Challenge G: An even more competitive and cost efficient railway

Risk-based method to Determine Inspections and Inspection Frequency

Johan van der Werf
Lloyd’s Register Rail Europe BV

Extending inspection periods generally results in a lower level of safety. Using a mathematical model more insight was obtained into the various risks. Based on these insights it was possible to use improvements to the rolling stock to create more efficient inspection schedules while maintaining the same level of safety.

INTRODUCTION

Until recently, the rolling stock of the Dutch Railways was inspected every day. The origin of these inspections lies in old laws and regulations. It described specific inspections and their frequency. The current legislation is more functional. It states that the train operating company (TOC) is responsible for a safe operation. Therefore, it has become possible to optimise the content and the frequency of the inspections (the inspection schedules).

In the safety management system of Dutch Railways it is stated that any changes should not lead to a lower overall level of safety and sufficient effort has to be done to prevent FWSI (Fatalities and Weighted Serious Injuries). For the optimisation of the inspections, these constraints form the boundaries of the optimisation.

In order to determine a new inspection schedule and to be able to prove that the new inspection schedule satisfies these two boundaries, it is necessary to know how the risks change in relation to the inspection frequency. For this, a mathematical model was developed.

This article describes the mathematical model and how this is used to determine the necessary inspections and their frequencies.

MATHEMATICAL MODEL FOR RISK

With a mathematical model we describe the relationship between inspections and their frequency and the risk on FWSI. For this, the failing of the rolling stock is split up in the different ways of failing, e.g. the defect of a break cylinder causes lesser breaking power. For every type of failing a model is set up as shown in the next figure. This model gives the relation between an inspection and his frequency and the number of FWSIs for one type of failure of the rolling stock.

![Image](image.png)

**Figure 1 Mathematical model for the relation between inspections and risk for one type of failure of the rolling stock**

In this model the relation is split up in two parts:

- The first part describes the relationship between the average number of failures of the rolling stock and the number of inspections (both per period). This is called the rolling stock failure model.
- The second part describes the relationship between the average number of FWSIs caused to a certain type of failure of the rolling stock and the average number of failing of the rolling stock. This is called the casualty model.
Challenge G: An even more competitive and cost efficient railway

In the next figure the complete mathematical model that gives the relation between a complete inspection schedule and the total risk on FWSIs is shown.

![Mathematical model for the relation between inspections and total risk](image)

**Modelling failure types**

**System description**

[RCM, 1997] describes how a relation can be found between the frequency of critical failure of a system, the frequency of inspections and the reliability of the components in the system.

The structure of the system determines this relationship. In [RCM, 1997] the relationship was made for a function that is unsafe if it fails and that has a safeguard in place.

The function that is unsafe when it fails we call the primary function. Only unsafe failing of this function is relevant for the risk. Therefore we need the MTBCF of this component/function. Different to the MTBF of a component is that the MTBCF is the average time between two failures of a component that leads to an unsafe situation. The MTBCF of the primary function is represented by $M_{prim}$.

If there is a safeguard, every critical failing of the primary function does not lead to an unsafe situation. If the safeguard always functioning, there will never be an unsafe situation. More realistic is that the safeguard can fail. According to [RCM, 1997] the time between two unsafe failures of the rolling stock is given with:

$$M_{unsafe\_failure} = \frac{M_{prim}}{NA_{safeguard}}$$

With NA the “Non Availability” . E.g.: With the safeguard having a non-availability of 1% the rolling stock fails unsafely with a cycle of 100 times the MTBCF of the component that causes an unsafe situation upon failure.

By keeping the Non Availability of the safeguard small, it is possible to ensure that an unsafe situation does not occur frequently. The safeguard is only necessary if the primary function fails. The safeguard can therefore fail without causing an unsafe situation directly. This function should therefore be inspected.
Challenge G: An even more competitive and cost efficient railway

If the safeguard is defective it is not necessarily noticeable. This is known as a hidden failure. By inspecting the safeguard function more often it is possible to ensure that the time that the safeguard is not available remains sufficiently small. According to [RCM, 1997] the NA can be determined as:

$$NA_{safeguard} = \frac{M_{inspection}}{2 \times M_{safeguard}}$$

With $M_{inspection}$ the time between two inspections and $M_{safeguard}$ the average time between two times critical failure of the safeguard. This gives us the equation that describes the relation between the frequency of unsafe failing and the inspection period.

$$M_{inspection} = \frac{2 \times M_{safeguard} \times M_{prim}}{M_{unsafe\_failure}}$$

From this, it is clear that for such a function the frequency of unsafe failure depends on the frequency of inspections but also on the reliability of the safeguard function.

