ARCHER

Architecture and Safety for Autonomous Heavy Vehicles

Publik rapport

Författare: Dr Johan Svahn (Scania).
Med bidrag från Per Roos (Scania), Naveen Mohan (KTH), Masoumeh Parseh (KTH), Prof. Martin Törngren (KTH)
Datum: 2019-04-30
Projekt inom arkitektur och säkerhet för tunga autonoma fordon

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

Innehållsförteckning

Kort om FFI

FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings- och innovationsaktiviteter 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.

För närvarande finns fem delprogram; Energi & Miljö, Trafiksäkerhet och automatiserade fordon, Elektronik, mjukvara och kommunikation, Hållbar produktion och Effektiva och uppkopplade transportsystem. Läs mer på www.vinnova.se/ffi.

1 Sammanfattning

Projektet Archer startades för att utveckla principer och metoder för fullt autonoma tunga fordon inom områdena arkitektur, personsäkerhet (specifikt funktionssäkerhet) och verifiering. Tre områden som bedömdes som centrala för att kunna industrialisera tunga fordon med en hög grad av autonomi. Speciellt beaktades bivillkoret att en arkitektur för autonoma fordon måste förhålla sig till en existerande arkitektur för icke autonoma fordon som även fortsatt måste kunna utgöra grunden för både det autonoma och icke autonoma fallet.

En metod, ATRIUM, har tagits fram för att undersöka och utveckla en systemarkitektur med avseende på dess robusthet mot olika feltyper i dess delar. I synnerhet måste en betydande osäkerhet i den arkitekturhypotes som utvecklas tas om hand på ett systematiskt och spårbart sätt. Successivt måste de antaganden som med nödvändighet behäftar den tidiga arkitekturutvecklingen elimineras till förmån för fakta.

För området personsäkerhet har fokus legat på hantering av risktagandet i autonom drift, och vad som kan klassas som tillräckligt säkert under de operationella omständigheterna. Inga befintliga metoder hanterar denna aspekt idag. Specifikt så har ett arkitekturmönster för höggradigt autonoma fordon utvecklats. Verifiering har fokuserat på hur modeller och simulering bäst kan avhjälpa den enorma verifieringsuppgift som krävs för att säkerställa dels att det autonoma fordonet fungerar som tänkt i alla tänkbara situationer och dels degraderar på ett säkert sätt när fel uppstår, komponenter går sönder eller när omgivningen inte längre är sådan att fordonet kan framföras säkert. Mycket komplicerade omgivningar behöver kunna modelleras och användas i simuleringar för att kunna resonera om verifiering, test och validering på ett tillfredsställande sätt. En modellering och simuleringsmiljö har utvecklats som tillåter utvärdering av systemarkitekturer medelst felinjicering.

Resultaten från projektet inkluderar en licentiatavhandling, ett 20-tal vetenskapliga artiklar, och 2 patentansökningar. Resultaten har kommunicerats via ett flertal presentationer vid vetenskapliga konferenser, vid ett flertal inbjudna föredrag, samt internt på Scania, där ATRIUM-metoden med framgång tillämpats.

2 Executive Summary in English

The purpose of project Archer was to develop principles and methods for developing autonomous heavy vehicles with respect to a legacy architecture within the areas of architecture, safety and verification (with specific emphasis on functional safety). These three areas were deemed central for industrialization of such vehicles. A method was devised for exploring and developing an existing architecture with respect to robustness against different fault types, under uncertain but traceable conditions. Management of risk during operation and a simulation environment for scenario verification has also been studied.

The results that were expected from the project have largely been achieved. One licentiate thesis has been successfully defended, in total about 20 scientific publications have been published within the three areas of Archer research, and 2 patent applications have been filed. The results have been continuously disseminated at a number of national and international conferences and symposia, as well as at Scania where also the case studies were presented, and the methodology ATRIUM were successfully applied.

