Rare Event Simulation to Optimise Maintenance Intervals of Safety Critical Redundant Subsystems

Raphael Pfaff[1], Karin Melcher[2], Julian Franzen[3]

[1] *FH Aachen University of Applied Sciences, Aachen, Germany*
pfaff@fh-aachen.de

[2] *FH Aachen University of Applied Sciences, Aachen, Germany*
melcher@fh-aachen.de

[3] *Ruhr-Universität Bochum, Bochum, Germany*
franzen@lps.rub.de

ABSTRACT

In the railway sector, many redundant subsystem structures are applied to increase the safety and availability of the overall railway system. Failures to single paths of these structures occur and are found during routine inspection. Routine inspections are, depending on their type and the equipment location, quite costly and limit the vehicle availablity.

The present paper analyses occurrences based on simulated data resembling field data of a fleet of rail vehicles. The system is analysed statistically to identify the wear mechanisms leading to the failures. Failure data is then used to identify wear models which are consequently used in a Markov Chain (MC) to simulate the probability of multiple path failure.

The failure rate of the overall system is typically expected to be in the range $\left(10^{-9} \cdots 10^{-6}\right)\ \mathrm{h}^{-1}$ due to the safety critical nature of the railway system. For this reason, it is required to apply rare event simulation techniques to the MC simulation in order to limit the number of simulations.

The simulation results are then applied to an optimisation of the inspection routine, which yields an appropriate failure rate for the associated hazards.

1. INTRODUCTION

1.1. Problem setting

A system structure omnipresent in railway vehicles is one using a cold redundancy, i.e. a redundant path in the system structure which is only used as a fallback. Applications of such structure include the connection of individual coaches, e.g. in a multiple unit, in the form of a drawbar with an elastomeric draft gear using a castle nut or the pneumatic fallback level to an otherwise electronic driver's brake valve.

In the drawbar application, there exists a potentially catastrophic outcome in the case of failure of the connection, since typically a connection between the vehicles is available to passengers via some sort of gangway. A failure of the connection may seriously harm or kill one or more persons using the gangway at the time of failure.

However, in both presented applications, a hot or even warm redundancy is not feasible and in the case of the drawbar, the failure of the first level will not even be noticed by any trainborne system. This makes an inspection, typically by human operators, of the connection and the securing elements necessary, a costly and also error prone operation reducing the availability of the rail vehicle.

The failure behaviour of such structures with $n-1$ levels of redundancy may be expressed in the form of a Markov Chain (MC) exhibiting these states:

- S_0 Fully operational system, primary level active
- S_1 System still operational, failure on primary level, secondary level active
- ...
- S_n System failure, no redundancy to recover

Depending on the reliability of the individual subsystems, the transition probabilities between the states $p_{(n)(n+1)}$ can be gained from prior information or observed failures.

1.2. Existing approaches

While the present work uses Monte Carlo Simulations, i.e. repeated simulations of the stochastic behaviour of the system

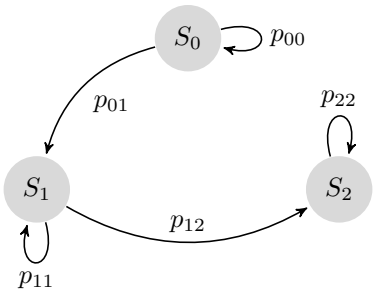

Figure 1. Markov Chain example for a system with $n = 2$

under consideration, in a most efficient way, still a comparably high computational load is exerted on the simulation system. This was impossible before the advent of accessible performant computer systems, thus many existing approaches to simulation of the reliability of redundant subsystems follow an analytical approach.

In (Misra, 1970) or more recently (Azaron, Katagiri, Kato, & Sakawa, 2006), the network structure and reliability functions of the subsystems are analysed analytically to yield an estimate of the mean time to failure (MTTF).

Around the same time, the first steps towards the simulation of rare events in Markov models were made in works of (Bayes, 1972; Kahn & Marshall, 1953)

Another popular approach is the RESTART method (Villen-Altamirano & Villen-Altamirano, 1991), which was later extended to to splitting techniques described in the sequel of this paper.

