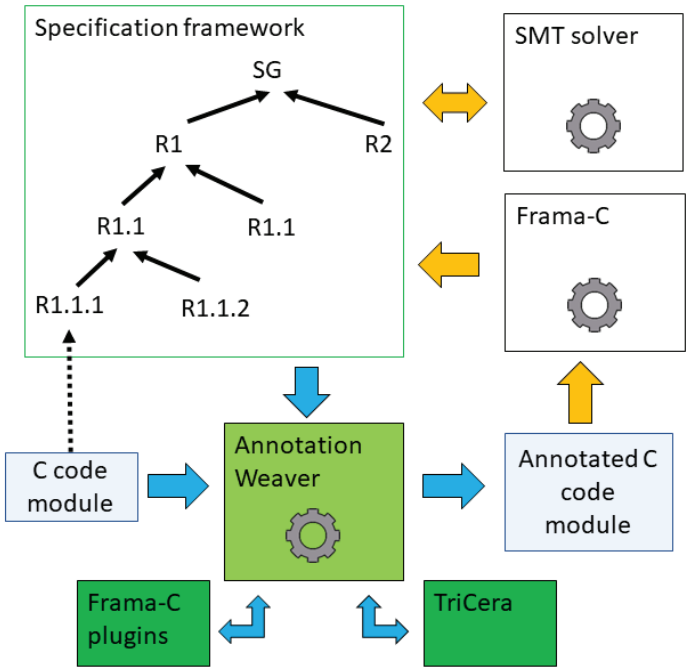
AVerT

Automated Verification and Testing

Publik rapport



Författare: Mattias Nyberg och Dilian Gurov
Datum: 2022-02-03
Projekt inom Delprogrammet Elektronik, mjukvara och kommunikation

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 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.

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

Innehållsmässigt var planen enligt ansökan att arbeta inom fyra arbetspaket:
- WP1 Project coordination
- WP2 Requirement decomposition
- WP3 Deductive verification of C-code
- WP4 Verification of Simulink models
- WP5 Machine Learning for Automated Testing on Virtual Vehicle Simulators

WP2 och WP3 har utförts enligt plan enligt vad som är beskrivet senare i denna text.

WP4 har utförst enligt plan också: verktyg har tagits fram, artiklar har skrivits, och ett antal case studies har utförts. Dock är slutsatsen att området är mer omfattande och komplicerat än vad vi trodde från början. För att nå en industrialisering krävs mycket mer jobb och en extern verktygsleverantör behöver delta; Scania och KTH kan inte bära detta själva. Därför har vi bestämt att i AVerT2 kommer vi inte att fokusera på "Verification of Simulink models". En annan motivering är också att om vi lyckas fullt ut med "Deductive verification of C-code" så behövs inte formell verifiering av Simulink-modeller.

WP5 uteslöts i början av projektet p.g.a. att den grupp på KTH som skulle jobba med detta drog sig ur av rättighetsskäl. De resurser som då blev frigjorda har istället använts för att stötta WP2 och WP4.

I ansökan, inom WP1, lovades också att organisera öppna workshops. Dessa har uteblivit pga Corona. Målet att arrangera sådana workshops är överfört till AVerT2.

WP3 har jobbat med automatisk formell verifiering av källkod skriven i C. Arbetet har i huvudsak utförts och drivits av KTH-doktoranden Christian. Status är att vi har lyckats automatiskt verifiera enkla industriella SW-moduler från Scania. Det som saknas är stöd för dels vissa C-objekt såsom arrayer, och dels flyttal. Dessutom behöver framtagna lösningar packeteras för lättare industriell användning. Allt detta kommer ske i det accepterade nya projektet AVerT2 som finansierar Christians sista år, en ny KTH-doktorand som fokuserar på flyttal, samt en Scaniaingenjör som fokuserar på packeteringen och teknologiöverföring till Scania.

WP2 har jobbat med strukturering av krav för att stödja en kompositionell formell verifiering av stora system, tex en lastbil. Arbetet har främst drivits från Scania, doch med hjälp av KTH. Utan att förutsätta formellt skrivna krav överallt, har vi formaliserat strukturingen av krav med syfte att dela upp verifieringen i mindre delar, s.k. kallad kompositionell verifiering.
Vi har lyckats applicera metoden och verktyg på små exempel och vi har sen försökt applicera dessa på större industriella system. Slutsatserna är:
- Stora industriella exempel kräver mycket arbete med dedikerade resurser, så i AVerT2 har vi säkerställt att vi har sådan resurs genom ovan nämnda Scaniaingenjör.
- Säkerhetskritiska system, som är det tänkta syftet med AVerT, innehåller krav med sannolikheter, i alla fall inom högre nivåers krav. Därför är de framtagna metoderna, som förutsätter icke-probabilistiska krav otillräckliga. Att generalisera metoderna till probabilistiska krav har därför blivit ett mål i AVerT2 och även ett annat uppstartat FFI-projekt SafeDim.

