# DevOps Safety – do not get left at the station!


Anders Cassel
*Qamcom*
Linköping, Sweden
anders.cassel@qamcom.se

Bengt Haraldsson
*Scania*
Södertälje, Sweden
bengt.haraldsson@scania.com

Daniel Sandberg
*Scania*
Södertälje, Sweden
daniel.x.sandberg@scania.com

Fredrik Beckman
*Magna Electronics*
Linköping, Sweden
fredrik.beckman@magna.com

Martin Törngren
*KTH*
Stockholm, Sweden
martint@kth.se

Mattias Nyberg
*Scania*
Södertälje, Sweden
mattias.nyberg@scania.com

Molly Hasselberg
*CAG Syntell*
Stockholm, Sweden
mollie.hasselberg@cag.se

Murat Erdogan
*Magna Electronics*
Linköping, Sweden
murat.erdogan@magna.com

Rolf Johansson
*Astus*
Mölndal, Sweden
rolf@astus.se

Sebastian Holmqvist
*Einride*
Göteborg, Sweden
sebastian.holmqvist@einride.tech

Tom strandberg
*CAG Syntell*
Stockholm, Sweden
tom.strandberg@cag.se

Xinhai Zhang
*Scania*
Södertälje, Sweden
xinhai.zhang@scania.com



***Abstract*—There is a strong business logic in the direction of software-defined vehicles (SDV), with new versions of functionality deployed at a high pace in the vehicles on the road. This is generally true for all highly complex features, as for example modern advanced driver-assistance systems (ADAS), but for automated driving systems this is a must. Even if there is a well-established tradition in other areas of continuous deployment (CD) by constantly learning from the operations (DevOps), the automotive driving functions are safety critical which adds a completely new dimension to the DevOps task. We claim that this calls for a capability to build complete and convincing assurance cases integrated in the automated framework denoted continuous integration (CI), conventionally only covering the software. We also claim that such a merge between best practices from safety, security and software engineering, only can become successful together with a systems approach including, architectural patterns suited for modular argumentation, an information model for automating assurance cases in CI, and a product increment plan for the necessary learning loops. Such a plan encompasses design for Ops-data collection, serving needs for future safety case evidence to achieve an overall Trustworthy Automated Driving DevOps.**



***Keywords— automated driving, safety, safety assurance, continuous safety assurance, DevOps, trustworthiness***


## I. Introduction

The automotive industry is going through a transformation, including a higher pace of development, an increased focus on software including data and further emphasis on decoupling hardware and software to support updates – together referred to as the "software defined" vehicle (SDV). At the same time, the push towards highly automated vehicles introduces new technical challenges and new types of complexity. Safety and security practices, including standards upon which these are built, reflect best practices and thus have to be updated to deal with those changes.

Two main driving forces are at play:

- Market adaptability: Staying attuned to the market by shortening time to market, being able to deliver upon, constantly changing and evolving, market needs including post initial deployment.
- Development efficiency: coping with evolving electrical architectures, learning from AV operations in the field and adapting to complex OEM-Tier1-Tier2 relationships.

Industry actors respond to these forces by adopting DevOps into their development processes to enable a steady flow of value to their customers. This includes the capability of introducing new features to systems existing in the field. Actors are opening up their development environments to enable tighter integrations between suppliers.

The tension is building up between being able to deliver quickly, and in maintaining rigor and completeness in safety and security practices. Then, do we continue in our tracks, adding further tension by solving our new challenges with existing old practices and tools, or do we adapt to the new way of working? In other words – the DevOps train is leaving the station to deliver value. Do we want to jump onboard or be left at the station?

## II. The complexity challenge

Automated vehicles (AV's), referring to level 3 and above for the SAE levels of Automation (standard J3016), may operate in very complex operational environments depending on the operational design domain (ODD). Considering more open ODD settings on public roads, the traffic environments include various road users, a very large number of potential traffic scenarios, as well as infrastructure and connectivity to cloud services. To deal with this complexity, AV's are filled with advanced technologies (high demand on computing resources, very complex software, machine learning, data maps, positioning systems and other external services etc.), supported by a digitalized infrastructure and interacting with humans in different roles!

