View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Nottingham ePrints

Vileiniskis, Marius and Remenyte-Prescott, Rasa (2016) Extended Bow-Tie model for asset risk and reliability modeling: application to a passenger lift. In: ESREL 2016, 25-29 Sept 2016, Glasgow, UK.

Access from the University of Nottingham repository:
http://eprints.nottingham.ac.uk/34547/1/Extended%20Bow%20-%20Tie%20model%20for%20asset%20risk%20and%20reliability%20modelling%20%20Application%20to%20a%20passenger%20lift%20.pdf

Copyright and reuse:

The Nottingham ePrints service makes this work by researchers of the University of Nottingham available open access under the following conditions.

This article is made available under the University of Nottingham End User licence and may be reused according to the conditions of the licence. For more details see: http://eprints.nottingham.ac.uk/end_user_agreement.pdf

A note on versions:

The version presented here may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher's version. Please see the repository url above for details on accessing the published version and note that access may require a subscription.

For more information, please contact eprints@nottingham.ac.uk

Extended Bow-Tie model for asset risk and reliability modelling. Application to a passenger lift

M. Vileiniskis & R. Remenyte-Prescott
Centre for Risk and Reliability Engineering, University of Nottingham, Nottingham, United Kingdom

ABSTRACT: A risk and reliability modelling framework for railway assets based on the Petri Net and the Bow-Tie models is proposed in this paper. A Petri Net model together with the Monte Carlo simulation is used to replicate the projected operational usage of the asset, inspection and maintenance policies and degradation of the asset and to estimate the future condition of the asset over time. Statistics obtained from the Petri Net are used as inputs to the Bow-Tie model, which is then used to estimate the risk of a hazardous event. The paper reports on the proposed methodology and the results of a case study of an underground passenger lift. In particular, the likelihood and the consequences of a lift getting stuck in shaft between landings are calculated.

1 INTRODUCTION

Quantitative risk assessment is a key in understanding the underlying risks in the operation of the asset. Results obtained from such analysis can help engineers to improve the design of the asset, to choose a maintenance schedule in order to minimise the risk or to justify that the risk has been reduced to the ALARP level, for example, as required by the regulators in railway industry (Office of Rail Regulations, 2015).

Cause and effect models have been increasingly used in railway industry to estimate the underlying risks in railway operations. For example, a Bow-Tie model, which is the state-of-the-art method to assess the risks quantitatively, is used by London Underground and Railway Safety and Standards Board to develop safety risk models (Taig & Hunt, 2012).

The Bow-Tie model is comprised of fault and event trees, where a number of hazardous events are considered as top events in the fault trees and initiating events in the event trees. In the Bow-Tie model, probabilities (or frequencies) of basic event occurrence are obtained from generic asset failure data (Muttram, 2002, Turner et al., 2002, Taig & Hunt, 2012).

Distinct features of the asset, such as the condition of the asset and its individual components, the planned operational usage, inspection and maintenance policies, can have a significant impact on risk assessment. Currently such features cannot be included in the Bow-Tie model, and therefore the analysis can be limited. The methodology proposed in this paper focuses on how such features can be taken into account by developing a simulation model for the operation and maintenance of the asset. Detailed information about the condition of the asset, its maintenance and operation can be used to simulate the outcomes and use the results, such as the frequency of failures in risk assessment. This paper demonstrates the proposed methodology and its illustration to a case study.

2 PROPOSED METHODOLOGY

The proposed methodology is based on the development of a Petri Net model, its simulation and the incorporation of the gathered statistics in the Bow-Tie model. The Petri Net model is built considering the condition and the deterioration of the asset and its components, the operation and the maintenance activities. The Bow-Tie model is then used to take account of the results of the Petri Net simulation in risk assessment. In this way, distinct features of assets and information about the condition of the asset can be taken into account when using a well-known approach of the Bow-Tie model to assess risks due to asset performance.

The main steps of the methodology are presented in the following sections.

2.1 *Main steps of the methodology*

1 The first step is to gather and analyse the information available about an asset, such as the de-

scription, failure and maintenance records, patterns of operational usage. Such information is also needed for the components of the asset.

2 The second step is to build a Bow-Tie model for a hazardous event, consisting of a fault tree and an event tree.

3 The third step is to build a Petri Net model using the asset information obtained in the first step, as well as considering what outputs are going to be necessary for the Bow-Tie model, developed in the second step. The Petri Net model can describe the following features: the daily operation, degradation, spurious failures, inspection and maintenance regimes and the related human errors.

