ESPLANADE

Efficient and Safe Product Lines of Architectures eNabling Autonomous DrivE

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

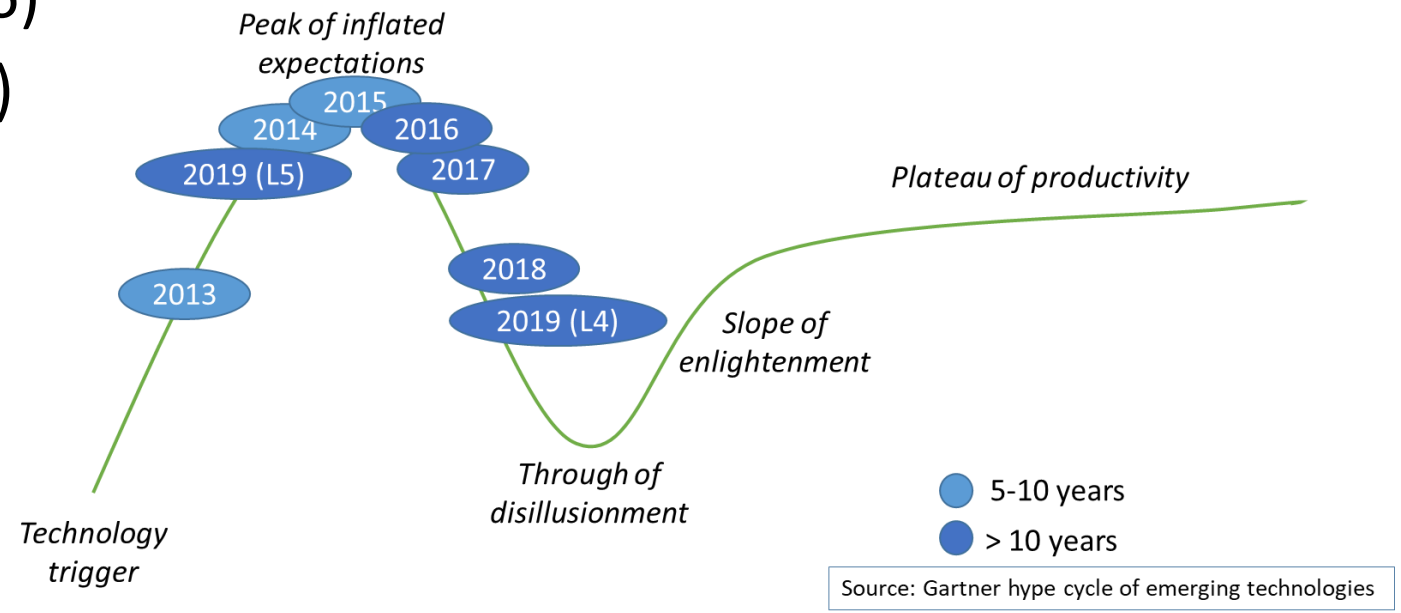
Fredrik Warg, Senior Researcher, RISE

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)

FUSE

***FU**nctional **S**afety and **E**volvable architectures for autonomy*



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?

