Fallback Strategy for Automated Driving using STPA

Dr. Thomas Raste, Hagen Böhmert, Ali Houry

3rd European STAMP Workshop, Amsterdam, October 6, 2015

Agenda

1 Automated Driving

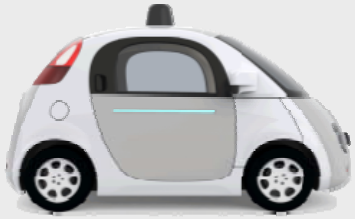
2 Road and Product Safety

3 Functional Safety Process

4 STAMP/STPA Results

Strategies and Levels of Driving Automation

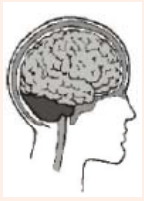
Automation Strategies



Google.com

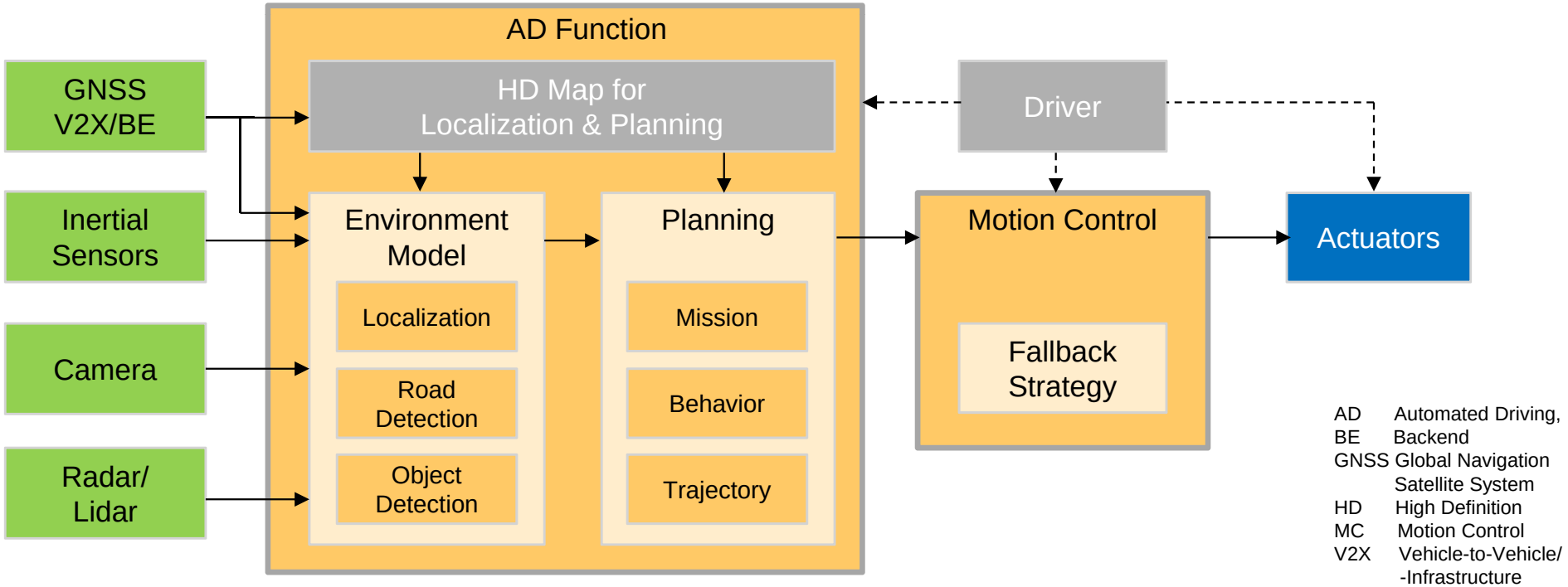
„Everything Somewhere“

„Something Everywhere“

						
SAE Level	0 No Automation	1 Driver Assistance	2 Partial Automation	3 Conditional Automation	4 High Automation	5 Full Automation
Fallback perfor-mance of dynamic driving task						
Today legally conformant				Law modifications required		