4 Once a Petri Net model is built, it is simulated using the Monte Carlo simulation technique to obtain the predictions about the performance, such as the frequency of component failures.

5 The outputs of the Petri Net model are then plugged into the Bow-Tie model to get risk estimates of the chosen hazardous event.

This paper focuses on the steps of the Petri Net development (step 3), therefore, other steps of the methodology are explained briefly. A short description of Petri Net is given below.

2.2 *Petri Net*

A Petri Net (PN) model provides a graphical representation of dynamic processes in a discrete event simulation framework. The original concept of the PN developed by Carl Petri (Schneeweiss, 2004) is a directed graph with two types of nodes, called places and transitions. These nodes are linked by directional arcs.

A place in the PN can be marked with a token and it usually represents a particular state or condition of the system. The tokens can move from one place to another in a PN through the use of transitions to mimic the change of the state.

The transition is enabled when all input places to the transition contain the amount of tokens that is equal to the multiplicity of the arc (usually the multiplicity is one, but a higher multiplicity can also be considered). Note that an inhibitor arc can prevent the transition to be enabled. These arcs are represented with an empty circle at the end of the arc.

Once the transition is enabled, a delay time is generated (from a distribution assigned to that particular transition) that has to run out before the transition is fired. Note that this delay time can also be constant, as well as zero.

After the transition fires, a token (or multiple tokens, depending on the multiplicity of the arc) is removed from each input place and one token (or multiple tokens, depending on the multiplicity of the arc) is deposited to each output place. This way the changing state of the system can be modelled through discrete events to capture its dynamics.

Several specific arcs and transitions are used in this study and they are discussed next.

2.2.1 *Reset transition*

When a reset transition (Andrews, 2013) fires, it resets the number of tokens in the selected places. It is represented by a rectangle with leaning line patterned fill, e.g. transitions T63 and T65 in Figure 9.

2.2.2 *Decision making transition*

When a decision making transition (Prescott & Andrews, 2013) fires, it adjusts the amount of tokens in the selected places, if the chosen conditions are true. It is represented by a rectangle with rounded edges, e.g. transition T64 in Figure 9.

2.2.3 *Probabilistic transition and arcs*

When probabilistic transition (Le & Andrews, 2016) fires, it puts a token to only one of the output places, based on the probability assigned. Output places are connected with probabilistic arcs. Probabilistic transitions are represented by a rectangle with a dashed line, e.g. transition T66 in Figure 10. Probabilistic arcs are represented by an arc ending with a filled square.

A number of PNs are illustrated in the following section.

3 THE METHODOLOGY ILLUSTRATION FOR A PASSENGER LIFT

A passenger lift in an underground station is considered in this illustration. A brief description of a traction lift is given first. Then, the Bow-Tie model for a hazardous event is developed, followed by the Petri Net model. Finally, two scenarios are used to illustrate how the estimate of the risk for a passenger lift depends on the features that are disregarded in the Bow-Tie model.

3.1 *Asset description*

The drive for a lift, shown in Figure 1 is provided by a motor, which operates a gearbox to turn the drive sheave. The suspension ropes are wrapped around the drive sheave and the deflector sheave and they are connected to the counterweight and the lift car. Such arrangement of a lift is referred to as a traction lift. The braking of the lift is provided by a brake unit, which consists of a brake drum and brake pads (with brake linings attached) that are pressed against the brake drum, when braking is applied.

For simplicity, only selected components of the traction lift are considered in this paper, such as motor, brake pads, gearbox, drive sheave and suspension ropes. The other components can also be considered as necessary. Note that, the distributions of failure times necessary to simulate the Petri Net

models are assumed in this study. For example, Exponential distribution was used to model spurious failures, since it has a constant hazard rate (parameter λ of Exponential distribution (Andrews & Moss, 2002)), i.e. the probability of failure does not change with time.

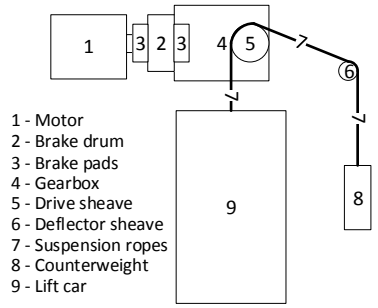

Figure 1. Simplified diagram of a traction lift

3.2 *Bow-Tie model*

A simple Bow-Tie model for a hazard "Lift gets stuck in between landings" is considered. The Bow-Tie model consists of one fault tree and one event tree. The fault tree is presented first.

