Open Sandbox: Automated Verification of Security and Safety for Fast Vehicle Software Deployment

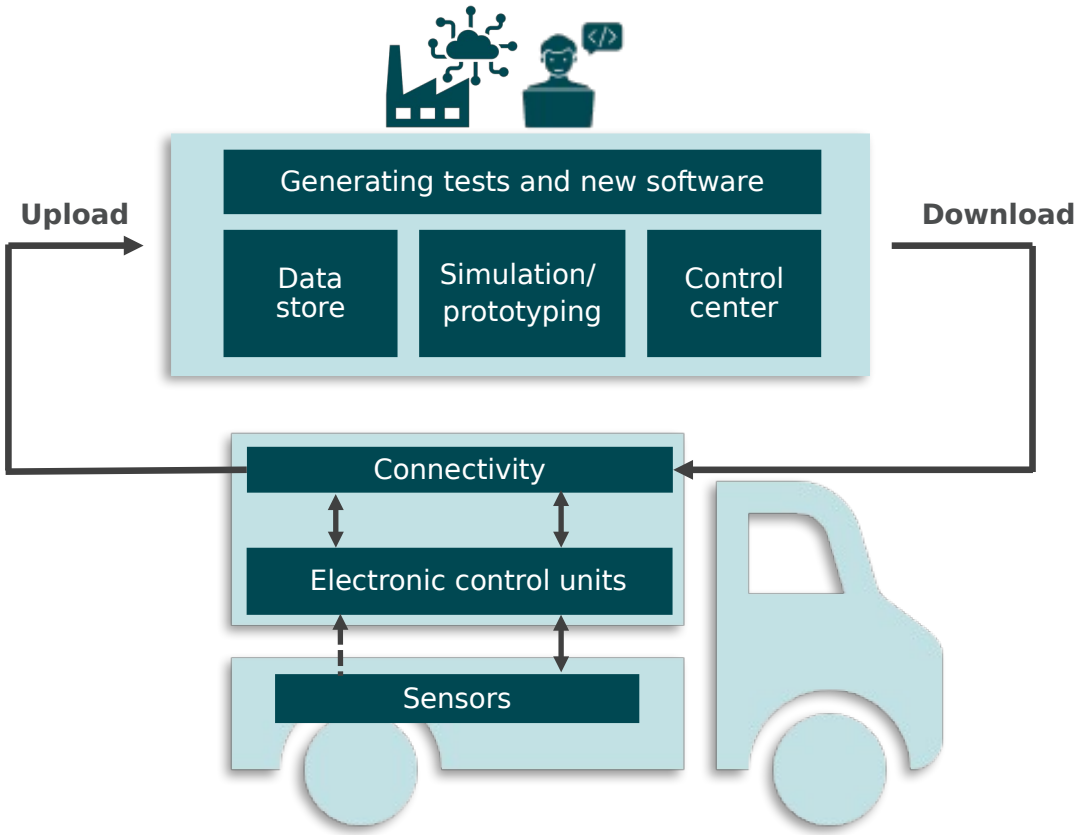
Karl Palmskog* Mattias Nyberg†

* PI, KTH; lecturer, KTH/EECS/CS/TCS
† project manager, Scania; adjunct professor, KTH

2024-05-21

Background and Motivation

- Scania vehicles increasingly depend on software
- software needs to be continually revised (fix issues, add features)
- deployment time for new revision ranges from **months** to **years**
- core problem: testing new revisions takes a long time