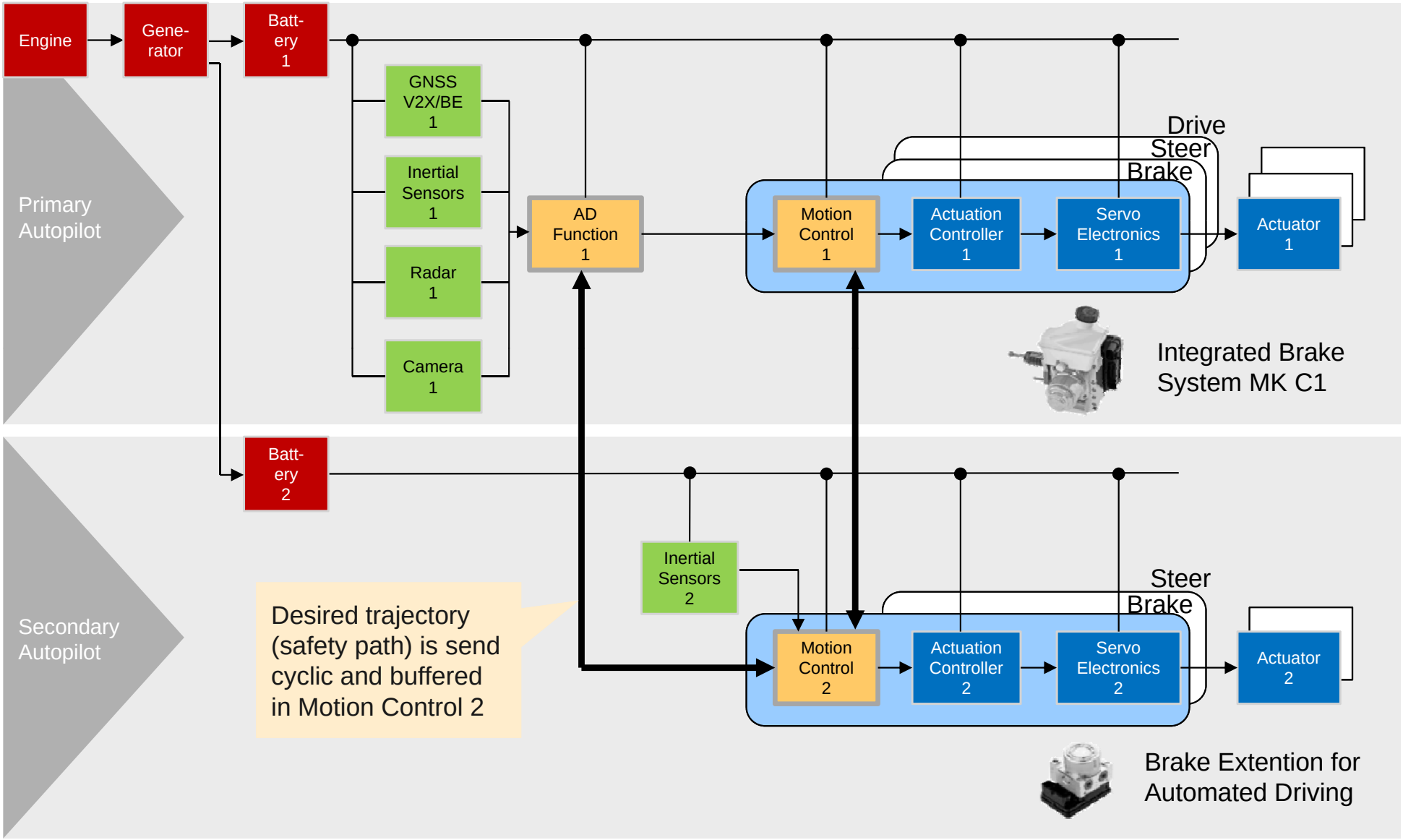
Automated Driving Building Blocks

- Use case: Highway Chauffeur
- AD Function calculates target trajectory
- MC provides trajectory tracking control
- Initial faults are tolerated
- Driver finally takes over or vehicle stops

