# Focusing on Worst Case Scenarios – efficiency or negligence

Bernhard Hulin

PHD Informatics, Accredited Assessor for railway vehicles, Safety Manager

Berner & Mattner, Erwin-von-Kreibig-Straße 3 | 80807 München (Germany)

SUMMARY

This contribution answers the question whether the typically focusing on worst case outcome scenarios is sufficient for a safety case. For this examples are given that answer this question with a clear “no”. It is shown that a hazard under scenarios with worst case outcome can have a lower SIL than the same hazard with a minor effect scenario. Moreover, it is shown that a hazard under scenarios with a high SIL can lead to a lower SIL for a special component than under a scenario with a lower SIL. The conclusion is to analyse all scenarios and not to focus on the worst case.

## INTRODUCTION

Current standards for functional safety require the determination of the safety criticality of all system functions. A good starting point for railway vehicles is the generic list of vehicle functions of the prEN15380-4. The safety criticality of a function is typically determined by analysing all the hazards linked to this function considering different scenarios. The most critical hazard under a worst case scenario then defines the criticality of the function.

For this analysis it is very important to identify as many hazards as possible for a function. And, for determining the criticality of a hazard it is important to analysis as many scenarios as possible for a hazard. This guarantees a good reasoning for the worst case criticality classification of a hazard and thus for the function.

For further analyses, e.g. the apportionment (see CLC/TR 50126-2), often just this worst case scenario is taken into account. Other scenarios are neglected to safe time without a loss of functional safety. A mistake – that is uncovered by this paper.

The paper highlights specialities that cause this mistake

1. A failure in a function can lead to different accident scenarios where the most severe is not necessarily the one with the highest safety criticality.

2. An accident scenario with a minor safety criticality can lead to a higher safety criticality for a special component than the worst case scenario

Finally, it is presented how highly important scenarios can be distinguished from less important scenarios.

## IMPACT OF SCENARIOS ON THE OUTCOME

The worst case outcome of a hazard, such as untimely door opening, is highly related to the circumstances of its occurrence. A set of circumstances can be described in a scenario. Beyond other circumstance the following are often relevant:

- Time (time zone, summer / winter time, time since start, …)

- Guest constitution (person with reduced mobility, sleeping, …)
- Operational phase (standing still, driving, breaking, acceleration, …)
- Operational mode (towing mode, parking mode, …)
- Weather condition
- Location (tunnel, bridge, curve, switches, level crossings, …)

It is obvious that a false behaviour of the system in one situation can have an outcome with many people being killed while in another situation the same false behaviour for example can at maximum cause only small injuries.

When formulating a scenario make sure that transitions between two values of a parameter (for example operational mode) are considered. Even if transitions logically are to have zero time in reality when performed by devices a transition lasts a certain time. It is necessary to remember this because wile a transition takes place something else can happen.

Determining all values of a scenario parameter for a hazard is sometimes not easy because some values of the parameters are very rare, e.g. a special level crossing exists only once in Germany.

## RISK ACCEPTANCE AND SAFETY TARGETS

If a risk – consisting of the outcome and the frequency of occurrence – is acceptable depends at least on the following circumstances:

- region (while in France nuclear power plants are an accepted risk they aren't in Germany)
- temporality (while nuclear power plants were an accepted risk in Germany they aren't any longer)
- modality – domain dependence (while in the machinery domain moving parts has to be protected by a fence this doesn't hold for railway domain)

If a risk is not acceptable actions for risk reduction have to be performed. The functioning and their portions of risk reduction have to be proofed. In the CSM EU directive there are defined three different methods for such a proof: code of practice, similar reference system and explicit risk estimation. For the rest of this paper we focus on the explicit risk estimation.

In some countries (e.g. in France) the tolerated occurrence rates of some hazards are predefined by the national safety agency while in other countries (e.g. in Germany) the risk acceptance criterion for the explicit risk estimation has to be determined by the one who asks for approval. These risk acceptance criterions are often referred to as safety targets. Safety targets can be expressed in different units, for example THR (tolerable hazard rate), SIL (safety integrity level) or killed persons per 1 million train kilometres.

Due to the previously mentioned impact of scenarios to the outcome of a hazard it seems to be estimation to safe side to classify a risk as a combination of the worst case outcome and the overall occurrence rate of this hazard, since the worst case outcome results just from view scenarios. However, it is possible (and – as we see later in this paper – necessary) to be classify hazards more precise by the limitation to scenarios. Thus, the occurrence rate of the hazard in this scenario is combined with the worst case outcome in the same scenario.

