Safety Impact Assessment

L3Pilot Final Event

SP7 Safety Impact Assessment Team

Felix Fahrenkrog, Pierluigi Olleja, Hendrik Weber, Marcel Borrack, Yves Page,
Anne Silla, Henri Sintonen, Jonas Bärgman, Thomas Streubel, Satu Innamaa, Thierry Hermitte

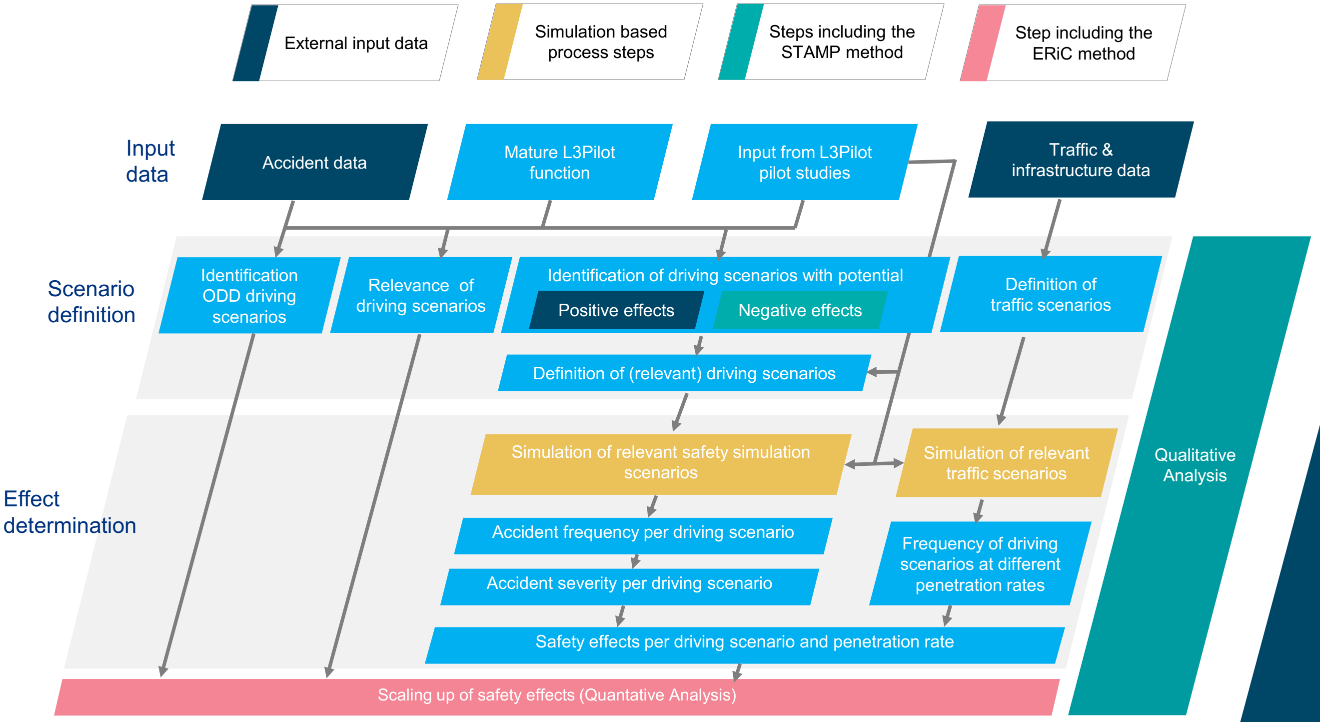
Our Mission:

Calculate the impact of automated driving on road safety in Europe

- No collision occurred during the pilot!
- L3Pilot reflects on tiny portion of the road traffic in Europe
  - 0.2 Million km driven in L3Pilot in automation mode
  - Annual driven milage of passenger cars in Europe only on motorways is above 643’000 Million km
- Additional methods are needed to derive the safety impact of automated driving.

L3Pilot Safety Impact Assessment
General Approach & Input

- Focus is on the quantitative analysis of effects on traffic safety.
  - Assessing positive and negative effects.
  - Utilizing different approaches and data sources
- The qualitative analysis completes the picture.



Input data for the Safety Impact Assessment.

Parameterization of L3Pilot mature ADF
Use the L3Pilot data to verify that the implemented ADF is in line with tested ADFs.

Parameterization simulated scenarios
Use the L3Pilot data to set up the simulated scenarios (distributions, driving scenarios).

Validation of traffic simulations
Use L3Pilot data to check whether the determined effects with respect to the frequency of scenarios in simulation can be found as well in the real world

National Accident Statistics
Complement the data of the European statistic (BAAC, STATS19, STRADA, Statistics Finland).

European accident database
The scaling up of safety impacts to European level exploited accident data from the European-wide CARE database (2019).

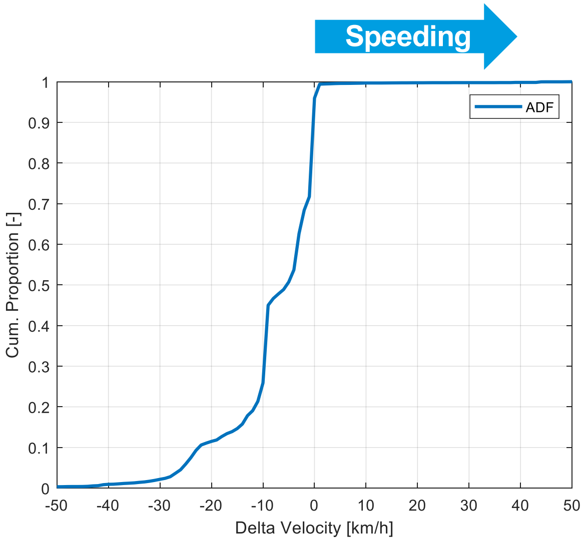
Questionnaires and Interviews
with participants, safety drivers and psychologists for the qualitative assessment.

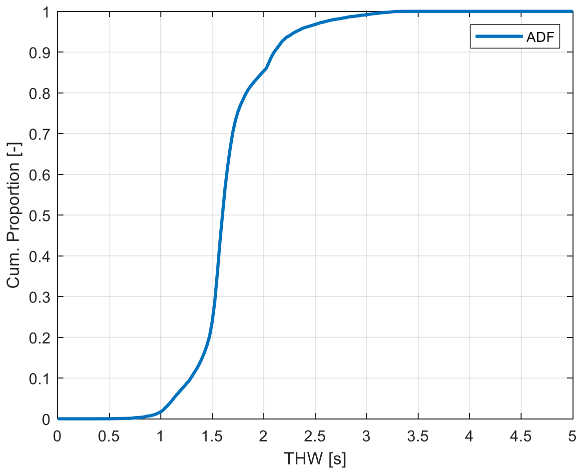
Insurance accident data
AZT insurance accident database has been used to for the safety impact assessment of the parking ADF.

In-depth accident data
Complement the data of the European statistic with respect to scenario and ODD analysis (FCD, IGLAD, GIDAS, Volvo Cars internal in-depth crash data, TASC, VOIESUR).

Near-crashes from naturalistic driving data
Data from the SHRP2 naturalistic driving dataset for the counterfactual simulation.

Mature L3Pilot ADF Parameters Selection. Validation with Pilot Data.

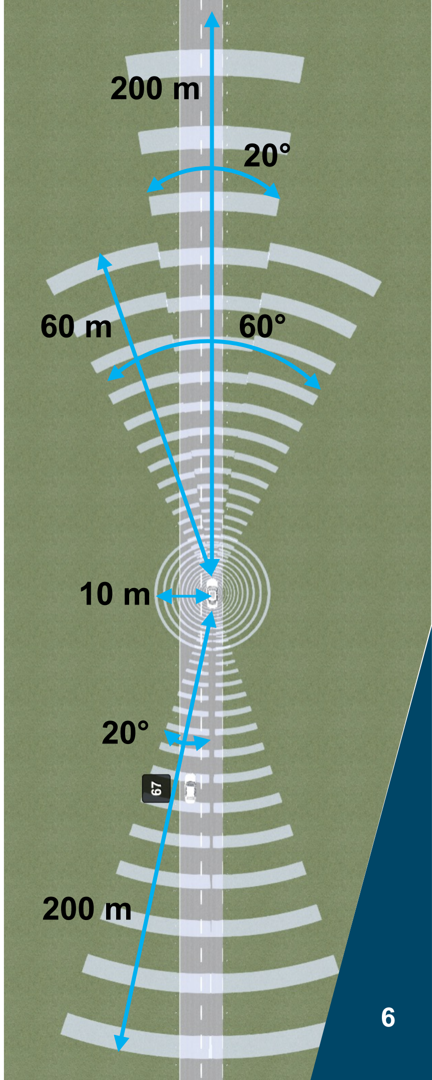




- Automated driving function shall not driver faster than the given speed limit.
- Time gap setting for the automated driving function is 1.6 s.

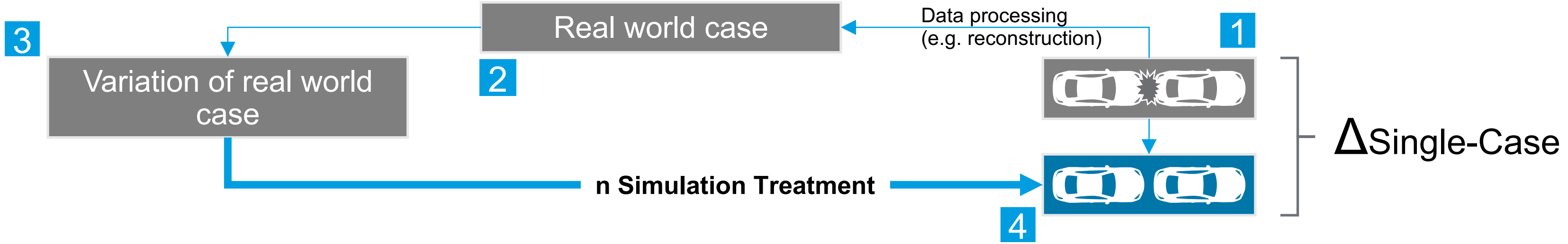
L3Pilot Mature ADF (Motorway & Traffic jam). Implementation.

- Assessment is done for the “L3Pilot Mature ADF”, since not a particular implementation of an automated driving function (ADF) should be investigated.
- The simulations require an explicit implementation of an ADF.
- Principles of the ADF:
  - Separate longitudinal and lateral control;
  - Comply with traffic rules (e.g. speed limit);
  - Max. speed of ADF is 130 km/h;
  - No overtaking on the right.
- Implementation of ADF based on the agreed definition per simulation partner (reference model in Simulink).

