Trustworthy Automated Driving DevOps - TADDO

Publik rapport

Författare: Martin Törngren
Datum: 2024-04-29
Projekt inom Trafiksäkerhet och automatiserade fordon

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.

Läs mer på www.vinnova.se/ffi.

1   Sammanfattning

Förstudieprojektet TADDO har haft som mål att bana väg för en ny metodik för autonoma fordon och deras stödjande digitaliserade infrastrukturer som tillåter frekventa uppdateringar av kärnfunktionalitet som perception och planering, samtidigt som personsäkerhet och andra pålitlighetsegenskaper garanteras. Vi kallar konceptet för "pålitlig DevOps" för autonoma fordon, och avser då behovet att kunna lita på hela kedjan från monitorering, över utveckling och uppgradering, till reella risker i den operationella miljön.

TADDO som ett förstudieprojekt har haft syftet att ta fram en synopsis för ett större fortsättningsprojekt. TADDO har resulterat i två inskickade forskningsansökningar som för närvarande är under utvärdering

Projektet har bedrivits med ett antal workshops, till vilka parterna har bidragit genom studier och presentatoner av state of the art, ny relevant lagstiftning/standards och med fallstudier. Genom workshoparna har relevanta områden för forskning där industribehov finns identifierats.

2   Executive summary in English

The TADDO prestudy project was approved in June 2023 by Vinnova for a project period of 2023-06-14 -2024-03-15. The project involved eight partners encompassing transport service providers, automotive OEMs, tier 1's and 2's, expert consultancy and KTH.

The key idea of TADDO was to investigate the gap between software (CI/CD) and safety practices, identify key challenges and directions, and formulate at least one corresponding follow-up larger scale research proposal. TADDO has resulted in the formulation and submission of two proposals in the area of safety assurance of continuously evolving automated driving systems; (1) one on efficient and effective virtual evaluation, and the second on (2) architecting and development methods.

TADDO chose to use workshops as a method to drive the work forward. This proved to be successful with strong engagement and contributions from all partners. In total, 7 physical workshop meetings were arranged complemented by several online meetings. The partners have contributed to the workshops by preparing inputs and by studying material including state of the art, industrial best practices and relevant regulations. During the workshops, gaps were also identified and used to flesh out the focus of the two proposals. The project has also had international interactions including with the German national project "AutoDevSafeOps" and its partners. Parts of TADDO findings have been (and will be) presented through keynotes and invited talks including at first Safe Autonomy workshop at EDCC in April, and at a forthcoming SAFER competence group meeting in May on safety assurance.

3   Bakgrund

It is clear that automated vehicles (AV's) will require software development methodologies that embrace continuous integration and deployment, with continuous learning from data collected in the operational environment to improve, verify and validate functionality and performance. DevOps is a standard practice in IT and cloud systems to reduce the time between Development and Operations, enabling frequent releases. The practice is closely related to agile development with abilities to quickly respond to changes in requirements.

As vehicles are becoming increasingly "software defined", the ability to incorporate new features, improve quality and deal with new security threats, provides strong drivers for new DevOps methodologies that are applicable also for safety-critical systems. This trend is further amplified by vehicles at high levels of automation since their maturation and improvements will necessitate learning and incorporating updates based on experiences in complex environments. At the same time, it is also clear that current DevOps methodologies do not sufficiently consider assurance in accordance with relevant safety and security standards, while current assurance practices prevent fast and frequent update and release cycles of software. The alternative of just combining current DevOps methods with traditional methods of safety and security standards is also not viable since this will result in many bottlenecks and long lead-times (many months). This is clearly not compatible with continuous deployment and neither efficient nor effective.

4 Syfte, forskningsfrågor och metod

The overall purpose of the prestudy project was to pave the way for a new methodology for connected automated vehicles (CAV's) to reconcile software DevOps and safety practices. Developments in this area were seen to be necessary for and contribute to enhanced traffic and work environment safety in an evolving road traffic landscape with automated and new types of vehicles, while also being key for industrial competitiveness.

In paving the way towards such a new methodology, the pre-study project set out to investigate state-of the art, industrial practices, and relevant legislation and standards, in order to identify gaps that deserved specific further collaborative research efforts.

TADDO chose to use workshops as a method to drive the work forward. This proved to be successful with strong engagement and contributions from all partners. In total, 7 physical workshop meetings were arranged complemented by several online meetings. The partners have contributed to the workshops by preparing inputs and by studying material including state of the art, industrial best practices and relevant regulations. During the workshops, gaps were also identified and used to flesh out the focus of the two proposals. The project has also had international interactions including with the German national project "AutoDevSafeOps" and its partners. Parts of TADDO findings have been (and will be) presented at keynotes and invited talks including at first Safe Autonomy workshop at EDCC in April, and at a forthcoming SAFER competence group meeting in May on safety assurance.

5 Mål

The TADDO prestudy proposal had the goals to, (1) identify important directions for Trustworthy DevOps, addressing gaps and barriers that needs to be overcome, and, (2) to develop a synopsis for a follow-up research project based on a prioritization of topics anchored with key automotive Swedish stakeholders.

6 Resultat och måluppfyllelse

The project results have met the expectations by creating two project proposals, VIVA (for the Vinnova Advanced Digitalization program), and TADDO2 (for FFI).

We believe that both proposals are highly industrially and scientifically relevant, and also that the proposals are competitive. We will see how they are evaluated. The TADDO project has also led to a tight collaboration between the partners that is likely to pave the way for a continuation in one way or the other.

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	The project has increased the knowledge in the area for all partners. Dissemination has so far taken place through a number of invited presentations, e.g. an invited presentation at the SAFER competence group on Safety assurance and a keynote at the first Safe Autonomy workshop.
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	The pre-study project submitted two proposals for larger-scale follow up projects.
Föras vidare till produktutvecklingsprojekt		The findings of the project have been internally disseminated by the industrial partners.
Introduceras på marknaden		Not applicable.
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		The partners are active in providing feedback to new related Swedish regulations. One of the follow-up projects directly plans to influence evolving standards in the area.

The TADDO project has yielded synergies with other ongoing projects which the partners are part of, including SALIENCE4CAV and EVIDENT. TADDO has helped to gather results from several projects such as these and the broader state of the art in formulating the follow-up proposals.

7.2 Publikationer

The prestudy has not directly yet resulted in any publication, apart from the two research proposals that were prepared. Research publications are however in progress.

8 Slutsatser och fortsatt forskning

The results from the TADDO project confirm that more research and industrial developments are needed to deal with the gap between software (CI/CD) and safety practices. Current practices will not scale in terms of cost, required efforts and safety; there is a need to develop new methodologies where the TADDO project identified two main larger areas to support for safety assurance of continuously evolving automated driving systems; methods and frameworks for trustworthy DevOps, and virtual verification.

9 Deltagande parter och kontaktpersoner

The TADDO project involved the following eight partners (with contact persons).

Partner:	Contact
CAG Syntell	Mollie Hasselberg
Einride Autonomous Technologies	Andreas Allström
KTH	Martin Törngren
Qamcom	Anders Cassel
Scania	Mattias Nyberg
Volvo Autonomous Solutions	Stefan Thorn
Veoneer / Magna	Carina Marcus
Zenseact	Håkan Sivencrona