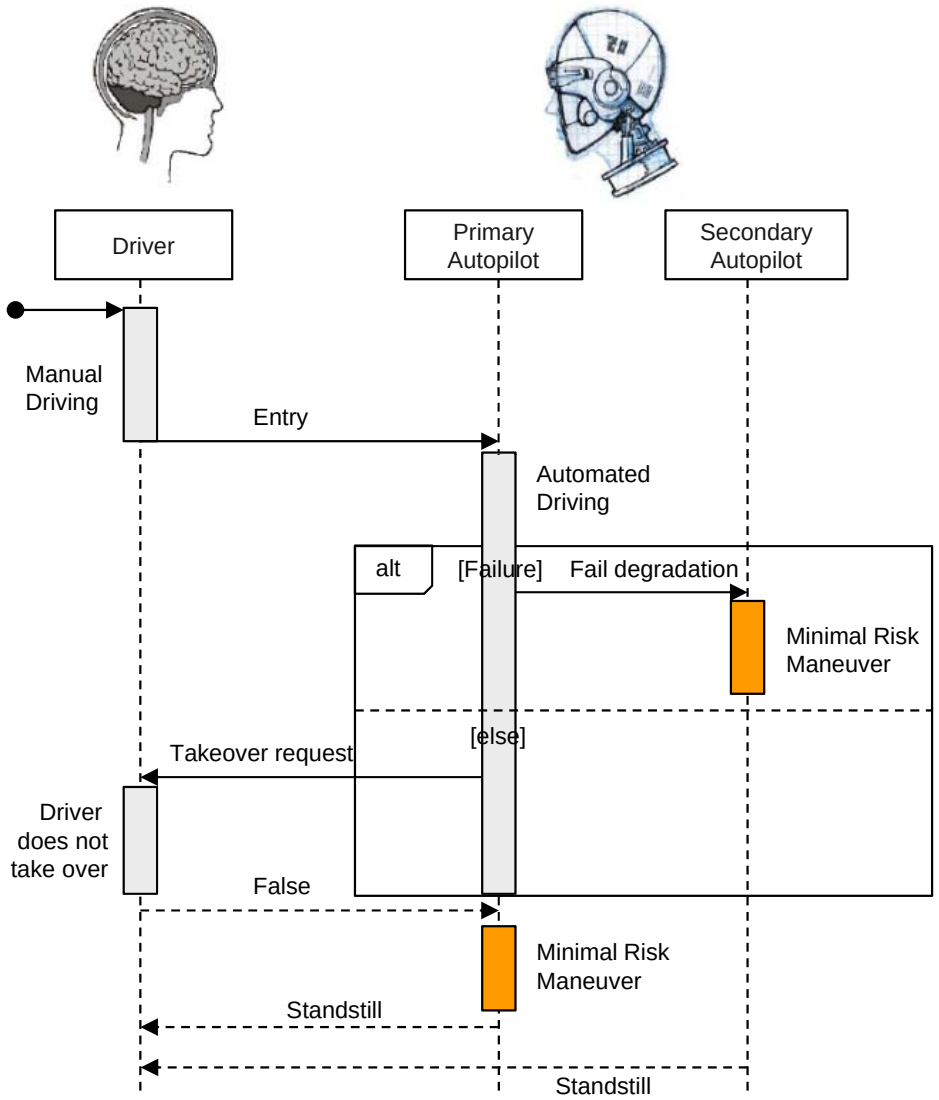


AD Automated Driving,
BE Backend
GNSS Global Navigation Satellite System
HD High Definition
MC Motion Control
V2X Vehicle-to-Vehicle/-Infrastructure

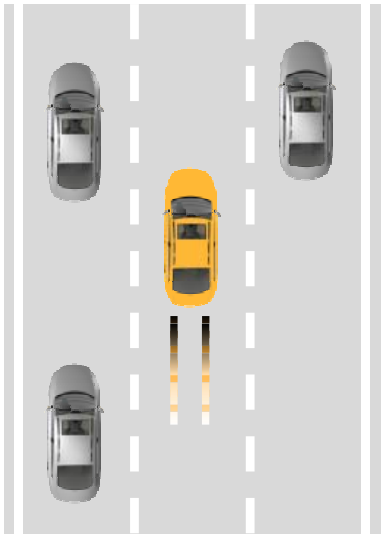
Redundancy for Automated Driving (Example)