Akademiska målen att producera artiklar samt att doktoranden ska genomgå första delen av forskarutbildning har lyckats fullt ut. Antal och kvalitet på artiklar har mer än väl motsvarat målen.

2 Executive summary in English

The purpose has been to create formal methods and tools for industrial development of safety-critical systems. The ambition was to work in four areas:
1. requirement decomposition
2. deductive verification of C-code
3. verification of Simulink models
4. Automated Learning based Testing

Due to IPR reasons, 4 was discontinued, and regarding 3, results were created but these are considered too demanding to maintain because an external tool supplier would be needed. Within 1 and 2, good results have been created and these are further developed within the continuation project AVerT2.

WP2 and WP3 have mainly created results in the form of methods and tools in two areas:
- structuring of requirements to support a compositional formal verification of large systems, such as a truck;
- automatic formal verification of source code written in C.

We expect these results to be transferred to Scania and also other companies. There is a great interest in this. However, the results are not yet ready for direct use in industry. Therefore, the continuation project AVerT2 has been created with a focus on packaging the results for industrial use.

Central to the project has been a doctoral student at KTH. He has partly performed academic research which has resulted in scientific articles, partly worked with the implementation of the tool AnnotationWeaver which is developed within the project, and then also worked with case studies. The project has also had thesis workers, summer workers, and project positions, all of which have contributed to tool development and case studies. The work with case studies has continuously provided feedback on what new research is needed and how the tool needs to be developed.

3 Bakgrund

Som FFI:s färdplansdokument påpekar går vi mot en transportmodell där autonoma fordon, sammankopplade med varandra och med transportinfrastrukturen, kommer att bilda ett komplext system-av-system, där fordonsmjukvaran behandlar ett kontinuerligt flöde av inkommande information, är utbyggbart och självanpassande och garanterar höga nivåer av säkerhet. Alla dessa utvecklingar resulterar i en ökning av mjukvarans och systemens. Särskilt, färdplanerna pekar på behovet av att hantera olika systemnivåer, att ge stöd för agil mjukvaruutveckling och kontinuerlig integration, samt uppfylla högre krav på funktionell säkerhet och tillhandahålla verktygsstöd för automatisering av själva V&V-processen.

4 Syfte, forskningsfrågor och metod

Syftet har varit att skapa formella metoder och verktyg för industriell utveckling av säkerhetskritiska system.

Central i projektet har varit en doktorand vid KTH. Han har dels forskat vilket resulterat i vetenskapliga artiklar, dels jobbat med implementation av verktyget AnnotationWeaver som utvecklas inom projektet, och sen också jobbat med case studies. Projektet har även haft exjobbare, sommarjobbare och projektanställningar som alla bidragit till verktygsutveckling och

fallstudier. Arbetet med fallstudier har löpande gett feedback om vilken ny forskning som behövs samt hur verktyget behöver utvecklas.

5 Mål

Ambitionen var att arbeta inom fyra områden:
1. requirement decomposition
2. deductive verification of C-code
3. verification of Simulink models
4. Automated Learning based Testing on Vehicle Simulators

Pga rättighetsskäl utgick det sista, och angående 3, så skapades resultat men dessa bedöms för krävande att förvalta ty en extern verktygsleverantör skulle behövas. Inom 1 och 2 har skapats bra resultat och dessa utvecklas vidare inom fortsättningsprojektet AVerT2.

6 Resultat och måluppfyllelse

De viktigaste **resultaten** från AVerT är:

1. Ett formellt ramverk för kravnedbrytning, baserat på resonemang över kontrakt i assume-guarantee-stil.
2. En metod och prototypverktyg för automatisk generering av annotationer för deduktiv verifiering av C-kod med verktyget Frama-C, för en betydande delmängd av C-språket.
3. Inledande resultat av att använda TriCera, en C-model checker, för automatisk generering av funktionskontrakt för C-funktioner, för en delmängd av C-språket.
4. En metod och prototypverktyg för bounded model checking av Simulink/Stateflow-modeller, baserad på en symbolisk exekveringssemantik av Stateflow som vi har utvecklat.
5. En utvärdering av vår verifieringsmetod på tre fallstudier från Scania. Alla formaliserade krav verifierades helt automatiskt.