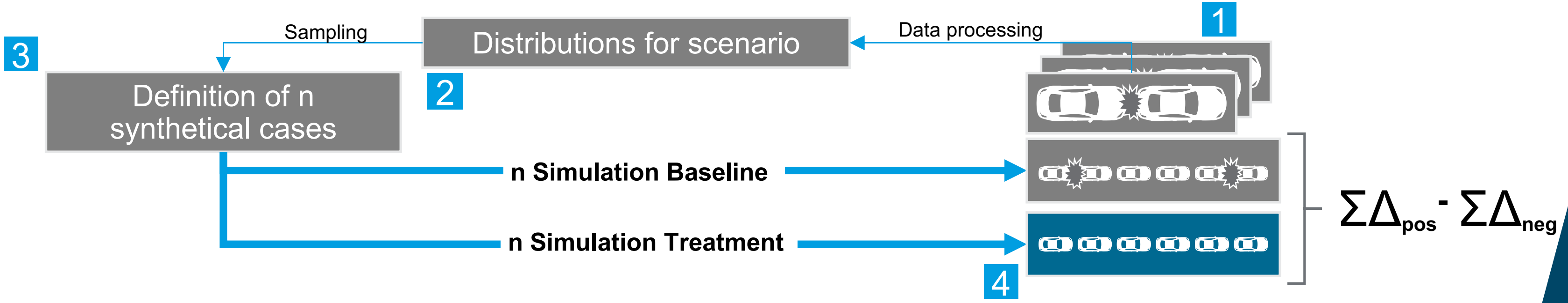


Simulation Approaches for the Safety Impact Assessment. Overview.

Counterfactual Simulation



Monte-Carlo (Traffic) Simulation



Simulation Approaches for the Safety Impact Assessment. Different Approaches.

Monte-Carlo Traffic Simulation-based Simulation

- Applied for **motorway**
- Focus on driving and traffic sc.
- Considers surrounding traffic
- Tool: openPASS
- Advantages
  - More independent of the number of real-world case
  - Input distributions can be derived from different input sources (crashes, pilot, etc.).
  - Can assess traffic effects

Counterfactual Simulation

- Applied for **motorway**
- Focus on driving scenarios
- Considers no surrounding traffic
- Tool: Python + ESmini
- Advantages
  - Direct link to real-world case
  - Covers crashes as well as near-crash situations

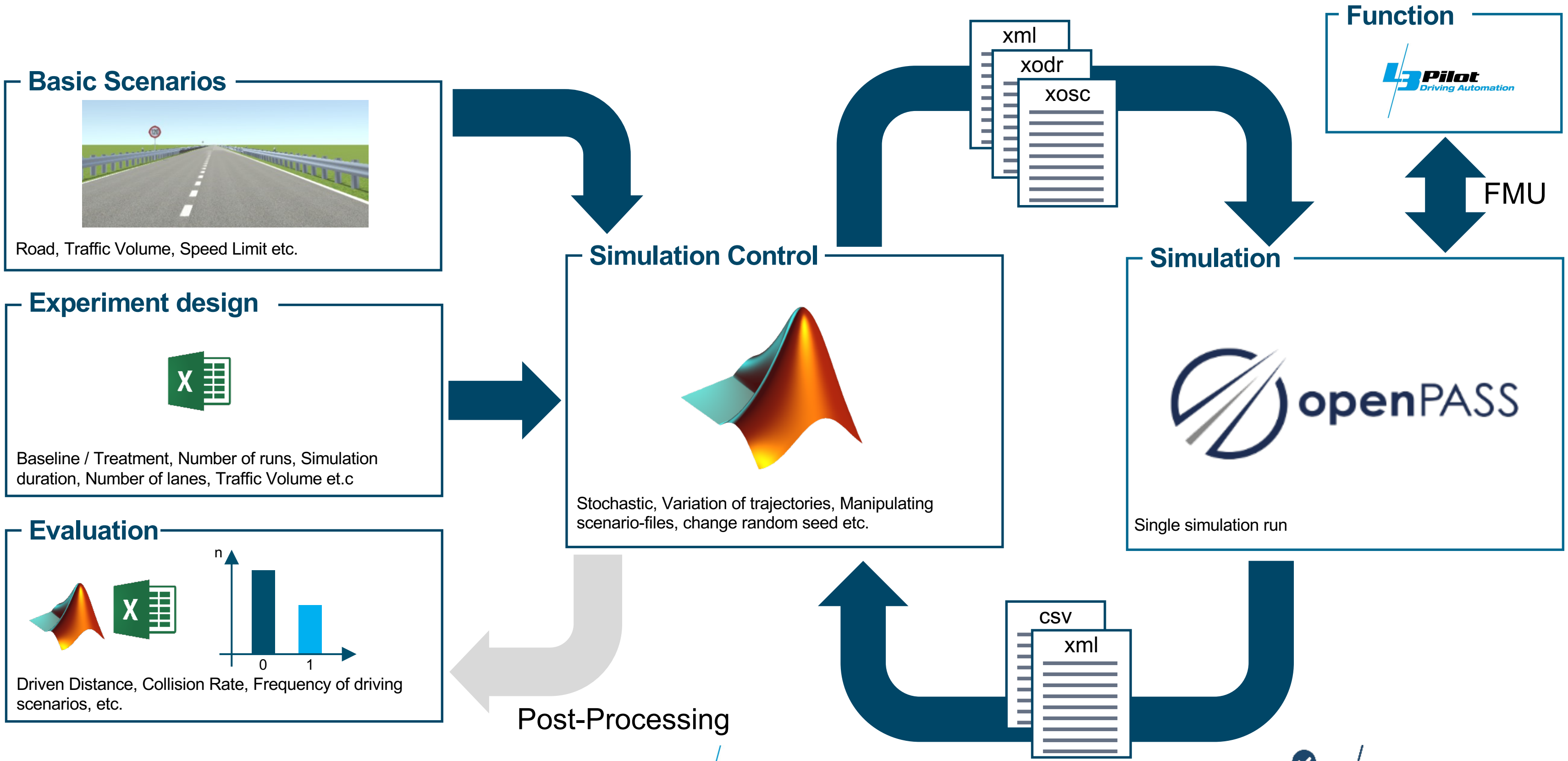
Monte-Carlo based Driving Scenario (Urban) Simulation

- Applied for **urban**
- Focus on driving scenarios
- Considers no surrounding traffic
- Tool: Virtual Test Drive
- Advantages
  - See motorway Monte-Carlo approach

Monte-Carlo Traffic Simulation-Based Assessment

Felix Fahrenkrog

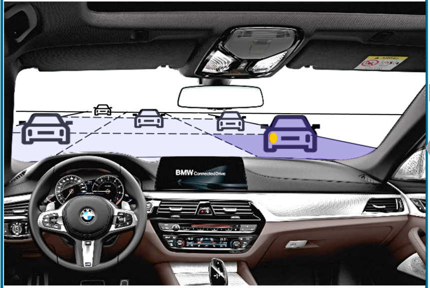
Simulation Process.



Prospective Effectiveness Assessment by Simulation.
Overview SCM Driver Model – Example Passive Cut-In Maneuvers.

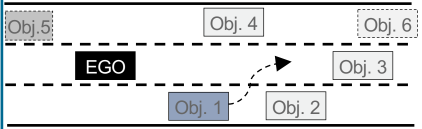
Driver Characteristics

Information Acquisition



Mental Model

- Currently observed object
- Useful field of view, faulty
- Periphery: extrapolation, faulty
- Not observed object(s)



Situation Manager

Evaluation of the scenario

Scenario	Intensity
Lane changer f. right	0.8
Traffic Jam	0.3
Free Driving	0.0
Object in the lane	0.0

Action Manager

Decision on action

Action	Intensity
Braking	0.7
Lane Change to the left	0.4
Keep Speed	0.1

→ Driver„A“ brakes; Driver„B“ changes lanes; Driver „C“ brakes …

Action Implementation

Overview Analysed Scenarios.

Tested Conditions

- Baseline (ego veh. without ADF)

Baseline: Traffic w/o AEB

Baseline AEB: Traffic 7.5% AEB

- Treatment (ego veh. with ADF)

Treatment 0: Traffic w/o ADF

Treatment 5: Traffic w. 5% ADF

Treatment 10: Traffic w. 10% ADF

Treatment 30: Traffic w. 30% ADF

Scenarios

- Lane Change Conflict (P4)
- VRU Conflict (P5)
- Minimal Risk Man. (C1)
- Wrong Activation (C2)
- End of Lane (C3)
- Obstacle in Lane (C4)
- Lower Speed Limit (C5)
- Motorway Entrance (C6)
- Endurance

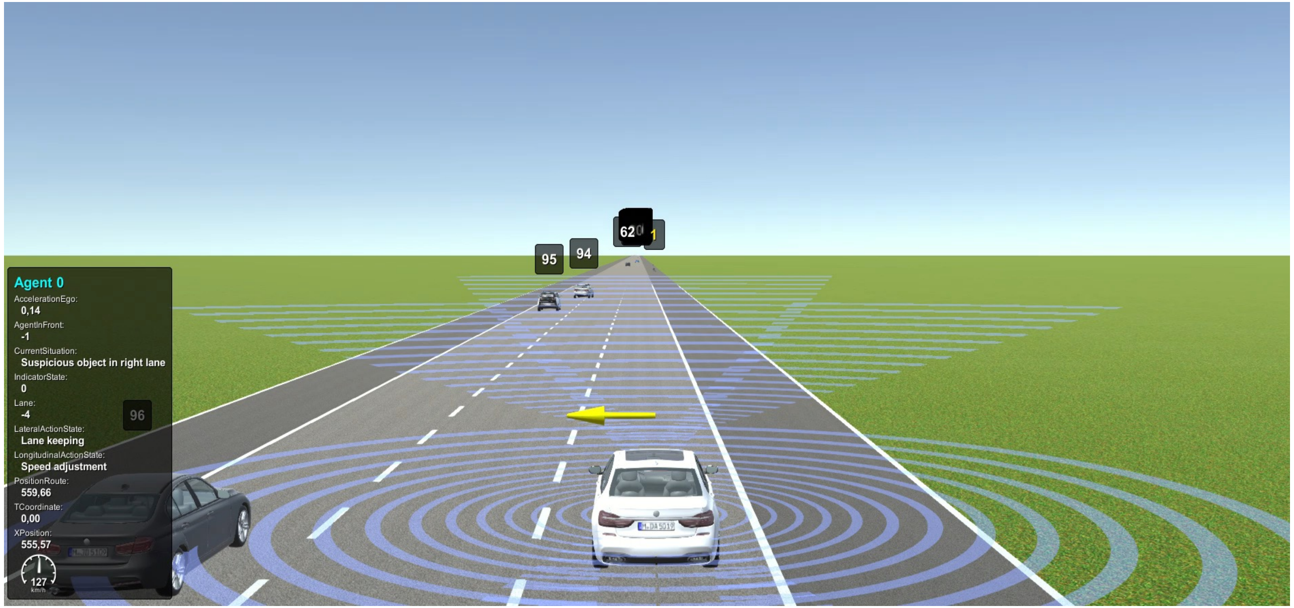
Traffic Parameters

- 2 & 3 lanes
- 250, 500, 1000 and 1500 veh. per lane and hour
- Speed limits: 80 kph, 100 kph, 120 kph, 130 kph, 140 kph, 55 mph, 70 mph, none

AEB: Autonomous Emergency Braking

Simulation.
Video of Example P5 VRU Conflict.