2. RARE EVENT SIMULATION

2.1. Introduction

Given that the effects of full failures tend to be catastrophic or at least highly disruptive and costly, they are acceptable only at a risk level that does not significantly increase endogenous mortality or is higher than the level accepted for service disruptions, respectively. Such levels tend to be extremely low, typically in the range of $\left(10^{-9} \cdots 10^{-6}\right)\ \mathrm{h}^{-1}$, with the lower level being below the endogenous mortality according to (*EN 50126 - Railway applications - the specification and Demonstraction of Reliability, Availability, Maintainability and Safety (RAMS)*, 2016). In order to estimate the overall failure probability for a given operation scenario, this will require a large number of simulations of the Markov chain, typically in the range of $N = \left(10^{10} \cdots 10^{13}\right)$ iterations in order to estimate the probability with an acceptable uncertainty.

Simulations of this size take a long time and in almost all case yield the result that the system does not fail in the given time frame. In order to make the calculations more efficient while at the same time more reliable, approaches to variance reduction can be employed. These approaches aim to increase the likelihood of the case under investigation for the simulation, thus providing more samples of the investigated outcome. While different approaches exist to such importance sampling (IS), the most effective for MC are splitting techniques.

2.2. Markov Chain splitting

In the sequel, following notations and concepts from (Rubino & Tuffin, 2009), a discrete time MC $X = \{X(t), t \in \mathbb{N}\}$ is assumed with state space E. Further assume $B \subset E$ the critical region, i.e. the subset of the state space representing the critical failure. As discussed above, B is attained at a very low probability. The aim is to compute the probability of the MC reaching state B,

$$\gamma = \mathbb{P}\left[T_B \leq T\right]$$

where $T_B = \inf\left\{t \geq 0 : X(t) \in B\right\}$ and T is a finite stopping time.

The idea of splitting bases on the idea that there exist intermediate subsets (in the case at hand represented by the partly failed states $S_j,\ j \in n$) that are reached more often than the rare subset B, which must be crossed by the sample path on their way towards B and are visited much more often than B.

Despite the application of a splitting algorithm, the step-by-step evolution of the MC is governed by its original probability measure, which makes the application more accessible to general technical personnel than other importance sampling approaches.

Be

$$E \subset B_1 \supset \ldots \supset B_k \supset \ldots \supset B_n = B$$

a decreasing sequence of sets, where the $B_k,\ k < n$ denote the intermediate sets before reaching the critical subset B. Let further

$$T_k = \inf\left\{t \geq 0 :\ X(t) \in B_k\right\}$$

be the entrance time into the region and define the event

$$A_k = \left\{T_k \leq T\right\},\ k = 1, \ldots, n$$

These events also form a decreasing sequence

$$A_1 \supset \ldots \supset A_k \supset \ldots \supset A_n = \left\{T_B \leq T\right\}$$

due to which the product formula

$$\begin{aligned}\mathbb{P}\left[T_B \leq T\right] &= \mathbb{P}\left(A_n\right) = \mathbb{P}\left(A_n \cap \ldots \cap A_k \cap \ldots \cap A_1\right) \\ &= \mathbb{P}\left(A_n | A_{n-1}\right) \cdots \mathbb{P}\left(A_k | A_{k-1}\right) \cdots \mathbb{P}\left(A_2 | A_1\right) \mathbb{P}\left(A_1\right)\end{aligned} \tag{1}$$

holds. Each of these conditional probabilities shall be estimated separately, however following the evolution of the MC.

For this purpose, a population on N_0 trajectories is simulated independently with initial state being S_0, the fully operational state. Of these initial trajectories, a number R_1 reach the first intermediate region B_1 before the maximum time T passes. In this case,

$$\hat{p_1} = \frac{R_1}{N_0}$$

yields an unbiased estimate of

$$\mathbb{P}(A_1) = \mathbb{P}[T_1 \leq T]$$

At this stage, each of the R_1 successful trajectories is cloned N_1 times and the simulation is continued with these. Of these cloned trajectories, again a number R_2 reach the subset B_2 before T is reached and

$$\hat{p_2} = \frac{R_2}{N_1}$$

is an unbiased estimator for

$$\mathbb{P}(A_2|A_1) = \mathbb{P}[T_1 \leq T \,|\, T_1 \leq T]$$

This process is repeated until the critical region $B_n = B$ is reached or the maximum time T is reached.