The project has been carried out as 3 PhD student projects, within architecture, safety and verification, led by Scania with a joint steering committee consisting of Scania and KTH (including PhD supervisors). Quarterly workshops complemented by regular bi-weekly telephone conferences have been milestones for planning and synchronization of activities and results. The PhD students have conducted case studies, published articles, participated and presented their work at various conferences as well as supervised master thesis students.

3 Bakgrund

Den svenska fordonsindustrin utgör en betydande del av Sveriges export. För svenska fordonstillverkare utgör den inhemska marknaden endast en liten del av del av affärsmodellen, trots att merparten av forskning och teknisk utveckling bedrivs där. En generationsväxling förväntas nu, där fordonskontrollen förväntas bli mer och mer automatiserad.

Denna förändring har redan påbörjats, med aktiva system som interagerar i kritiska situationer för att undvika olyckor och öka säkerheten. Semiautonoma funktioner som ”adaptiv farthållare” finns nu tillgängliga från i stort sett samtliga fordonstillverkare. Den adaptiva farthållaren är ett autonomt system där föraren lämnar över den longitudinella kontrollen av fordonet till systemet. I tillägg till säkerhetsaspekten som den adaptiva farthållaren ger så får föraren även vinst i form av förbättrad bränsleekonomi.

Ett autonomt fordon förväntas hantera även komplexa körsituationer. Det är välkänt att den underliggande orsaken till många singelolyckor och olyckor vid vägarbeten beror på trötthet eller distraktion hos föraren som ofta uppkommer på grund av en monoton körsituation. Genom att automatisera monotona uppgifter kan denna typ av olyckor minimeras och trafiksäkerheten ökas.

Det pågående skiftet mot autonomi möjliggörs av kostnadseffektivitet och teknisk mognad av sensorer, ställdon, halvledarteknik och artificiell intelligens/maskininlärning. Som ett resultat av detta har den svenska fordonsindustrin svängt från en mekatronikfokuserad industri till att bli en fullskalig CPS-industri (Cyberfysiska system), med ett starkt fokus på autonoma funktioner som realiseras i mjukvara samt fokus på fordonskommunikation.

Med tanke på utvecklingstakten inom autonomiområdet är det extremt viktigt att starta svenska projekt med fokus på autonoma fordonskoncept som utvecklas och testas i verklig miljö. Med hjälp av påtagliga forskningsprojekt med robusta autonoma forskningsplattformar borde Sverige klara att behålla sin position inom fordonsautomatisering, och samtidigt fördjupa kompetensen för att klara generationsskiftet som påverkar hela fordonsmarknaden.

Det är tydligt att ett antal aktiviteter behöver startas för att erhålla större bredd och djup inom autonom fordonsutveckling. Detta beror dels på en pågående samhällsförändring och förändringar i transportsystem, och dels på ett tydligt önskemål från visionära kunder.
Områden som ”sensorfusion”, ”funktionssäkerhet” och ”verklighetsuppfattning” får mycket fokus från forskning både inom fordonsindustrin och akademin, men begränsade resurser läggs på frågor runt elsystemsarkitektur, funktionssäkerhet och verifiering, särskilt inom området fullt automatiserade kommersiella fordon. Avsaknaden av en mänsklig förare skapar särskilda utmaningar för tunga kommersiella fordon med avseende på vikt, storlek, livslängd och komplexitet i form av den kunddrivna konfigurationsvariabiliteten. Utvecklingen av fullt autonoma tunga fordon drivs av ett tydligt marknadskrav, då det i de flesta tillämpningar inte behövs mänsklig närvaro (förutom ur säkerhetsperspektiv).

4 Syfte, forskningsfrågor och metod

Syftet med projektet Archer var att utveckla principer och metoder för utveckling av tunga autonoma fordon i en existerande elsystemsarkitektur, inom områdena arkitektur, funktionssäkerhet och verifiering, tre områden som bedömdes som centrala för att kunna industrialisera autonoma tunga fordon. En metod har tagits fram för att undersöka och utveckla en existerande systemarkitektur med avseende på dess robusthet mot olika feltyper, under osäkra men spårbara antaganden. Hantering av risktagandet i autonom drift, och simuleringsmiljöer för scenarioverifiering har också studerats. Nedan redovisas, per område, vad som studerats och dess resultat.