- Approx. 158’000 simulations have been conducted for the safety impact assessment in openPASS.
- In these simulations the ego vehicle drove approx. 240 000 km.
- Focus is on critical scenarios.
- All simulated vehicles drove a total distance of 29.4 million km.



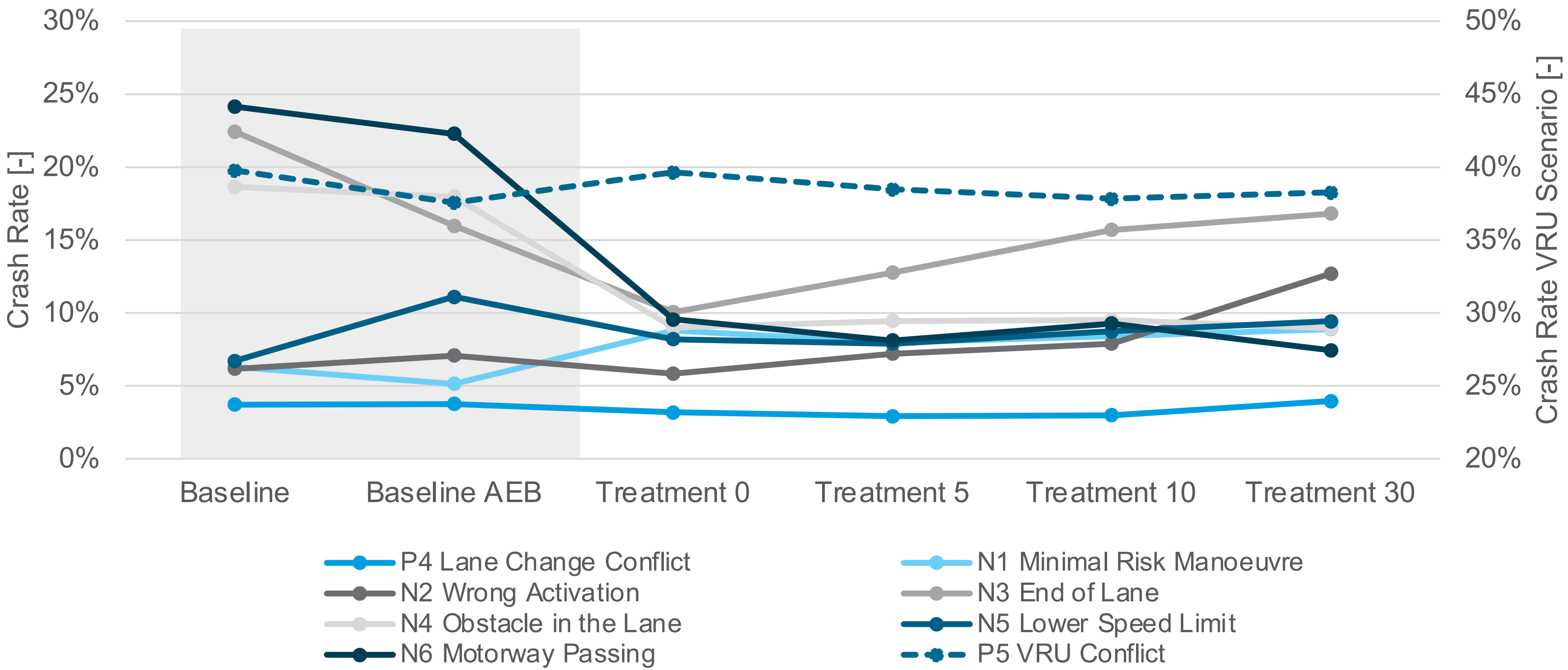
Open-source simulation tool: openPASS

Simulation Results.
P5 VRU Conflict.

- The velocity of the VRU is equally distributed between 0 km/h, 1.5 km/h, 3 km/h, 7 km/h.
- The crash rate does not show any major differences between the baseline and treatment conditions. The lowest crash rate is detected for the baseline AEB scenario.
- In terms of crash severity, a clear difference between the baseline condition can been identified. The probability of having a fatal accident reduces from 62% - 66% to 37% - 39%.
- The reduction shows a safety benefit of the ADF in this scenario.

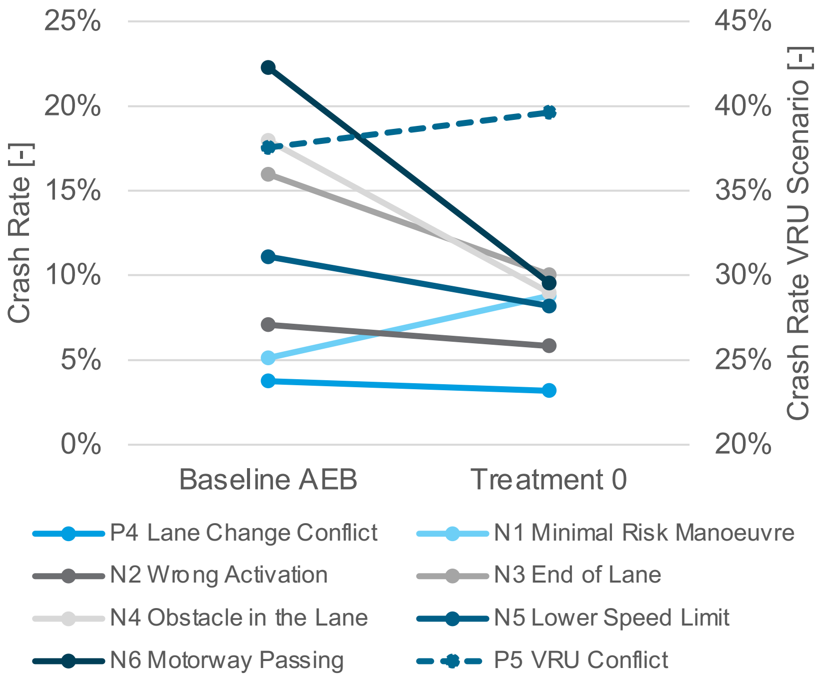
P5 VRU Conflict	Crash Rate (ego) [-]	Probability of slight injury [-]	Probability of severe injury [-]	Probability of fatal injury [-]
Baseline	39.8%	9.7%	28.4%	61.9%
Baseline AEB	37.6%	7.4%	27.0%	65.6%
Treatment 0	39.6%	21.5%	39.3%	39.2%
Treatment 5	38.5%	21.6%	41.2%	37.2%
Treatment 10	37.8%	22.7%	38.7%	38.6%
Treatment 30	38.3%	22.6%	38.3%	39.0%

Simulation Results.
Overview – Driving Scenarios.



Simulation Results.
Overview – Driving Scenarios.

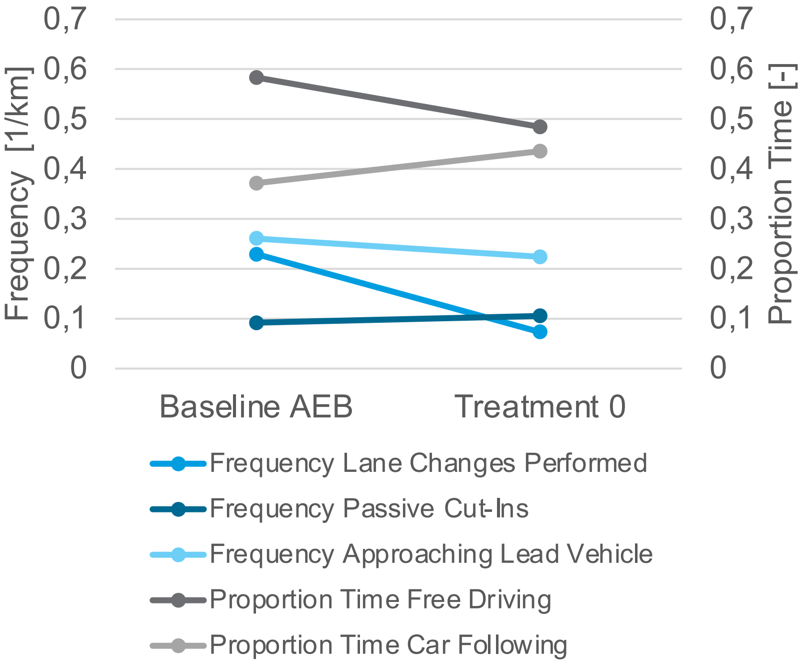
- A direct comparison between the baseline and treatment is given for the baseline condition AEB and the treatment condition 0, since both condition the penetration rates of the AEB and ADF is the same.
- An increase of the crash rate can be observed in the MRM scenario.
- The crash rate in the VRU scenario increases slightly. However, the accident severity is heavily reduced.
- For the other scenarios a reduce in the crash rate is detected.



Simulation Results.
Overview – Endurance / Traffic Simulation.

