Continental
The Future in Motion

University of Stuttgart
Germany

Missing no Interaction – Using STPA for Identifying Hazardous Interactions of Automated Driving Systems

Asim Abdulkhaleq, University of Stuttgart, Germany
Markus Baumeister, Systems & Technology, Continental Chassis & Safety Division

Agenda

1 Motivation – Safety in Automated Driving

2 Safety in Use vs. Functional Safety

3 Safety in Use Analysis

4 Applying STPA for Safety in Use

5 Results

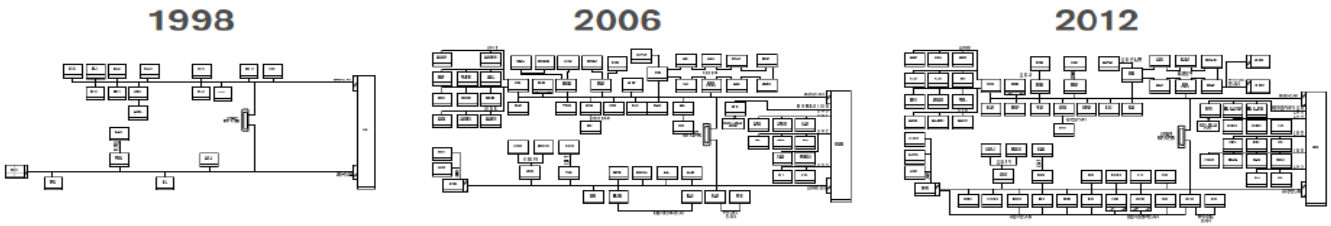
6 Conclusion & Future Work

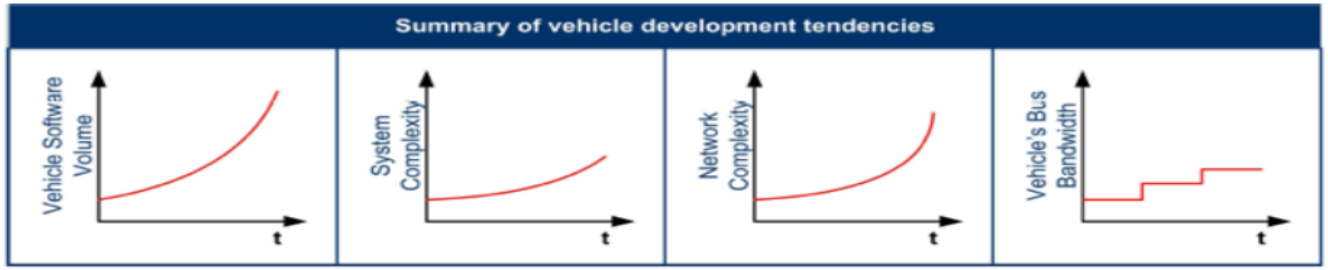
Automated Driving

Safe and Dynamic Driving towards Vision Zero

Motivation

Automotive architecture trend



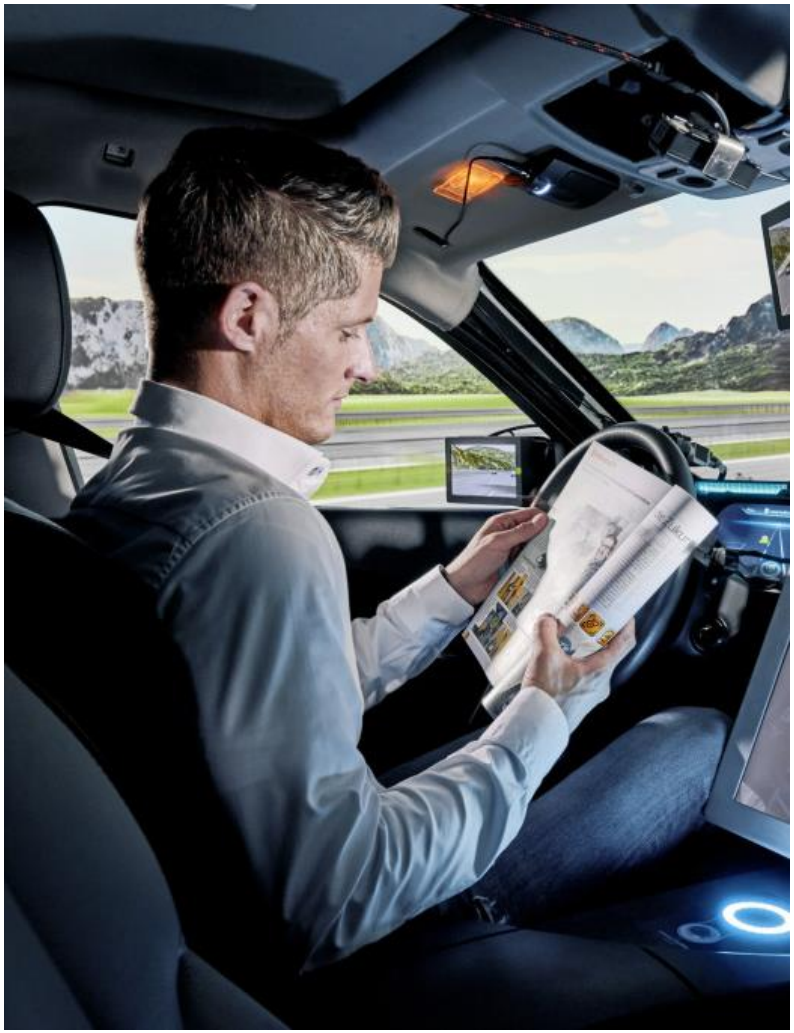


Source: WRC Market Report E/E Architecture 2013

Continuously growing complexity, number of functions and networked ECUs results in:

- Increased chance for random & systematic failures to cause behaviour deviations of functions
- Increased potential of functions to be unsafe as specified

Motivation
Safety for automated driving



- Starting with AD L3: Driver may distract himself
  - No immediate human fallback!
- Thus most intelligent, independently powered safety mechanism no longer available
  - Partial fail-operational (or fail-degraded) mechanisms necessary
    - Functional Safety
  - Specified behaviour must work in all situations
    - Safety in Use

Relationship between Functional Safety and Safety in Use

Agenda

1 Motivation – Safety in Automated Driving

2 Safety in Use vs. Functional Safety

3 Safety in Use Analysis

4 Applying STPA for Safety in Use

5 Results

6 Conclusion & Future Work

Safety in Use vs. Functional Safety

Location in the development cycle

Safety in Use

Failures between

Real World

Item Definition

Function Spec

Architecture

Implementation

Execution

Failures between

Func-tional Safety

Specification

Realization

Collision Avoidance Example	Potential failures
Objects can occur in front of the car and should not be hit	› **Sensor performance insufficient for planned maneuver** › **Not all situation might allow evasion, breaking maneuver missing**
Evasion maneuver by function, Required actuator performance, Required sensor performance	› **Driver might countersteer maneuver** › No interface for function to influence steering; wrong granularity of values › Function running on too slow MCU
Module and Interface specification Allocation of SW to Components	› SW steers in wrong direction › Environmental model orders objects incorrectly › OS executes SW only every 2_{nd} cycle
Executable and Parameterization Hardware components	› SW was disabled by application driver › Sensor breaks (e.g. no video) › Bit flip in parameters disables function
Behaviour in the field	› Bit flip in memory causes steering in wrong direction

Safety in Use vs. Functional Safety

Different Definitions

[from Böhmert, Blüher 2016]

Availability[1])
[readiness for correct service]

Reliability[1])
[continuing for correct service]

Safety[2])
[absence of unreasonable risk]

Functional safety[2])
[absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems]

Integrity (Functional)
[absence of unreasonably hazardous functionality]

Safety in use
[absence of hazards due to human errors]

Roadworthiness (Operational Safety)
[property or ability of a car, bus, truck or any kind of automobile to be in a suitable operating condition or meeting acceptable standards for safe driving and transport of people, baggage or cargo in roads or streets]

In this presentation: Safety in Use

Maintainability[1])
[ability to undergo modifications and repairs]

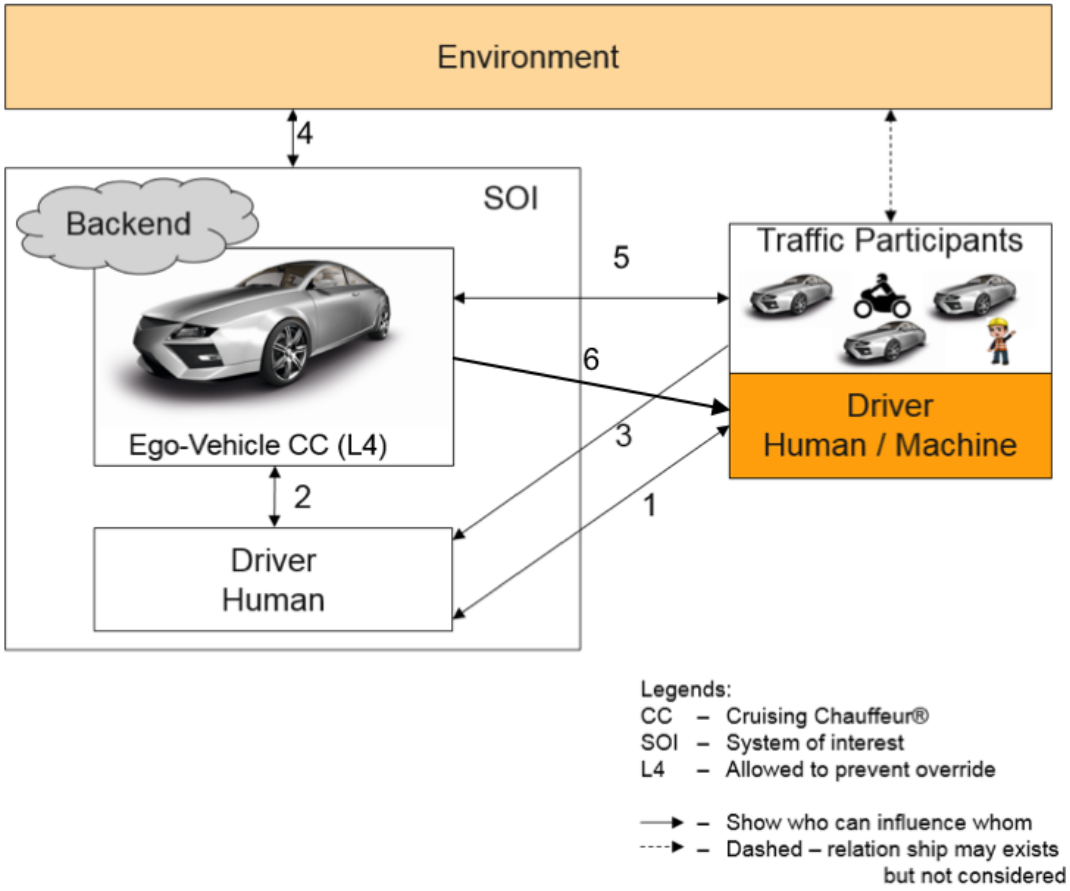
Source:
[1]) Diagram: Basic Concepts and Taxonomy of Dependable and Secure Computing (IEEE Transactions on dependable and secure computing, Vol.1 No.1, January-March-2004;
[2]) Definition Safety: ISO26262-1:2011 first edition

