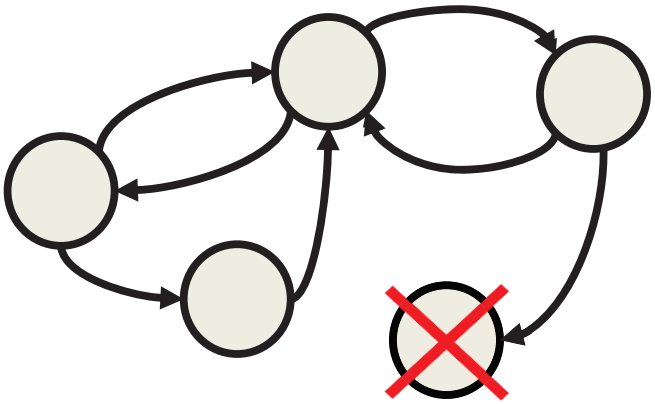
Automatically Assessing Correctness of Autonomous Vehicles — Auto-CAV

Public report



$$
\dfrac{\dfrac{\dfrac{\dfrac{*}{x \geq 0 \land v \geq 0 \land r \geq 0 \vdash x + v\,r + r^2 \geq 0)}[\mathbb{R}]}{x \geq 0 \land v \geq 0 \vdash r \geq 0 \rightarrow x + v\,r + r^2 \geq 0)}[{\rightarrow}\mathrm{R}]}{x \geq 0 \land v \geq 0 \vdash \forall t\,(t \geq 0 \rightarrow x + v\,t + t^2 \geq 0)}[\forall\ \mathrm{R}]}{x \geq 0 \land v \geq 0 \vdash [\,x' = v, v' = 2\,]\,x \geq 0}[']
\qquad
\dfrac{}{\vdash x \geq 0 \land v \geq 0 \rightarrow [\,x' = v, v' = 2\,]\,x \geq 0}[{\rightarrow}\mathrm{R}]
$$

Project within FFI <Traffic Safety and automated vehicles>

Author Yuvaraj Selvaraj

Date 2023-05-22

FFI Fordonsstrategisk Forskning och Innovation

VINNOVA Energimyndigheten TRAFIKVERKET FKG VOLVO SCANIA VOLVO

Content

1. Summary

The project aimed to establish formal verification as an efficient tool in the development of safety-critical software for automated vehicles. The project was carried out as an industrial PhD project in collaboration between Zenseact (formerly Zenuity) and Chalmers University of Technology. The results and deliverables of the project include academic publications, with a doctoral thesis being the main outcome. The project evaluated various formal methods for modeling, specifying, and verifying automated driving systems. It provided insights into the differences between these methods and the associated challenges. The project also identified an integrated approach to argue the safety of automated vehicles and published modeling guidelines for the safety verification of these vehicles. Additionally, the project developed methods to identify and address modeling errors. Furthermore, a systematic approach to obtain formal models automatically, and a structured approach to using formal artifacts as evidence for safety arguments were also developed. In terms of the FFI objectives, the project contributed to achieving safer vehicles and increasing road safety by focusing on software development for automated vehicles. Overall, the project results align with the milestones outlined in the project work packages, demonstrating progress towards establishing formal verification as an efficient tool for developing safe and correct software for automated vehicles.

2. Sammanfattning på svenska

Denna rapport ger en översikt över forskningsprojektet Auto-CAV, som fokuserade på att etablera formella metoder som ett effektivt verktyg för att utveckla säkra automatiserade fordon. Projektet genomfördes som ett industridoktorandprojekt i samarbete mellan Zenseact (tidigare Zenuity) och Chalmers tekniska högskola. Målet var att undersöka tillämpningen av formell verifiering på automatiserade fordon, ta itu med de utmaningar som är förknippade med deras antagande och tillhandahålla bevis för säkerhets-argumentet för dessa fordon.