- Total driven distance:
  - Manual driven vehicles 5’906’201 km (ego vehicle 23’885 km)
  - Automated vehicles 415’823 km (ego vehicle 35’473 km)
- Analysis for the ego-Vehicle between Baseline AEB and Treatment 0:

Indicator	Simulation	Pilot
N(lane change)/h	-71%	-57%
N(Approaching)/h	-21%	-52%
N(Cut In)/h	+5%	-11%
%(Uninfluenced)	-17%	+11%
%(Following)	+17%	+10%



L3Pilot Driving Automation

Counterfactual Simulation

Safety Benefit Assessment: Cut-in and rear-end

Pierluigi Olleja

Chalmers University of Technology

CHALMERS UNIVERSITY OF TECHNOLOGY

VOLVO

Counterfactual safety assessment

Pre-crash kinematics of case (real-world conflict)

original → **synthetic variant**

Simulation of case with

no alteration ("as is")	Automated Emergency Brake	Automated Driving Function
Baseline	**Baseline AEB**	**ADF**

Comparison of crash

Avoidance	**Mitigation** (Injury risk function)

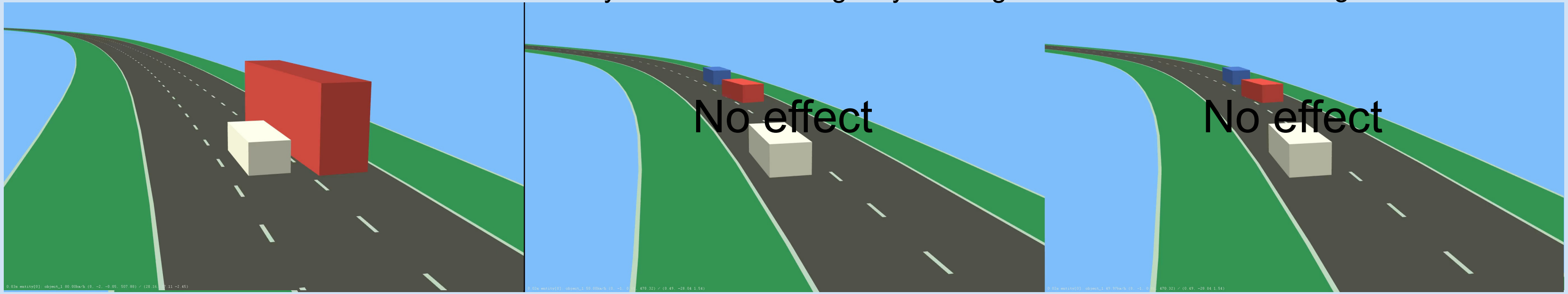
Analysed Driving Scenarios

P1 Rear-end (car-following) conflicts	P2 End of traffic jam (rear-end) conflicts	P3 Cut-in (rear-end) conflicts	P3 Cut-in (sideswipe) conflicts

Baseline
No automation

Baseline AEB
Only Automated Emergency Braking

ADF
Automated Driving Function



Used datasets

Dataset name	Description	Source / Region	Count (total)
Volvo Cars original	Sample directly from Volvo Cars Corporation in-depth crash database (VCTAD)	Volvo Cars/ Sweden	94

Used datasets

Dataset name	Description	Source / Region	Count (total)
Volvo Cars original	Sample directly from Volvo Cars Corporation in-depth crash database (VCTAD)	Volvo Cars/ Sweden	94
Volvo Cars synthetic variations	Variants of the original VCTAD crashes. Within-reconstruction bounds: speed, timing and vehicle dimension	Volvo Cars/ Sweden	940
Volvo Cars CDB-speeds	Variants of the original crashes. Modifying speeds to be those from the L3Pilot database (ADF active only)	Volvo Cars/ Sweden + L3Pilot CDB	706

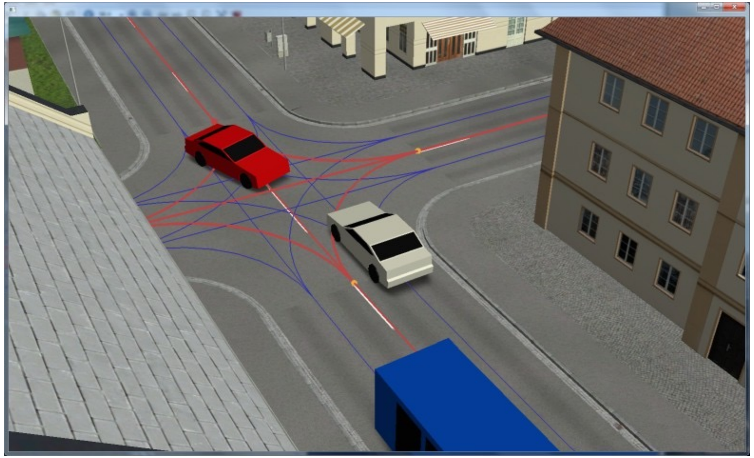
Used datasets

Used for main assessment			
Dataset name	**Description**	**Source / Region**	**Count (total)**
Volvo Cars original	Sample directly from Volvo Cars Corporation in-depth crash database (VCTAD)	Volvo Cars/ Sweden	94
Volvo Cars synthetic variations	Variants of the original VCTAD crashes. Within-reconstruction bounds: speed, timing and vehicle dimension	Volvo Cars/ Sweden	940
Volvo Cars CDB-speeds	Variants of the original crashes. Modifying speeds to be those from the L3Pilot database (ADF active only)	Volvo Cars/ Sweden + L3Pilot CDB	706
+ **TASC (via Toyota Motor Europe)**	Pre-crash data from the German state of Saxony, reconstructed from police reports (collaboration between TME and Fraunhofer IVI)	TASC (TME+ Fraunhofer)/ Germany	167
+ **SHRP2 near-crashes**	Near-crashes extracted through reconstruction of cases through manual annotation of forward video + recorded kinematics data	SHRP2-VTTI/ USA	50

Used datasets

Used for sensitivity analysis			
Dataset name	**Description**	**Source / Region**	**Count (total)**
Volvo Cars original	Sample directly from Volvo Cars Corporation in-depth crash database (VCTAD)	Volvo Cars/ Sweden	94
Volvo Cars synthetic variations	Variants of the original VCTAD crashes. Within-reconstruction bounds: speed, timing and vehicle dimension	Volvo Cars/ Sweden	940
Volvo Cars CDB-speeds	Variants of the original crashes. Modifying speeds to be those from the L3Pilot database (ADF active only)	Volvo Cars/ Sweden + L3Pilot CDB	706
TASC (via Toyota Motor Europe)	Pre-crash data from the German state of Saxony, reconstructed from police reports (collaboration between TME and Fraunhofer IVI)	TASC (TME+ Fraunhofer)/ Germany	167
SHRP2 near-crashes	Near-crashes extracted through reconstruction of cases through manual annotation of forward video + recorded kinematics data	SHRP2-VTTI/ USA	50