3.2.1 *Fault tree for the hazard "Lift gets stuck in between landings"*

The hazard "Lift gets stuck in between landings" is considered to occur when the lift is in between landings and the drive for the lift gets cut off. The drive for the lift can be cut off due to a number of reasons, as identified from FMEA (London Underground Ltd (LUL), 2015b):

- Rope slip triggers unintended movement device. In this case study it is considered that this only happens when the drive sheave wears out.
- Lift is over speeding and the overspeed governor is engaged. In this case study it is considered that this happens when either suspension ropes break or brake linings wear out.
- Gearbox fails in operation.
- Motor fails in operation.

The fault tree developed for the considered hazard is given in Figure 2.

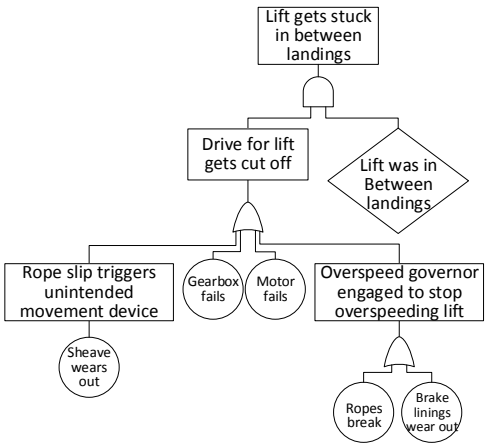

Figure 2. Fault tree with a top event "Lift gets stuck in between landings"

Note that the logic of lift getting stuck in between landings is represented in the system failure Petri Net, which is given in section 3.3.5.

The rare event approximation (Andrews & Moss, 2002) is used to obtain the probability of the top event:

$$P(TOP) \approx P(AB) + P(AC) + P(AD) + P(AE) + P(AF) \quad (1)$$

where A is the event "Lift was in between landings", B – "Drive sheave wears out", C – "Gearbox fails", D – "Motor fails", E – "Suspension ropes break", F – "Brake linings wear out".

Note that the probabilities for minimal cut sets, i.e. P(AB), P(AC), P(AD), P(AE) and P(AF) will be obtained from a Petri Net.

3.2.2 *Event tree for hazard "Lift gets stuck in between landings"*

The Event tree for the hazard considered consists of two events that help to classify the consequences of a lift getting stuck in between landings, as shown in Figure 3. The first event is whether there is a lift engineer present on site to deal with the hazard. The second event is whether there are any people trapped in the lift. Combination of these two events lead to different end states, which are expressed in terms of lost customer hours. Note that the numbers of lost customer hours are only for the illustration and they do not represent the actual consequences.

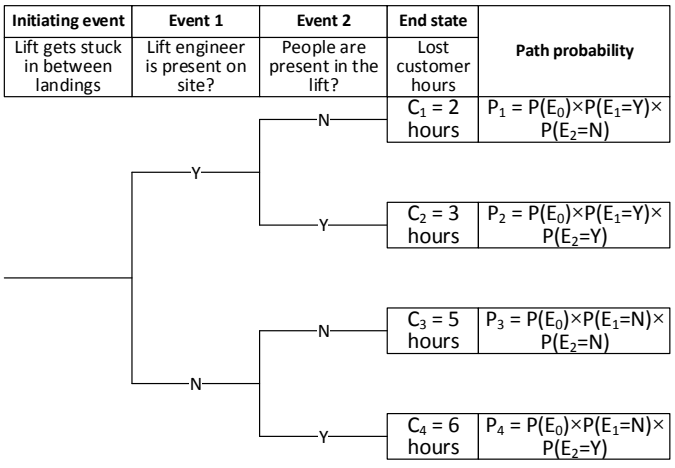

Figure 3. Event tree for the hazard "Lift gets stuck in between landings"

The following notation is used in Figure 3: C_i – consequence of each path i, P_i – path i probability, E_0 is the initiating event, i.e. the hazard, E_j, j=1,2 are events 1 and 2, $E_j = Y$ means that the event E_j is true, $E_j = N$ means that the event E_j is false.

The risk for the individual consequence is calculated by multiplying the value of the consequence (lost customer hours, in this particular case) by a path probability leading to the consequence (Ostrom & Wilhelmsen, 2012). In turn, the collective risk for an initiating event (in this case, the hazard "Lift gets

stuck in between landings") is then simply a sum of risks for the individual consequences:

$$R = \sum_{i=1}^{4} P_i \times C_i \quad (2)$$

where R is the collective risk of the hazardous event "Lift gets stuck in between landings".

Note that the probability for people to be present in the lift will be obtained from Petri Net, while the probability for a lift engineer to be present on site is assumed, as described in Section 3.4.