Metoder och principer för säkerhetsanalys:

Projektet satte upp ett iterativt arbetssätt. Väldefinierade fallstudier valdes och studerades ur aspekterna arkitektur, säkerhet och verifiering. För varje iteration fördjupades fallstudierna med ökande komplexitet för att skapa ett inkrementellt resultat. Resultatet bestod av kravställning, specifikationer och metoder. Detta resultat har utvärderats efter varje iteration.

Den enskilt viktigaste faktorn för utveckling av autonoma fordon är personsäkerhet (specifikt funktionssäkerhet). Dagens säkerhetsanalys baseras på mänsklig förares närvaro, som alltid är tillgänglig som sista instans i en degraderingskedja. För en autonom körnivå utan mänsklig kontroll måste nya degraderingsprinciper utvecklas, likväl som ny metodik och nya principer för säkerhetsanalys.

Forskningsfrågor ur säkerhetsaspekt:

- Vilka brister finns i aktuella standarder och metoder för att analysera ett autonomt fordon?
- Hur bör aktuella standarder och metoder förbättras för att ge en tillförlitlig och effektiv analys vid utveckling av tunga autonoma fordon?
- Hur bör säkerhetskraven formuleras för att hantera avvägningen mellan säkerhet och tillgänglighet?
- Hur påverkas säkerhetskraven med avseende på fordonets tänkta körfall?
- Vilka principer bör gälla för diagnostik av ett förarlöst fordon?

Leverans:

- Definierade principer och metoder för säkerhetsanalys av fullt autonoma tunga fordon, inklusive säkerhetsrelaterade konstruktionsprinciper för att kompensera för förarfrånvaro.
- Krav och en definierad metod för analys av säkerhet-/tillgänglighetsparadoxen.

Metoder och principer för området verifiering:

Verifieringsaspekter måste inkluderas redan i utvecklingsfasen, under framtagandet av arkitekturen, då fullt autonoma tunga fordon inte kan verifieras med nuvarande testmetoder. Principer för effektiv testning som når acceptabla säkerhetsnivåer har studerats, som till exempel definition av emulerings- och simuleringspunkter i systemet för verifiering och felsökningsändamål. Området har även studerat metodik som kombinerar moderna testmetoder med simulering och formell testning. Metoden undersöker karaktäristik i form av fel och feltillstånd, beteenden och strukturella aspekter (inklusive arkitekturella mönster), verifieringstekniker och formalisering (inklusive automatisk testning) såväl som kritikalitet av fel och feltillstånd.

Forskningsfrågor för verifiering:

- Hur påverkas dagens testprinciper av ett fullt autonomt tungt fordon?
- Vilka simulerings- och emuleringspunkter är lämpliga i en arkitektur för ett fullt autonomt tungt fordon?
- Hur bör fel och feltillstånd diagnosticeras, omhändertas och rapporteras för ett fullt autonomt tungt fordon?

Leveranser för verifiering:

- Principer och metodik för fullt autonoma tunga fordon.
- Arkitekturella krav som gör testning och verifiering pålitlig och effektiv.
- En modellering och simuleringsmiljö för utvärdering av systemarkitekturer medelst felinjicering.

Framtagning av referenssystemsarkitektur:

Baserat på resultat från övriga områden har tillämpbarheten av en referensarkitektur för fullt autonoma tunga fordon studerats. Applikationsberoende aspekter som kan påverka arkitekturen har beaktats (till exempel motorvägs- kontra gruvapplikationer). Referensarkitekturen måste uppfylla säkerhetskrav, verifieringskrav, applikationskrav och ta hand om arkitekturella flaskhalsar. Även rimliga begränsningar gällande infrastrukturens tillgänglighet, befintlig elsystemsarkitektur, produktifierbarhet och kostnad vägdes in i detta.