Safety in Use vs. Functional Safety

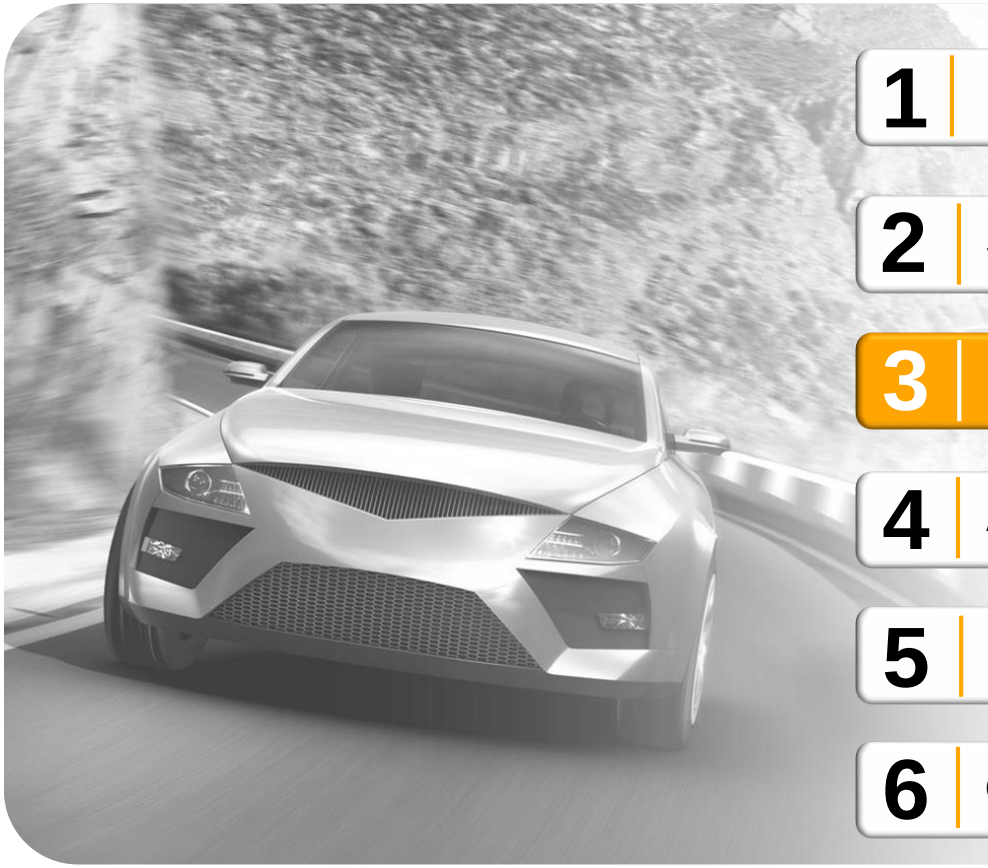
Safety in Use and interactions

› Specification failures often happen due to missed potential interactions

1. Driver Human-and-Driver Human Interaction (**HIH**)
   misunderstanding, aggression, …
2. Driver Human-and-Driver Machine Interaction (**HIM**)
   confusion, misuse, inaction, ….
3. Driver Human-and-other Traffic Participants Interaction (**HIP**)
   bad estimations, ….
4. Automated Driving System-and-its Environment Interaction (**AIE**)
   overload, missing participants, ….
5. Automated Driving System-and-other Traffic Participants (**AIP**)
   feedback loops, different behaviour,
6. Automated Driving System and other Driver Humans (**AID**)