Let's illustrate this on the example "vehicle moves into wrong direction". The worst case outcome would probably be catastrophic based on the following assumptions:

- many passengers are on board the train
- it moves 1km into the wrong direction
- it rams a train (for example side swipe collision)

This can be rated by SIL 3 based on the following considerations:

- many persons can be killed
- it is very unlikely that this hazard lead to such an accident

- passengers are exposed to this hazard over the whole journey
- passengers cannot protect themselves from injury or dead

Another scenario for the hazard “vehicle moves into wrong direction” is:

- vehicle is standing in a parking position
- there are some other vehicles around, especially there is another vehicle located behind the first vehicle with a distance of one meter
- a worker is walking through this gap
- the driver wants to go ahead, but the vehicle moves quickly into the other direction and squeezes the worker

This scenario can be rated by SIL 2 based on the following considerations:

- at most reasonably one person (the worker) is killed
- it is unlikely that this hazard lead to such an accident
- the worker is exposed very short to this hazard
- the worker cannot protect himself from injury or dead

A third scenario for the hazard “vehicle moves into wrong direction” is:

- the train is to start moving from a stop position
- behind the train there is a level crossing just for pedestrians
- pedestrians crossing the rails
- the train moves into the wrong direction an hits pedestrians

This scenario can be rated by SIL 1 based on the following considerations:

- Some pedestrians can be killed
- it is very unlikely that this hazard lead to such an accident
- the pedestrians are exposed very short to this hazard
- usually pedestrian recognized a train approaching and thus can prevent an accident

Although the second scenario has a lower outcome than the third the second scenario has got a higher SIL than the third. We’ve seen this outcome-SIL inversion in many projects. Often, the manufacturer determines the SIL just for the scenarios with the worst-case outcome. This example shows that this limitation is not sufficient for the safety case.

## APPORTIONMENT

There exist different methodologies for apportioning safety requirements as well as safety targets to subsystems. The one that is highly recommended in Germany is apportionment via hazard trees. Hazard trees are fault trees that apportion SIL to the next sublevel of the tree. The apportionment rule is the same as for the automotive domain (see ISO 26262). Each subelement below an OR-gate inherits the SIL of the element above. The sum of the SIL of the subelements below an AND-gate must be at least as high as the SIL of the element above. For more details on the apportionment rules see SiRF (Sicherheitsrichtlinie Fahrzeug) that is freely available.