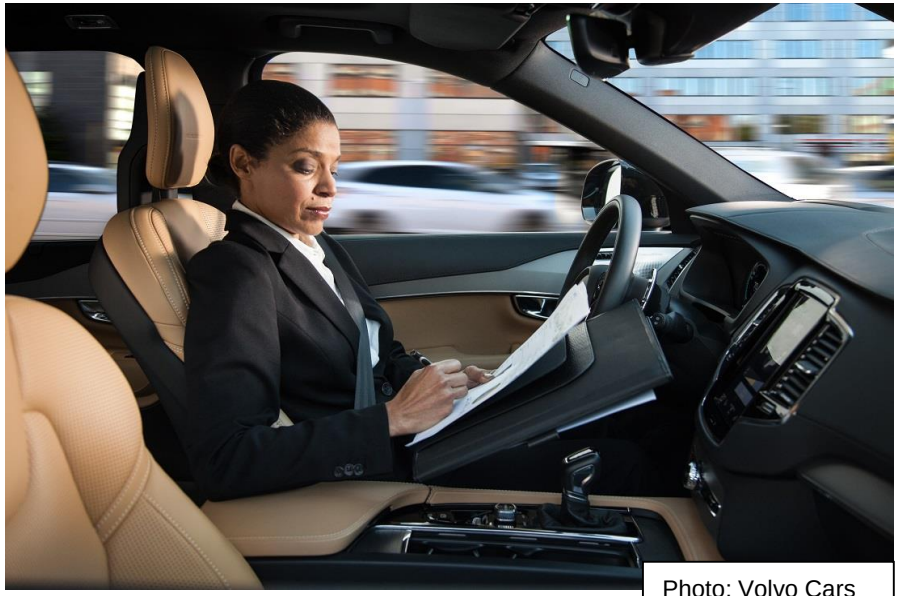
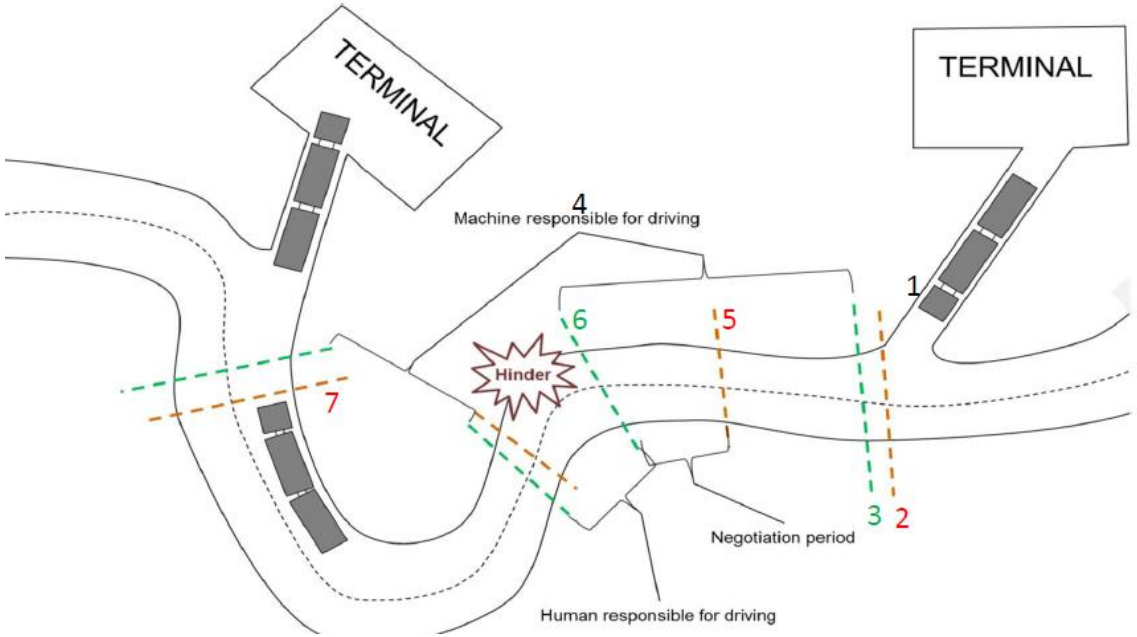