An overarching problem for applying DevOps to automated driving systems (ADS) is that of complexity management. For ADS, this includes design for safety and security, defining appropriate risk metrics for safety and

providing support to assess what ADS changes are needed based on continuous learning of how well the ADS operates in the actual environment. To achieve this, operational performance needs to be evaluated and relevant changes planned in response to collected Ops data, to be able to assess what the potential safety implications are, also considering AV interactions with other road users. Further requirements include establishing a supporting architecture and methodology that allows to effectively, and more efficiently than today, assess the residual risks and update the safety and security assurance cases to enable DevOps for AV's.

To address both the market and development risks and the complexity challenge introduced above, DevOps practices are employed. However, the two contemporary practices of Software development, and Safety and Security assurance, come from two, not yet harmonized perspectives as depicted in figure 1:

- Software (SW) development – encompassing continuous integration and continuous deployment (CI/CD) of SW including machine learning components, 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.
- Safety and security assurance in critical systems development in accordance with relevant standards and regulations. These engineering practices place a stringent emphasis on design for safety and security, and processes, typically characterized by high effort and very slow cycles. Assurance cases must be compiled and assessed, covering all evidence and arguments that the product (i.e., all the elements comprising the ADS), is safe and secure to operate, and that all corresponding activities are correct and complete. Assurance is required for each release of new/changed functionality, and much of the corresponding analysis is still manual, including assessing when changes have been made and their impact. A key reason for the assurance complexity is that safety and security depend on the behavior of a system as-a-whole, in its environment. It is not enough to focus only on the SW, requiring costly analysis, verification and validation (V&V) efforts for each ADS release.

AV's will require DevOps to address the challenges. At the same time, it is also clear that current DevOps methodologies do not sufficiently consider assurance, 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 in best case, or years in worst case).

To conclude, Trustworthy DevOps methods and process frameworks need to be defined which can deliver safety and security assurance cases continuously deployed together with every ADS release.

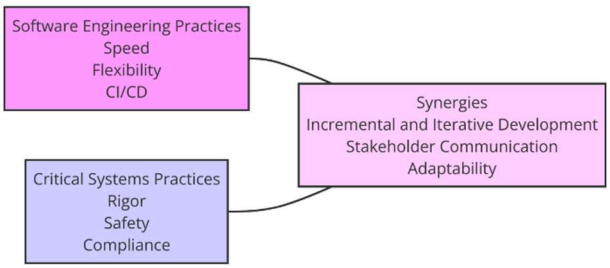


*Figure 1. Contrasting DevOps properties and synergies*

## III. Research directions

*Trustworthy DevOps* methods and process framework integrated in a CI/CD pipeline have to meet the need that safety and security assurance cases can be incrementally improved and where every change is supported by arguments and evidence that the ADS operation is safe and secure. All relevant information needs to be expressed in a unified information model describing ADS functionality, safety and security properties, their requirements and solutions by a formal syntax at all abstraction levels from ADS Item level down to realization in HW and SW. Furthermore, the methods and process framework shall support automatic impact analysis, safety and security analysis, and analysis of safety performance indicators, enabling instant evaluation of alternative solutions, and impact of changes driven by Ops data. The target is to support a modular component-based design and separation of concern, where the impact of changes is known at every instance and the rigorous effort of V&V activities can be limited to only those components that are impacted by the change.

Our research aims to address the challenges, harmonize the synergies between existing DevOps with safety and security practices, and develop new methodologies and frameworks for trustworthy DevOps including

- Specification, analysis and architectural design for safety and security, covering a unified architecture and information model supporting evolving modular product architecture, continuous analysis of changes, evidence of completeness and correctness that can be integrated as part of a CI/CD pipeline.
- Efficient and effective V&V activities by using e.g. digital twins, satisfying safety and security standards and regulations, e.g. the EU 2019/2144, 2022/1426 and 2022/2236.
- Specification, planning, monitoring, and feedback of a sufficient and correct set of Ops data in the DevOps loop.
- Continuous generation of safety and security assurance cases, based on safety argumentation and evidence compiled from the information model.
- Organizational and business considerations of all relevant actors along the DevOps chain supporting incremental planning, fast feedback and learning cycles, that could impact safe and secure deployment and operation of ADS, and corrupt or invalidate the monitoring of Ops data.

*This work is supported by FFI, the Swedish Strategic Vehicle Research and Innovation program, through the TADDO2 project (2024-00816).*