In this way and with (1), the probability of reaching the critical and rare set B is estimated by help of the transition probabilities to the successive state. The estimator for the probability γ of the rare event

$$\hat{\gamma} = \hat{p_1} \cdots \hat{p_k}$$

is unbiased, as shown in e.g. (L'Ecuyer, Demers, & Tuffin, 2007).

2.3. Implementation strategies

Taking into account that the user is free to select the strategy of selecting and cloning the trajectories, some popular implementation strategies are:

Fixed Splitting implementations assign a fixed number O of offsprings to each successful trajectory, thus rendering $N_k = R_{k-1}O$ a random variable. However this random behaviour yields advantages in the software implementation, as only one entrance level needs to be stored at each level.

Fixed Effort implementations use a total number of offsprings for each level of the simulation, which makes it necessary to run the simulation sequentially for each level.

Fixed success denotes an implementation where offsprings are generated and simulated until a predetermined number of instances reaches the successive state.

Table 1. Simulation results

	$\mathbb{E}(A_2)$	$var(A_2)$
Crude MC	$4.8 \cdot 10^{-6}$	$2.5 \cdot 10^{-3}$
Splitting	$5.15 \cdot 10^{-6}$	$9.5 \cdot 10^{-4}$

2.4. Illustrative example

In order to allow for a comparison between basic MC simulation and Importance Sampling, a fixed splitting implementation is tested in comparison to a crude MC method. The underlying Markov model is as depicted in Figure 1, with a transition matrix

$$P = \begin{pmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{pmatrix} = \begin{pmatrix} 1-10^{-3} & 10^{-3} & 0 \\ 0 & 1-10^{-4} & 10^{-4} \\ 0 & 0 & 1 \end{pmatrix}$$

yielding a rare occurrence of the full failure state S_2 in comparison to the selected MC length.

For the purpose of comparison, the MC implementation with fixed splitting was executed $N = 1000$ times for a discrete Markov process with $M = 100$ samples. The initial number of simulations was $L = 1000$ instances, each successful intermediate outcome (i.e. one attaining S_1) was cloned $O = 1000$ times. Following each instance of the importance sampling variant, a standard MC simulation with the identical number of instances, $L' = L + R_1 O$ was run.

Due to the relative rare occurrence of S_2, 580 out of these 1000 simulations did not reach S_2 at all, the rare failure event was not observed in these simulations. The estimated probabilities for the N runs are given in Table 1, which shows a variance reduction by a factor of 2.7 as well as the usability of the resulting figures. The resulting histograms are depicted in Figure 2.

3. APPLICATION EXAMPLES

3.1. Connection element application

3.1.1. Problem setting

The semi-permanent coupler (SPC) of railway vehicles is typically combined with a gangway, allowing passengers the transfer between two coaches of the consists. For design reasons, there is no opportunity to have redundancy in the coupler function as such, however from field experience as well as mechanical design considerations, one SPC bar is an acceptable solution from a safety perspective.

However in such an arrangement, it is vital that the connecting elements, such as nuts, are securely held in place. In most

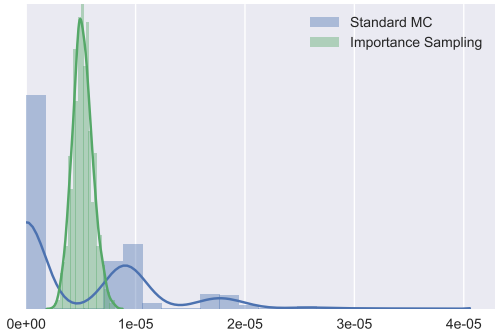

Figure 2. Comparison between standard MC simulation and IS approach using fixed splitting

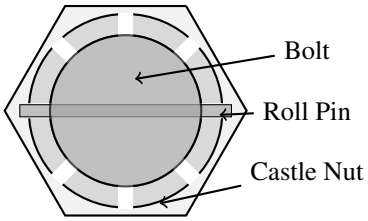

Figure 3. Castle nut and roll pin assembly

designs of SPC, this is achieved by help of a castle nut, which is locked against relative motion by a pin, e.g. a roll pin. A total failure of the securing element would lead to a train separation, which in the case of persons on the gangway may severely injure or kill these.