3.3 *Building Petri Net model*

The Petri Net model is used to describe the following processes:

- Operational usage
- Degradation process and spurious failures of individual components
- Inspection
- Maintenance
- Functional failures
- Human error in inspecting or maintaining the asset

Note that individual PN models are built for each of the processes mentioned above, except for the human error in inspecting or maintaining the system, which is modelled in inspection and maintenance PNs.

All of the individual PN models are then joined into a single PN model. The structure of the resulting PN model is shown in Figure 4. Note that the arrows in Figure 4 indicate the dependencies between the PNs. For example, once a failure occurs in a "Degradation and failure" PN it interacts with "System failure" PN, which in turn interacts with "Inspection" and "Operational" PNs.

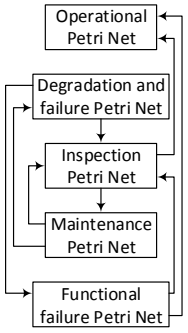

Figure 4. Structure of a Petri Net model for a passenger lift

The individual Petri Nets that are built for each of the processes mentioned above are presented in the following sections.

3.3.1 *Operational Petri Net*

It is assumed that the lift serves two landings: top landing (TL) at the street level, where passengers arrive to the underground station, and the bottom landing (BL) at the platform level, where underground trains are operated. Thus the Petri Net developed has the same structure for each landing, as seen in an almost symmetric Petri Net given in Figure 5.

When the passengers arrive at TL (indicated by place P3), they request the lift (transition T1 fires a token to place P5 and straight back to P3). If the lift is in TL (a token present in place P1) and no passengers are leaving the lift (no tokens in place P11), the passengers waiting at TL can enter the lift (transition T3 fires and puts a token in place P7 and back in place P5, this way enabling transition T5). It takes some time for passengers to board the lift, therefore transition T5 fires after a delay and puts a token in place P15, representing that now there are passengers in the lift. Since the lift is in TL and the passengers called the lift to go to the BL and the passengers are already in the lift, the lift can depart to the BL. This is done by firing transition T9 to put a token in place P9, which then enables transitions T15 and T19. The transition T19 fires instantly and puts a token in place P16 (and back to P9) to indicate that the lift is in between landings. The transition T15 fires after a time lag to indicate that the lift has descended to BL (a token is put in place P2). The passengers can then leave the lift (transition T12 fires and puts a token in place P12, which enables and later fires a token into place P14). This way the journey from TL to BL is completed. If there are passengers already present at the BL they can now board the lift and travel to the TL in the same manner. The process is then continued until there are passengers present.

Note that inhibitor arcs are used here in order to reassure that the lift journey follows the order that it needs to. For example, the transition T3 allowing passengers to board the lift cannot be fired if the passengers from BL just arrived and they need to leave the lift first.

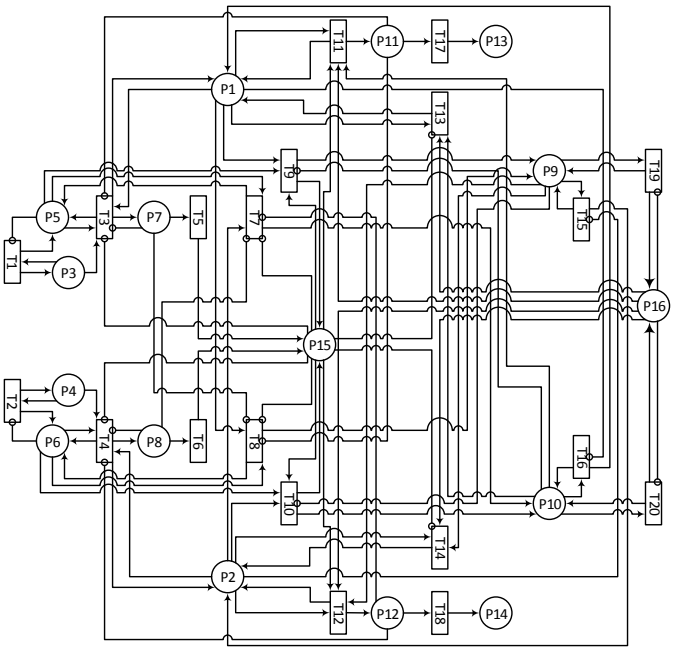

Figure 5. Petri Net to model operational logic of a lift

The flow of passengers, requiring a lift, is modelled in Figure 6.

