Is it safe enough?

Railway risk acceptance in times of fundamental changes.

Jan van Veen MSc

Lloyd's Register Rail Europe

SUMMARY

Railway undertakings worldwide cherish the safe image of rail travel. Serious accidents in the European rail sector are fortunately very rare. The rail system is currently changing rapidly and numerous new and complex techniques are introduced. With increasing complexity, the risk of accidents increases almost exponentially. Identifying the risks involved and, especially deciding whether a risk is acceptable or not, has become of vital importance to the railway undertaking and infrastructure manager. Drafting valid risk acceptance criteria is in itself a daunting task. The question is; when is it safe enough?
This presentation is intended to give context to the subject risk acceptance criteria. Furthermore it gives practical solutions that may help.

INTRODUCTION

Railway undertakings worldwide cherish the safe image of rail travel. The entire organizational structure, sturdy stock, and well-organized processes are aimed to get technical safety at the level of "zero error" Also legislation is heavily focused on "total safety" on the track. Serious accidents in the European rail sector are fortunately very rare.

The absence of serious accidents also has a downside: after such a rare serious accident, we can count on enormous attention from media, politics and law enforcement. Because "zero error" simply does not exist, identifying the risks involved and, especially deciding whether a risk is acceptable or not, has become of vital importance to the railway undertaking and infrastructure manager.

RISKS

The rail system is currently changing rapidly and numerous new techniques are introduced. Just think of all obligations under the various TSI's, the deployment of ERTMS, longer trains, new materials, a higher density on the track. With increasing complexity, the risk of accidents increases almost exponentially.

With risks, one should think about risks occurring with:
• the (train) equipment
• the infrastructure
• the operation of both
• environmental factors
• interfaces between all the above topics

Conducting a risk analysis on a sub-system seems very simple. It is of great importance however, that in this analysis every interaction with the rest of the system is assessed. Recall that the space shuttle Challenger crashed because of one malfunctioning O-ring.

When systems become more complex, Complex Systems Modeling could be a useful tool. The study of complex systems represents a new approach to science, that investigates how relationships between parts give rise to the collective behaviors of a system and how the system inter-acts and forms with its environment. The disadvantage is that this approach by itself is already complex. Therefore, it's likely that we just keep using the good old-fashioned testing. The question remains whether you discover something with a failure rate of say 10^{-6} or 10^{-7} during testing.

It is of the utmost importance that all conceivable risks of the analyzed subject, including all risks that may arise from interactions within the entire system are identified, before you can start answering the question whether a risk is acceptable or not.

RISK ACCEPTANCE CRITERIA

Drafting valid risk acceptance criteria is in itself a daunting task. The question is; when is it safe enough?

Fortunately, our EU legislator gives us guidance by way of the CSM RA[1] methodology. The CSM RA describes in reasonable detail how a risk analysis should be conducted. The use of the CSM RA is mandatory. Whit every conceivable alteration within the rail system, the risks are to be identified and analyzed in accordance with the CMS RA methodology.

Note; an alteration of something existing. The premise is that the current situation is safe.

The methodology prescribes a risk evaluation to determine whether an acceptable level of risk is achieved. This evaluation should take place based on one or more of the following risk acceptance criteria:

- the application of codes of practice
- a comparison with similar systems
- an explicit risk estimation

1 Common Safety Method - Risk Analysis; Regulation EU 352/2009, and per 21-05-2015 Regulation EU 402/2013

The application of codes of practice is the simplest risk acceptance criterion. Regulations, statutory or otherwise, makes life easy. For instance, the necessary braking deceleration of a new train is proscribed by legislation. If the brakes on your new train are able to achieve that deceleration, then the risk is acceptable. No discussion, you don't have to wonder if that is safe enough. Unfortunately, not every conceivable risk is covered by codes of practice.

Comparison to similar existing systems is also a fairly simple risk acceptance criterion. If it already exists and it's widely accepted that it is safe enough, then the risk is acceptable. For example, the platform at a railway station is more or less constructed the same for over more than 170 years.

The explicit risk estimation is somewhat more difficult. First, an appropriate method should be selected that suits the subject to be evaluated. QRA[2], FTA[3], ETA[4], FMEA[5] or FMECA[6] or something else? The trouble in this respect is, that the success of the analysis is determined by the right choice.

For quick and easy determination whether an identified risk is acceptable or not, a so- called "risk matrix" is often used. This matrix can be created by yourself using topics and values which are appropriate for your organization. A guide on how to make and use such a matrix can be found in the EN 50126-1. When you create a risk matrix for your organization, you must of course, keep in mind that you use realistic values. In addition, it should be approved by the Chief Executive of your organization.

Hereinafter, in Figure 1, a very simple example.