Agenda



1 Motivation – Safety in Automated Driving

2 Safety in Use vs. Functional Safety

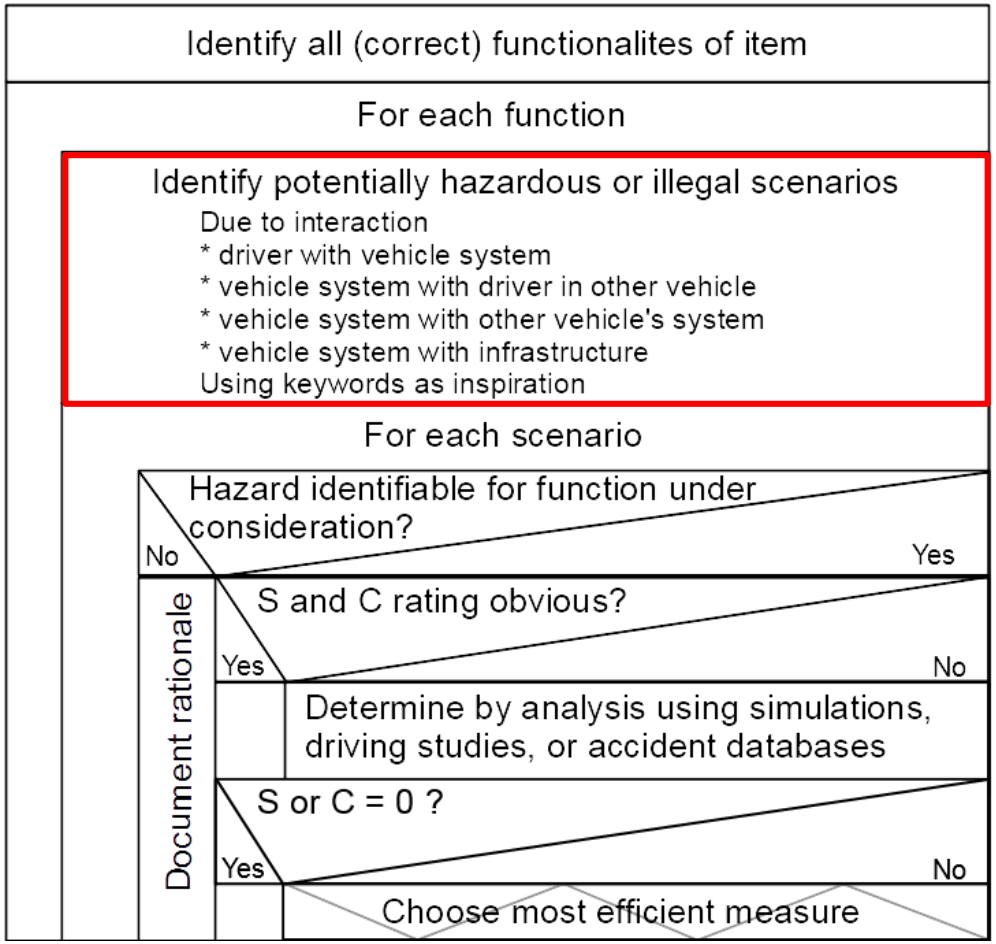
3 Safety in Use Analysis

4 Applying STPA for Safety in Use

5 Results

6 Conclusion & Future Work

Safety in Use Analysis
Approach at Continental



- Situation + Behaviour = potentially hazardous scenario
- Keyword-guided brainstorming of situations
  - Dependent on experience of analyst
- Evaluation of risk
  - Similar to HARA for functional safety

Is there a method less dependent on inspiration?

Safety in Use Analysis
Excerpt of SiU Results for Lane Change

› Four (out of six) SiU requirements mainly relevant for “Lane Change” functionality:

ID	SiUA-Requirements	Cause of hazard
SIUR-16	Lane changes shall only be conducted when the vehicle can determine **sufficient length** of the **new lane** for at least a brake to standstill.	Potential violation of known requirement in seldom situation
SIUR-33	There shall be no automated lane change **while** handing over control to the driver (**Take over Request**).	Normal behaviour causing hazard by mode interaction.
SIUR-38	**Motorcycles** overtaking **on the lane markings** (i.e. between the lanes) shall be observed during lane changes.	Potential violation of known requirement in seldom situation
SIUR-45	The automated vehicle shall not block a formed **corridor for emergency vehicles** while changing lanes.	Normal behaviour causing hazard in special situation

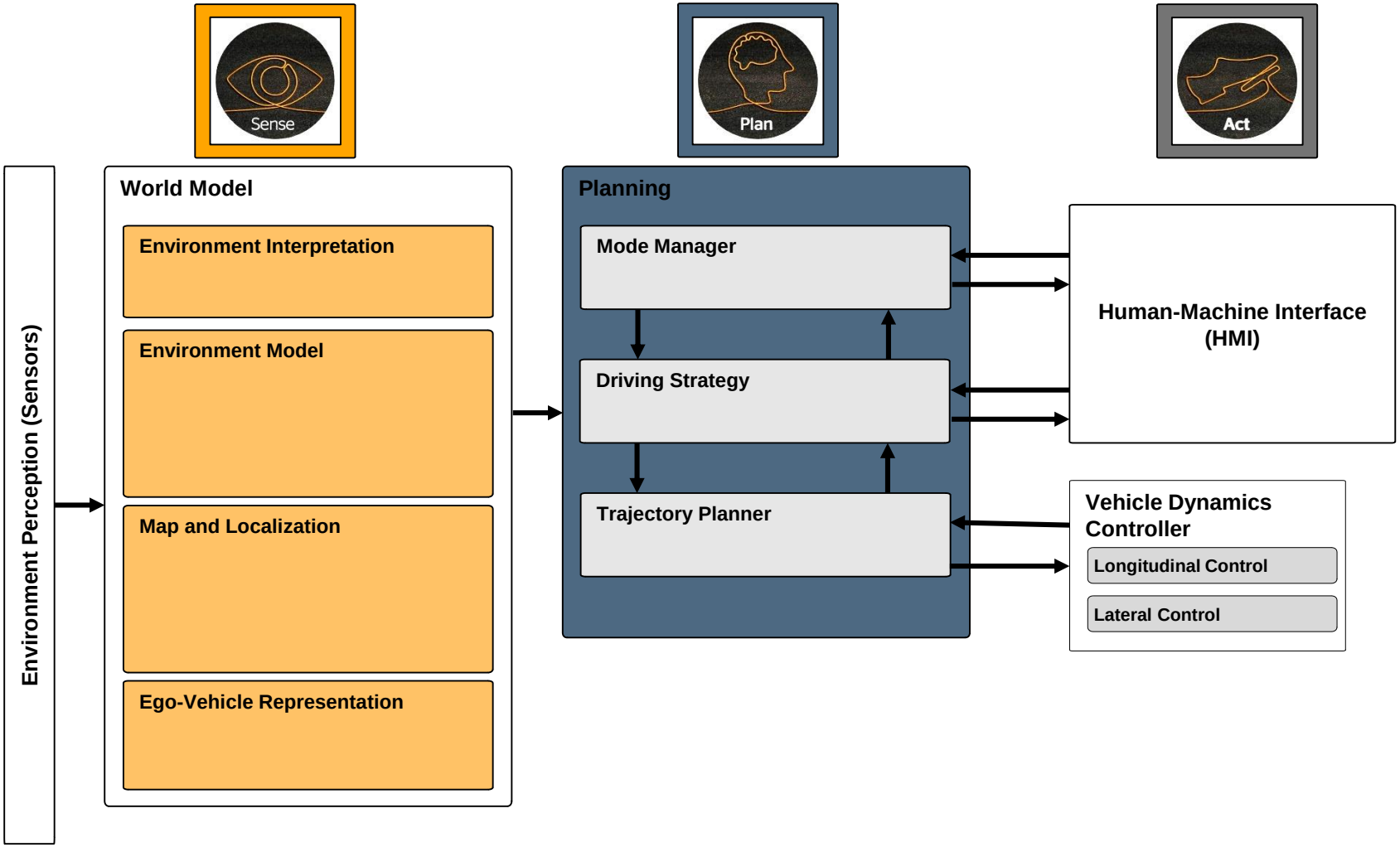
Will STPA find these requirements or others?

Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work

Prototype Realization of Automated Driving

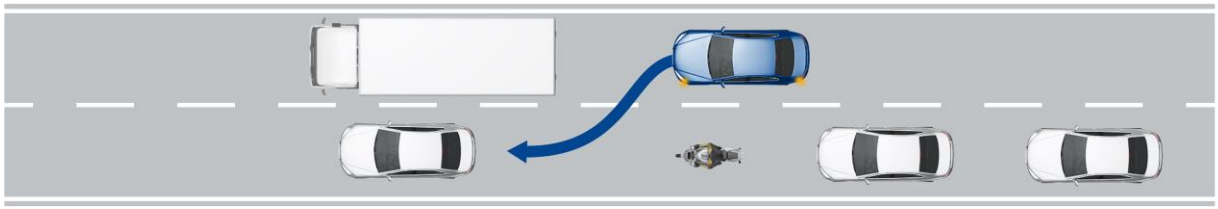
Layered Functional Architecture

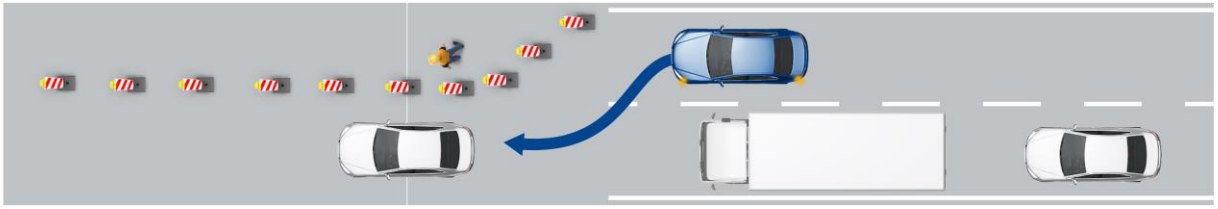


Change Lane Function by Ego Vehicle Cruising Chauffeur

Examples of the Traffic Situations of Change Lane

› We apply STPA to identify the hazardous situations of the lane change function and develop detailed safety requirements/controls.





Our main question: Can STPA derive the Safety in Use requirements (SiU) ?

Agenda

1 Motivation – Safety in Automated Driving

2 Safety in Use vs. Functional Safety

3 Safety in Use Analysis

4 Applying STPA for Safety in Use

5 Results

6 Conclusion & Future Work

STPA Results

STPA Step 0: Establish the fundamentals of analysis

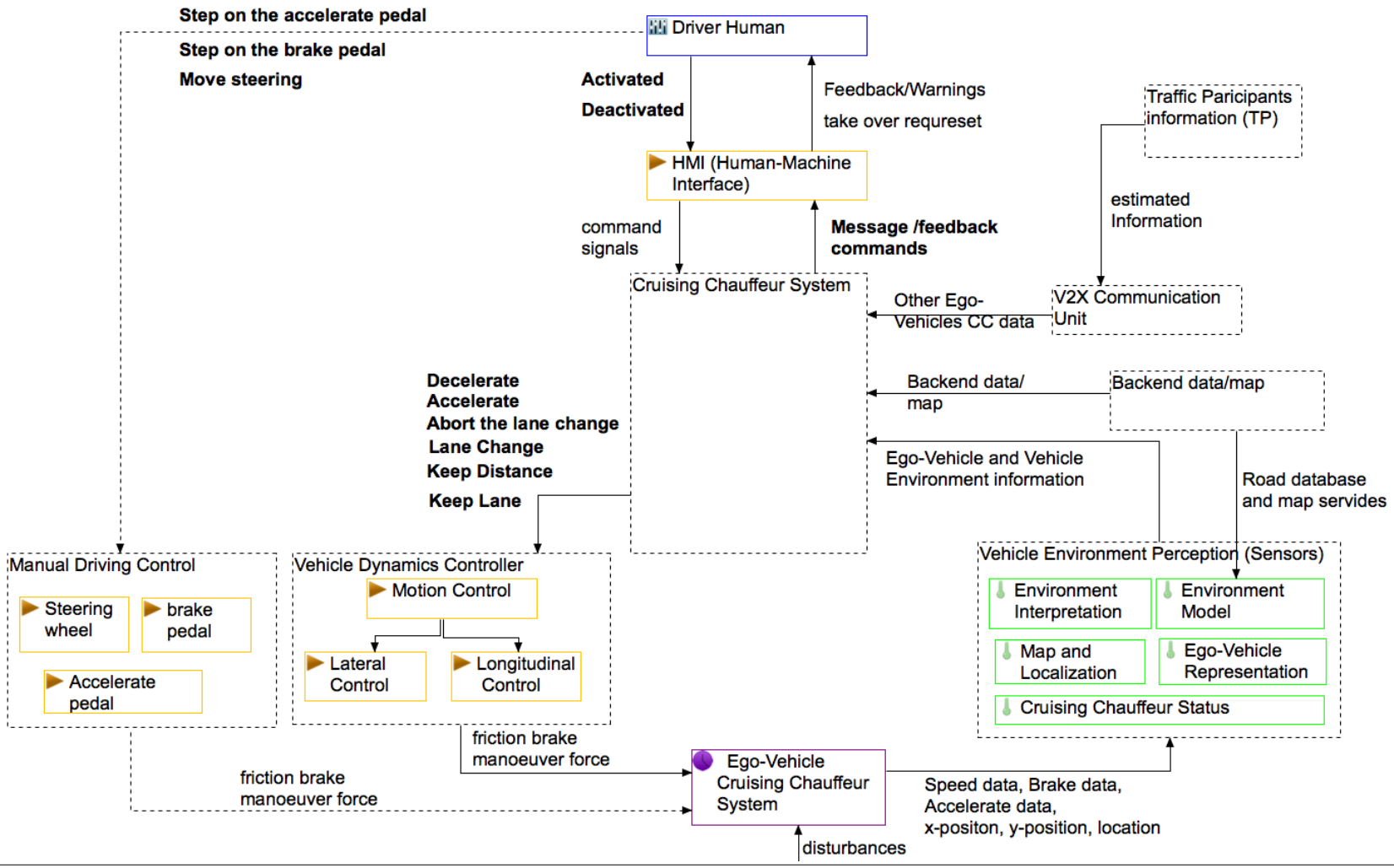
- We identify one accident which automated driving can lead to (lane change function).
- We identify 12 hazards which can lead to this accident and
- We translate these 12 hazards into system-level safety constraints.

