KI ABSICHERUNG
Safe AI for Automated Driving

Evidence-based Safety Argumentation Approach and Organizational Setup

Andreas Rohatschek[1],
Thomas Schulik[2], Christian Pfister[3]

Safety Argumentation

Assurance Case

According to the principles of ISO 26262, ISO/DIS 21448, and ISO/TR 4084, the assurance case shall state in a convincing way: "The system is safe because...".
However, the assurance of DNNs leads to several problems, since this technology requires new paradigms in development. The software is no longer explicitly developed. Instead, the neural network is trained, and the network's behaviour is implicitly influenced by the training models and data.
The combination of safety evidences in the assurance case provides central elements for a holistic assurance strategy.

Goal Structuring Notation (GSN)

The goal structuring notation (GSN) can be used to assemble evidences collected from various methods to provide a structured overall safety argumentation. The GSN visualizes the elements of the safety argumentation. An assurance case can be presented in a clear and structured way in the GSN. A GSN tree consists of three central elements: the argumentation goal, the description of the argumentation strategy and the evidence. These three elements are supported by assumptions, justifications and context information.

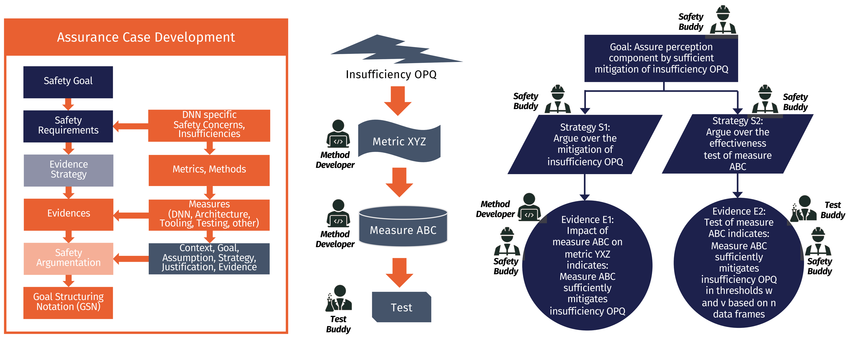

Figure 1: How to create Evidences from Methods and Tests

Evidence-based Safety Argumentation

The central aspect of safety argumentation is to show that the mitigation of insufficiencies was successful. If the insufficiency is reduced to an acceptable level, this provides evidence to be used in the safety argumentation.
One possibility to combine safety evidences in the assurance case is to start on the top level with the definition of safety goals. These are goals that define mandatory steps to avoid hazards. Then the safety requirements are refined step-by-step based on the causal model of SOTIF-related risk using several categories of evidences. This is supported by considering DNN-related safety concerns. Moreover, several metrics are defined to show the effectiveness of measures that mitigate the effects of insufficiencies.

Organizational Setup

We organized our work on the evidence-based safety argumentation in three clusters.

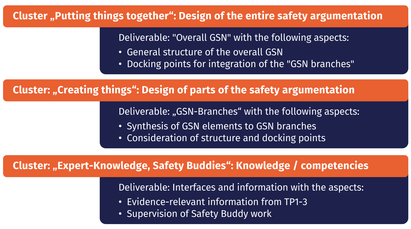

Figure 2: Organizational Setup

A central aspect is the iterative nature of this technique to refine understanding of insufficiencies in the function. Further iterations are started on the top level.

For more information contact:
andreas-juergen.rohatschek@de.bosch.com
thomas.schulik@zf.com
christian.pfister@astech-auto.de

KI Absicherung is a project of the KI Familie. It was initiated and developed by the VDA Leitinitiative autonomous and connected driving and is funded by the Federal Ministry for Economic Affairs and Climate Action.

Supported by:
Federal Ministry for Economic Affairs and Climate Action
on the basis of a decision by the German Bundestag

https://www.ki-absicherung-projekt.de @KI_Familie KI Familie

Image sources: Robert Bosch GmbH