The above equation only describes one failure type. In [RCM, 1997] more equations are described in the case of redundancy. For creating the risk model this was not sufficient. In the rolling stock we found other types of failing. More than twenty relations were derived. Below a number of examples:

- A component that upon failure directly results in an unsafe situation, the failure of which cannot be determined in advance. In that case the period of unsafe failure is equal to the MTBCF of the component and therefore independent of inspections carried out. Or:

$$M_{unsafe\_failure} = M_{prim}$$

- A component for which it can be determined that it will fail within a certain time. The function is not safeguarded. The period between the moment that the future failure can be determined and the actual failure is called the pf interval ($M_{pf}$). If the inspection interval is smaller than the pf interval, then, if the inspections are carried out correctly, it will always be possible to prevent the rolling stock failing unsafely. The risk here is therefore 0. Applicable for $M_{pf} < M_{control}$ is:

$$M_{inspection} = \frac{M_{pf} \times M_{unsafe\_failure}}{M_{unsafe\_failure} - M_{prim}}$$

- A safeguard that is implemented redundantly but with one part of the safeguard being determined by an MTBCF and the other part determined by NA.

$$M_{inspection} = 2 \times M_{safeguard} \times \left[ \frac{M_{prim} \times (1 - NA_{safeguard}) \times M_{unsafe\_failure}}{1 - NA_{safeguard}^2} \right]$$

Possible Failure Types

It is important that all possible failures of the rolling stock are identified. In order to discover all possible failure types a complete FMEA or RCM analysis must be carried out.

This was not done in our case. For the analysis an existing installation with a given inspection schedule was assumed. Based on these inspections it is possible to indicate which components or functions are being inspected and are therefore relevant to safety. By considering this set of failure types one is considering that part of the risk that is currently covered by inspections.

Possible other failures are also considered because malfunctions of a dangerous nature are reported and registered as safety failures (Safety Management System). By also considering these failures we have considered all failures that realistically can be expected. This is an accepted approach in Risk Based Management.

---

1 Here we talk of $M_{inspection}$. In the RCM literature they talk about the FFI which stands for Fault Finding Interval. We use $M$ here to indicate a period.
Challenge G: An even more competitive and cost efficient railway

Based on inspections carried out under the existing inspection schedule the components or functions that are inspected can:

- upon failure lead to an unsafe situation
- be part of a safeguard that must detect failure of the rolling stock or take over the function.

Functions that upon failure can result in an unsafe situation must be examined to see if there is a safeguard in place for them. If a safeguard is found it must be examined to determine which function is safeguarded and what it does.

By searching for failure types in this way it is possible that failure types are found that were already identified. The intention is that a failure type only be described once.

Functions, both the primary and the safeguard, can also be redundantly implemented. This must be included in the description of the failure type. The following figure is a diagrammatical representation of how different failure types can be determined from an existing inspection list and safety malfunctions.

![Figure 3. Finding the different failure types from an existing inspections and safety malfunctions](image)

**Components and other availability data**

The failure model uses reliability data. The derived or otherwise determined data must be of as high a quality as possible. Data that are necessary are, for example:

- MTBCF values of components ($M_{primary}$ and $M_{safeguard}$).
- PI-intervals ($M_p$)
- Non-Availability data ($NA$) of a function.

Empirical data from the maintainer of the rolling stock have been used here. Data from suppliers can also been used.

In some functions human failure is also a determining factor for the final risk. The question is whether this should be included in determining the risk as we have done here. It concerns mainly the risk from technical failure of the rolling stock, not the failure of, for example, the driver. The calculations therefore determine the risk with a certain inspection schedule with different non-availability for, for example, the driver, (10%, 1% en 0%). The latter is used for situations in which failure of the driver, for example, is not taken into account.

**Casualty Model**

The failure types of the rolling stock that could possibly result in FWSI are examined. For each failure an assessment is made of whether 1 or more FWSIs could occur.

An FWSI will not be the direct result of each failure. If the brakes fail, for example, there are multiple boundary conditions that would need to be present before the failure leads to an FWSI. For example, another train in the vicinity, on the same tracks. That failures do not always result in casualties follows, for example, from the fact that annually about 300 trains ignore red signals, however there have been hardly any FWSIs as a result.
Challenge G: An even more competitive and cost efficient railway

MATHEMATICAL MODEL COSTS vs. RISKS

The risk for an FWSI generally decreases with more frequent inspections. More frequent inspections represent higher costs. In Figure 4 a fictional relationship is laid between inspection costs and the related risk. The horizontal axis shows the annual costs for a certain inspection frequency, the vertical axis shows the risk in FWSI/year.

![Figure 4. Risk as a function of inspection costs.](image)

On the left side of the graph a relatively large reduction in the risk is achieved at very little cost in comparison to the risk reduction on the right hand side of the graph. In order to satisfy the ALARP boundary conditions one needs to go sufficiently far in the graph to the right. The relationships between extra costs and the associated risk reduction is a measure for the amount of extra to prevent an extra FWSI. The costs per FWSI are called $K_{ALARP}$.

$$K_{ALARP} = \frac{\Delta \text{costs}}{\Delta \text{risk}}$$

The total costs consist of labour costs and rolling stock costs. In our case we have only taken labour costs into account. The costs of the rolling stock are the price for the extra rolling stock that is necessary because of the time the inspections need and the rolling stock can not be used.

The costs of a single inspection depend on the duration and rate. The number of inspections per year is determined by the inspection period. This makes it possible to determine the annual costs for a specific inspection.