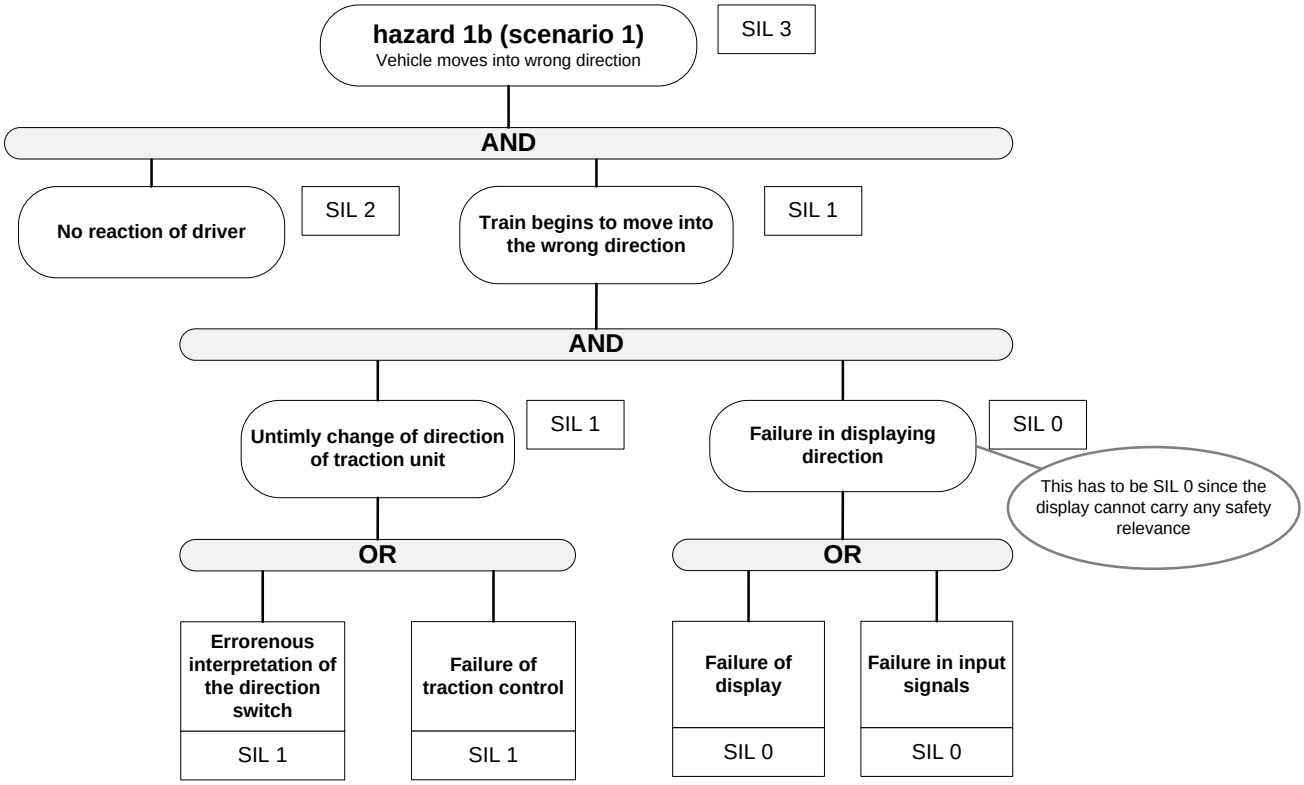


***Figure 1: hazard tree for scenario 1***

For showing the necessity of incorporating the scenarios for a hazard we take the example “vehicle moves into wrong direction” of the previous chapter. Figure 1 shows the hazard tree for this scenario. It is obvious that a train driver will recognize a movement into the wrong direction and will react to it. Thus, he stops the train before it moved a long distance into the wrong direction by commanding the brakes. Since this is a driving rule in Germany it is allowed to put a SIL 2 to the driver. SIL 2 is the highest SIL a train driver is allowed to get.

Note, that the display has got a SIL 0 since the manufacturer bought commercial of the shelf displays that are not developed according to any SIL. Note, that SIL 0 in context of hazard trees means “not safety relevant”.

Looking to scenario 2 we assume that a vehicle can move 1m in a period of time that is less than a reaction of the driver can have an effect. This holds for movements into the wrong direction, too. Therefore, the driver’s reaction cannot be recognized in the hazard tree for scenario 2 (see figure 2).

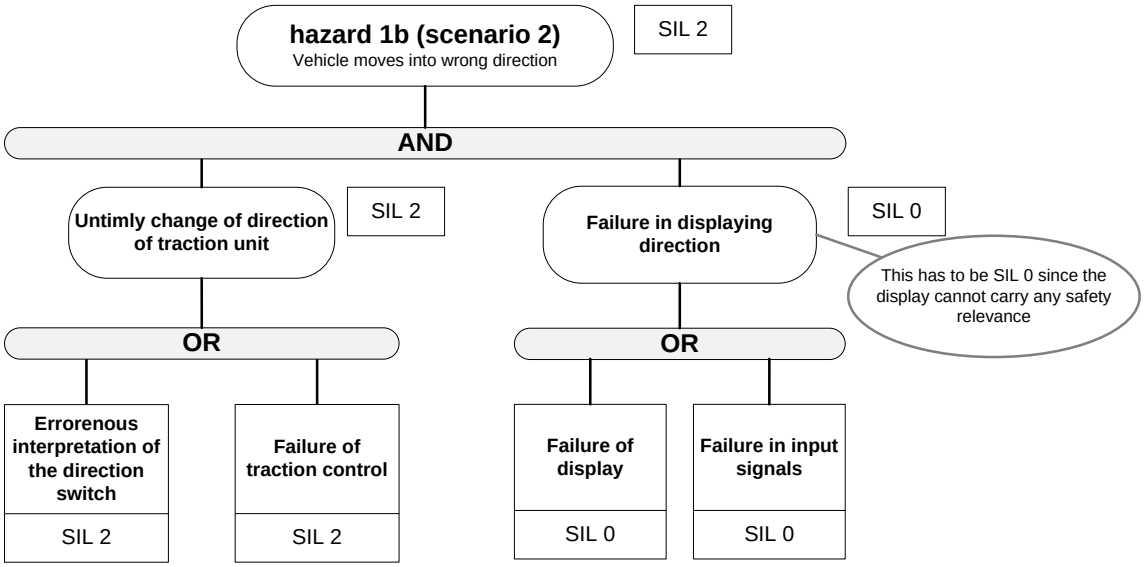


***Figure 2: hazard tree for scenario 2***

Comparing both hazard trees we see that some events have got a lower SIL in first hazard tree (see figure 1) than in the second (see figure 2). For example “Errorenous interpretation of the direction switch” has got a SIL 1 in the first scenario and a SIL 2 in the second scenario. This is interesting since the hazard in the first scenario has got a higher SIL than in the second scenario.

We observed this SIL inversion from hazard to component level many times on other hazards and over many projects.

## CONCLUSION

The examples of SIL determination show that for a safety case it is not sufficient just to focus on these scenarios with the worst case outcome. Other scenarios can lead to higher SIL than those with the worst case outcome. Moreover, the results of the apportionment show that it is not enough just to focus on scenarios with the highest SIL for a safety case. Instead all scenarios for a hazard shall be analysed. If some scenarios of a hazard are not analysed in detail it shall be reasoned that completeness is given, nevertheless.