Owing to the vital role of the securing element, it is part of the routine inspection of the vehicle. According to the European Regulation on entities in charge of maintenance (ECM) (*445/2011/EU: A system of certification of entities in charge of maintenance*, 2011), the maintenance regime of a rail vehicle needs to be constantly adapted following field experience. Among the field experience, there are inevitably failures of the system, in the present example single side failures of the roll pin used for securing the castle nut. Naturally, this raises concerns whether the current inspection regime, a bi-weekly visual check, is sufficient to ensure safety.

3.1.2. System model

It is possible to derive a system structure directly from Figure 3, taking into account that both sides of the roll pin (RP1, RP2 in Figure 4) are not likely to be fully loaded at the same time due to machining tolerances. Obviously, after failure of both sides of the roll pin, there is still sufficient thread (TH) to avoid the catastrophic failure for some time, with respect to the random nature of nut loosening this is not considered in

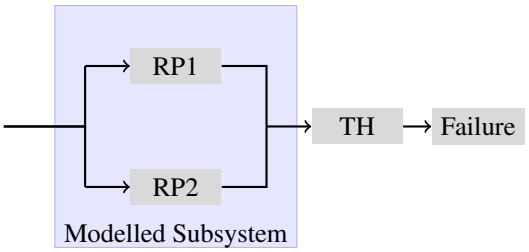

Figure 4. Redundancy structure of the system to be analysed

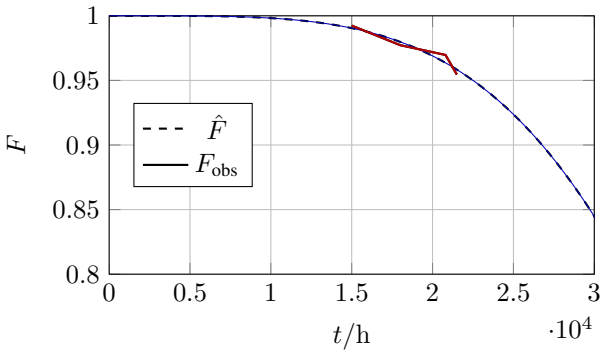

Figure 5. Weibull curve fitting from observed failure data

the safety analysis. The failure mode may thus be considered a precondition for a catastrophic failure of the SPC system.

A total of four single sided failures were reported from the field after several thousands hours of operation of the vehicles, which were analysed by help of a Weibull identification procedure. The identification yields the hazard rate at the current age of the roll pin in service, which is approximately $\lambda_1 = p_{01} = 1.5 \cdot 10^{-5}\,\text{h}^{-1}$. Since the second side of the roll pin is priorly unloaded, the age of the component is reduced, yielding $\lambda_2 = p_{12} = 1 \cdot 10^{-7}\,\text{h}^{-1}$[1].

The system state can, from a safety and reliability perspective, be expressed in these states:

- S_0 All securing elements in place
- S_1 One side of roll pin failed, second side keeps castle nut secured
- S_2 Both sides failed, castle nut no longer secured
- S_3 Loss of castle nut, train separation

3.1.3. Simulation results

An MC simulation was executed with initially $N = 10^7$ simulations and $T = 196\,\text{h}$, relating to the bi-weekly inspection interval and a daily time in service of $14\,\text{h}$. In order to increase the number of realisations of S_2, the preparation for a catastrophic failure, fixed splitting was implemented for the

[1]Data is generated to resemble fielded systems behaviour closely, however the data does not represent any particular vehicle or operator.

final stage of the MC evolution with $N_2 = 10^5$. Implementation was done in Jupyter, using the `numpy.random.rand` random generator to switch between states (Oliphant, 2007).

The algorithm yields $R_2 = 3036$ realisations of the state in question, while the fixed splitting increases the total number of MC runs to $N + N_2 = 3.005 \cdot 10^8$.

The resulting probability of event S_2 is $\gamma_2 = 1.55 \cdot 10^{-10}\,\mathrm{h}^{-1}$, which is well below the accepted risk of $\cdot 10^{-9}\,\mathrm{h}^{-1}$.

An extension of the inspection interval to 30 days can also be simulated, with the resulting probability estimated to be $\gamma_2 = 3.2 \cdot 10^{-10}\,\mathrm{h}^{-1}$, making an extension of the inspection interval safely feasible.