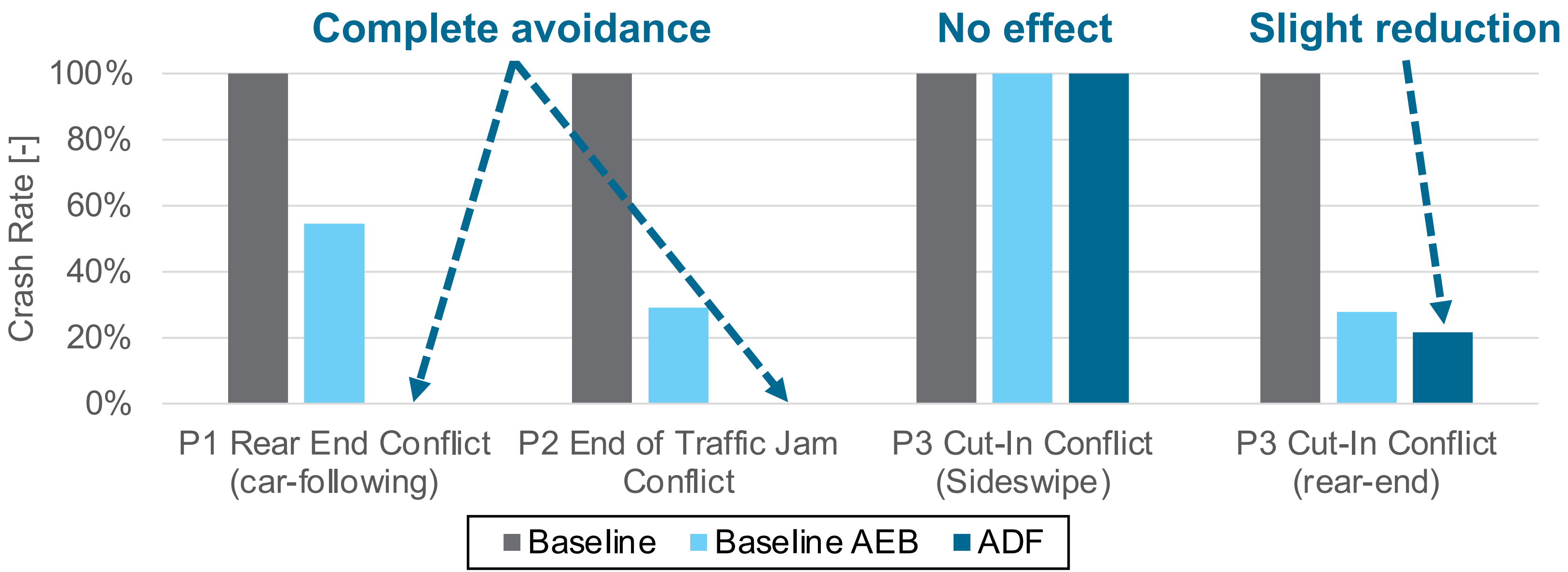
Simulation tool



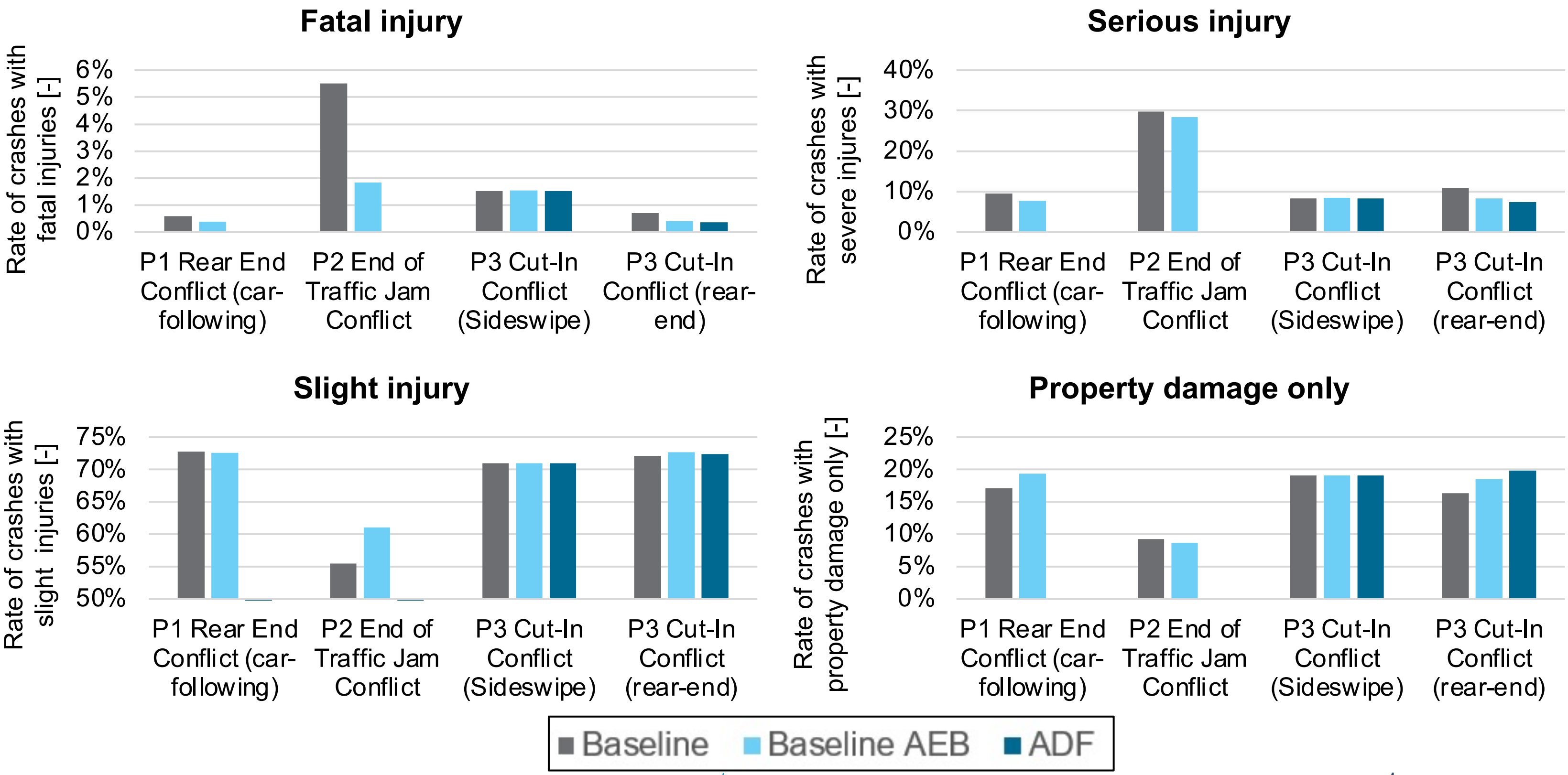
- **esmini** – an open-source simulator that can be used as a ”virtual-simulation engine”
  - Uses OpenScenario/OpenDrive files
- Python used for batching, vehicle and system modelling
- Post-simulation weighting procedure and analysis performed in Matlab

Simulation Results - Crash avoidance

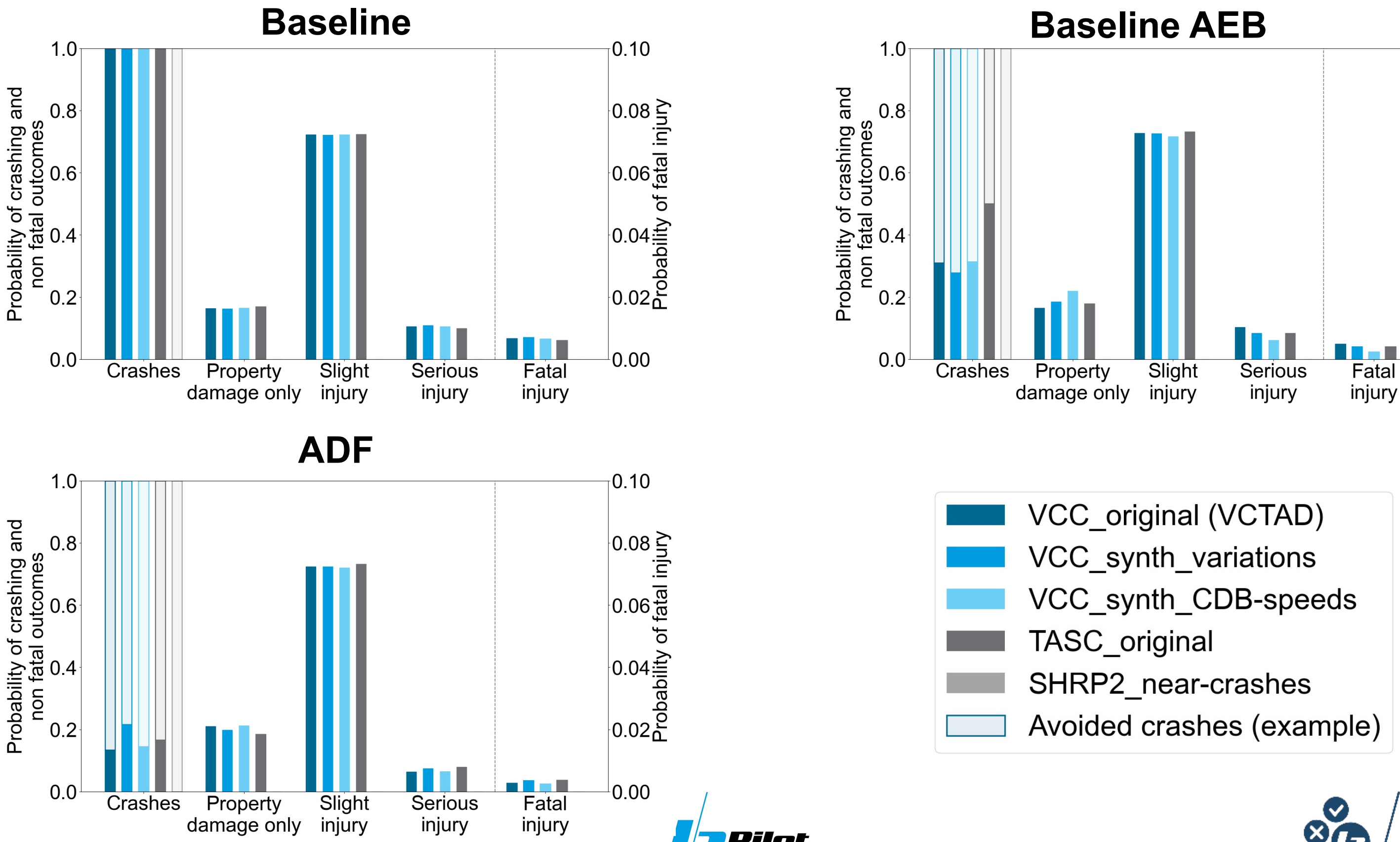
- Based on a total of 440 “rear-end” and 500 “cut-in” cases (VCC_synth_variations)



Simulation Results – Crash mitigation (severity)



Results - Sensitivity analysis (exemplary for P3 Cut-in (rear-end))



Summary & Limitations

- ADF avoids all rear-end crashes (*P1 Rear-end car-following* and *P2 End of traffic jam rear-end*) while AEB still crash at 54% and 29%, respectively
- ADF avoids none of the *P3 Cut-in (sideswipe)* – due to system limitations (no predictions or precautionary safety)
- ADF and AEB avoid approximately the same amount of *P3 Cut-in (rear-end)* crashes (i.e., not much extra benefit of ADF)
- ADF did not “cause” any *P3 Cut-in (rear-end)* crashes applied to SHRP2 near-crashes
- Sensitivity analysis shows reasonably similar ADF performance across datasets
- Challenges and limitations are described in Deliverable chapter 7.4
- Future studies using the virtual simulation assessment method should work to overcome some of the challenges, such as the systems limitations, the inclusion of driver models and the validation and verification of the process

Monte-Carlo based Driving Scenario (Urban) Simulation

Hendrik Weber

ika | RWTH AACHEN UNIVERSITY

Introduction
The Challenge of Assessing Urban Automated Driving

- Urban scenarios are complex and diverse
  - Different types of road users, many VRU interactions
  - Intersections
- Resulting challenges:
  - Large amounts of detailed data are needed for parameterization
  - Complexity of scenarios carries over to models used for simulation
    - No commercial models available yet to cover all intended scenarios
  - Overall Impact Assessment requires some simplification

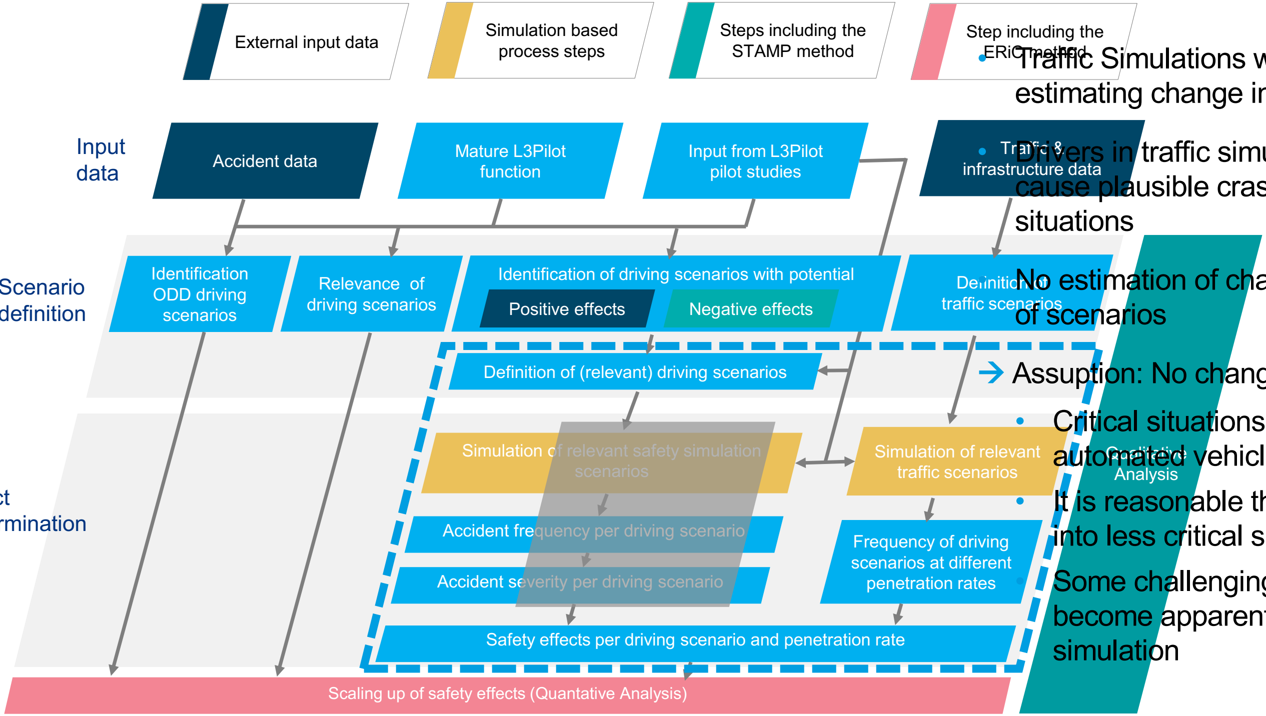
Some elements designed by macrovector / Freepik