Forskningsprojektet behandlade tre huvudsakliga forskningsfrågor:

1. Faktorer som påverkar tillämpningen av formell verifiering på automatiserade fordon och de nuvarande utmaningarna i befintliga metoder.
2. Hur man kan hantera dessa utmaningar och skala lösningarna.
3. Hur formella metoder kan användas för att ge bevis i säkerhetsargumentet för automatiserade fordon.

Forskningsmetodiken inkluderade litteraturstudier, fallstudier, proof of concept-studier, matematisk modellering och matematiska bevis. Arbetet var uppdelat i fyra arbetspaket (WP):

1. Verktyg och kvalitetsfaktorer för formell modellering: Utvärdering av tillgängliga verktyg och modelleringsriktlinjer lämpliga för formell verifiering av automatiserade fordon.
2. Säkerhetskrav och formella specifikationer: Formalisering och verifiering av säkerhetskrav för automatiserade fordon.
3. Algoritmer och metoder för formell verifiering: Utveckling av metoder för att möta de utmaningar som identifierats i de tidigare arbetsgrupperna.
4. Integration och validering: Integrering av formella verifieringsmetoder i den industriella utvecklingsprocessen och validering av deras effektivitet.

Projektets resultat inkluderar akademiska publikationer, med en doktorsavhandling som huvudresultat. Projektet utvärderade olika formella metoder för att modellera, specificera och verifiera automatiserade körsystem. Detta gav insikter om skillnader mellan, och utmaningar med, dessa metoder. Projektet identifierade också ett integrerat tillvägagångssätt för att argumentera för säkerheten för automatiserade fordon och publicerade modelleringsriktlinjer för säkerhetsverifiering av dessa fordon. Dessutom utvecklade projektet metoder för att identifiera och åtgärda modelleringsfel, ett systematiskt tillvägagångssätt för att erhålla formella modeller automatiskt och ett strukturerat tillvägagångssätt för att använda formell bevisföring för säkerhetsargument. Dessa bidrag syftar till att förbättra tillförlitligheten och säkerheten för automatiserade fordon genom att säkerställa noggrann verifiering av deras programvara.

När det gäller FFI-målen bidrog projektet till att uppnå säkrare fordon och ökad trafiksäkerhet genom att fokusera på mjukvaruutveckling för automatiserade fordon. Projektet främjade samarbete mellan industri (Zenuity/Zenseact) och akademi (Chalmers tekniska högskola). Det bidrog också till den svenska fordonsindustrins konkurrenskraft genom att föra fram kunskap inom området och etablera samarbeten med internationella forskare.

Sammantaget gjorde forskningsprojektet betydande framsteg i tillämpningen av formella metoder för att utveckla säkra automatiserade fordon. Dess resultat ökar trafiksäkerheten, främjar samarbete, bidrar till den svenska fordonsindustrins konkurrenskraft och stärker forsknings- och innovationsmiljöer i Sverige.

3. Background

Road traffic accidents are a leading cause of global deaths, resulting in 1.35 million fatalities annually [1]. They also incur significant economic losses, accounting for 3% of the gross domestic product in most countries [2]. Human error contributes to over 90% of these accidents [3]. The global automotive industry is experiencing a significant shift as software systems become integral to vehicles, particularly in the development of automated vehicles as they have the potential to improve traffic safety. However, the implementation of higher levels of automation poses technical, business, and regulatory challenges. Ensuring the safety and functionality of automated vehicles is becoming increasingly challenging due to its complexity.

An automated vehicle consists of several software and hardware components that constantly interact with each other to solve a variety of driving tasks. The interaction between these components creates a complex system where subtle and potentially dangerous bugs can occur. Detecting such bugs is a non-trivial task because they result from unforeseen interactions and statistically rare edge case driving scenarios. This makes the design and verification of an automated vehicle particularly challenging. Moreover, since the failure rate of automated vehicles need to be lower than human driving for successful commercial deployment, the need for strict methods to ensure safety of automated vehicles is paramount.