Photo: Volvo Cars

Methodology

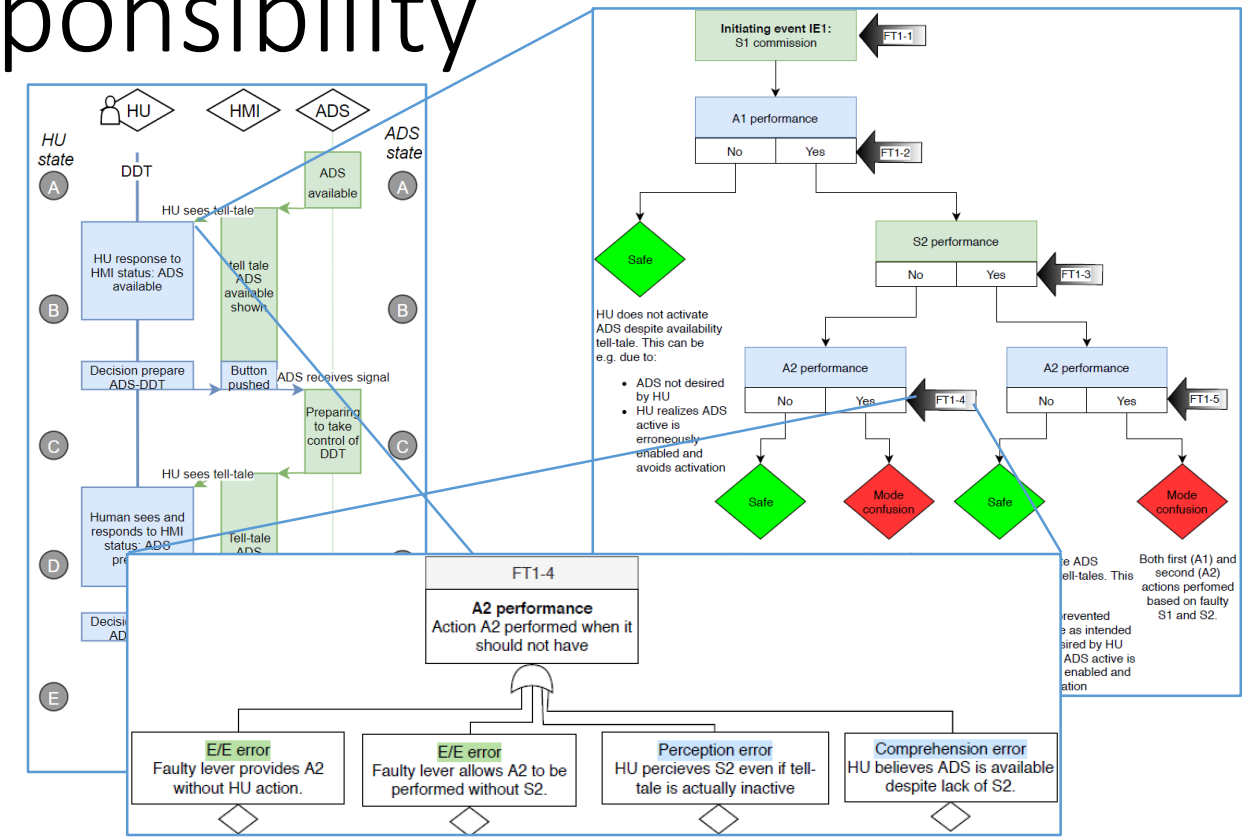
- Method development considering the example of two use cases
  - Trucks – “terminal to terminal”
  - Passenger cars – “highway pilot”



Highlights

Safe Transitions of Responsibility

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



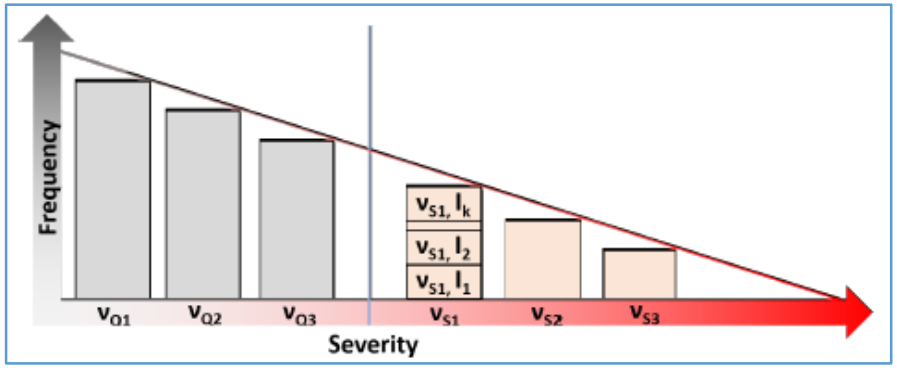
ESPLANADE papers:

- *Safe Transitions Between a Driver and an Automated Driving System* - in International Journal of Advances in Systems and Measurement, 2017.
- *Safer Transitions of Responsibility for Highly Automated Driving: Designing HMI for Transitions with Functional Safety in Mind* - in ERTS 2020.
- *Towards Safety Analysis of Interactions Between Human Users and Automated Driving Systems* - in ERTS 2020.

