Architecting Safe Automated Driving with Legacy Platforms

Modern vehicles have electrical architectures whose complexity grows year after year due to feature growth corresponding to customer expectations. The latest of the expectations, automation of the dynamic driving task however, is poised to bring about some of the largest changes seen so far. In one fell swoop, not only does required functionality for automated driving drastically increase the system complexity, it also removes the fall-back of the human driver who is usually relied upon to handle unanticipated failures after the fact. The need to architect thus requires a greater rigour than ever before, to maintain the level of safety that has been associated with the automotive industry.

The work that is part of this thesis has been conducted, in close collaboration with our industrial partner Scania CV AB, within the Vinnova FFI funded project ARCHER. This thesis aims to provide a methodology for architecting during the concept phase of development, using industrial practices and principles including those from safety standards such as ISO 26262. The main contributions of the thesis are in two areas. The first area i.e. Part A contributes, (i) an analysis of the challenges of architecting automated driving, and serves as a motivation for the approach taken in the rest of this thesis, i.e. Part B where the contributions include, (ii) a definition of a viewpoint for functional safety according to the definitions of ISO 42010, (iii) a method to systematically extract information from legacy components and (iv) a process to use legacy information and architect in the presence of uncertainty to provide a work product, the Preliminary Architectural Assumptions (PAA), as required by ISO 26262. The contributions of Part B together comprise a methodology to architect the PAA.

A significant challenge in working with the industry is finding the right fit between idealized principles and practical utility. The methodology in Part B has been judged fit for purpose by different parts of the organization at Scania and multiple case studies have been conducted to assess its usefulness in collaboration with senior architects. The methodology was found to be conducive in both, generating the PAA of a quality that was deemed suitable to the organization and, to find inadequacies in the architecture that had not been found earlier using the previous non-systematic methods. The benefits have led to a commissioning of a prototype tool to support the methodology that has begun to be used in projects related to automation at Scania. The methodology will be refined as the projects progress towards completion using the experiences gained.

A further impact of the work is seen in two patent filings that have originated from work on the case studies in Part B. Emanating from needs discovered during the application of the methods, these filed patents (with no prior publications) outline the future directions of research into reference architectures augmented with safety policies, that are safe in the presence of detectable faults and failures. To aid verification of these ideas, work has begun on identifying critical scenarios and their elements in automated driving, and a flexible simulation platform is being designed and developed at KTH to test the chosen critical scenarios.