→ *L3Pilot impact assessment makes a start estimating the safety impact of urban ADF*

→ ***But:*** *Still a lot of research is required to address the complexity in impacts of urban automation.*

! These challenges and necessary assumptions made need to be considered for interpreting the results

Method for Urban Safety Impact Assessment



- Traffic Simulations were considered for estimating change in frequency
- Drivers in traffic simulations do not cause plausible crashes or critical situations
- No estimation of changes in frequency of scenarios

→ Assuption: No change in frequency

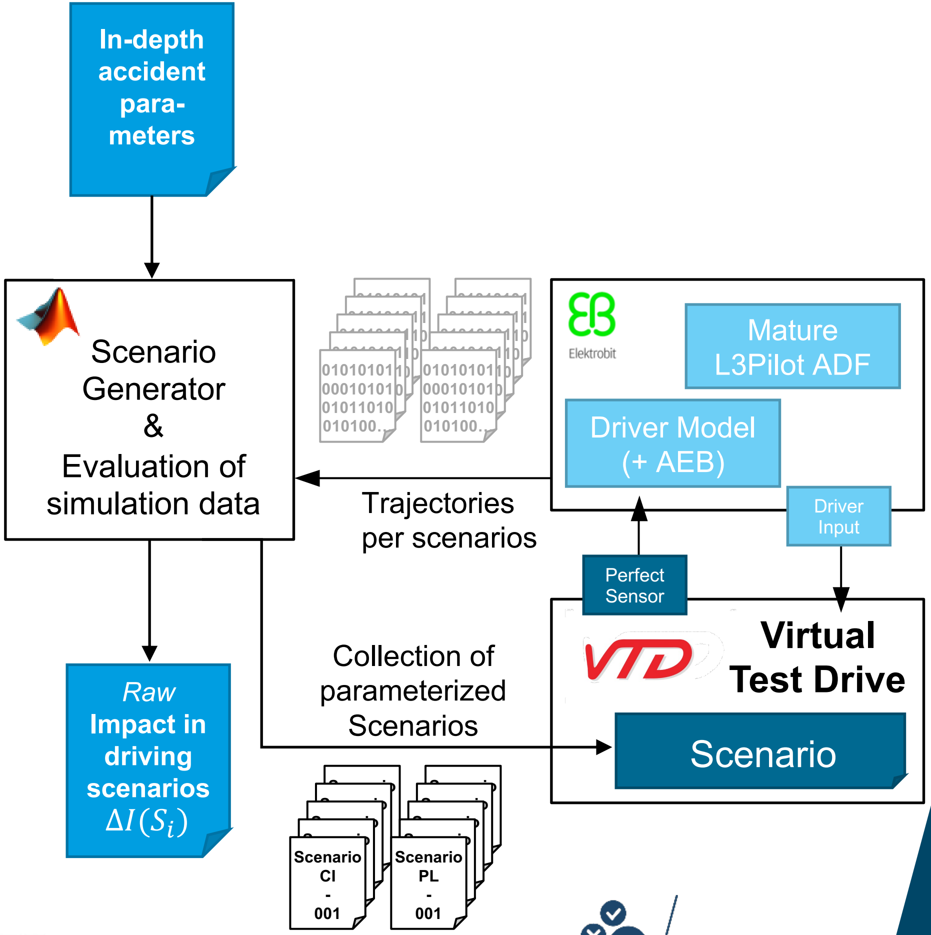
- Critical situations not induced by automated vehicle
- It is reasonable that an ADF will get into less critical situation
- Some challenging situations might become apparent in traffic simulation

Method
Simulation Toolchain

- Basis was the existing ika-toolchain
  - Initially developed in [1]
  - Models developed in house
- Further development:
  - Greater number of driving scenarios
  - Variation of pedestrian speed
    - Parameterized using inD-Dataset [2]
  - Cyclist scenario added (also using inD)
  - Considering object deceleration at intersections

[1] Rösener, C., *A traffic-based method for safety impact assessment of road vehicle automation*, PhD Thesis, RWTH Aachen University, 2020

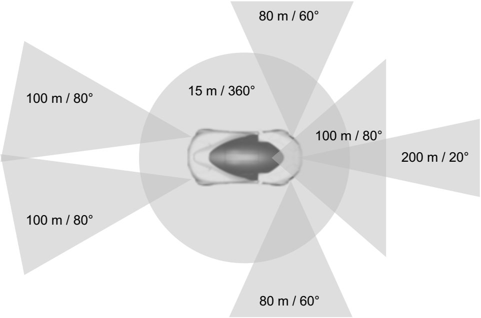
[2] J. Bock, R. Krajewski, T. Moers, S. Runde, L. Vater and L. Eckstein, *The inD Dataset: A Drone Dataset of Naturalistic Road User Trajectories at German Intersections*, 2020 IEEE Intelligent Vehicles Symposium (IV), 2020



Method
Models & Mature Function

Mature function

- Sensor Setup:



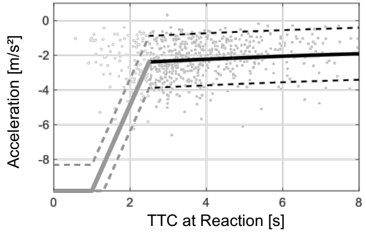
- Behaviour:
  - Max Speed 50 km/h
  - Manoeuvre in critical scenarios is always braking
  - Comparable to state-of-the-art AEB but advanced sensor setup and prediction of object moving laterally towards path

Driver Performance Model

- Reaction in crash relevant situation is always braking

Scenario	Braking reaction time [1]
Aproaching static object	0.95 s
Approaching lateral object	
Approaching lead vehicle	0.95 s
Approaching traffic jam	
Cut-In (passive)	
Lane Change	0.71 s
Overtaking (passive)	
Turning	0.4 s
Crossing	

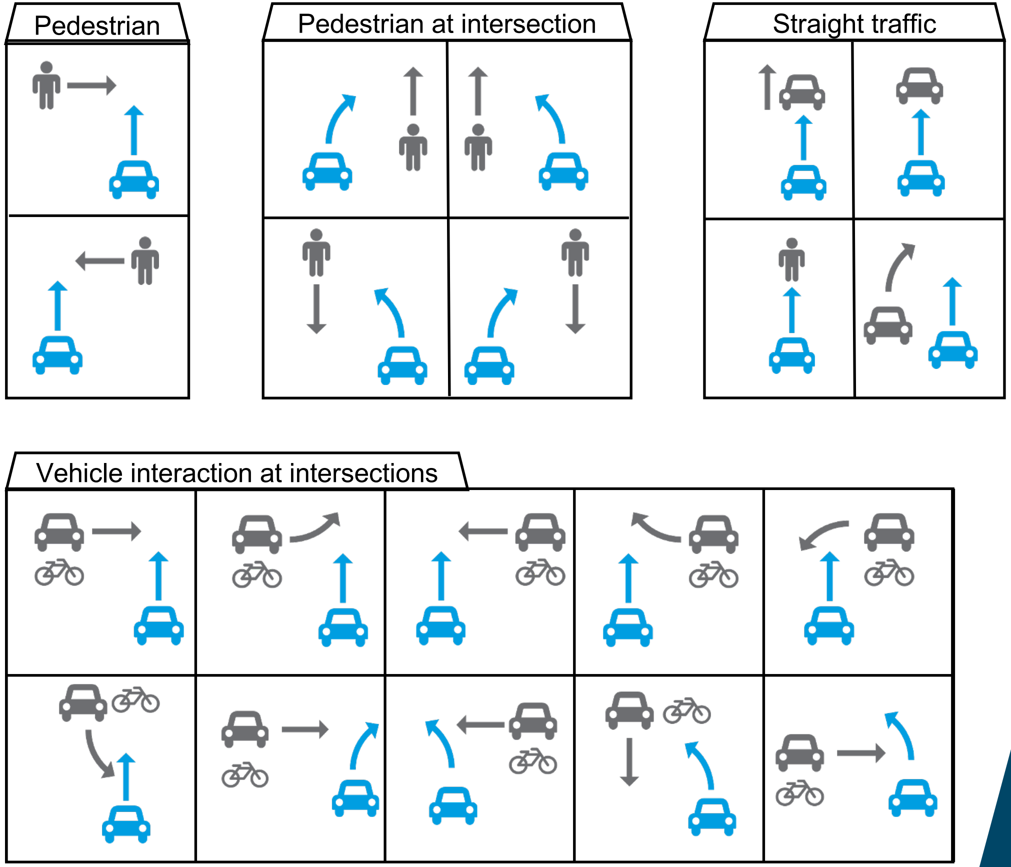
- Reaction intensity:
  - TTC-dependent braking model



Input Data
Simulated Scenarios

- Conflict scenarios with ego vehicle and second traffic participant
- Second participant induces the conflict
- Ego vehicle needs to avoid the collision
- 200 – 500 simulated parameter combinations per scenario

Overall number of evaluated cases	**7600**
Crashes for the driver model (baseline)	1138
Crashes for the AEB	745
Crashes for the mature ADF	267



Input Data
Scenario Generator

Simulation of artificial scenarios

- Generation of artificial cases per driving scenario
- Copula sampling approach preserves distributions and correlations of GIDAS input data

Sample Simulation output

- Object vehicle executes an open loop maneuver
  - No closed loop reaction to ego-vehicle
  - Deceleration of object is part of scenario
- Simulation evaluated

Crossing with vehicle from right | **Pedestrian crossing from right**

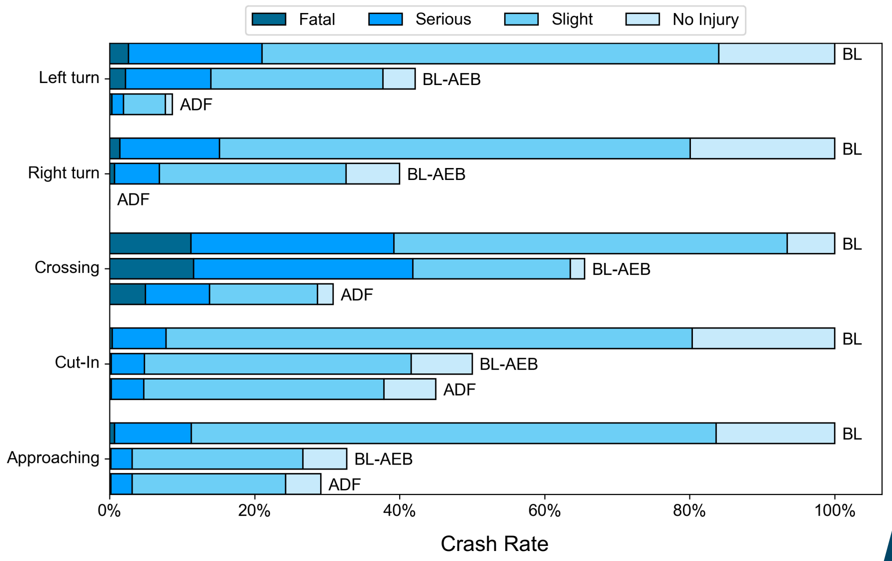
BL - Driver

BL - AEB

ADF

Results
Car-to-Car Scenarios

- *Simulated scenarios weighted equally*
  → different relations between scenarios in scaling
- Reduction in crash rates of at least 78% - apart from Cut-In Scenario
- Scenarios in longitudinal traffic overall only low injury risks due to low driven speeds in urban areas
- Great avoidance potentials for scenarios with ego vehicle turning
  - *ADF performs slower turning manoeuvre compared to human driver in baseline*
- No relevant changes in relation of injury risks
- ***Note:*** *In few scenarios, driver model did not generate any collisions*