A token loops through different times of day, for example place P17 represents "Off-peak 05:30 – 06:30", P18 represents "Peak 06:30 – 09:30"). Each transition contains the information of passenger flows at each interval during the day (corresponding to an identified distribution from analysis of London Underground timetables (London Underground Ltd (LUL), 2015c). For example, for the morning peak time (06:30 – 09:30) represented by place P17, transition T21 becomes enabled and it fires at a frequency, modelled with a Normal distribution with mean of 90 seconds and standard deviation of 47 seconds. Therefore the passenger flow is generated to the bottom and top landings (puts a token in places P3 and P4 in Figure 5).

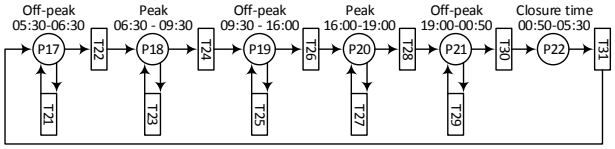

Figure 6. Petri Net to model passenger flow

3.3.2 *Degradation and failure Petri Net for individual components*

London Underground has a list of critical components of the lift (London Underground Ltd (LUL), 2015a), whose condition has to be inspected. These include:

- Gearbox
- Motor
- Brake linings
- Drive sheave
- Suspension ropes

Several states of the critical components are defined by engineers and these are used to build the degradation and failure PN models for the individual components. Different PN models are built for repairable (gearbox, motor) and non-repairable (drive sheave, brake linings, suspension ropes) components.

For example, a gearbox degradation and failure PN model is given in Figure 7. The gearbox can be in one of the following states (each state is represented with a place in the PN):

1 As good as new (P23).
2 Worn with normal noise (P24).
3 Worn with unusual noise (P25).
4 Requires urgent attention (P26).
5 Failed (P27).

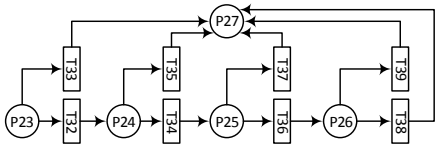

Figure 7. Degradation and failure Petri Net for a gearbox (repairable component)

The gearbox is assumed to be degrading (e.g. bearings are wearing out) over time, for example, going from state 1 to state 2 using transition T32. There is a probability of spurious failure (going straight to state 5 (transitions T33, T35, T37 or T39 firing)), which can occur whilst being in any of the first four states. All of the repairable components are modelled in the same way in the proposed methodology.

The degradation and failure PN model for the drive sheave (refer to Figure 8) differs from the degradation model in Figure 7. The reason behind this is that the drive sheave is a non-repairable component and it actually incurs physical damage throughout the operation. Suspension ropes are looped around the drive sheave and thus the friction between ropes and drive sheave incurs groove wear on the sheave. Thus there is no spurious failure for this component. All of the non-repairable components are modelled in the same way.

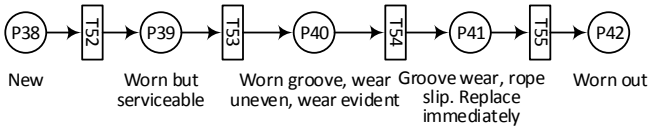

Figure 8. Degradation Petri Net for a drive sheave (non-repairable component)

3.3.3 *Inspection Petri Net*

The inspection PN model for the lift is shown in Figure 9. For each component, whose condition is modelled with the degradation and failure PN, an individual inspection PN model is created. Two types of inspections are modelled in this PN: scheduled inspection (place P48) and emergency inspection (place P54).

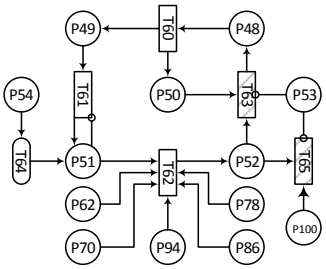

Figure 9. Inspection Petri Net for a lift

When the scheduled inspection starts the transition T60 fires and puts a token in place P49 ("Inspection has to start") and P50 ("Lift has to be out of service, planned") to put the lift out of service and stop passengers from using the lift (the passenger flow to the lift is stopped by inhibiting the transitions (T21, T23, T25, T27 and T29 in Figure 6 in the operational PN model).

The transition T61 fires after a delay, once the engineers have prepared the lift for inspection and the inspection is underway (token is put in place P51). Once all of the components have been inspected (tokens are present in places P62, P70, P78, P86

and P94 representing the end of inspection for each component) the token is put in place P52 to represent that the inspection has finished. Given the findings of the inspection (if there was any maintenance identified, tokens in place P53 are present) the lift can either be put back to service (transition T63 fires, if not inhibited by tokens in place P53), or maintenance is scheduled and lift is kept out of service until all of the failed components have been repaired (or replaced).

