RISK IDENTIFICATION IN COMPLEX RAILWAY SYSTEMS

Jan van Veen MSc

Sr. Consultant Safety & Risk management

Ricardo Rail

SUMMARY

Railway undertakings worldwide cherish the safe image of rail travel. 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 has become of vital importance to the railway undertaking and infrastructure manager. However, the more complex a system is, the more difficult it is to identify all the risks.

This presentation is intended to give context to the subject risk identification in complex systems. Furthermore it gives a practical solution that may help you.

INTRODUCTION

Mind the gap; everyone who has been in London knows this phrase. It is the gap between the underground train and the platform. And it's been there for decades! If you think about it, is either the platform which was build wrong or the train that was ordered in a wrong size.

In the Netherlands, an extra Doppler radar was mounted on some ERTMS (European Rail Traffic Management System) test trains. Almost forgotten was that these trains also needed their normal maintenance in workshops. Since the on/off switch of these experimental radars was unknown to these mechanics there was a real risk of dangerous non ionizing radiation for the workshop mechanics.

An then there is the story of some kilometers renovated tracks in Belgium. The track was laid perfect on a new foundation. This elevated the tracks several feet. Unfortunately the catenary was not renovated, and during testing they found out that the train didn't fit between catenary and track anymore.

These examples have one thing in common; someone failed to oversee the whole system.

RISK ANALYSIS OF A COMPLEX SYSTEM

Numerous new techniques are introduced in the rail system. Just think of all obligations under the various legislations, the deployment of ERTMS, longer trains, new materials, and a higher density on the track. With increasing complexity, the risk of accidents increases almost exponentially. The rail system consists of the following components:

- the (train) equipment
- the infrastructure
- the operation of both
- environmental factors
- the interfaces between all the above topics

Together they certainly form a complex system, but also the sub-systems can already be seen as very complex indeed.

A complex system is typified by a very large amount of components and factors with a certain degree of mutual interaction, which together form a working system. In order to carry out a risk analysis to such a system, it is very important that all interactions that are useful for the analysis, are identified and assessed.

Recall that the space shuttle Challenger crashed because of one malfunctioning O-ring.

When systems become 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.

So let's focus on something in between; How to conduct a proper risk analysis on a complex system in a low-tech and humanly understandable way.

Step one: The team

If you are brilliant, you can do this alone, lesser mortals usually surround themselves with as many experts in different disciplines as possible. A team of 5 to 10 experts is quite normal. Important is that if you notice a knowledge shortage in the team during the analysis, you have to augment your team with the right knowledge. "We didn't know, so we ignored it" is unacceptable!

Step two: Determine the initial scope

You choose the initial scope of your risk analysis and level of detail you need. If for instance you are assessing a railway station, you might also have to consider the trains that stop at your station, the tracks that lead to your station, the timetables and the general surroundings of your station.

If you are only altering a PCB in a locomotive you probably also have to consider the casing in which the PCB is placed, and perhaps the rest of the locomotive.

If you choose your scope to small you risk missing crucial hazards, if you choose your scope too big, you risk ending up with tons of unnecessary work. Fortunately we humans have a tendency to downsize the problem to a size that we can comprehend, so usually you choose to small. And there is nothing wrong with that, as long as you keep in mind that your initial scope is what it is; Initial! The pit-fall lies in failing to identify the relevant interactions.

Step three: Determine final scope by identifying relevant interactions

With the chosen initial scope your start your analysis. Identify the relevant interactions of your (sub-)system with the rest of the system using the following guide-words:

Hard-ware

People

Surroundings

Procedures

Hard-ware

This is usually the subject you are analyzing, could be something mechanic or electronic, or something else. Small like a bolt or a PCB, big like a complete train or railway station.

What does it do, how does it function, what does it need from the rest of the system, what does it deliver to the rest of the system, how does it connect to the rest of the system, can it influence the rest of the system, can it be influenced by the rest of the system, what happens when it fails?

People

Several groups to think of; operating staff, maintenance staff, passengers, others inside and outside the system

Does your subject needs operating or maintenance? Can it be misused unintentional or intentional? Can it give any hazard; in working or failing condition? Think of energy, radiation, EM, heat, cold.