Accident AC-1: The ego vehicle cruising chauffeur collides with a vehicle during the lane change procedure and people dies/ are harmed.

ID	Hazards
H-1	The Cruising Chauffeur system did not estimate correctly the position and velocity of the other traffic participants in the lane.
H-2	The Cruising Chauffeur system did not recognize the lane markings.
H-3	The Cruising Chauffeur system did not turn on the light of the direction indicators.
H-4	The Cruising Chauffeur system steered the ego vehicle in the wrong direction.

STPA Results

STPA Step 0: Safety-Control Structure Diagram



STPA Results

STPA Step 1: Unsafe Control Actions

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Lane Change	*The CC system did not provide the lane change when it is involved due to an emergency situation (e.g. accident occurred before the Ego vehicle).	**UCA1.1** The CC system provided incorrect lane change request to the motion control to change lane while there is no gap in the target lane.	**UCA1.5**. Too early: The CC system started the lane change function too early while the gap has not been reached yet.	**UCA1.8**. Stopped too soon: The CC system provided a lane change request too short to the motion control that was not enough to change the vehicle to the target lane.
	*[Not Hazardous]	[H-1][H-2][H-7] [H-8] [H-9] [H-12]	[H-1] [H-2] [H-4] [H-5] [H-10]	[H-4] [H-5]
	Interaction: AIE	AIP	AIE, AIP	AIP

Each unsafe control action is translated into a corresponding safety constraint.

STPA Results

STPA Step 2: Causal Factor Analysis

Unsafe Control Action: UCA1.1 The CC provided incorrect lane change request to the motion control to change lane while there is no gap in the target lane.			
Associated Hazards: [H-1][H-2][H-7] [H-8] [H-9] [H-12]			
Component	Causal Factors	Safety Constraints/Controls	Notes / Rationale
Cruising chauffeur System	√ **Process model incorrect:** The CC estimated a wrong position of other traffic participant in the adjacent lane (target lane). The CC incorrectly believes that there is an enough gap to change lane in the target lane. The CC received a wrong ego vehicle width. The CC incorrectly estimated the traffic conditions. √ **Control input wrong**: The driver is request a lane change in non-highway road.	1. Make the CC system able to be a self-adaptive system to the traffic changes during the lane change procedure. 2. If the backend or V2x communication unit is unavailable, the CC system should be immediately warned the driver to take over control and transited automatically to inactive status.	

Mapping STPA Results to Safety in Use Requirements

Mapping SiU Results

- We identify 41 STPA safety requirements for the lane change function.
- We evaluated the resulting safety requirements against the requirements created in the SiU analysis

ID	SiUA-Requirements	Mapping	Cause of hazard
SIUR-16	Lane changes shall only be conducted when the vehicle can determine sufficient length of the new lane for at least a brake to standstill.	**(SR 1.6)**	Potential violation of known requirement in seldom situation
SIUR-33	There shall be no automated lane change while handing over control to the driver (ToR).	**No mapping**	Normal behaviour causing hazard by mode interaction.
SIUR-38	Motorcycles overtaking on the lane markings (i.e. between the lanes) shall be observed during lane changes.	**No mapping**	Potential violation of known requirement in seldom situation
SIUR-45	The automated vehicle shall not block a formed corridor for emergency vehicles while changing lanes.	**(SR 1.1)**	Normal behaviour causing hazard in special situation

Overall six SiU requirements were analyzed and for three of them a mapping towards STPA requirements could be found.