When the emergency inspection starts (a token is present in place P54) the transition T64 fires a token to place P51 after a delay (the time it takes for an engineer to start the emergency inspection). Then the inspection follows the same routine as before, only this time the transition T65 is fired, once the lift is put back to operation.

Transition T63 is a reset transition that resets the number of tokens in places representing inspection findings when no maintenance is necessary. Transition T65 resets the number of tokens in the same places as for transition T63 and in addition for the place that represents the scheduling of inspection.

The transition T64 is a decision making transition (Prescott & Andrews, 2013), that adjusts the amount of tokens in the selected places, if the chosen conditions are true. It is used to reset the tokens in the places that represent the fact that the lift got stuck in between the landings and the lift had to be taken to one of the landings and the passengers had to be released.

The PN for the inspection of individual component is built next. Since the inspection PN models for all of the components have identical structure, only a single PN is presented.

The inspection PN model for a gearbox is given in Figure 10.

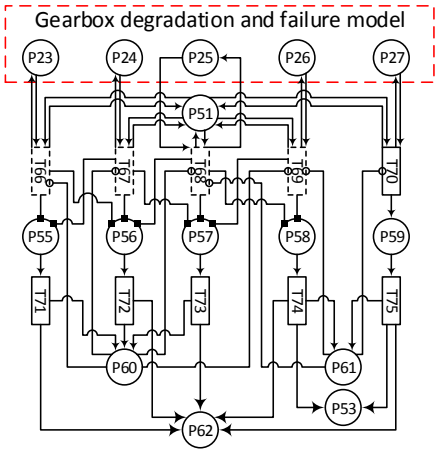

Figure 10. Inspection Petri Net for a gearbox

Once the inspection is underway (a token is in place P51) the condition of the gearbox is identified. The possible revealed conditions of a gearbox (places P55, P56, P57, P58 and P59) are identical to the conditions modelled in the degradation PN (places P23, P24, P25, P26 and P27). The possible revealed conditions are connected to the gearbox degradation and failure model developed previously (refer to Figure 7) through transitions and arcs, as well as probabilistic transitions and probabilistic arcs.

The probabilistic transitions and arcs are used to model human error during the inspection process. The actual condition of the component can be overlooked when performing the inspection. Thus, a probability to incorrectly identify the current condition of the component is considered, except for the failed state, where it is assumed that the failure will be revealed during the inspection.

For example, when the condition of gearbox is "Worn with unusual noise", it is assumed that there is a 98% chance of correctly identifying this particular condition, a 1% chance to misidentify the current condition as a better one ("Worn with usual noise") and a 1% chance to misidentify the condition as a worse one ("Gearbox requires urgent attention").

The resulting findings of inspection for a component then influence the maintenance actions: no maintenance (place P60) or maintenance necessary (place P61). If maintenance is necessary a token is placed in place P53, which counts the number of components that need maintenance. This information is then passed onto the maintenance PN model.

3.3.4 *Maintenance Petri Net*

The maintenance PN is built to model the way the condition of the individual components is restored to a certain health state after maintenance is carried out. A maintenance model for a gearbox is presented in Figure 11.

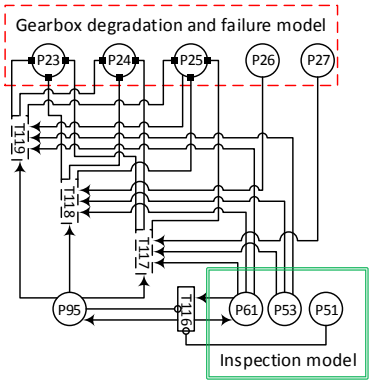

Figure 11. Maintenance Petri Net for a gearbox (repairable component)

Once the need for the maintenance is identified (a token is present in place P61) after the end of inspection (no tokens in place P51), the transition T116 becomes enabled and maintenance of the component is scheduled. After the time to prepare for maintenance has passed, and the transition T116 fires, a token is placed in place P95 to indicate that the maintenance is underway. Depending on the actual condition of the gearbox one of the transitions T117, T118 or T119 is enabled. These probabilistic

transitions have individual probabilities to restore the condition of the component to a certain state. For example, transition T117 has a probability of 0.8 to fire to place P23 (as good as new) and probabilities of 0.1 to fire either to place P24 (worn with normal noise) or P25 (worn with unusual nose). This way, imperfect maintenance can be modelled.