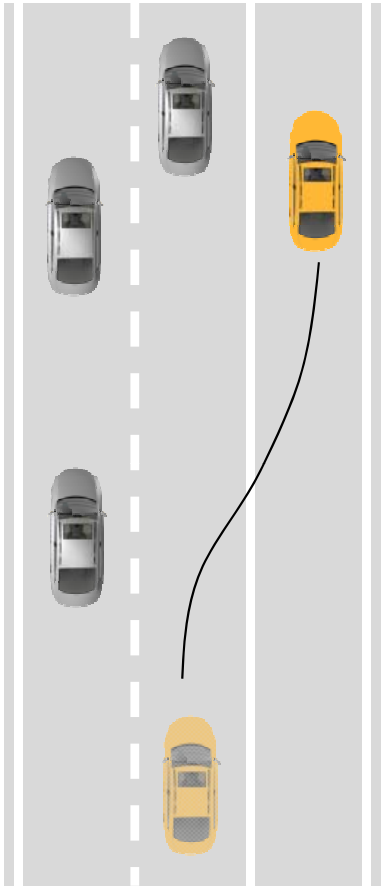
Minimal Risk Condition as Fallback Strategy



Minimal Risk Maneuver



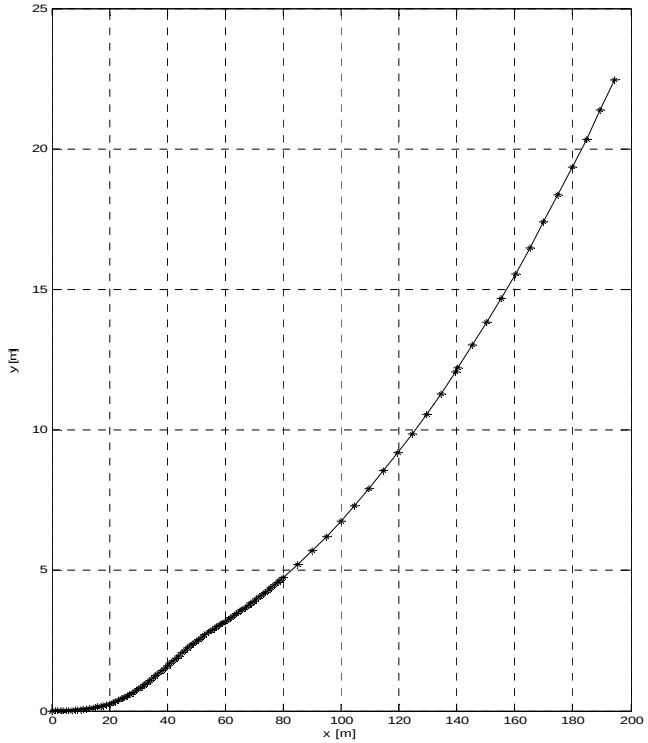
a)
System provides standstill in the ego lane



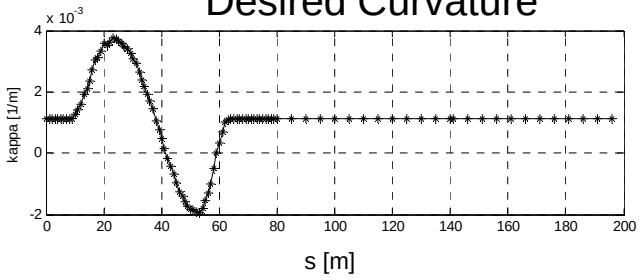
b)
System provides standstill in service or rightmost lane

