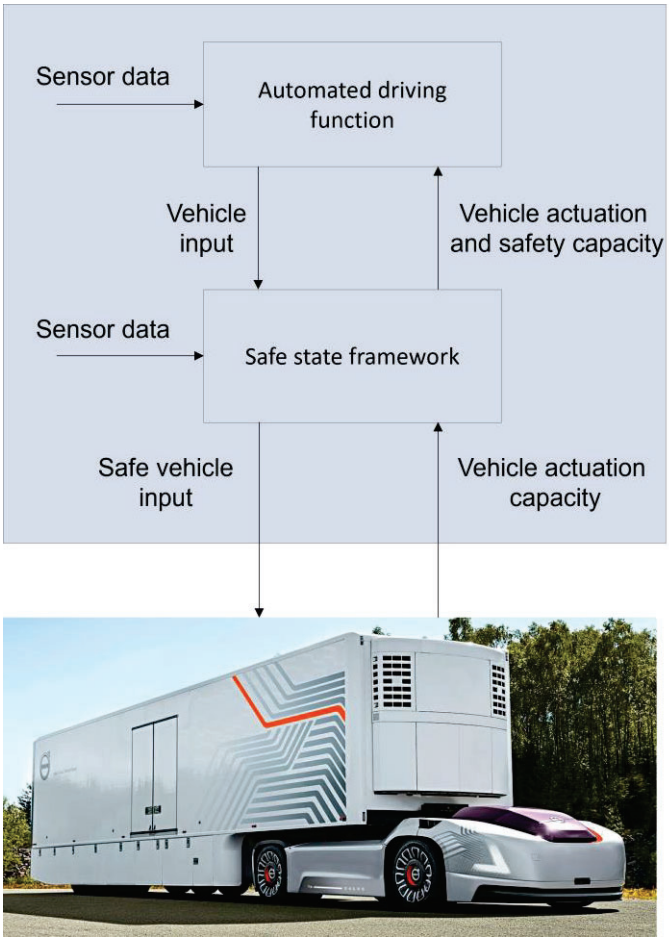
Högintegritetssystem för att säkra säkerheten för automatiserade körsystem

Publik rapport



Författare: Stefan Kojchev
Datum: 2024/05/07
Projekt inom Trafiksäkerhet och automatiserade fordon

FFI Fordonsstrategisk Forskning och Innovation
VINNOVA Energimyndigheten TRAFIKVERKET FKG VOLVO SCANIA VOLVO

Kort om FFI
FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings- och innovationsaktviteter med fokus på områdena Klimat & Miljö samt Trafiksäkerhet. Satsningen innebär verksamhet för ca 1 miljard kr per år varav de offentliga medlen utgör drygt 400 Mkr.

Läs mer på www.vinnova.se/ffi.

1 Sammanfattning

Autonoma fordon kommer industrialiseras i höga volymer inte så långt fram i tiden. Dessa fordon måste vara flexibla för att integrera och uppdatera kontrollalgoritmer i hög takt. Så snart det finns förbättringar i transporteffektivitet eller till det avsedda verksamhetsområdet, bör dessa förbättringar användas i så många fordon som möjligt för att få maximal nytta och produktivitet. Det är emellertid en utmaning att verifiera att risken är tolerabel att ett autonomt fordon skapar en situation som kan vara skadlig. Därför måste ett system som är i bruk vara robust mot att ta emot uppdateringar för vissa delar av systemet, eftersom dessa uppdateringar inte kan äventyra systemets verifierade säkerhet, men ändå ge förbättrad funktionalitet. Ett sätt att uppnå ovannämnda flexibilitet och robusthet är att skilja systemet som säkerställer fordonets säkerhet från de komponenter som utför taktisk och strategisk uppdragsplanering och tillåter ändringar endast till de senare delarna. Hypotesen är att detta kan ske så att uppdateringar till ett autonomt fordon kan implementeras i högre takt än vad som skulle vara möjligt om processen som verifierar systemets underliggande säkerhet tillämpas varje gång. Det underliggande antagandet är att det kommer vara svårt att verifiera säkerheten hos ett system med hög komplexitet som kan göra praktiskt taget allting, medan ett system med låg komplexitet som ansvarar för att undvika kritiska fel kan verifieras lättare och vara oförändrad under en längre tidsperiod.