Bidrag till FFI:s mål:

Öka den svenska kapaciteten för forskning och innovation och därigenom säkerställa konkurrenskraft och arbetstillfällen inom fordonsindustrin. Verktygen som levererades av AVerT-projektet är öppen källkod och är tillgängliga för den svenska fordonsindustrin. Detta gör det möjligt för fordonstillverkare, som Scania och Volvo Cars, att införliva dessa verktyg i sina verktygskedjor och V&V-processer, och därmed stärka sina fordons konkurrenskraft genom att ge ännu högre garantier för funktionssäkerhet.

Utveckla internationellt sammanlänkade och konkurrenskraftiga forsknings- och innovationsmiljöer i Sverige. AVerT-projektet har genomförts inom ramen för flera andra relaterade projekt, varav tre är europeiska. Detta har främjat detta mål.

Främja tvärindustriellt samarbete. Medan verktygsutveckling och fallstudier har varit till övervägande del utförda på Scania, omfattade spridningen öppna workshops och demodagar som var öppna för svensk fordonsindustri. I synnerhet har vi bjudit in utvecklare från Volvo Cars som redan hade uttryckt intresse för de potentiella resultaten av AVerT. Detta, tillsammans med verktygens öppen källkodskaraktär, bidrar till ett tvärindustriellt samarbete.

Främja samarbetet mellan industri, universitet och högskolor. AVerT är unikt genom att det omfattar ett antal forskare som är anställda både på Scania och KTH. Projektledaren, prof. Mattias Nyberg från Scania, är adjungerad professor på KTH, medan alla återstående deltagare från KTH har tillbringat tid på Scania i samband med olika föregångarprojekt till AVerT. Projektet har också främjat samarbetet genom deltagarnas industriella och akademiska nätverk. Särskilt kan vi nämna KTH Innovativa Centrum för inbyggda system (ICES) (www.ices.kth.se/), som involverar medlemmar från flera forskargrupper vid KTH och har ett nära samarbete med en lång rad industriella partners.

Bidrag till delprogrammets mål:

Simulering och validering på olika systemnivåer. Hela konceptet med AVerT var att möjliggöra den formella verifieringen i kombination med testning på olika systemnivåer, fångad av en hierarkisk arkitekturmodell. Nyckeln till att koppla ihop de olika nivåerna är ramverket för kompositionsresonemang som har utvecklats inom AVerT. Alla aspekter av detta stöds av automatiserade verktyg som syftar till att dölja det mesta av komplexiteten bakom tillvägagångssättet.

Stöd för tidig och kontinuerlig integration. Kompositionsaspekten av vårt tillvägagångssätt tillåter modularisering av V&V (i vårt fall, formell verifiering och testning). Detta innebär att V&V kan utföras inkrementellt, och V&V-resultat (d.v.s. feedback från verifiering och testning) kan lagras, spåras och återanvändas. Detta är nyckeln till agil mjukvaruutveckling med integrerad V&V, eftersom det gör att små ändringar i kodbasen snabbt och fullständigt kan verifieras.

Funktionell säkerhet och certifiering. Målet för AVerT är funktionssäkerhet för enskilda fordon såväl som för fordon inom en transportinfrastruktur. Vi har inriktat oss på ISO 26262-standarden, både med avseende på nedbrytningen av säkerhetskrav och till det faktiska sättet för deras V&V. Standarden rekommenderar formell verifiering (bland andra tekniker). AVerT bidrog till att öka mognaden för formell verifiering inom fordonsindustrin. De kommande standarderna för autonoma fordon förväntas följa denna linje.

Mjukvarubaserad V&V-metodik. Den långsiktiga visionen för AVerT är en helautomatiserad V&V-metodik som är integrerad i mjukvaruutvecklingsprocessen. AVerT tåg ett synligt steg mot detta mål genom att utveckla verktyg som automatiserar några av de mest arbetsintensiva och kompetenskrävande uppgifterna för traditionell formell verifiering av programvara.

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	Genom forskning och industriella fallstudier
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	Förs vidare till fortsättningsprojektet AVerT2 och därigenom också till Scania och annan fordonsindustri tack vare ett planerat stort fokus på tekniköverföring.
Föras vidare till produktutvecklingsprojekt	X	Den stora fallstudien i AVerT2 är ett projekt som är planerat att föras i produktion.