Det finns ett antal prototypsystem för olika nivåer av autonom körning. Arbetet med referensarkitekturen beaktade och förbättrade dessa, antagande total frånvaro av förare samt rimligheten i produktifiering av ett elsystem för ett kommersiellt fordon. Detta introducerar nya

kravnivåer inom både funktionell användarsäkerhet och tillgänglighet, med möjlighet att skapa en kommersiell produkt.

Forskningsfrågor för referensarkitektur:

- Vilka tidigare förslag på referensarkitektur existerar?
- Hur påverkar producerbarhet och kostnad den ultimata referensarkitekturen?
- Vilka kompromisser kan accepteras beroende på existerande elsystemsarkitektur?

Leverans från referensarkitektur:

- Beskrivning av återanvändningsbara arkitekturmönster samt en systemarkitektursbeskrivning som inkluderar
  - en arkitekturell tillämpning av säkerhetskoncept
  - testbarhetsmekanismer
  - tillämpbarhet för produktion av ett fullt autonomt fordon
  - en tillräckligt robust och effektiv lösning för tillgänglighet för tänkta användarscenarion

5 Mål

Målet med projektet var att utveckla en uppsättning krav, konstruktionsprinciper, arbetsmetodik samt en referensarkitektur för ett fullt autonomt kommersiellt fordon. Givet att majoriteten av industriprojekt tillämpar en relativt låg TRL-nivå (”Technology Readiness Level”) så finns ett behov att beakta arkitekturaspekten i syfte att hantera komplexitet, säkerhet, tillgänglighet och kostnadseffektivitet.

Arkitektur, validering, verifiering och säkerhet är starkt kopplade. Det är därför av stor vikt att analysera dessa tillsammans. Med detta fokus har ARCHER brutit mark för ökande TRL-nivåer i industriprojekt.

6 Resultat och måluppfyllelse

De konkreta resultaten som projektet producerat utgörs av totalt 19 artiklar inom de tre forskningsområdena, samt en licentiatuppsats inom arkitekturområdet. Dessutom har en simuleringsmiljö byggts upp på KTH för test av arkitekturer. Inom test och säkerhet har doktoranderna inte hunnit fram till licentiatuppsatsen ännu pga. studieuppehåll respektive nyrekrytering.

Det inledande arbetet handlade, utöver grundläggande litteraturstudier, mycket om att konkretisera de generella problemformuleringarna i projektbeskrivningen till hanterbara frågor. För säkerhetsområdet handlade det om en kartläggning och undersökning av olika aspekter av säkerhetskultur och befintlig säkerhetsmetodik inom Scanias organisation, exempelvis hur och på vilket sätt informationsflödet relaterad till säkerhetsarbetet fungerar och hur detta förhåller sig till ISO26262’s krav. Detta resulterade i dels en modell för säkerhetskultur, och dels ett frågebatteri för undersökningar av detta slag: ’Preparing for autonomy: Benchmarking safety culture and processes´. Därefter har forskningen på säkerhetsområdet koncentrerats kring manöverplanering och riskreducerande manövrar kopplat till relevanta arkitekturmönster för att hantera säkerhet. .

För arkitektur inleddes arbetet med att hitta en metod (ATRIUM - ’Architecting under Uncertainty’) för att utvärdera och förbättra arkitekturförslag baserade på befintlig arkitektur så att en tillräcklig redundansnivå relativt en given grad av autonomi och operationell miljö kan ansättas för en inledande arkitekturiteration. Denna metod, testades inom Scania på den systemarkitektur som idag finns och som kommer at bli basen även för autonoma fordon. Metoden visade på ett systematiskt sätt på vilka behov av säkerhetsmekanismer och alternativa lösningar som dagens arkitektur måste kompletteras med. I detta arbete söktes även och beviljades två patent [se 7.3]. Nästa spår som utforskades var användandet av historisk diagnosinformation för att identifiera arkitekturrelevant information under autonom körning där föraren inte är en del av felhanteringskedjan, utan där systemet självt måste agera på viss diagnosinformation.

