ESPLANADE
Efficient and Safe Product Lines of Architectures eNabling Autonomous DrivE

An FFI project running from 2017-01-01 to 2020-03-31.

Fredrik Warg, Senior Researcher, RISE
Background

• Increased interest in vehicle automation in early 2010s
  • Challenges for safety assurance
  • Uncertain relation to safety standards (e.g. ISO 26262)

• FUSE project (2013-2016)
• ESPLANADE (2017-2020)
Research Questions in ESPLANADE

• How to show that interactions between ADS and human users are safe?
• How to ensure that the hazard analysis is complete and the safety goals are useful for implementing the ADS?
• How to create an architecture where decisions are aligned with the current operational capability to ensure safe operation?
• How to ensure the safety integrity of a sensor system (redundancy and degradation concepts)?
• How to structure safety requirement refinement to be able to ensure completeness and consistency in the requirements hierarchy?
Methodology

• Method development considering the example of two use cases
  • Trucks – “terminal to terminal”
  • Passenger cars – “highway pilot”
Safe Transitions of Responsibility

- Transition of control between human driver and ADS
  - Hazards
  - Design principles
  - Safety analysis

ESPLANADE papers:
Hazard analysis for an ADS

• Proposing a new kind of hazard analysis better suited for an ADS
  • Risk norm with tolerated frequencies of incidents
  • Incident types mapped to risk norm
  • Safety goals based on incidents

ESPLANADE papers:
• *Introducing ASIL Inspired Dynamic Tactical Safety Decision Framework for Automated Vehicles* – in ITSC 2017
• *The Quantitative Risk Norm - A Proposed Tailoring of HARA for ADS* – in SSIV 2020
• *Concepts and Risk Analysis for a Cooperative and Automated Road Vehicle System* – in SERENE 2020
Operational Design Domain (ODD)

- Using an ODD to confine the safety argument
- Properties of an ODD
  - Defining operating conditions (OCs)
  - Verification against OCs
- Strategies to remain within ODD

ESPLANADE papers:
- The Frequency-based Operational Design Domain and the Role of Minimal Risk Condition for Safe Automated Driving Systems (not yet published)
Thank you for your attention!

- Visit the project website for more information
  - Public report
  - Links to the 17 publications