Several approaches have been adopted by the automotive industry to ensure safety and quality. One prominent approach to finding bugs is through traditional testing techniques, where test cases are written and executed in simulated or real environments. However, testing is time-consuming, expensive, and impractical for large software systems, typically used in automated vehicles. Additionally, testing can only identify the presence of bugs but cannot guarantee their absence.

Industry-specific safety standards such as the ISO 26262 [4], the ISO/PAS 21448 [5], and the UL 4600 [6] have also been used to design, develop, and argue safety of automotive systems. While conformance to these standards avoids and/or mitigates unreasonable risks caused due a variety of malfunctions, challenges exist in demonstrating safety of an automated vehicle [7]-[8].

Formal methods use rigorous mathematical models to build hardware and software systems. Formal methods can provide a mathematical proof of correctness of the system and can, unlike testing, demonstrate the absence of errors in a system. Formal methods include many different techniques and one useful technique when it comes to proving safety of automated vehicles is formal verification. Given a formal model of a system and a formal specification of the intended behaviour of the system, formal verification is the act of proving or disproving the correctness of the system with respect to the specification. Though formal verification has been shown to be beneficial in designing automotive systems [9]-[11], it is not widely established in the industry. The aim of the

project was to explore the barriers to adopting formal methods, and in particular formal verification in the automotive industry, specifically for the development of safe automated vehicles.

4. Purpose, research questions and method

The purpose of the project was to investigate how to establish formal methods as an efficient tool to develop safe automated vehicles. The project was carried out as an industrial PhD project where an industrial PhD student was employed by Zenseact (formerly Zenuity) in collaboration with Chalmers University of Technology. The project started with the hypothesis that formal methods can be used in the industrial development process to provide rigorous evidence for the safety argument of automated vehicles. The challenges that hinder widespread industrial adoption of formal methods were investigated and solutions to address some of the challenges were identified and developed. Three research questions were considered:

> **RQ 1** What factors affect the application of formal verification to automated vehicles and what are the current challenges in existing methods?
>
> **RQ 2** How can the challenges be addressed, and can the solutions be scaled?
>
> **RQ 3** How can formal methods be used to provide evidence in the safety argument of automated vehicles?

Since the research was motivated by the need from the industry, the research methods adopted in the project were tightly connected to the industrial research and development of automated vehicles. The research questions have been investigated and answered by applying several different methods including extensive literature studies, case studies, proof of concept studies, mathematical modelling, and mathematical proofs.

5. Objective

The project aimed to contribute to the following FFI objectives:

- Contribution to achieve safer vehicles and increase road safety
- Contribution to promote cooperation between industry, universities, and other institutions
- Contribution towards the Swedish vehicle industry to ensure global competitiveness
- Contribution to build international competitive research and innovation environments in Sweden
- Promoting cross industrial cooperation and stronger R&D operations

With respect to answering the research questions considered in the project, the work was divided into four work packages (WPs) as outlined in the project application. The four WPs are briefly described below.

WP 1: Tools and quality factors for formal modelling

The aim of WP1 was to identify and evaluate the different tools that can aid in formal verification of automated vehicles. WP1 corresponds to RQ 1, and the deliverables include an evaluation of the available tools and modelling guidelines suitable for automated vehicles.

WP 2: Safety requirements and formal specifications

This WP aimed to investigate how safety requirements for automated vehicles can be formalized and verified. The work in WP 2 corresponds to RQ 1 – RQ 3 and the deliverables include systematic approaches to formalize and refine safety requirements for formal verification.

WP 3: Algorithms and methods for formal verification

WP3 aimed to identify solutions and develop methods to address the challenges identified in WP 1 and WP 2. The work involved significant scientific research and the main deliverable of this WP is the doctoral thesis. Like WP 2, the work in WP 3 corresponds to all the research questions.

WP 4: Integration and validation

The final WP dealt with the integration and validation of the methods developed in WP 3 in the day-to-day industrial development process. The main deliverables included a framework for integrating formal verification in the development process.

