsen, and J. I. Rasmussen. Priced timed automata: Algorithms and applications. In *Formal Methods for Components and Objects*, volume 3657 of *LNCS*, pages 162 – 182, 2005.
3. A. Bobbio and D. Codetta-Raiteri. Parametric fault trees with dynamic gates and repair boxes. In *Proc. Reliability and Maintainability Symp.*, pages 459–465, 2004.
4. G. Bucci, L. Carnevali, and E. Vicario. A tool supporting evaluation of non-markovian fault trees. In *Proc. 5th Int. Conf. on Quantitative Evaluation of Systems (QEST)*, pages 115–116, September 2008.
5. K. Buchacker. Modeling with extended fault trees. In *Proc. 5th IEEE Int. Symp. High Assurance Systems Engineering (HASE)*, pages 238–246, 2000.
6. P. Bulychev, A. David, K. G. Larsen, M. Mikučionis, D. B. Poulsen, A. Legay, and Z. Wang. UPPAAL-SMC: Statistical model checking for priced timed automata. In *Proc. 10th workshop on Quantitative Aspects of Programming Languages*, 2012.
7. L. Carnevali, M. Paolieri, K. Tadano, and E. Vicario. Towards the quantitative evaluation of phased maintenance procedures using non-markovian regenerative analysis. In *Proc. 10th European Performance Engineering Workshop (EPEW)*, volume 8168 of *LNCS*, pages 176–190, September 2013.
8. J. B. Dugan, S. J. Bavuso, and M. A. Boyd. Fault trees and sequence dependencies. In *Proc. Reliability and Maintainability Symp.*, pages 286–293, 1990.
9. G. Fishman. *Monte Carlo: Concepts, Algorithms, and Applications*. Springer, 1996.
10. A. Legay, B. Delahare, and S. Bensalem. Statistical model checking: An overview. In *Proc. 1st Int. Conf. on Runtime Verification (RV)*, volume 6418 of *LNCS*, pages 122–135, November 2010.
11. E. Ruijters, D. Guck, P. Drolenga, and M. Stoelinga. Fault maintenance trees: reliability centered maintenance via statistical model checking. In *Proc. Reliability and Maintainability Symp.*, January 2016.
12. E. Ruijters and M. Stoelinga. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer Science Review*, 15–16:29–62, 2015.
13. A. Sharma, G. S. Yadava, and S. G. Deshmukh. A literature review and future perspectives on maintenance optimization. *Journal of Quality in Maintenance Engineering*, 17(1):5–25, 2011.
14. J. M. van Noortwijk and D. M. Frangopol. Two probabilistic life-cycle maintenance models for deteriorating civil infrastructures. *Probabilistic Engineering Mechanics*, 19(4):345–359, October 2004.
15. W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. *Fault Tree Handbook*. Office of Nuclear Regulatory Reasearch, U.S. Nuclear Regulatory Commision, 1981.
16. G. Westinghouse. Improvement in steam-power-brake devices, 1869. US Patent 88,929.