Fallback Strategy Testing

Desired Position

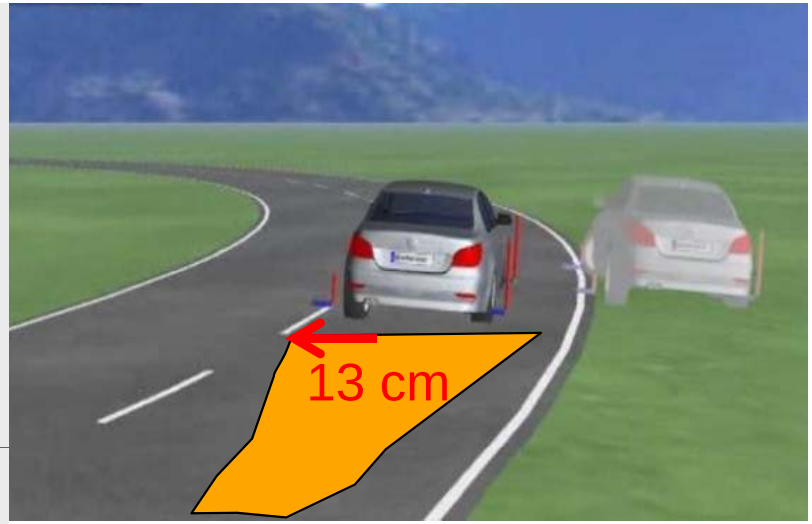


Desired Curvature

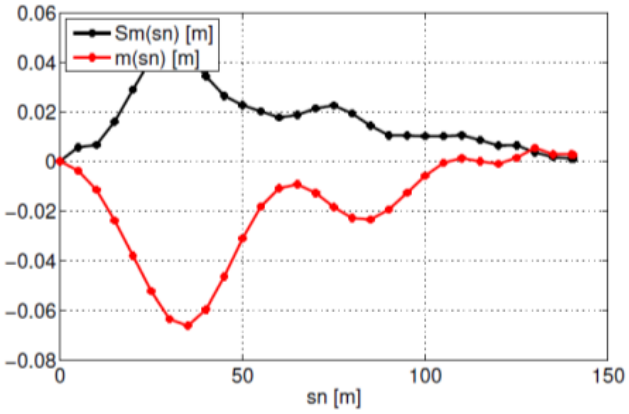


Test Case
- 900m radius circle with lane change
- Braking into standstill from 105 km/h
- Localization based only on inertial sensors (odometry)
- 12 Samples