Mapping STPA Results to Safety in Use Requirements

Mapping STPA Results

› We evaluated the 41 STPA safety requirements against the requirements created in the SiU analysis

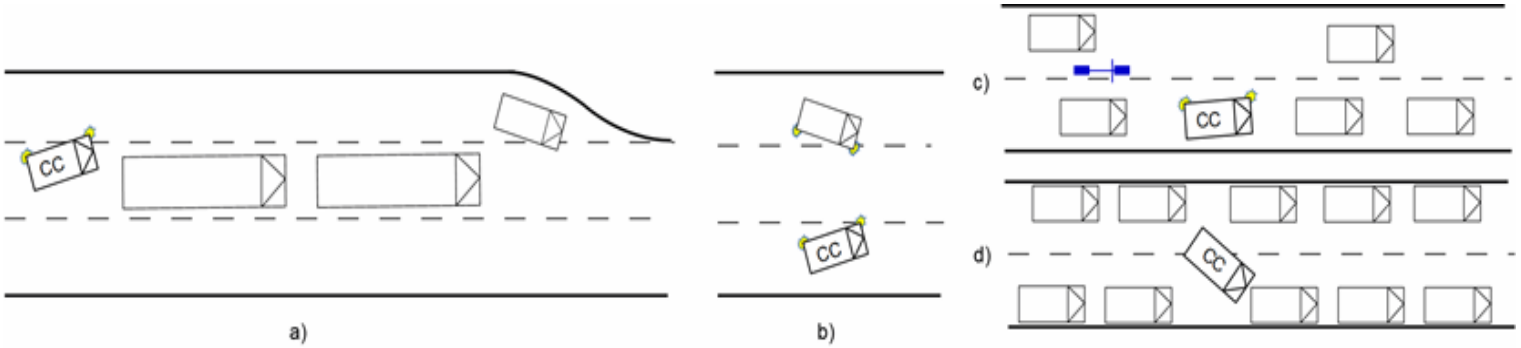
ID	STPA Safety Requirement	Type *	Mapping	Interaction
SR 0.5	The traffic markings must be in a good quality and visibly.	?	Special	AIE
SR 0.7	CC must not lose the detection of other traffic participants while CC changes lanes	FuSa & SiU	No mapping	AIP
SR 0.8	CC must not steer the ego vehicle in the wrong direction.	FuSa	N/A	AIE
SR 0.10	CC must estimate the lane velocity correctly.	FuRe & FuSa	N/A	AIP
SR 1.1	The CC must not send a lane change request to the motion control while it is not allowed due to the traffic road conditions.	SiU	(SIUR-45)	AIE/AIP
SR 1.6	CC must abort a lane change due to unexpected changes in the prerequisites of the lane change function.	SiU	(SIUR-16)	AIE

*Legends: FuSa (Functional Safety), SiU (Safety in Use), FuRe (Functional Requirements), ? Difficult to classify

Overall 41 STPA requirements were found on different analysis levels, Many of these are related to the basic driving task as SR0.8 und SR 0.10.

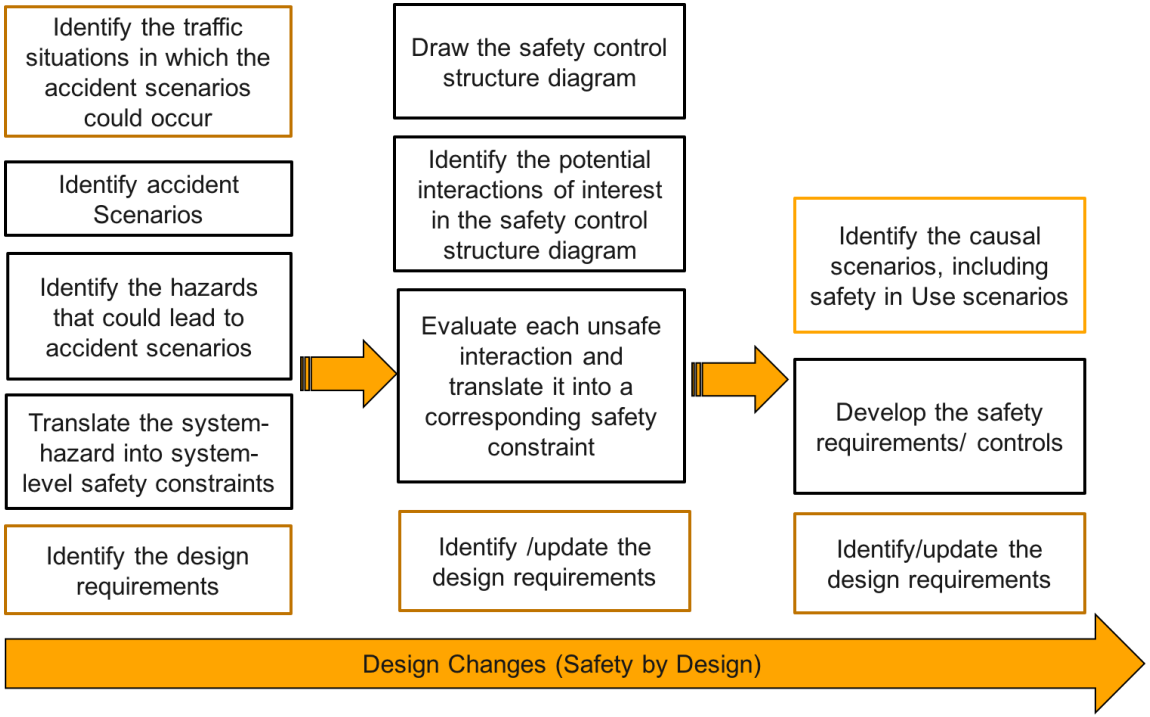
Discussion

- **Quantity**: STPA created safety requirements also outside the domain of SiU in the form of functional safety requirements, and “normal” functional requirements.
- **Abstractness**: Many STPA safety requirements describing SiU issues are relatively abstract with respect to the involved hazard.
- **Level of analysis:** On detailed analysis level (i.e. causal factor analysis), the discovered STPA safety requirements are in a great majority not SiU-related due to analyzing the malfunction of some system component.
- **Scenarios**: Whereas STPA analyzed only the two traffic situations, the SiU analysis typically has analyzed a different scenario for each resulting requirement.