6. Results and deliverables

The results from the project are primarily documented in the form of academic publications including a doctoral thesis. The various publications that resulted from the project are listed in Section 7 of this report. Briefly, several formal methods to model, specify, and verify automated driving systems were evaluated. Insights into how the evaluated methods differ and the challenges involved were documented and published. An integrated approach to argue safety of automated vehicles was identified and modelling guidelines on the different methods and their applicability to the safety verification of automated vehicles were published. Methods to identify and address subtle modelling errors were developed, thereby avoiding the risk of fallacious safety arguments. A systematic approach to automatically obtain formal models was developed and validated by a proof of concept. A structured approach on how to use various formal artefacts to provide evidence for safety arguments of automated driving systems was also

published. More details on how the different publications answer the research questions can be found in the doctoral thesis [12].

With respect to the FFI objectives, the project contributed in the following manner.

- **Contribution to achieve safer vehicles and increase road safety**
  The project contributed by focusing on software development for automated vehicles. The methods developed and the insights obtained contribute to developing formally correct software, thereby improving the reliability of automated vehicles. By ensuring that the software has been rigorously verified, it minimizes the chances of errors or malfunctions that could compromise safety.

- **Contribution to promote cooperation between industry, universities, and other institutions**
  The project was carried out in collaboration with Zenuity (initial), Zenseact (final), and Chalmers University of Technology (two different research groups).

- **Contribution towards the Swedish vehicle industry to ensure global competitiveness**
  Overall, the application of formal methods in developing safe automated driving makes a significant contribution to the global competitiveness of the Swedish vehicle industry. By focusing on safety, innovation, collaboration, talent development, and global influence, the involvement of Zenuity and Zenseact ensures that the Swedish vehicle industry remains at the forefront of automated driving technology.

- **Contribution to build international competitive research and innovation environments in Sweden**
- **Promoting cross industrial cooperation and stronger R&D operations**
  The project contributes to these objectives through various collaborations and network resulted from the different academic publications and conference talks in the doctoral student's PhD journey. Zenseact's involvement in the establishment of AI Sweden also contributed towards new collaboration with fellow Swedish and international researchers.

7. Dissemination and publications

7.1 Dissemination

How are the project results planned to be used and disseminated?	Mark with X	Comment
Increase knowledge in the field	X	
Be passed on to other advanced technological development projects	X	
Be passed on to product development projects	X	
Introduced on the market		
Used in investigations / regulatory / licensing / political decisions		

7.2 Publications

7.2.1. Theses

1. Selvaraj, Y. (2020). On Provably Correct Decision-Making for Automated Driving. Licentiate thesis, Chalmers University of Technology, 2020.

2. Selvaraj, Y. (2022). Safety Proofs for Automated Driving using Formal Methods. Ph. D. dissertation, Chalmers University of Technology, 2022.

7.2.2. Journal publications

3. Selvaraj, Y., Farooqui, A., Panahandeh, G., Ahrendt, W., & Fabian, M. (2022). Automatically Learning Formal Models from Autonomous Driving Software. Electronics, 11(4), 643.

4. Selvaraj, Y., Ahrendt, W., & Fabian, M. (2022). Formal development of safe automated driving using differential dynamic logic. IEEE Transactions on Intelligent Vehicles.

5. Krook, J., Selvaraj, Y., Ahrendt, W., & Fabian, M. (2022). A Formal-Methods Approach to Provide Evidence in Automated-Driving Safety Cases. ArXiv Preprint ArXiv:2210.07798.

7.2.3. Conference publications (peer-reviewed)

6. Selvaraj, Y., Ahrendt, W., & Fabian, M. (2019). Verification of decision making software in an autonomous vehicle: An industrial case study. Formal Methods for Industrial Critical Systems: FMICS 2019.

7. Selvaraj, Y., Fei, Z., & Fabian, M. (2020). Supervisory Control Theory in System Safety Analysis. Computer Safety, Reliability, and Security. SAFECOMP 2020.

