UNIVERSITY OF LEICESTER

Data-Driven Safety Analysis of Autonomous Vehicle Functions

Level	PhD
First Supervisor	Prof Mohammad Mousavi
Second Supervisor	Dr José Rojas
Application Closing Date	27th June 2019
Subject Areas	Computer Science & IT Data Analysis Software Engineering

Highlights

- Providing mechanised support for safety analysis of autonomous vehicle functions
- Automating scenario generation for testing autonomous vehicle functions
- Contributing to a platform of establishing trust for AI and learning components

Autonomous vehicle concept by Mercedes presented at Shanghai Auto Show 2015
Source: https://pxhere.com/en/photo/734237

Overview

Establishing trust in autonomous vehicles is a major component of their widespread public adoption. Rigorous and explainable safety analysis of autonomous vehicle functions play a major role in establishing trust. There are existing standards for establishing safety in automotive systems, of which the ISO 26262 standard is the most prominent one. Safety case analysis in these standards involves defining a safety item and analysing and providing a safety case for the item by analysing the hazards in typical scenarios of use and foreseeable misuse. To analyse the hazards rigorously, different safety integrity levels (ASIL) are attached to them, and different analysis techniques are prescribed for different ASIL. At high ASIL, formal verification and model-based testing are prescribed as appropriate techniques for the analysis.

Hitherto, much of the safety case analysis process has been manual, involving tedious scrutiny of possible scenarios and turning them into appropriate models for further analysis. For autonomous vehicles, however, such a manual process becomes extremely laborious and error-prone and mechanisation support is inevitable. Also, in the presence of adaptive and AI-enabled systems, adapting safety cases and their analysis should inevitably be mechanised or otherwise will be infeasible.

This project aims at providing mechanised support for safety-case analysis of automated and autonomous functions. To this end, we will build upon our past experience with automated test-case and scenario generation to turn structured English safety case and item descriptions into rigorous models from which use and misuse scenarios are generated automatically.

Methodology

Our approach builds upon a number of fundamental developments in the area of software and systems testing to which the PIs have contributed. Namely, we base our approach on test-case generation from natural language documentation and also model-based testing. We start with structured English and diagrammatic description of safety items and turn that into a model from which typical (use and misuse) scenarios can be generated. While testing the system, we also explore its behaviour using machine-learning techniques in order to enrich the model and generate more diverse and more effective scenarios. We assure traceability from textual descriptions to test results in order to automatically generate a safety case when the process is concluded.

Further Reading

1. H. Araujo, G. Carvalho, M. Mohaqeqi, M.R. Mousavi, and A. Sampaio. Sound Conformance Testing for Cyber-Physical Systems: Theory and Implementation. Science of Computer Programming. Elsevier, 2018.
2. B.K. Aichernig, W. Mostowski, M.R. Mousavi, M. Tappler, and M. Taromirad. Model Learning and Model-Based Testing. In Machine Learning for Dynamic Software Analysis. Volume 11026 of LNCS, Springer, 2018.
3. Ermira Daka, José Miguel Rojas, and Gordon Fraser. Generating Unit Tests with Descriptive Names Or: Would You Name Your Children Thing1 and Thing2? In *ACM Int. Symposium on Software Testing and Analysis (ISSTA)*, pages 57-67. ACM, 2017.
4. B. Oliveira, G. Carvalho, M.R. Mousavi, and A. Sampaio. Simulation of Hybrid Systems from Natural Language Specifications. Proceedings of the 13th IEEE International Conference on Automation Science and Engineering (CASE 2017), IEEE, 2017.
5. José Miguel Rojas, Mattia Vivanti, Andrea Arcuri, and Gordon Fraser. A detailed investigation of the effectiveness of whole test suite generation. *Empirical Software Engineering (EMSE)*, pages 1-42, 2016.
6. H. Beohar and M.R. Mousavi. Input-Output Conformance Testing for Software Product Lines. Journal of Logic and Algebraic Methods in Programming, 85(6): 1131-1153. Elsevier, 2016.