3.2. Drivers' brake valve application

3.2.1. Problem setting

Similar to the first example, a viable case for the application of MC-simulations of Markov processes may also be found in the drivers' brake valve (DBV) system of a rail vehicle. While failures to this system do not lead to catastrophic outcomes, they incur a stop on the line which results in a blocked line and typically delays in the range of hours as well as high penalties by the infrastructure manager.

In order to keep availability high, these systems are also present in a redundant form. Typically in addition to the electronic DBV, a pneumatic or electro-pneumatic backup system is installed on the vehicles. Both are rather complex pneumatical systems and require costly maintenance actions, for which reason it is desirable to lengthen the maintenance interval as much as possible while maintaining the desired overall reliability.

As the DBV system is typically fitted to locomotives, frequently used in freight operations by smaller railway operators, there is a less deterministic schedule of operation. For this reason, the likelihood of a fault occurring within a 30 day interval is investigated.

3.2.2. System model

The system architecture of the DBV system typically comprises

- a brake control unit (BCU),
- the drivers brake valve component (DBV) as well as
- a electro-pneumatic Backup (BU).

in a cold redundancy structure as depicted in Figure 6. The purpose of the system is to convert the setpoint (SP), i.e. the brake command from the driver, to the pressure in the main brake pipe (MP).

This results in a Markov model with the states

- S_0: Normal operation (BCU and DBV)

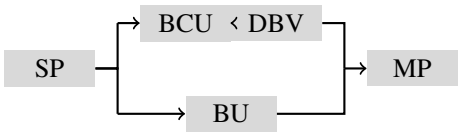

Figure 6. DBV system architecture

Table 2. Time to failure (TTF) for the individual subsystems of the DBV system

#	TTF (DBV)/a	TTF (BCU)/a
1	4.4 a	0.24
2	5.6	0.30
3	5.7	0.35
4	5.7	0.53
5	6.3	2.71
6	6.3	3.08
7	6.7	3.44
8	6.9	3.46
9	7.1	5.05
10	7.6	7.44
11	7.7	-
12	7.8	-
13	7.8	-
14	7.9	-
16	8.0	-

- S_1: Backup operation
- S_2: Failure

and a transition matrix

$$P = \begin{pmatrix} p_{00} & p_{01} & 0 \\ 0 & p_{11} & p_{12} \\ 0 & 0 & p_{22} \end{pmatrix}$$

3.2.3. Simulation results

As a basis for this example serve observed failures of the DBV systems' standard operation level, showing a total of 16 failures for a fleet of 100 vehicles as given in Table 2 over the typical maximum maintenance interval of 8 years. From these observed failures, a recording which is available to virtually any operator, failure rates were estimated using appropriate failure distributions, i.e. a Weibull distribution for the electro-pneumatic DBV portion and an exponential distribution for the BCU. These distributions were used to project the failure rate for the case that the system is operated one more year without maintenance, yielding a hazard rate of $\hat{\lambda}_{\mathrm{DBV}} = 2.6 \cot 10^{-5}\,\mathrm{h}^{-1}$ and $\hat{\lambda}_{\mathrm{BCU}} = 9.5 \cot 10^{-6}\,\mathrm{h}^{-1}$ for the electro-pneumatic and the electronic portion, respectively. Using manufacturer data for the cold redundancy, $\lambda_{\mathrm{BU}} = 10^{-4}\,\mathrm{h}^{-1}$ was assumed.

Based on these transition probabilities, an MC simulation was carried out aiming at estimating the risk of reaching the S_2-fault state within the time interval $[1, 720]\,\mathrm{h}$.

Due to the comparably high hazard rates, $N = 10^5$ together

with fixed splitting and $N_2 = 10^4$ is sufficient to estimate a hazard rate of $\gamma = 1.31 \cdot 10^{-6}\,\mathrm{h}^{-1}$ for the occurrence of S_2. The MC was cloned $N_1 = 2645$ times to reach S_2 in $9.4 \cdot 10^5$ realisations, which can be used for maintenance development in comparison to the associated cost of a stop on line.