Inom test har det under de år projektet löpt blivit allt mer uppenbart i branschen att simuleringar kommer att bli ett helt oundgängligt verktyg för att kunna visa en tillräcklig grad av verifiering för

att kunna köra autonomt i allmänna miljöer. Simuleringar kommer också att behöva kompletteras med formella metoder för att reducera behovet av praktiska tester och fordonsprov.

Resultaten har förmedlats på ett stort antal både nationella och internationella konferenser och symposier, samt inom Scania, där också fallstudierna presenterats, både inom arkitektur och säkerhetskultur, och där även den inom projektet utvecklade metodiken ATRUIM tillämpats framgångsrikt. Flera processer och metoder har bedömts kunna förbättras med utgångspunkt i resultaten.

I den kraftfulla modellerings- och simuleringsmiljö för autonoma scenarier som har byggts upp möts de tre forskningsområdena, och i denna miljö har olika såväl övervakningsarkitekturer som säkerhetshypoteser testats under olika bivillkor och i olika situationer.

Ett antal inbjudna föredrag har hållits i olika forskningsmiljöer under projektets gång, och flera examensarbeten har också genomförts. Ett flertal konferenser och seminarier har anordnats på Archers teman, och på än flera har artiklarna presenterats. Samarbeten med andra projekt, såsom AutoDrive, har också såväl vidgat nätverket, som givit värdefulla synergieffekter på t.ex. hazardanalysmetodikområdet.

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	Doktoranderna har samlat data både från den akademiska världen och från domänexperter i industrin. Resultat och diskussioner har medfört kunskapsökning inom akademi och industri
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	Resultatet har presenterats på flertalet konferenser i forskningsvärlden, samt utgöra basen för det fortsatta samarbetsprojektet mellan KTH – Scania PRYSTINE.
Föras vidare till produktutvecklingsprojekt	X	Domänexperter på Scania har involverats både i frågeställningar och resultat
Introduceras på marknaden	X	Introduktion av autonomi ligger fortfarande en bit in i framtiden
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		

7.2 Publikationer

Challenges in Architecting Fully Automated Driving; with an emphasis on Heavy Commercial Vehicles
doi: 10.1109/WASA.2016.1

A Method towards the Systematic Architecting of Functionally Safe Automated Driving- Leveraging Diagnostic Specifications for FSC design
doi: 10.4271/2017-01-0056

ATRIUM — Architecting under uncertainty: For ISO 26262 compliance
doi: 10.1109/SYSCON.2017.7934819

Applying systems-theoretic process analysis in the context of cooperative driving
doi: 10.1109/SIES.2016.7509433

Architecture exploration for distributed embedded systems: a gap analysis in automotive domain
doi: 10.1109/SIES.2017.7993377

Safe Stop Trajectory Planning for Highly Automated Vehicles: An Optimal Control Problem Formulation
Proceedings of 2018 IEEE Intelligent Vehicles Symposium (IV), 2018

Architecting Safety Supervisors for High Levels of Automated Driving
Proceedings of the 21st IEEE International Conference on Intelligent Transportation Systems

Architecting Safe Automated Driving with Legacy Platforms
Licentiate Thesis, 2018

A practical simulation toolchain for the early verification of Functional Safety Concepts.
SAE Technical Paper 19AE-0203/2019-01-0126

Tuning permissiveness of active safety monitors for autonomous systems
Nasa Formal Methods, April, 2018

Improving Image Classification Robustness using Predictive Data Augmentation
W AISE 2018

Industrial Safety-Related Considerations to Introducing Full Autonomy in the Automotive Domain
DeCPS workshop, Vienna, 2017