2 Executive summary in English

Autonomous vehicles need to be industrialized in high volumes in the not so far future. These vehicles will need to be flexible towards incorporating updated control algorithms at a high pace; as soon as there are improvements in transport efficiency or to the intended area of operation, these improvements should be used in as many vehicles as possible for maximum benefit. How ever, it is a challenge to verify that the risk is tolerable that an autonomous vehicle creates a situation that can be harmful. Therefore, a system in use must be robust tow-ards receiving updates to some parts of the system in the aspect that these updates cannot compromise the verified safety of the system yet provide improved functionality. One way of achieving the aforementioned flexibility and robustness is to separate the system that ensures the safety of the vehicle from the components that conduct the tactical and strategic mission planning and allow changes only to the latter parts. The hypothesis is that this can be done such that updates to an autonomous vehicle can be implemented at a higher pace than hat would be possible if the process that verifies the underlying safety of a system is applied each time. The underlying assumption is that it w ill be hard to verify the safety of a high complexity
system that can do virtually anything, w-hereas a low -complexity system
responsible for avoiding critical errors can be verified more easily and be unchanged for a longer period of time.

3 Bakgrund

Safety-critical systems are systems which, when failing, can cause consequences deemed unacceptable, generally referring to accidents involving humans or damage to property or the environment. This puts strict requirements on parts of the development process, such as specification, architecture as well as verification of the system. Systems for autonomous road vehicles can be considered safety-critical as they have the potential to cause accidents with both material damage and human injury. Automated driving systems can be automated to various degrees, ranging from adaptive cruise control to driving completely autonomous

without the need for a standby driver. Vehicles with a higher degree of automation have more and stricter safety requirements since they do not demand a human driver as back-up solution.

4 Syfte, forskningsfrågor och metod

Developing a system that is hard to change is typically uneconomical as the requirements for a system tend to change during its lifetime. When the functionality is changed to meet new requirements, the system needs to be tested to verify that it performs as expected. Furthermore, to ensure that old functionality still works, everything that could have been affected by the change also needs to be tested by doing regression testing. Safety-critical systems often need extensive testing to receive a certificate that they are proven, to some degree of uncertainty, to be safe for production. The tests for these types of systems thus need to cover as many scenarios as possible and can be both time consuming and costly to run.

An underlying assumption is that it will be hard to verify the safety of a high-complexity system that can do virtually anything, whereas a low-complexity system responsible for avoiding critical errors can be verified more easily and be unchanged for a longer period of time. The framework is from now on denoted *safe state framework*. This opens up for a series of interesting and relevant research questions in order to develop the safe state framework:

- Under which conditions can a low-complexity system, designed to have a high integrity with respect to critical failures, be responsible for the safety of a high-complexity system? What safety guarantees can we make for the complete system if the high-level control actions, belong to the safe control set?
- What information, constraints and safe control set needs to be transmitted from the low complexity system for the high-complexity system to be able to fulfil its task efficiently (without getting interrupted)?
- Can there be traceability of a particular action such that it can be determined on which basis that action was judged safe? And can the inverse analysis be facilitated such that it can be determined which safety critical components need to be further developed or invented in order to enable certain high-level tasks safely?
- What does the models look like inside the low-complexity system and which safety aspects can be proven using these models?

In the last decades, set-based methods have become an interesting method to determine a system's performance bound and it also provide very important information needed for complete system verification. Set-based methods, and specifically reachability analysis can be used to generate over-approximations of the set of possible behaviours to prove that they all satisfy a given property. The idea is to use set-based methods or concepts from these methods to answer the above-mentioned questions. One of the benefits with set-based techniques is that they do not require any hypotheses on the distribution of the perturbations and the measurement noises; it only assume bounds on the perturbations and noises. On the other hand, to be computationally viable and real-time implementable many approximations have to be made on the model of the system. In this way, the low complexity level can deliver a safe set, and the high complexity level is then allowed to take any action within this set. This project will, as mentioned look into what type of models that are needed and which safety aspects can be proven using these models, under computation and real-time constraints. The problem is a multi-dimensional optimization problem, with trade-offs between among others model accuracy, computational feasibility and conservatism of the solution.