Damage	**Injury**	**Environmental damage**
Up to € 50.000	Minor injuries without lost time	Minimal damage to the environment
€ 50.000 – € 150.000	Injuries resulting in absence	Limited damage to the environment
More than € 150.000	Severe injuries / death	Extensive damage to the environment

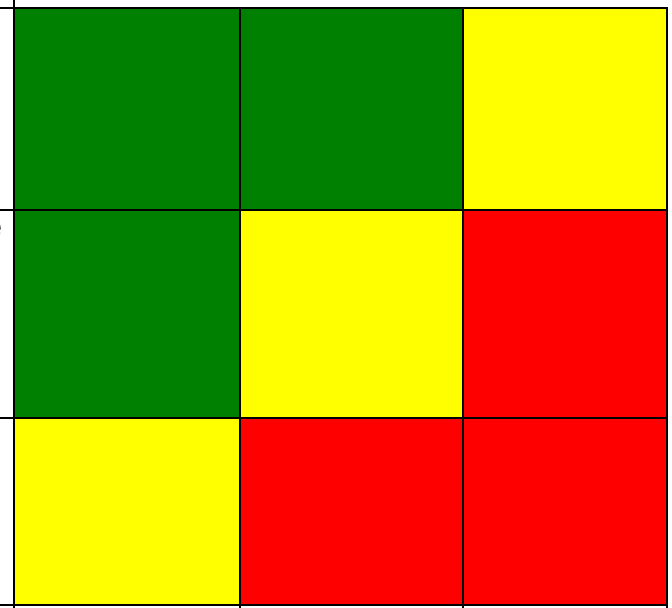

Figure 1; Risk matrix

2 Quantitative Risk Analysis
3 Fault Tree Analysis
4 Event Tree Analysis
5 Faillure Mode and Effects Analysis
6 Faillure Mode, Effects and Criticality Analysis

The color indicates whether the risk is considered acceptable (green), or unacceptable (red). The yellow areas indicate that mitigation of the risk has to be considered, if mitigation is reasonably possible. Usually the cost of the mitigating measures should not outweigh the achievable safety improvement. A common method for this assessment is the ALARP[7] method.

A weakness of the aforementioned risk matrix is that you actually decide on the values in the margins yourself. As a result, it may happen that the very same risk at one organization is considered red (unacceptable), while in another organization it is labeled yellow.

QUANTATIVE APPROACH

In order to prevent before mentioned situation, a quantitative risk analysis is often is chosen. With In this method, the hazard identification is followed by determination of the probability of occurrence for each individual hazard. This determination is usually preformed in a probabilistic manner.

The CSM RA provides the risk acceptance criterion;

"For technical systems where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour". Unfortunately there is no risk acceptance criterion for non-technical systems mentioned. However, in my experience its often easy to use 10^{-9} per X in a risk analysis on a non-technical topic.

This EU provided risk criterion is fortunately quite consistent with the risk acceptance criteria that the Dutch government sets in the "Purple Book" of the series " Colored books" on mandatory risk analysis methods to be used in the external safety domain. For example "Basisnet", the Dutch dangerous goods transportation routes are assessed with the risk acceptance criterion 10^{-9} per exposure hour for the "group risk".

In spite of its strengths, the quantitative risk analysis also has its weaknesses. It's not called the explicit risk estimation for nothing. When the explicit risk estimation is performed on a subject that is totally new and to which no experience exists, there is always a certain risk that things are overlooked which, in retrospect, were extremely relevant. Furthermore, most of the used data would be educated guesses. Unfortunately, a man can only identify risks that he can imagine.

Is it therefore a completely useless exercise? No, definitely not!
It is always good to think about safety, and you have at least a moral obligation to make your design as safe as reasonably possible, A well-conducted risk analysis will absolutely help you do this.

ARE YOU READY?

Anyway, you have done your risk analysis properly, with the right method, you applied the appropriate risk acceptance criteria correctly, you documented the process extensively in such a way that all the necessary evidence is showing the suitability of both the application of the risk management process and of its results. And these are accessible to an assessment body. Is it safe enough now?

The answer is JAEIN, a beautiful word in the German language, which translated means yes and no.

7 As Low As Reasonably Possible

As already pleaded by Murphy; "If it can go wrong, ultimately it will go wrong".
An incident with catastrophic consequence with a chance of occurrence of 10^{-9} will probably not occur during your lifetime, BUT, it is possible that it will happen within the next 10 minutes.

Yes, the measures taken will probably prevent you from being criminally prosecuted. After all, you demonstrably done your best to manage the risk. You have fulfilled your legal duty of care.

No, because the cherished public perception of absolute safety and zero error is violated. When an accident, despite the promise of absolute safety, does occur, then society is "shocked." Administrators and policy makers should act “immediately” to manage the consequences and to formulate policies so that such an incident would "never" occur again. In the end, the way the incident is placed in the media will determine whether administrators, policymakers and management are judged on their “failed” policies[8].

In retrospect everything is much clearer, hindsight has a 20/20 vision..

Is there something we can do about that?
Certainly. With the assumption that you are indeed a conscientious person, and that you took the proper precautions to minimize the risk, it is advised to expand your organizations risk management process with a scenario "What do we do in the unlikely event of a catastrophic accident".

This scenario should contain at least communication strategies and a prepared message to convey. These preparations should prevent a lot of unnecessary reputational damage. Keep in mind, your organization will be judged largely on actions taken AFTER an incident.

CONCLUSION

I apologize, I probably raised more questions than I’ve given answers. Though I hope that I’ve given you some “food for thought”. Now let’s answer the question “Is it safe enough?”

Yes, I genuinely believe Railway systems, at least in Western Europe and at this moment, are safe enough. Just look outside where it’s happening and see for yourself that serious incidents are really very rare.

But with all the fundamental changes we are facing and foremost the increasing complexity of interacting systems, I don’t think that will automatically last. We have to be very careful not to lose the present high safety standard. And that, Ladies and Gentlemen, is our responsibility.

8 Raad voor Maatschappelijke Ontwikkeling (2003), Advies 26 Medialogica.