4. CONCLUSION AND PERSPECTIVE

An approach to model the behaviour of redundant systems using MC simulations and importance sampling based on observed reliability data was presented and applied to two examples, one resembling observed data from field operation closely. It is possible to derive the risk associated with either an increased inspection interval or an extended maintenance interval and to adapt it accordingly, potentially increasing safety while optimising cost.

While for one subsystem, the extension of maintenance intervals tends to appear economical, for the full system, bundling of activities may be more sensible as discussed in (Pfaff & Schmidt, 2016). It will be of large interest to study the failure risk of a given set of subsystems and to derive the optimum maintenance time for all subsystems under consideration of basic costs of the maintenance delivery function.

Both examples presented in this paper are based on large fleets of vehicles, which is, due to ongoing privatisation in the railway sector, no longer the typical case. For this reason, the authors work on making the techniques used available to operators of smaller fleets. Further steps will include the acceptance of importance sampling by homologation bodies, which currently accept MC simulations for some purposes, however do not mention importance sampling in their regulations.

REFERENCES

445/2011/EU: A system of certification of entities in charge of maintenance. (2011). European Railway Agency.

Azaron, A., Katagiri, H., Kato, K., & Sakawa, M. (2006). Reliability evaluation of multi-component cold-standby redundant systems. *Applied Mathematics and Computation*, *173*(1), 137–149.

Bayes, A. J. (1972, October). A minimum variance sampling technique for simulation models. *J. ACM*, *19*(4), 734–741. doi: 10.1145/321724.321736

En 50126 - railway applications - the specification and demonstraction of reliability, availability, maintainability and safety (rams). (2016). Beuth-Verlag.

Kahn, H., & Marshall, A. W. (1953). Methods of reducing sample size in monte carlo computations. *Journal of the Operations Research Society of America*, *1*(5), 263–278.

L'Ecuyer, P., Demers, V., & Tuffin, B. (2007). Splitting for rare event simulation. *ACM Transactions on Modeling and Computer Simulation*, *17*(2), Article 9.

Misra, K. B. (1970, Nov). An algorithm for the reliability evaluation of redundant networks. *IEEE Transactions on Reliability*, *R-19*(4), 146-151. doi: 10.1109/TR.1970.5216434

Oliphant, T. E. (2007). Python for scientific computing. *Computing in Science & Engineering*, *9*(3).

Pfaff, R., & Schmidt, B. (2016). Daten in der cloud - und dann? *Deine Bahn*(6), 50 – 55.

Rubino, G., & Tuffin, B. (2009). *Rare event simulation using monte carlo methods*. John Wiley & Sons.

Villen-Altamirano, M., & Villen-Altamirano, J. (1991). Restart: A method for accelerating rare event simulation. In *13th int. teletraffic congress, itc 13 (quequing, performance and control in atm)*.

BIOGRAPHIES

Raphael Pfaff was born in Hagen, Germany in 1977. He pursued studies in Mechatronics (FH Bochum, Germany, Dipl.-Ing. (FH) 2006), Mathematics (FeU Hagen, BSc 2007) and Control Engineering (Coventry University, UK, MSc 2006, PhD 2013). He worked with Siemens and Faiveley Transport as System Engineer and Engineering Manager before receiving the call for his current position as Professor of Rail Vehicle Engineering at FH Aachen. His research interests include digitisation of railway rolling stock, reliability engineering and big data usage as well as wheel-rail contact modelling. He is member of the board of Interdisciplinary Railway Research Network (IfV Bahntechnik) and German Rail Engineering Society (DMG) as well as member of German Mathematical Society (DMV). Raphael is cofounder and CEO of RailCrowd.com, a collaborative maintenance data platform for railway operators.

Karin Melcher was born in Vienna, Austria in 1979. After her Diploma in Mathematics at the Technical University in Vienna in 2002 she received her PhD in Computational Finance from HU Berlin in 2006 with a work on the numerical treatment of the Black-Scholes variational inequality. After working in testing and reliability engineering in the engine development department at BMW in Munich, she became a professor for mathematics at FH Aachen University of Applied Science.

Julian Franzen was born in Essen, Germany in 1990. He studied Mechanical Engineering with focus on automation (Ruhr-University Bochum, Germany, MSc 2015). He is currently PhD-Student at Ruhr-University Bochum. His research interest is the field of railway digitalisation, especially the realisation of autonomous driving and proactive maintenance strategies.