Complexity Challenges in Development of Cyber-Physical Systems
Proc. of Principles of modelling Essays dedicated to Edward Lee. 2018

Industrial Safety-related Considerations to Introducing Full Autonomy in the Automotive Domain
DeCPS: Focus on Transportation of the Future. In conjunction with the 22nd Int. Conf. on Reliable Software Technologies Ada-Europe 2017 (Vol.38, Issue 4, P218-221)

Verification Methodology for Fully Autonomous Heavy Vehicles
2016 IEEE International - Conference on Software Testing, Verification and Validation (ICST)

An Architectural Solution for Achieving Fair Data Age Distribution in Vehicular Communications
2017 IEEE Real-Time and Embedded Technology and Applications Symposium

Industrial Safety-Related Considerations to Introducing Full Autonomy in the Automotive Domain
Proc. of the Workshop on Challenges and New Approaches for Dependable and Cyber-Physical System Engineering, (at Ada Europe 2017), Ada User Journal, Vol 38, No. 4, Dec 2017

Automated Driving Safer and More Efficient - Future Driving, Editors: Daniel W atzenig and Martin Horn
ISBN 978-3-319-31893-6

Systems engineering and architecting for autonomous driving
ISBN 978-3-319-31893-6

7.3 Patent

- N. Mohan, P. Roos & J. Svahn, “System and Method for Controlling a Motor Vehicle to Drive Autonomously”, Filed at Swedish Patent Office, PRV; no 1751581-8, 2017.
- N. Mohan, P. Roos & J. Svahn, “System and Method for Controlling a Motor Vehicle to Drive Autonomously”, Filed at Swedish Patent Office, PRV; no. 1751580-0, 2017

8 Slutsatser och fortsatt forskning

De övergripande forskningsfrågor som formulerades i projektbeskrivningen har behövt brytas ned i mindre delfrågor, och en hel del frågor återstår för fortsatt forskning inom ECSEL-projektet Prystine, (https://www.kth.se/en/itm/inst/mmk/forskning/mekatronik-och-inbyggda-styrsystem/projekt/systemarkitektur/prystine-1.859543) som utgör en direkt fortsättning av ARCHER med en breddning som innefattar internationellt samarbete. Archer har varit väldigt värdefullt genom att etablera forskargruppen som en ledande aktör inom området ”safety engineering for automated driving”.

Resultaten i form av metodik och hittills uppnådda insikter kommer att användas i det fortsatta arbetet med autonoma fordon på Scania.

9 Deltagande parter och kontaktpersoner

Projektet ARCHER drevs som ett samarbete mellan Scania och KTH, med Scania som finansiellt sökande och projektledare. Projektet drevs från Scania av en arbetsgrupp ansvarig för elsystemsarkitektur och säkerhetsanalys. Kontaktperson för denna gruppering är Dr Johan Svahn. Ett flertal andra grupper inom Scania involverades vid behov av spetskompetens inom specifika områden.

KTH-delen av projektet genomfördes av avdelningen för Mekatronik och inbyggda system, ledd av professor Martin Törngren. Mekatronikenheten är en ledande grupp i Europa inom cyberfysiska och inbyggda system, med nyckelkompetens inom funktionell säkerhet, systemarkitektur, modellbaserad utveckling och integrerad mekatronikutveckling. Teamet är aktivt i ett flertal europeiska projekt i detta område, inkluderande AutoDrive, Fed4SAE, PRYSTINE och SCOTT. Samarbete sker också med Zenuity och Volvo personvagnar inom elsystemsarkitektur för autonoma fordon (ESPLANADE FFI projektet). Mekatronikavdelningen leder kompetensnätverket ICES (www.ices.kth.se), vilket ger utmärkta kontakter med industrin. Teamet har också ett väletablerat samarbete med (bland annat) EECS vid University of California at Berkeley, OFFIS (forskningsinstitut i Oldenburg, Prof. Werner Damm), och FORTISS (forskningsinstitut i Munchen kopplat till TUM).