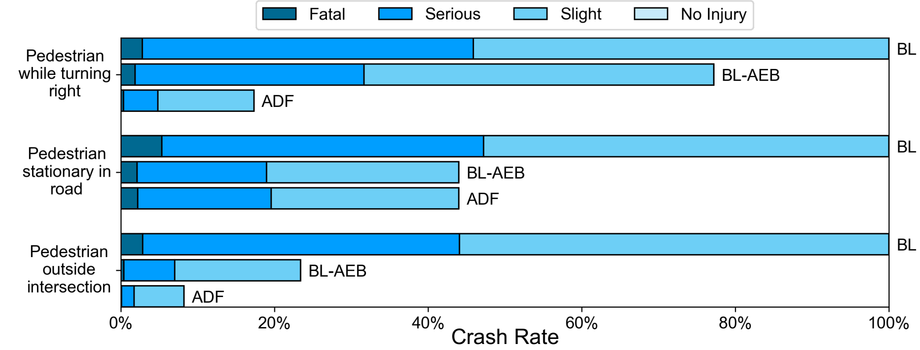
Results
VRU Scenarios

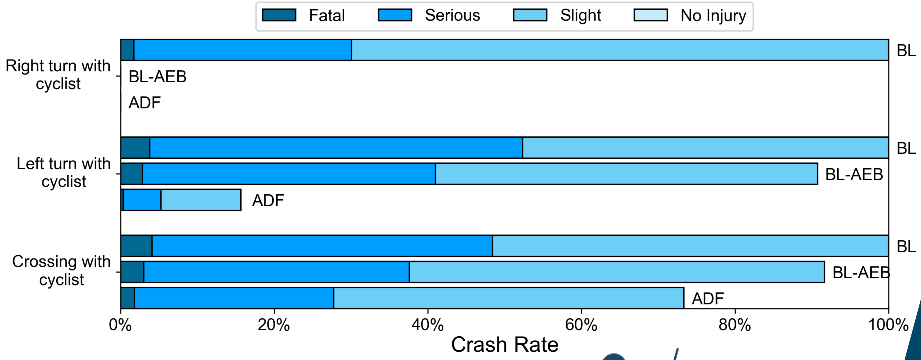
Pedestrian scenarios

- Effect for ADF and AEB perform similarly well for simple interactions pedestrian (> 50% reduction)
- While turning, ADF has a much larger accident avoidance potential (82%) compared to AEB (21%)

Cyclist scenarios

- Great impact for ADF during turning scenarios with cyclists
  - Notable difference for AEB between left and right turn possibly caused to overall low number of crashes
- Lower impact when going straight through intersection





Summary and Limitations

- Great potential for accident avoidance for ADF in crash relevant scenarios in urban areas
- In simple scenarios (longitudinal traffic, crossing at intersections) smaller benefits for ADF compared to AEB
- Applied approach has to make quite some simplification to make huge variety of scenarios manageable. Parameter space in reality has more dimension which can be considered
- Complexity of road layout and obstructions should be addressed in more detail
- Behaviour during crash-relevant scenarios or frequency of incidents cannot be observed during piloting
  - Setup of experimental probably safer compared to a “mature” function
- Complexity of possible driver reactions had to be simplified. A uniform and validated model for the human performance in all relevant scenarios is still a great research effort.
  - Further crash causation mechanism may need to be considered
- Scenarios with potential negative impacts need to be analysed using traffic simulation

Parking ADF

Marcel Borrack

Method
Safety Impact Assessment of Parking ADF – Approach

- Estimation of the effects of parking ADF by means of **identifying the share of accidents** that could be prevented with the L3Pilot mature parking ADF under real road traffic conditions
- Determination of the proportion of addressable damages in **accident databases**
  - Parking accidents are typically underreported in the national accident statistics, which base often on police reported accidents
  - Parking accidents are not well represented in the CARE database
  - Insurance claims offer a comprehensive basis for the evaluation, since parking and maneuvering accidents are in most cases reported only to the insurance company

→ Case-by-case analysis of **insurance claims databases** using accident descriptions

→ Assignment of addressable accidents to the respective functionality of the **mature parking ADF**

Method
L3Pilot Mature Parking ADF „Parking Chauffeur“ - Description

- The parking ADF handles actual parking manoeuvres and the final stages of driving to the parking spaces at private homes, dedicated parking areas, or public parking
- Parking chauffeur has two functionalities: home zone parking and public parking
- Home zone parking: covers all types of parking on private grounds/ private driveway
- Public parking: covers parallel and perpendicular parking in public parking spaces
- Presence of other vehicles and VRU can be handled
- ODD special conditions:
  - weather: light rain ok
  - light: all conditions ok
  - surface condition: ice and snow excluded

Method
Key Elements for Safety Impact Assessment of Parking ADF

I. Target Accidents

- The theoretical maximum percentage of claims that can be addressed by the parking ADF (within ODD)
- Mature L3Pilot ADF descriptions and their ODD as basis for definition of target accidents

II. Effect:

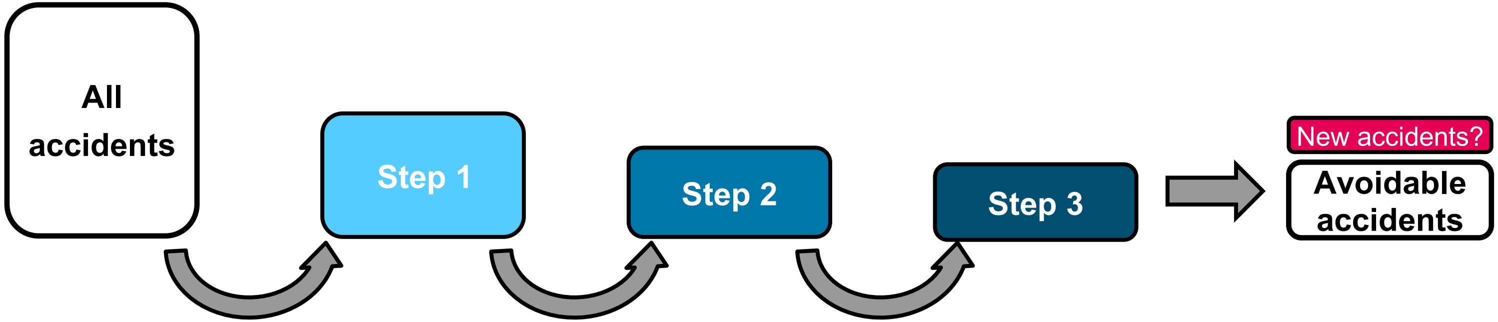
- Proportion of target accidents that can be prevented under real road traffic conditions
- Considering of limitations (e.g. weather conditions, sensor capability, technical failures reduce efficiency of a system)
- Estimation required: several studies on real-world effectiveness of automatic parking systems show claims reduction up to 50%
- Setting of **two scenarios** of effect for assessment: **75%**, **100%**

Method
Key Elements for Safety Impact Assessment of Parking ADF

III. Usage: The extent to which the parking ADF is used by drivers (switched on/off by drivers)

IV. Market penetration: The percentage of cars on the road that is equipped with parking ADF

→ Usage & market penetration are combined in scenarios for **penetration rate in use** within the ODD (**5%**, **10%**, **30%** and **100%**)



Target accidents		Effect		Penetration rate in use		Expected benefit
30%	x	40%	x	50%	=	6%

(values are example)

Data Source - AZT Insurance Claims Databases

Type (countries)	Year of damage	Number of claims
1st Party/Motor own Damage collision claims (Allianz Germany)	2004 & 2007	1,916
	2011	853
	2013 & 2014	2,754
	2018	332
	Total MoD	**5,855**
Motor 3rd Party Liability claims with only property damage (Allianz Germany)	2004 & 2007	1,979
	2011	939
	2013 & 2014	1,797
	2018	364
	Total MTPL-PD	**5,079**
Motor 3rd Party Liability claims with bodily injury (Allianz Germany)	2011	824
	2013 & 2014	631
	2018	204
	Total MTPL-BI	**1,659**

MoD: Motor own Damage
MTPL: Motor 3rd Party Liability

PD: Property Damage
BI: Bodily Injury

Databases: Allianz Center for Technology (AZT)

Results
Number & Share of Target Accidents by Parking ADF Functionality

Database / Insurance Type		Mature parking ADF						Number of claims AZT Database
		Parking ADF Home Zone		Parking ADF Public		Parking ADF (total)		
		Target accidents inside ODD	Share	Target accidents inside ODD	Share	Target accidents inside ODD	Share	
1st party / MoD-Collision		298	5.1%	820	14.0%	1,118	19.1%	5,855
3rd party / MTPL	Property Damage	13	0.3%	1,379	27.2%	1,392	27.5%	5,079
	Bodily Injury	0	0%	59	3.6%	59	3.6%	1,659
	Total*		0.3%		25.1%		25.4%	
Overall collision claims*		311	2.0%	2,258	21.2%	2,569	**23.2%**	

*Weighted and merged according to the respective share within insurance claims to determine the proportion of target accidents within the total motor insurance collision occurrence.