All of the components, such as motor, that are repaired (rather than replaced) during maintenance are modelled in the same way.

A maintenance PN model for non-repairable components is presented next. The difference from previous maintenance model is that there are no probabilistic transitions, i.e. since the component is being replaced rather than repaired or refurbished, the condition of the component is considered to be as good as new after maintenance takes place. Thus the transitions T129, T130 and T131 always fire a token to place P52 (refer to Figure 12). Maintenance PN models for the non-repairable components have an identical structure to the drive sheave maintenance PN model.

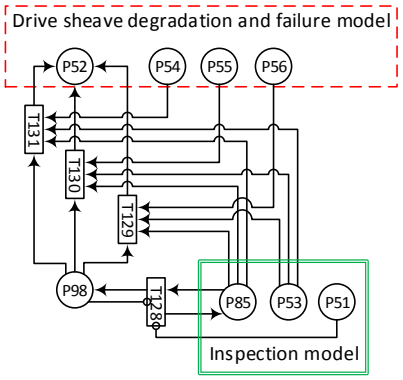

Figure 12. Maintenance Petri Net for a drive sheave (non-repairable component)

3.3.5 *System failure Petri Net*

The system failure Petri Net model, given in Figure 13, simulates the way the hazardous event for a lift can occur using the failure logic provided by the fault tree (refer to section 3.2.1).

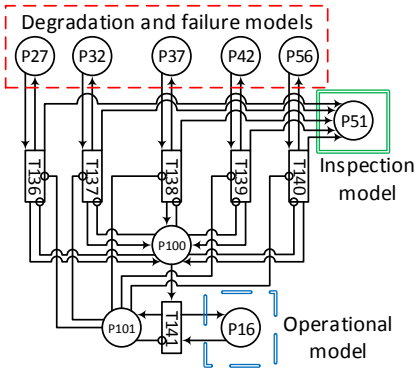

Figure 13. System failure Petri Net for a lift

Any failure of the critical components will put the lift out of service (a token is fired to place P100). If the lift was in between the landings (token is present in place P16), a token is fired into place P101 to indicate that the lift gets stuck in between landings. An emergency inspection is requested (a token is placed in place P54) at the same time as the lift goes out of service. When the lift is out of service the passenger flow to the lift is stopped by inhibiting the transitions (T21, T23, T25, T27 and T29 in Figure 6) in the operational model.

3.4 *Estimating the risk of lift getting stuck in between landings*

The fourth and fifth steps of the proposed methodology are illustrated in this section. Bespoke C++ software with a graphical user interface was developed to perform Monte Carlo simulations. Two scenarios are considered to illustrate how the risk changes based on the asset specific features. In particular, different conditions of individual components are simulated in the PN. The scenarios that are considered for the Monte Carlo simulation are summarised in Table 1.

Table 1. Two scenarios for Monte Carlo simulations

Scenario	#1	#2
Number of simulations	10000	
Start time	05:30	
Duration	30 days	
Frequency of inspection	2 weeks	
Gearbox condition	Worn with normal noise	
Motor condition	Worn with normal noise	
Drive sheave condition	Worn but serviceable	Groove wear
Brake linings condition	Worn but serviceable	
Suspension ropes condition	Worn but serviceable	

The condition of the drive sheave is different in the selected scenarios. The outputs obtained from Monte Carlo simulations (marking of selected places for each simulation) for the fault and event tree are summarised in Table 2. For example, if there were tokens in places P27 and P101, it indicated that the gearbox failed, when the lift was in between landings, thus giving a minimal cut set *AC* for the considered simulation.

Table 2. Outputs for fault and event trees from Monte Carlo simulations for two scenarios

Scenario	#1	#2
Drive sheave wears out, P(*AB*)	0	0.0072
Gearbox fails, P(*AC*)	0.0028	0.0011
Motor fails, P(*AD*)	0.0028	0.0023
Suspension ropes break, P(*AE*)	0	0
Brake linings wear out, P(*AF*)	0	0
People are present in the lift, P($E_2 = Y$)	0.8036	0.8113

Note that the frequencies (as representatives of probabilities) for fault trees are expressed as numbers of occurrences of considered minimal cut sets divided by the total simulation runs. For example, in the 2nd scenario, a minimal cut set *AB* (event *A* – lift

was in between landing and event, token in place P101 in PN, *B* – drive sheave wears out, token in place P56 in PN) has occurred in 72 out of 10000 simulations. Thus the frequency is calculated as P(*AB*) = 72/10000 = 0.0072 / 30 days.

