

A semi-quantitative function-oriented approach for the safety life-cycle of future driver assistance systems

U. Steininger, A. Bartels, U. Becker, T. Ständer, T. Weidl

Future driver assistance systems will be able to take over more and more parts of the primary driving tasks. Not only authorities but also customers and manufacturers rate reliability and safety of such systems as highly important, therefore.

A risk analysis is a suitable instrument for identifying system weak points and for evaluating these qualitatively or quantitatively. This evaluation is the basis for any decision about safety relevant measures during design, test and implementation of the system. More over the developed approach considers current state and future development of standards and directives for official approval and homologation for road service.

The contribution describes the entire process for realising a semi-quantitative scenario-based risk analysis for future driver assistance systems, based on the safety life-cycle defined in IEC 61508 (see figure 1).

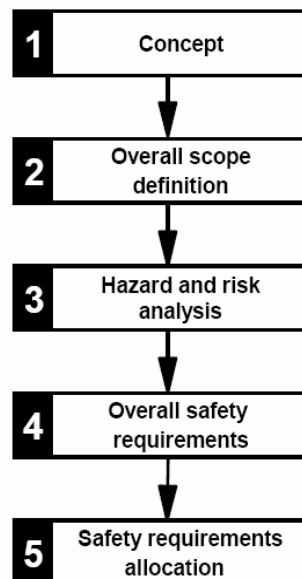


Figure 1: Cut-out of the safety life-cycle according to IEC 61508

A semi-quantitative approach was chosen because it enables the consideration of existing incident and field data as well as expert's estimations and experiences. This is especially useful in case of future systems where field experience is not yet available for.

Starting with a structured identification of potential scenarios for the operation of the system, we determine the target functions which have to be fulfilled to realise the systems functionality.

If a malfunction or a damaging event occurs, either has to be analysed due to its risk share. This is carried out similar to a fault tree analysis (FTA) with a TOP-DOWN approach by using a risk matrix. It is investigated which hazards and root causes are the underlying reasons for the damaging event. Moreover, the probability of occurrence of these releasing events and the measure of damage to be expected are estimated.

Taking the approach a step further, we examine how to counteract damaging events with high risk potentials. Therefore safety measures are assigned to root causes, hazards and the damaging event itself, in order to minimise the risk (see figure 2). Whether an efficient risk reduction can be reached, is verified by means of repeated risk assessment. It is essential that this risk assessment includes those measures which influence the probability of occurrence and/or the measure of damage.

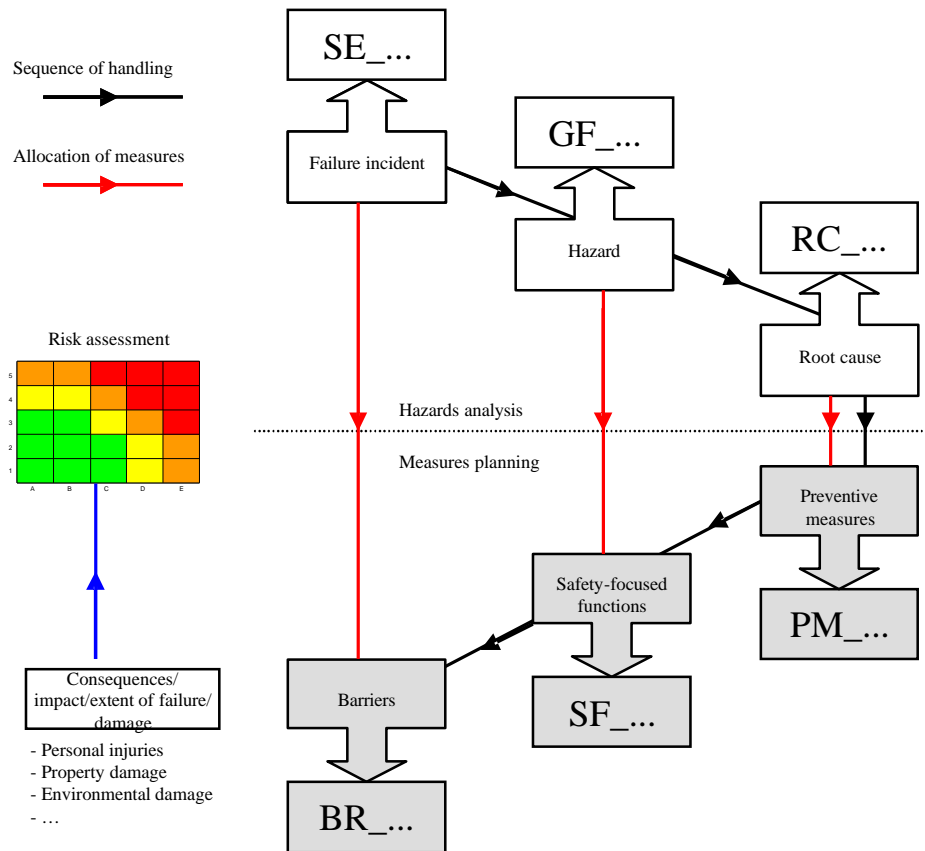


Figure 2: Model to allocate measures

Eventually, the entirety of measures which decrease the risk posed by the new system to an acceptable remaining risk has been summarized to form specific safety concepts for design, test and implementation of the new system. The aim is to ensure, that there follows no higher risk from the operation of a vehicle with the new system than from the operation of a conventional equipped vehicle in every foreseeable traffic situation.

Currently, this new developed approach is used in a research & design project for a future driver assistance system in Volkswagen Research. The contribution will show the application during the design phase of the system and will give a demonstration of the utilisation during the entire safety life-cycle of the system.