5 Mål

The main objective of this project is, as mentioned earlier, to develop methods that are necessary for testing safety-critical systems and which safety aspects can be proven using these methods, under computation and real-time constraints. The developed methods will benefit FFI's engagement in *Traffic Safety and Automated Vehicles* and ensure that Sweden can take a world-leading role in autonomous vehicles or automated driving. That the project is conducted in close collaboration between Volvo and Chalmers enables high quality of research and facilitates the exchange of skills between industry and academia. Together, these factors create a unique opportunity for rapid development and early launch of these vehicles on roads.

The project will also contribute to the FFI programme *Traffic Safety and Automated Vehicles* by

- creating methods for providing customers with the latest technology, safe software updates.
- creating more effective and robust methods for safety-critical system verification.

According to the *Traffic Safety and Automated Vehicles*' Roadmap, development of methods for verification and validation of automated vehicles is an important and identified area of research, it is a main challenge for several programme areas, programme area E and G. This project aims at addressing this challenge and its results can be used for fulfilling the Milestone 2:2 in Safety concept 2. The developed method will be made available to other companies and universities through academic publications and collaborative projects. This can create new jobs in the academy and industry, strengthen the region's competitiveness and develop skills in the field. Publication also involves evaluation of results by reference review.

6 Resultat och måluppfyllelse

The results of the project can be summarized as:

1. A novel safety supervisor architecture and method that monitors the automated driving functions and can intervene when necessary to ensure the safety of the automated driving function. The method is general, meaning that it can be applied to different automated driving functions.

2. Optimization-based methods for the safe and efficient coordination of automated vehicles in confined sites.

The contributions in 1. and 2. aim at bridging the practical application and implementation of automated driving functions.

The safety monitoring concept is design to function with different automated driving functions. In terms of architecture it is below the automated driving function, i.e., it receives the input to the vehicle from the automated driving function and determines if that input leads to safe behavior. In the cases it does not, the concept overwrites the input to the vehicle.

The optimization-based coordination algorithm takes as input the vehicle routes and provides velocity profiles that the vehicles should follow such that safe and efficient behavior is achieved.

7 Spridning och publicering

7.1 Kunskaps- och resultatspridning

Hur har/planeras projektresultatet att användas och spridas?	Markera med X	Kommentar
Öka kunskapen inom området	X	Through knowledge sharing with industry partners and presentations at conferences
Föras vidare till andra avancerade tekniska utvecklingsprojekt		
Föras vidare till produktutvecklingsprojekt		
Introduceras på marknaden		
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		

7.2 Publikationer

Google Scholar profile where the published articles are available
https://scholar.google.com/citations?user=sb6ptlsAAAAJ&hl=en&oi=ao

Chalmers University of Technology profile
https://www.chalmers.se/personer/kojchev/?tab=1

8 Slutsatser och fortsatt forskning

In conclusion, the conducted research investigated an important topic that will be an enabler for autonomous driving.

Future extensions of the approach is to have a more complex control law that could further increase the volume of the backward reachable sets. Furthermore, it is interesting to investigate if it is possible to express the LMI conditions when the sets are not necessarily centered around the origin and increasing the dimension of the backward reachable set, this could further contribute to volume increase. Considering uncertain parameter varying systems is also part of future extensions to this work.

Furthermore, some interesting research areas are:

1. Improved prediction of the human driven vehicles motion and considering uncertain path of the human driven vehicles.
2. Experimental implementation and validation.

9 Deltagande parter och kontaktpersoner

Volvo Autonomous Solutions: **Stefan Kojchev**
Chalmers University of Technology: **Jonas Fredriksson**
Volvo GTT: **Mari Lindegren**