Results: Expected Benefit - Share of Insurance Collision Claims Potentially Prevented through Parking ADF (MoD-Coll & TPL)

Target accidents parking ADF	Effect	Penetration rate in use	Expected benefit - avoidable share of insurance collision claims
23.2%	75%	5%	0.9%
		10%	1.7%
		30%	5.2%
		100%	17.4%
	100%	5%	1.2%
		10%	2.3%
		30%	7.0%
		100%	23.2%

Summary & Limitations

- High potential for parking ADF for avoidance of parking & maneuvering accidents (up to 23% of insurance collision claims)
- Lack of information on the number of minor damages that are not reported to insurances. It can be assumed that most of them happen during parking due to the low amount of damage. Additional avoidance potential to be expected
- The provided results are only valid for the mature L3Pilot ADF, which simplifies certain technical aspect of a real ADF
- Analysed data based on insurance claims of Allianz Germany only
- No information available considering the potential for new crashes through the use of parking ADF
- The factor effect used in the calculation is based on assumptions

Safety Impact Assessment Qualitative Analysis

Yves Page

Renault Group

1. Research Questions

Research questions

1. To what extent the calculated expected reduction(s) is(are) due to the ***underlying* assumptions** (*in the simulations*)?
2. What are the **effective mechanisms leading to an overall reduction** (we do actually not expect an increase) in crash and injury risks thanks to automation?
3. How do we **explain the magnitude of the reduction**?
4. Are we capable, via the pilots, to **identify**, underline or highlight **remaining design issues** that would help increasing the level of safety of ADF?

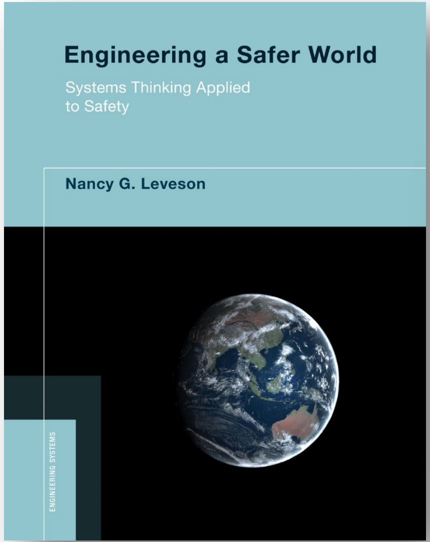
Assumption(s)

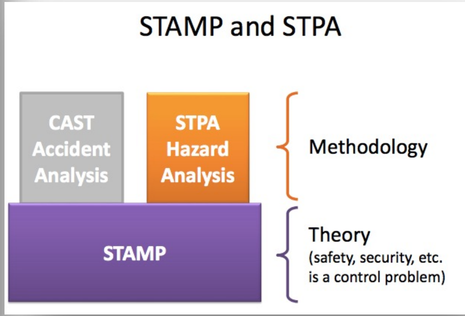
The identification of « **safety requirements** » while designing and validating the AD Functions would help in answering the questions and would highlight where efforts are still needed.

2. Method

How did we proceed to answer these research questions ?

Example of STPA analysis: The method





STAMP System-Theoretic Accident Model and Processes
STPA System-Theoretic Process Analysis

01 Establish the system engineering foundation
- Define accidents, hazards and constraints
- Build control structure

02 **STPA step 1:** Identify potentially unsafe control actions

03 Define safety requirements using the identified unsafe control actions

04 **STPA step 2:** Determine how each unsafe control action could occur
- Generate scenarios
- Establish additional (refined) safety requirements

Source: Stephanie Alvarez, 2017

Example of STPA analysis: The method

Establish the system engineering foundation
- Define accidents, hazards and constraints
- Build control structure

Accidents	Hazards	Constraints
ACC-1: People die or get injured due to a vehicle collision.	H-1: The vehicle violates the safety distance to other road users or objects on the road.	SC-1: The control structure must prevent the vehicle from violating the safety distance to road users or objects on the road.
ACC-2: Property damage due to a vehicle collision.	H-2: The vehicle leaves the roadway.	SC-2: The control structure must prevent the vehicle from leaving the roadway.

3. The data

Renault Pilot site

STPA Analysis
+

L3PILOT Questionnaires

Interview with psychologist

Interviews with safety drivers

4. Main outcome

Macroscopic Safety Requirements

First Outcome
63 macroscopic safety requirements

1. Technology-related (sensors, actuators)
2. Technology-related (algorithms)
3. HMI related
4. Driver related
5. Procedures related

Refined Safety Requirements (1)
Technology-related (sensors, actuators)

SR-1: Vehicle sensors that measure the necessary feedback to determine that ADF is available or that a takeover request is needed, must have an adequate operation (including accuracy of measures and adequate feedback, and also including internal and external sensors)
SR-44: The vehicle sensors that take measures on ADF conditions and the traffic environment must have an adequate operation (including delay and accuracy)
SR-46: The feedback provided by vehicle sensors on ADF conditions driver monitoring, and the traffic environment, must be adequate
SR-63: The actuators and commands to implement ADF engagement validation must have an adequate operation

Refined Safety Requirements (2)
Technology-related (algorithms)

SR-2: Automation must detect when the vehicle sensors that provide the necessary feedback to determine that ADF is available or that a takeover request is needed, have adequate operation
SR-3: Automation must have an adequate model of ADF conditions (parameters describing the ODD)
SR-4: Automation must have an adequate model of ADF conditions status (i.e. knows perfectly the values of parameters of the ODD)
SR-5: Automation's control algorithm must not generate ADF availability notification when the ADF conditions are not met
SR-6: Automation's control algorithm can generate ADF availability notification when ADF conditions are met
SR-7: Automation's control algorithm must not generate TOR when ADF conditions are met
SR-8: Automation's control algorithm must generate TOR when ADF conditions are not met
SR-9: Automation must generate appropriate measures if driver conditions are not met
SR-10: Automation must ensure that the actions generated by the control algorithm to send the ADF availability notification or the takeover requests to the HMI, are executed without delay of … (*tbd*)
SR-26: Automation must have an adequate model of the status of ADF engagement / disengagement

Refined Safety Requirements (3)
HMI related

SR-12: The HMI must provide adequate feedback to the driver on ADF availability notification and takeover requests
SR-22: The HMI commands must have an adequate operation and there must be an adequate communication between the HMI and automation
SR-23: The HMI commands, pedals and steering wheel must be reliable and provide on-time feedback to driver on ADF engagement/disengagement and takeover decision
SR-40: The HMI commands and vehicle actuators that enable ADF disengagement must have an adequate operation and communication
SR-41: The HMI commands and vehicle actuators must provide adequate, on-time feedback on driver's actions
SR-42: HMI must receive adequate feedback on the driving mode status (manual or automated driving mode)
SR-61: The HMI design must enable the driver to safely validate ADF engagement and release control of the vehicle
SR-57: The HMI must provide adequate feedback to the driver on ADF status
SR-58: The HMI must provide feedback to assist the driver in the validation of ADF engagement and release control of the vehicle

Refined Safety Requirements (4)
Driver related

SR-13: The mental model of the driver must include the procedures and knowledge necessary to understand and react to the feedback provided by the HMI
SR-14: The driver must value being receptive to the feedback provided by the HMI
SR-15: The driver must be able to perceive and detect the aspects that make it inappropriate to engage the ADF
SR-20: The mental model of the driver must include safety values that encourage an adequate decision-making process regarding ADF engagement and takeover request validation
SR-18: The mental model of the driver must include knowledge on the takeover procedures
RSR-34: The driver must perceive the HMI information regarding ADF disengagement
RSR-35: The driver must perceive the driving environment before disengaging the ADF
SR-36: The mental model of the driver must include knowledge on ADF disengagement procedure and the HMI (sequences, buttons, HMI displays, etc.)
SR-37: The driver must have an adequate model of the traffic environment before the decision of the ADF disengagement (including safety values)
SR-38: The driver must not provide unintended ADF disengagement
SR-53-The driver has to be aware of the driving mode status (taking into account other available systems in the vehicle)

Refined Safety Requirements (5)
Procedures related

SR-16: The takeover procedures must enable the driver to perceive the traffic environment and gain situation awareness before the validation of the takeover request
SR-17: The takeover procedures must ensure the driver is capable of responding to a TOR
SR-19: The procedures to validate a takeover request must be easy and supportive to perform by the driver
SR-21: The procedures and commands to validate ADF engagement and takeover requests must limit unintended validations

Therefore, … Are we able to answer the questions ?

1. To what extent the calculated expected reduction(s) is(are) due to the ***underlying* assumptions** (*in the simulations*)?
2. What are the **effective mechanisms leading to an overall reduction** (we do actually not expect an increase) in crash and injury risks thanks to automation?
3. How do we **explain the magnitude of the reduction**?
4. Are we capable, via the pilots, to **identify**, underline or highlight **remaining design issues** that would help increasing the level of safety of ADF?

Therefore, … Are we able to answer the questions ?

1. To what extent the calculated expected reduction(s) is(are) due to the ***underlying*** **assumptions** (*in the simulations*)?

   All safety requirements are implicitly supposed to be fulfilled in most of simulations. The benefit of the qualitative analysis is to make the implicit explicit.

Therefore, … Are we able to answer the questions ?

2. What are the **effective mechanisms leading to an overall reduction** (we do actually not expect an increase) in crash and injury risks thanks to automation?

   Assuming that lower speeds, lower speed variances, longer time headways are more likely to be associated with automated driving and with a lower crash risk, the results are in line with expectations.

   Behind lower speeds and longer time headways is technology design (perception and decision algorithms). The safety requirements again give some explicit insights into how technology should lead to safe driving.

Therefore, … Are we able to answer the questions ?

3. How do we **explain the magnitude of the reduction**?

   Magnitude of reduction is more explained by changes in risks within driving scenarios and frequencies across scenarios than through qualitative analysis.

Therefore, … Are we able to answer the questions ?

4. Are we capable, via the pilots, to **identify**, underline or highlight **remaining design and Validation & Verification issues** that would help increasing the level of safety of ADF?

❑ Motives for **rejection** (and therefore less usage and less safety) to be tackled

- **Inconsistency** between what the driver sees and what the driver feels the vehicle sees.
- Drivers expect the vehicle to **behave** like a human being, or at least like themselves. Is it **realistic** ?
- How to combine **safety** and **comfort** ? Obeying traffic rules lead to discomfort (especially in looooong overtaking situations)

Therefore, … Are we able to answer the questions ?

4. Are we capable, via the pilots, to **identify**, underline or highlight **remaining design and Validation & Verification issues** that would help increasing the level of safety of ADF?

❑ Motives for **proper usage** or **improvement**

- Vehicle should be **visible** and **recognizable** as an automated vehicle
- HMI plays a crucial role (understandability, recognizing AD status, smooth alert, etc.) that it was not possible to analyse in the Pilot.
- ODD **Fragmentation** kills value (we had long stretches and short stretches of roads)
- **Driver education**: declarative and procedural knowledge should be transmitted before use to get a calibrated correct mental model for trust. Content, duration, time, used medium, target population, of the training is still under debate.
- L3Pilot did not allow to study “stressful“ situations and edge cases. To be further investigated…

This was part one of the safety impact assessment.

See you after the break for the final results!