The frequency for an event "People are present in the lift" to be true is obtained by dividing the number of occurrences when people were present in the lift during an initiating event and the number of times the initiating event occurred. For example, for the 1st scenario, people were present in the lift 45 times out of 56, when the lift got stuck, thus the frequency is $45/56 \approx 0.8036$.

The presence of a lift engineer was not modelled in the Petri Net, thus the frequency for a lift engineer to be present at site is assumed to be P(E_1 = *Y*) = 0.75 for both scenarios.

Using the fault tree analysis (see equation (1)), the top event frequency (the initiating event frequency in the event tree) is found as:

$$P\left(TOP_{\#1}\right) \approx 0.0028 + 0.0028 \approx 0.0056 / 30\, days \quad (3)$$

$$P\left(TOP_{\#2}\right) \approx 0.0072 + 0.0011 + 0.0023 \approx 0.0106 / 30\, days \quad (4)$$

where $P(TOP_{\#1})$ and $P(TOP_{\#2})$ is the top event frequency for the first and second scenario, respectively.

The top event frequencies in equations (3) and (4) are fed into the event tree (see Figure 3) and the frequency of occurrence for each path is calculated. The total risk of the hazardous event is then calculated using equation (2) and gives:

$$R_{\#1} = 0.0199\, lost\ customer\ hours / 30\, days \quad (5)$$

$$R_{\#2} = 0.0377\, lost\ customer\ hours / 30\, days \quad (6)$$

where $R_{\#1}$ and $R_{\#2}$ is the total risk for the first and second scenario, respectively.

Even though, the numbers of lost customer hours are artificial, they indicate that the risk of the considered hazard depends on the actual condition of the lift.

4 CONCLUSIONS AND FUTURE WORK

A methodology to extend the Bow-Tie model with a Petri Net simulation model was proposed in this study. Petri Net models are very flexible, thus asset specific features, such as operational usage, degradation process of individual components, inspection and maintenance regime and human error in inspecting or maintaining the asset, are easy to include into the model and were all considered in this study. This way up-to-date information about the asset instead of generic failure rates is used for estimating risk. The proposed methodology was applied to an underground lift and it was shown how asset specific features can impact the estimate of risk.

The proposed methodology can be further developed to take into account different maintenance policies, as only corrective maintenance was modelled so far; include other components of the lift, such as the safety circuit; to account for entering additional evidence in the Petri Net, for example, how much time the component has spent in the current condition; and apply the methodology to other railway assets, such as railway points and underground rolling stock.

ACKNOWLEDGMENT

This work is funded by Innovate UK through project PCIPP: People-Centred Infrastructure for Intelligent, Proactive and Predictive Assets Maintenance with Condition Monitoring. The authors greatly acknowledge the support from Innovate UK and project partners Thales Research & Technology and London Underground.

REFERENCES

ANDREWS, J. 2013. A modelling approach to railway track asset management. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 227, 56-73.

ANDREWS, J. D. & MOSS, T. R. 2002. Reliability and risk assessment / by J.D. Andrews and T.R. Moss, Professional Engineering Publishing.

LE, B. & ANDREWS, J. 2016. Modelling wind turbine degradation and maintenance. Wind Energy, 19, 571-591.

LONDON UNDERGROUND LTD (LUL). 21/01/2015 2015a. RE: Critical component checklist. Type to PCIPP PROJECT PARTNERS.

LONDON UNDERGROUND LTD (LUL). 21/01/2015 2015b. RE: FMEA Traction lift. Type to PCIPP PROJECT PARTNERS.

LONDON UNDERGROUND LTD (LUL). 2015c. Timetables [Online]. Available: https://tfl.gov.uk/travel-information/timetables/ [Accessed 12/11/2015].

MUTTRAM, R. I. 2002. Railway Safety's Safety Risk Model. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 216, 71-79.

OFFICE OF RAIL REGULATIONS 2015. Common Safety Method for risk evaluation and assessment.

OSTROM, L. T. & WILHELMSEN, C. A. 2012. Risk assessment: tools, techniques, and their applications, John Wiley & Sons.

PRESCOTT, D. & ANDREWS, J. 2013. A track ballast maintenance and inspection model for a rail network. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 227, 251-266.

SCHNEEWEISS, W. G. 2004. Petri net picture book, LiLoLe-Verlag GmbH.

TAIG, T. & HUNT, M. 2012. Review of LU and RSSB Safety Risk Models.

TURNER, S., KEELEY, D., GLOSSOP, M. & BROWNLESS, G. 2002. Review of Railway Safety's Safety Risk Model HSL/2002/06.