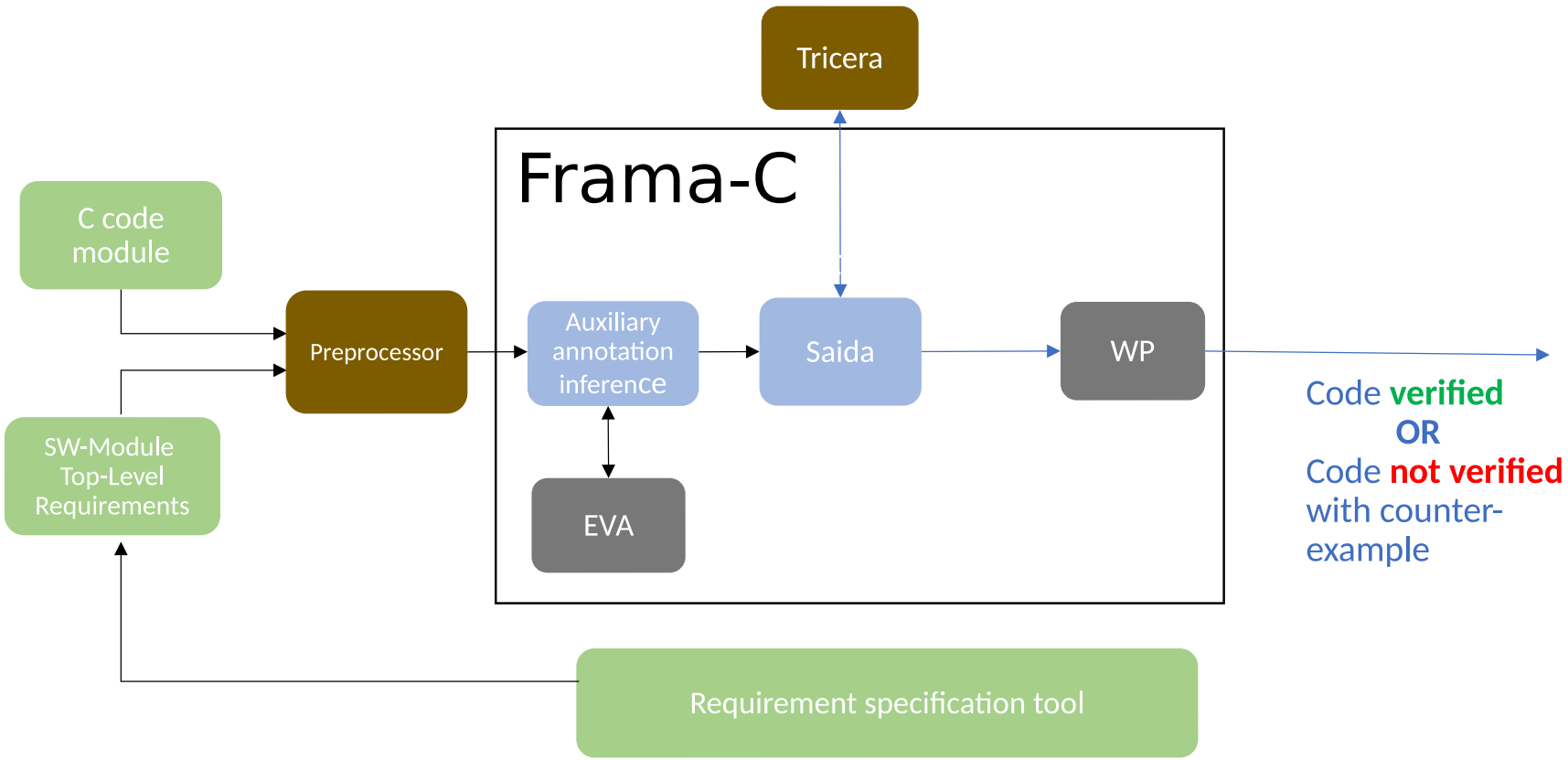
Project Objective

Shorten time-to-deployment for new vehicle software.

- approach: automated, **incremental** formal verification of code
- safety and security guaranteed using **code contracts**

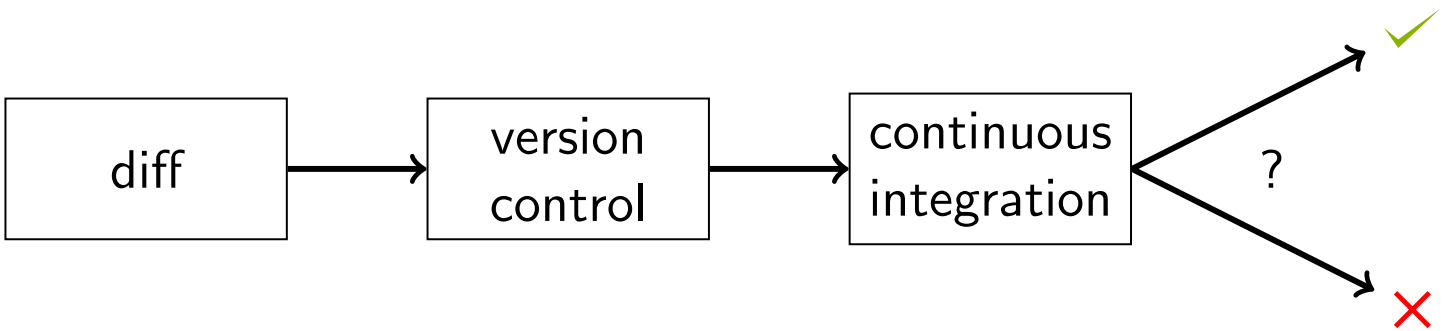
The Autodeduct Toolchain for C Code

Jointly developed by Scania and KTH



Project Goals

1. develop incremental verification techniques for Autodeduct
2. develop support for safety & security in Autodeduct
3. evaluate techniques on real vehicle software revisions from Scania
4. develop case study and demonstrator on using industrial code



Potential Impact

From Years to Hours

Whenever required, processes and tools shall enable quality-checked over-the-air release of code to rolling-fleet on hourly-basis, with quality...