Surroundings

You have to consider “surroundings” very broad. Can the surroundings influence your subject? Can your subject influence the surroundings? Think of collision, derailment, fire, explosion, vibration, moisture, heat, cold, snow, wind, earthquake or flooding. But also environmental issues, pollution, radiation, noise or stench.

Procedures

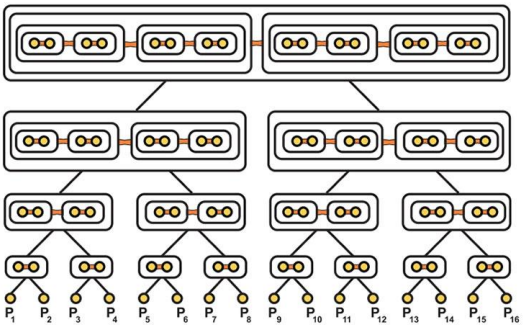
Procedures can be legislation or self-imposed rules like manuals or maintenance instructions.

Is the object subject to rules or legislation, does it affect existing procedures, do you have to change procedures?

The trick is to repeat this process with every discovered relevant interaction. The process ends when there are no new interactions found. You usually find your scope has grown a bit. And as a bonus you probably also have identified some risks already.

Side step 1: how to document your scope

It helps if you start with a drawing of schematic representation of the subject you are going to analyze. Then you have to document all the interactions you found. Usually it helps to visualize them to. This can be done by extending your original drawing, or by simply using post-it’s on a brown paper. A bit more hi-tech is using Exel of MindMap.



Side step 2: what if you end up with a really big scope

If you end up with a really big scope, I advise you to downsize the problem to a size that you can comprehend. This means dividing your scope into several smaller logic parts. You start with the original subject and end at the fist interface. The next part starts at this interface and ends at the next interface, and so on. Each part can then be analyzed separately, with special attention to in- and output of the interfaces.

Step 3: risk identification

The next step is focus on your new scope and try to identify the risks that may arise. You use of course all the information you collected with the previous exercise. It might be useful to develop failure scenario's, but you can also use the same guide-words again; now with the question "what can go wrong"? At the end of this step you should have a list of all conceivable risks of the analyzed subject, including all risks that may arise from interactions within the entire system.

Step 4: rating the identified risks

Usually you give values to the identified risks; probability of occurrence and gravity of the effect. Some methods also add a value for the number of people exposed to the effect. What you use is not that important, as long as you can differentiate the various risks.

Step 5: risk acceptance criteria

For those whom attended my presentation last year in Berlin; this is a tricky one. You have to decide whether or not you accept a risk. This is usually done by comparing the risk rating to a formally accepted criteria. If the risk is acceptable no further action is required, if the risk is not acceptable you have to take mitigating measures to bring it within acceptable values.

Step 6: Are we all done?

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

Yes, you have performed a risk analysis on a complex system. You identified all conceivable risks of the analyzed subject, including all risks that may arise from interactions within the entire system. You have made your design as safe as reasonably possible and you have fulfilled your moral and legal obligations.

No, Unfortunately, a man can only identify the risks that he can imagine. You may have missed the risks you didn't think of, or couldn't imagine. But don't worry, it's not your fault, because humans are imperfect beings.

Risk analysis is not an exact science. You never have a 100% guarantee that you have identified all possible risks. That doesn't mean a risk analysis is a useless exercise. You have at least the moral obligation to make your design as safe as reasonably possible. A risk analysis will absolutely help you to achieve that.

What you can do, is try to reduce the chance that you miss something. There are two major pit-fall's you have to avoid when conducting a risk analysis on a complex system;

1. The team hasn't the necessary in-depth knowledge on the analyzed subjects
2. You fail to identify an interaction

Actually there two are somewhat linked. The consistency of the team is of the utmost importance. You need to have all the necessary disciplines in your team. You need knowledgeable people that are inquisitive, critical and not afraid to give their point of view. They will help you identifying both interactions and risks.

Failing to identify an interaction is usually the result of one of two things; you didn't have the necessary disciplines in your team, or you simply didn't follow the method conscientiously and took short-cuts..

So, let avoid these pit-fall's and conduct your risk analysis on complex systems and make the railway system a little bit safer each time you do. And that, Ladies and Gentlemen, is our joint responsibility.