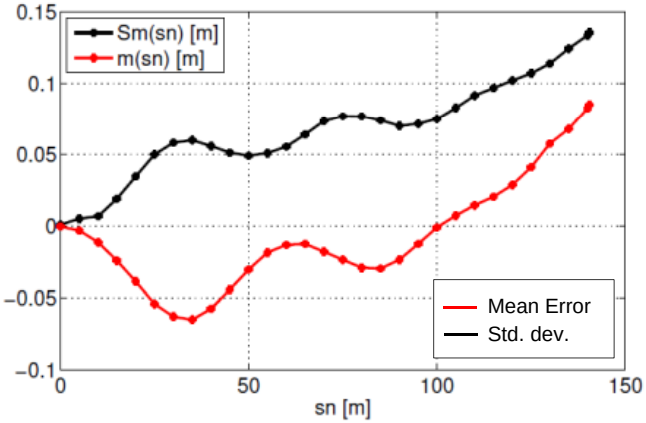
Result
- 13 cm max. uncertainty



Control Uncertainty



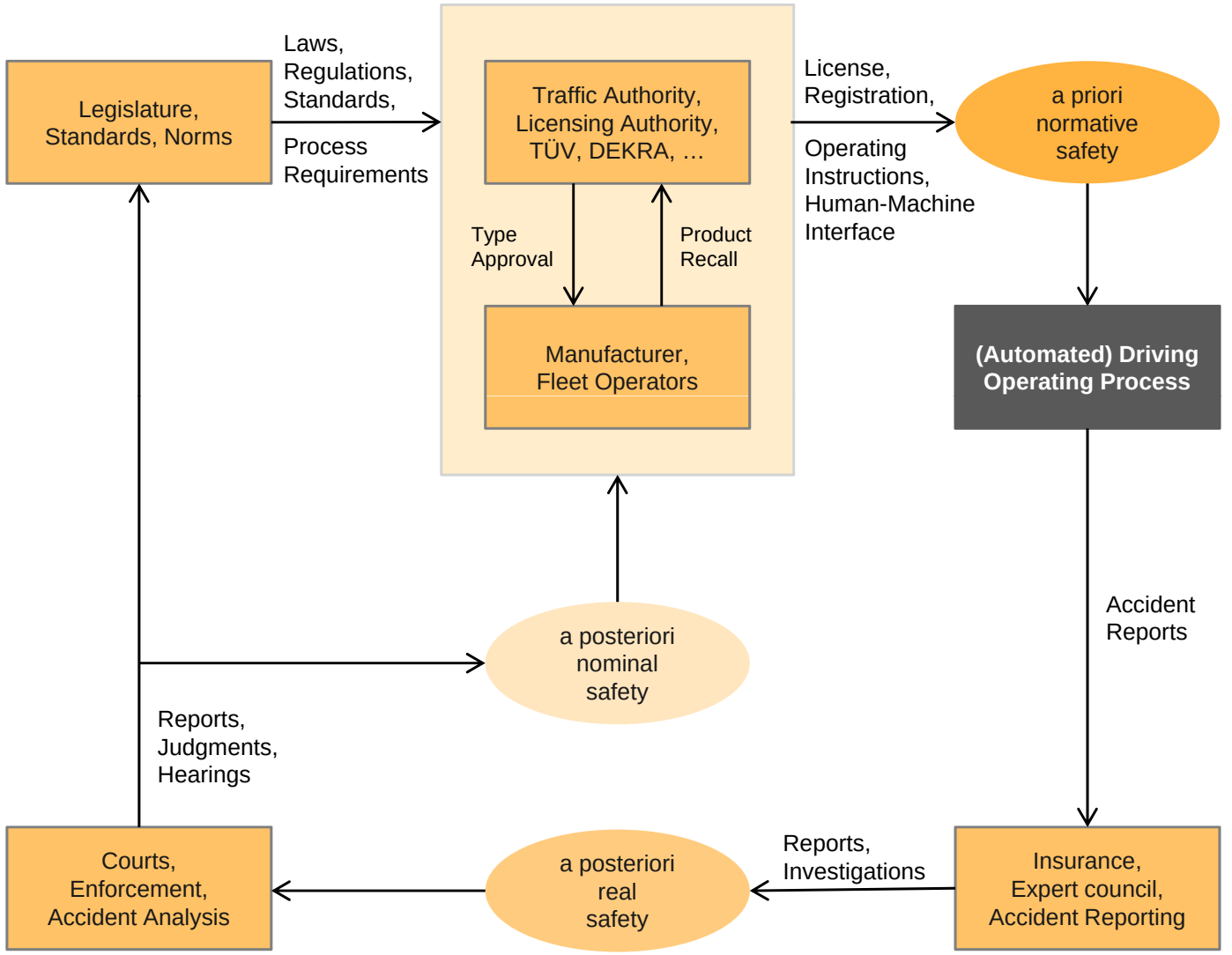
Control + Odometry Uncertainty



Socio-Technical System for Road Safety

Dynamic process

- Determines normative safety (control action) in a complex feedback loop
- Ideally all three safety levels (normative, real, nominal) are equal
- Unstable, if real safety is accepted to be normative safety (positive feedback)



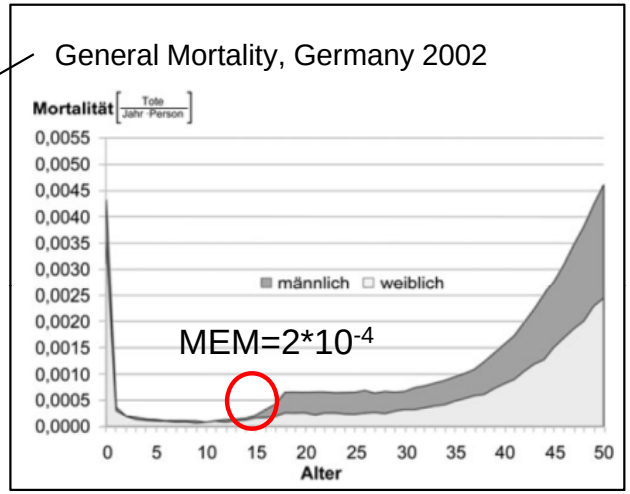
Schnieder, E.; Schnieder, L.: Verkehrssicherheit (Road Safety, in German). Springer Vieweg, Berlin, 2013

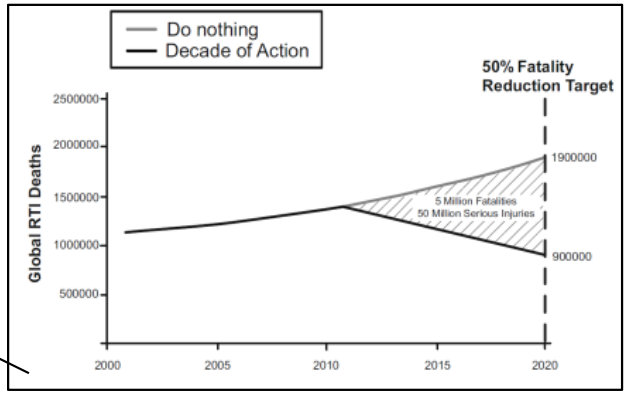
Road Safety Goals

Relative Goals: At least the same or increased safety level over time
Absolute Goals: Socially accepted reference values for risk level

	qualitative	quantitative
absolute		Minimum Endogenous Mortality (MEM) w.r. to traffic „Vision Zero“: Reduce number of fatalities to zero until 2050
relative	Automotive Safety Integrity Level (ASIL)	Reduce number of fatalities by 50% until 2020

