Safe AI in an Automotive System Context

Dr.-Ing. Lukas Hacker (Mercedes-Benz AG)
Dr.-Ing. Patrick Feifel (Opel Automobile GmbH)

SAFE AI ENGINEERING

Motivation: AI is typically embedded in a larger system

AI is increasingly used as an enabling technology for complex perception tasks, such as object detection in automated driving (AD). Since AI-based functionality is embedded in a larger system context (see Figure 1), safety cannot be assessed at AI component level alone. Safety-related risks need to be considered in the context of the overall system, its intended use, and the operational environment.

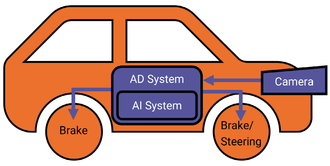


Figure 1: The exemplary AI system is embedded in the overall AD system, which outputs actuation requests (e.g., braking and steering) based on sensor inputs (e.g., camera data).

System & Use Case: AI-based Pedestrian Detection in Urban Scenarios

The project defines an exemplary system and use case to support a systematic safety consideration at system level. The selected example is an automated emergency braking (AEB) function in a highly automated vehicle (SAE Level 4), focusing on a camera-based AI system for pedestrian detection in an urban scenario (see Figure 2). A detailed architecture of the AD system and the AI system is shown in Figure 3.

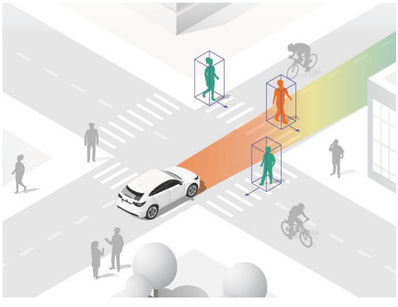


Figure 2: AI-based pedestrian detection with bounding boxes in an urban environment. The safety zone highlights the safety-critical area in front of the ego vehicle. (Source: Safe AI Engineering)

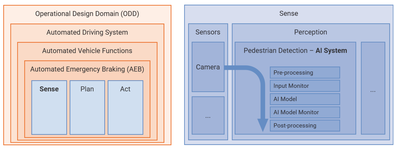


Figure 3: Detailed architecture of the exemplary AD system and AI system.

System Engineering meets AI Engineering

Based on the system description and the environmental context, a hazard and risk analysis is performed. High-level safety goals are derived and refined into AI safety requirements. These requirements provide the context for AI engineering activities, including data curation and analysis, model training, monitor design, testing, safety argumentation, and activities during operation (see Figure 4). To ensure traceability across the system development and the AI development, the engineering artifacts are managed using a docs-as-code approach.

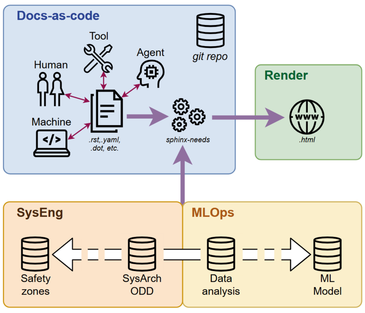


Figure 4: System and AI engineering activities are supported by a docs-as-code approach. (Source: Robert Bosch GmbH)

Safe AI Engineering Methodology

The engineering work in this project contributes to a structured Safe AI Engineering Methodology. The methodology addresses relevant process steps in AI engineering and builds on insights from the project as well as relevant safety standards, including ISO 26262, ISO 21448, and ISO/PAS 8800.

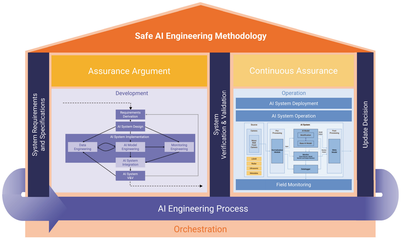


Figure 5: The Safe AI Engineering Methodology and its key process steps. (Source: DLR)

For more information regarding the poster, contact:

lukas.l.hacker@mercedes-benz.com
patrick.feifel@stellantis.com

Safe AI Engineering 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 Energy.

VDA LEITINITIATIVE
KI FAMILIE
Supported by: Federal Ministry for Economic Affairs and Energy on the basis of a decision by the German Bundestag

linkedin.com/company/ki-familie
www.safe-ai-engineering.de