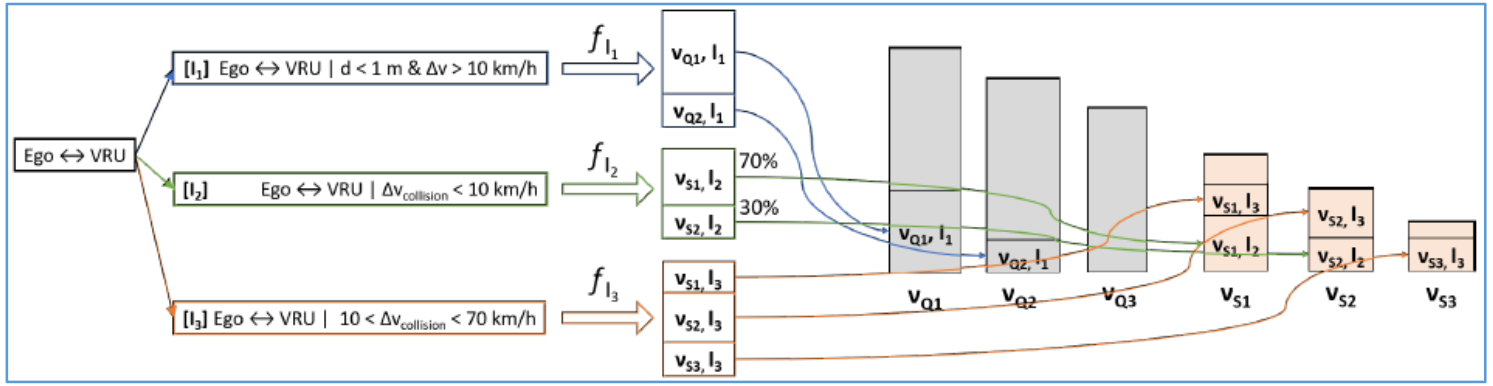
Highlights

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



SG-I_2:
Avoid collision Ego↔VRU with $\Delta v < 10$ km/h
within f_{I_2}



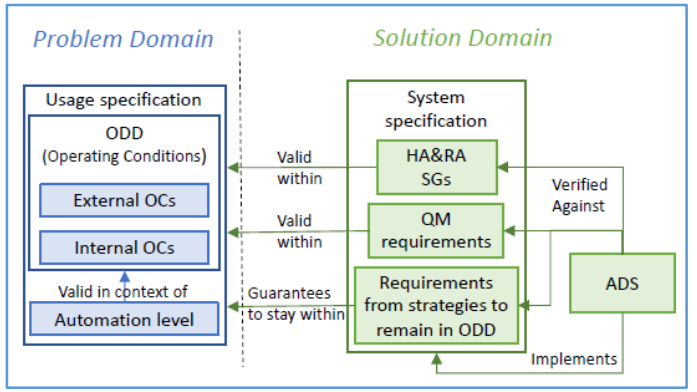
ESPLANADE papers:

- *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*

Highlights

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



Strategies			Need to estimate inside ODD in design-time.	Need to define triggering cond. for DDT-fallback	Need for reliable map info.	Need for sensors capable of measuring condition
I	Internal	Inherent in ADS feature definition	N	N	N	N
II	External	Checking mission when accepting strategic task	Y	N	Y	N
III		Statically defined, spatial and temporal triggering conditions	Y	Y	Y	N
IV		Run-time measurable triggering cond. related to OC	N	Y	N	Y

ESPLANADE papers:

- *Towards an Operational Design Domain That Supports the Safety Argumentation of an Automated Driving System* - in ERTS 2020.
- *Design of a Knowledge-Base Strategy for Capability-Aware Treatment of Uncertainties of Automated Driving Systems* - in WAISE 2018
- *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