Using the same failure model for rolling stock and the casualty model from this article it is possible to determine the related risk for a certain inspection period. The extra costs to avoid an extra FWSI can be calculated per failure type using a numerical approximation of the derivative of the costs vs. the risk.

DETERMINING A NEW INSPECTION SCHEDULE

To determine a new inspection schedule, the following steps are taken:

- Writing down which inspections have to be done.
- Calculating the minimum inspection periods to assure that enough is done to prevent FWSIs.
- Check if the new inspection schedule fulfills the stand still requirement.

Inspections to be Carried Out

Inspections are intended to reduce the risk. When creating the mathematical model the inspections that influence the risk were determined. Which inspections affect the risk depends on the type of failure. Depending on the structure of the installation the following inspections affect the risk.

- In systems with safeguards the safeguards must be inspected. The non-availability of the safeguard influences the chance of unsafe failure of the rolling stock. By inspecting more
regularly the non-availability of the safeguard diminishes so that the reliability increases. The safeguard must therefore be inspected.

- In the case of redundancy the availability of the redundant function must be ensured by inspection.
- In the case of a component with a pf interval, this component must be inspected for symptoms indicating failure (wear, heat development, etc).

In order to determine the cost increase for a certain reduction of a certain risk per failure type it is important regarding the inspections to make a good estimate of the required time for carrying out the inspection. In addition one must take multiple inspections into account. Just carrying out a single specific inspection will be inefficient and time consuming.

**Calculating the minimum inspection periods to assure that enough is done to prevent FWSIs.**

To start with this step, the ALARP level has to be given. In “the yellow book” the principle is introduced that companies are obliged to invest in order to prevent accidents with possible casualties.

The first step to come to the minimum inspection frequency is using the ALARP principle. Given a certain ALARP level, the minimum inspection frequency per inspection can be calculated. The system with the minimum level of costs vs. risk gives the ALARP level of all the inspections. When this level is below the required ALARP level, inspections has to be done more frequent. For the inspections with a high ALARP level, the frequency of inspections can be lowered.

The following figure shows how an inspection regime that satisfies the ALARP principle can be determined.

![Figure 5. Determining the inspection periods that complies with the ALARP principle.](image)

**Sufficiently Low Level of Risk (Stand Still)**

The new inspection schedule had to comply with the so-called “stand still” principle. This means that the risk may not increase.

The following figure is a diagrammatic representation of how, using iteration, it is possible to determine inspection periods whereby the total risk is not greater than an acceptable risk (AR).

![Figure 6 Determining inspection periods based on an acceptable risk](image)

For “stand still”, the current risk can be determined using the mathematical model with the inspection periods equal to the current periods. See Figure 7
In the first instance it appears that extending the inspection period based on the “stand still” principle is not possible. After all, increasing an inspection period results in an increase of the risk (barring exceptions). There are three situations that allow lowering the inspection frequency:

- In the new situation the rolling stock has become more reliable for other reasons or
- certain inspections do not impact the risk or
- by carrying out more inspections for high risk and less inspections for low risk a more optimal inspection schedule can be drawn up.

An example of the first possibility is the improvement in reliability of the axle bearings. By introducing the GOTCHA wheel monitoring system, see www.gotchamonitoringsystems.com, the reliability of the axle bearings has improved considerably. The result is that the risk for a defective axle bearing has diminished considerably. The space this has created in the risk has been used to extend the inspection periods. The current situation is therefore defined as the situation before the introduction of GOTCHA.

The current risk is calculated with Figure 7 using the reliability data from prior to the introduction of GOTCHA and the former inspection periods. Using the new reliability figures of the components and the new inspection periods the new risk can be determined.

In the case that risk in the new situation is higher than in the current situation then the inspection interval must be shortened. The following is the procedure:

- Find out which risk is the most sensitive for reduction of the inspection period. Reduce subsequently the daily periods in the following sequence: e.g. 90days – 45days – 30days – 14days – 7days – 2days – 1day.
- Try initially to intensify the inspections that require a lot of time, as little as possible. This would lead to the most increase in inspection time. Only when the impact on the risk makes up for the necessary time could this be worthwhile.

**CONCLUSION**

A risk model that describes the relationship between inspection periods and risks clarifies:

- How the risks are related to each other.
- That many risks hardly increase with an extended inspection period.
- How improvements to the reliability of a component result in a reduction of the risk.
- How the reduction of the risk from the previous point can be used to carry out less inspections while the total risk does not increase.

Using these methods it is possible to derive a number representing risk. This makes it possible to compare various inspection schedules and determine whether they comply with a “stand still” requirement and if sufficient provision has been made to avoid casualties.

**EPILOGUE**

This article describes how a relation can be found between inspection periods and risk. In existing RBM software packages the possibility of including this method in such a package has been sought. It would be a good addition to such programs to include this part (or at least a link to it).
The same modelling can also be used to lay a relation between inspections and for example costs caused by standing still of a train or other installation. This method can therefore be applied to many more areas than just safety.

REFERENCES