The Safety-in-Use Approach based on STPA

- We proposed an extension to STPA for safety in use analysis by including the traffic situation analysis as a part of the STPA Step 0 to help the safety in use analysis engineers to focus the time and efforts only on safety in use aspect.
- We include also a step for identifying design requirements at the end of each STPA steps to help the safety in use engineers to identify/refine their design based on the STPA results.



Agenda

1. Motivation – Safety in Automated Driving
2. Safety in Use vs. Functional Safety
3. Safety in Use Analysis
4. Applying STPA for Safety in Use
5. Results
6. Conclusion & Future Work

STPA for Safety in Use Analysis
Conclusion and Future Work

- We investigated the application of the STPA approach in identifying the safety in use requirements.
- We applied STPA to the Cruising Chauffeur© at Continental.
- We found that the STPA approach can address different kinds of the interaction between the automated driving system and others.
- We found also STPA is a useful approach for identifying more types of the detailed requirements, including safety in use
- One challenge is that the STPA approach is not specific for any safety aspects (functional safety or system-level safety). Therefore, output of STPA includes different types of safety requirements.
- As a future work, we plan to improve our first proposed extension to STPA for safety in use to help the safety in use experts in addressing only the safety in use requirements.

Thank you

for your attention!

With contribution from
Hagen Boehmert (Continental, Frankfurt)
Prof. Dr. Stefan Wagner (University of Stuttgart)

Safe and Dynamic Driving
towards Vision Zero

SensePlanAct
Chassis & Safety

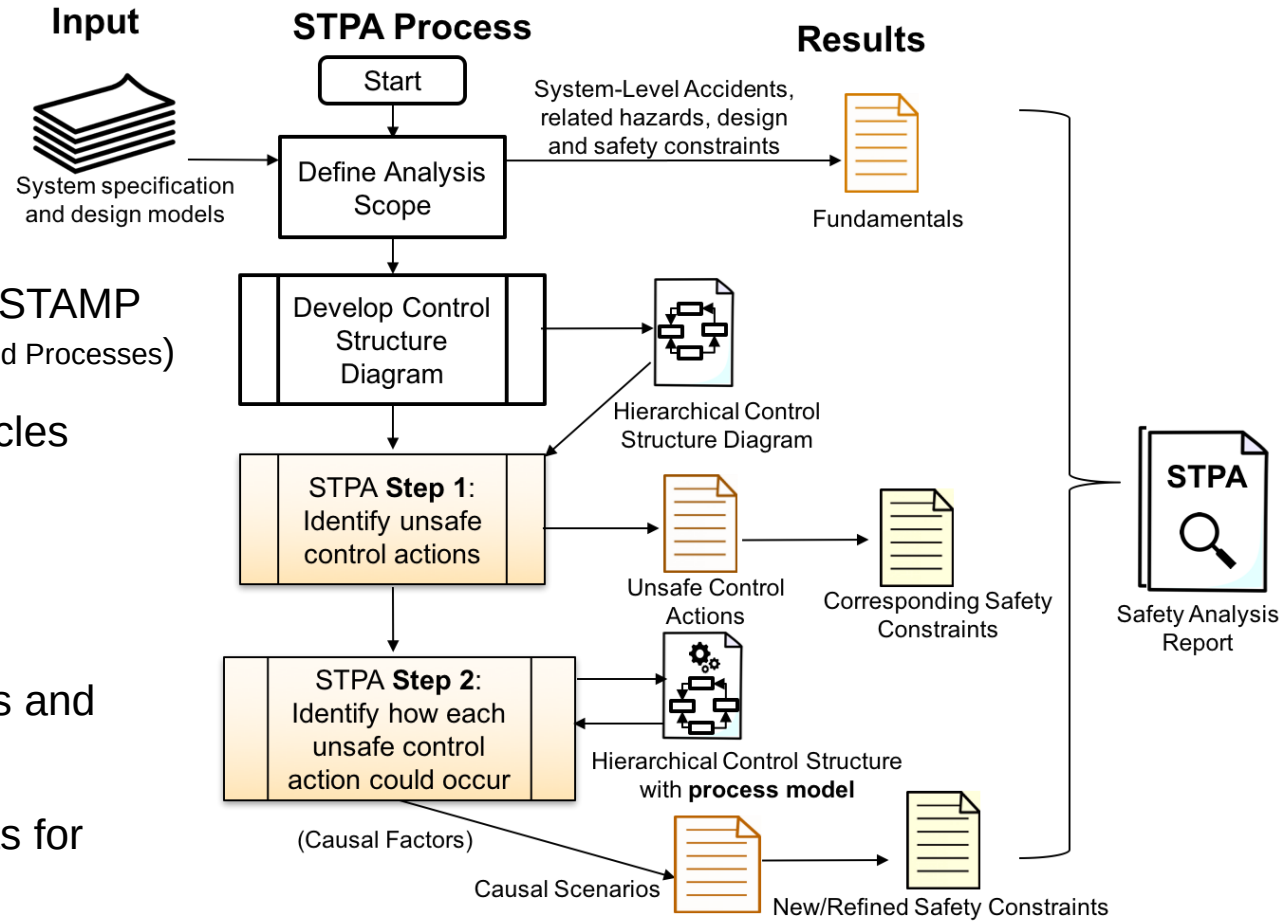
Continental

Introduction to STAMP/STPA

Safety Analysis Approach

Systems Theoretic Process Analysis (STPA)

- Sees hazards as a control problem (based on STAMP =Systems-Theoretic Accident Model and Processes)
- Modells process control cycles within system
- Searches for inadequate control actions
  - Identifies causal factors and flaws leading to them
- Results in safety constraints for system



[Abdulkhaleq 2017]