8. Selvaraj, Y., Farooqui, A., Panahandeh, G., & Fabian, M. (2020). Automatically learning formal models: an industrial case from autonomous driving development. Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: MODELS 2020.

9. Selvaraj, Y., Krook, J., Ahrendt, W., & Fabian, M. (2022). On how to not prove faulty controllers safe in differential dynamic logic. Formal Methods and Software Engineering: ICFEM 2022.

10. Huck, T. P., Selvaraj, Y., Cronrath, C., Ledermann, C., Fabian, M., Lennartson, B., & Kröger, T. (2022). Hazard Analysis of Collaborative Automation Systems: A Two-layer Approach based on Supervisory Control and Simulation. International Conference on Robotics and Automation, ICRA 2023.

8. Conclusions and future research

This project focused on the application of formal methods, specifically formal verification, in the development of safe automated vehicles. The research aimed to investigate the factors affecting the use of formal verification, address the challenges involved, and explore how formal methods can provide evidence in the safety argument of automated vehicles. The results and deliverables of the project include academic publications, with a doctoral thesis being the main outcome. Overall, the research project makes significant strides in the application of formal methods for developing safe automated vehicles.

The possibilities for future research include conducting more in-depth empirical case studies to further evaluate different formal methods. Though the project included proof of concept studies and preliminary results on integrating the evaluated methods in the day-

to-day development process, the scope for further industrial adoption is significant. Exploring the adoption of the different evaluated methods in isolation as well as developing efficient frameworks to combine multiple methods is a promising area for further research. Investigating the limits of the safety argument approach, as proposed in the project, through multiple concrete examples from the industry will further aid in the removal of barriers hindering the industrial adoption of formal methods in ensuring automated vehicle safety.

9. Participating parties and contact persons

Zenseact (formerly Zenuity)	Yuvaraj Selvaraj (contact person) Ali Hedayati Ghazaleh Panahandeh Zhennan Fei Jonas Krook
Chalmers University of Technology	Martin Fabian (contact person) Wolfgang Ahrendt

10. References

[1] "Global status report on road safety 2018." (2018), [Online]. Available: https://www.who.int/publications/i/item/9789241565684.

[2] World Health Organization (WHO). "Road traffic injuries." (2022), [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-njuries.

[3] Regulation (EU) 2019/2144 of the European Parliament and of the Council on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, url: http://data.europa.eu/eli/reg/2019/2144/oj, Dec. 2019.

[4] ISO 26262:2018, "Road vehicles – functional safety," International Organization for Standardization, Tech. Rep., Dec. 2018.

[5] ISO/PAS 21448:2019, "Road vehicles – safety of the intended functionality,"

International Organization for Standardization, Tech. Rep., Jan. 2019.

[6] ANSI/UL, ANSI/UL 4600 - Standard for Evaluation of Autonomous Products, https://ul.org/UL4600, 2020.

[7] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," IEEE Intelligent Transportation Systems Magazine, vol. 9, no. 1, pp. 90–96, 2017.

[8] P. Koopman, A. Kane, and J. Black, "Credible autonomy safety argumentation," in 27th Safety-Critical Sys. Symp. Safety-Critical Systems Club, Bristol, UK, 2019.

[9] G. Bahig and A. El-Kadi, "Formal verification of automotive design in compliance with ISO 26262 design verification guidelines," IEEE Access, vol. 5, pp. 4505–4516, 2017.

[10] V. Todorov, F. Boulanger, and S. Taha, "Formal verification of automotive embedded software," in Proceedings of the 6th Conference on Formal Methods in Software Engineering, 2018, pp. 84–87.

[11] A. Zita, S. Mohajerani, and M. Fabian, "Application of formal verification to the lane change module of an autonomous vehicle," in 2017 13th IEEE Conference on Automation Science and Engineering (CASE), IEEE, 2017, pp. 932–937.

[12] Y. Selvaraj. (2022). Safety Proofs for Automated Driving using Formal Methods. Ph. D. dissertation, Chalmers University of Technology, 2022.