Introduceras på marknaden	X	Ja, se ovan.
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		Inte direkt, men om vi kan påvisa att formell verifiering fungerar bra industriellt, kan standarder inom tex. funktionell säkerhet komma att påverkas, eftersom sådana standarder löpande uppdateras för ta in nya tekniska framsteg.

7.2 Publikationer

Formal Verification in Automotive Industry: Enablers and Obstacles Mattias Nyberg, Dilian Gurov, Christian Lidström, Andreas Rasmusson, and Jonas Westman In Proceedings of: ISoLA'18 Lecture Notes in Computer Science, vol. 11247, pp. 139-158, 2018

A Hoare Logic Contract Theory: An Exercise in Denotational Semantics Dilian Gurov, and Jonas Westman
In: Müller P., Schaefer I. (eds) Principled Software Development Springer, Cham, pp. 119-127, 2018

Improved Pattern for ISO 26262 ASIL Decomposition with Dependent Requirements Christian Lidström, Carl Bondesson, Mattias Nyberg, and Jonas Westman QRS Companion, pp. 28-35, 2019

Formally Proving Compositionality in Industrial Systems with Informal Specifications Mattias Nyberg, Jonas Westman, and Dilian Gurov In Proceedings of: ISoLA'20 Lecture Notes in Computer Science, vol. 12478, pp. 348-365, 2020

Constraint-Based Contract Inference for Deductive Verification Anoud Alshnakat, Dilian Gurov, Christian Lidström, and Philipp Rümmer
In: W. Ahrendt et al. (Eds.) Deductive Software Verification Lecture Notes in Computer Science, vol. 12345, pp. 149-176, 2020

Practical Abstractions for Automated Verification of Shared-Memory Concurrency Wytse Oortwijn, Dilian Gurov, and Marieke Huisman In Proceedings of: VMCAI'20 Lecture Notes in Computer Science, vol. 11990, pp. 401-425, 2020

An Abstraction Technique for Verifying Shared-Memory Concurrency Wytse Oortwijn, Dilian Gurov, and Marieke Huisman Applied Sciences, vol. 10, no. 11, pp. 1-48, 2020

An Abstract Contract Theory for Programs with Procedures Christian Lidström, and Dilian Gurov In Proceedings of: FASE'21 Lecture Notes in Computer Science, vol. 12649, pp. 152-171, 2021

Dynamic Vulnarability Detection on Smart Contracts Using Machine Learning Mojtaba Eshghie, Cyrille Artho, and Dilian Gurov In Proceedings of: EASE'21 ACM, pp. 305-312, 2021

Bounded Invariant Checking for Stateflow Programs Predrag Filipovikj, Dilian Gurov, and Mattias Nyberg Technical Report, 35 pages, November 2021

Category Theory Framework for Variability Models with Non-Functional Requirements Daniel-Jesus Munoz, Dilian Gurov, Mónica Pinto, and Lidia Fuentes In Proceedings of: CAiSE'21 Lecture Notes in Computer Science, vol. 12751, pp. 397–413, 2021

Alice in Wineland: A Fairy Tale with Contracts Dilian Gurov, Christian Lidström, and Philipp Rümmer Submitted, 2021

An Exercise in Mind Reading: Automatic Contract Inference for Frama-C Jesper Amilon, Zafer Esen, Dilian Gurov, Christian Lidström, and Philipp Rümmer Submitted, 2021

Advanced Reasoning of Quality Valued Configurations in Category Theory Daniel-Jesus Munoz, Monica Pinto, Dilian Gurov, and Lidia Fuentes Submitted, 2021

8 Slutsatser och fortsatt forskning

De viktigaste **slutsatserna** från projektet är att automatisk deduktiv verifiering av C-kod och modellkontroll av Simulink/Stateflow-modeller är möjligt, men kräver ytterligare arbete med kravformalisering och verktygsautomatisering, för att ta med vår verifieringsmetod till en mognadsnivå som möjliggör överföring till industriell praxis.

Vi fortsätter vårt arbete med **fortsättningsprojektet AVerT2**, som kommer fokusera just på kravformalisering och verktygsautomatisering, och på överföring av våra metoder och verktyg till industriell praxis.

9 Deltagande parter och kontaktpersoner

Scania
Adj. Prof. Mattias Nyberg

KTH
Assoc. Prof. Dilian Gurov