General Mortality, Germany 2002





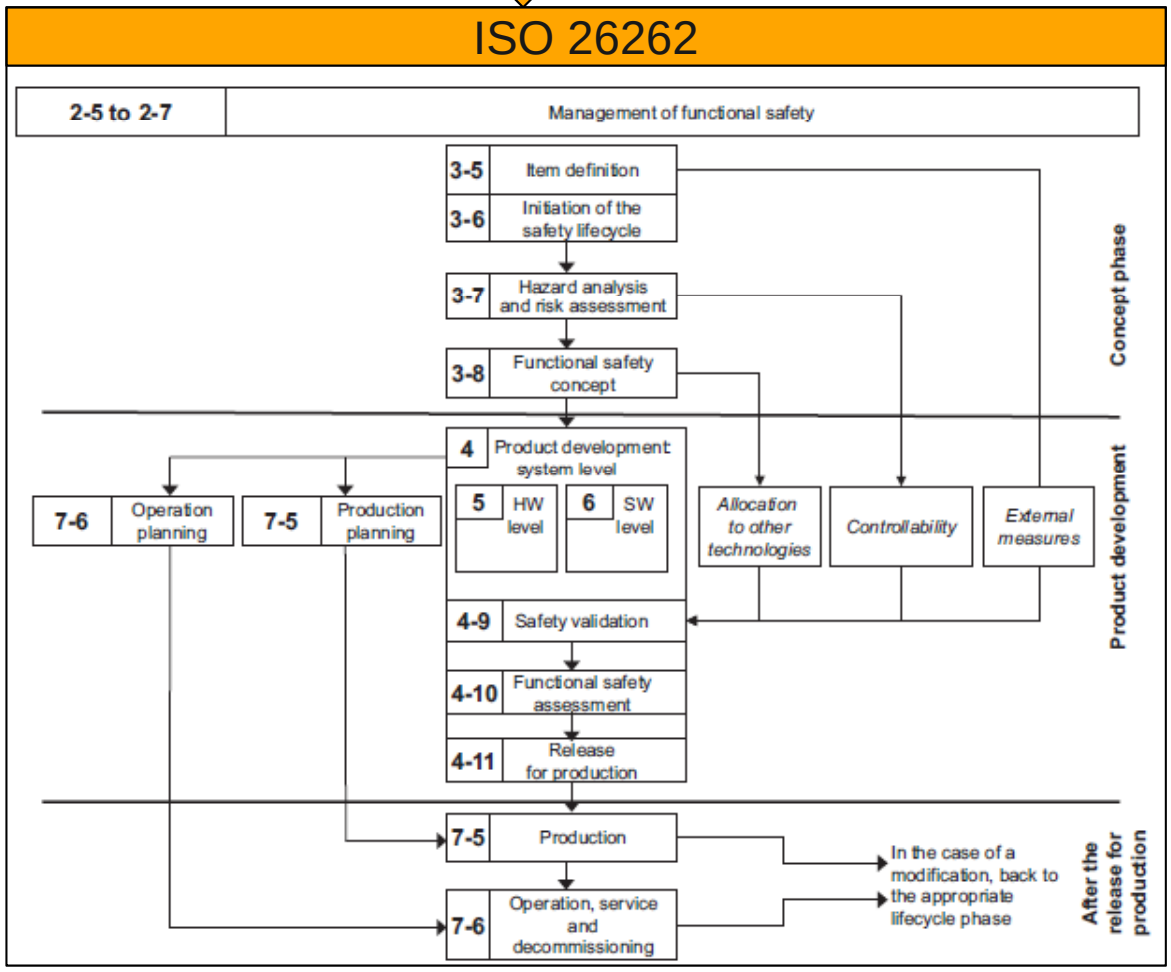
Schnieder, E.; Schnieder, L.: Verkehrssicherheit (Road Safety, in German). Springer Vieweg, Berlin, 2013

Automotive Product Safety

Product Safety (Germany e.g. GPSG, ProdHaftG, BGB)

International Functional Safety Standard IEC 61508

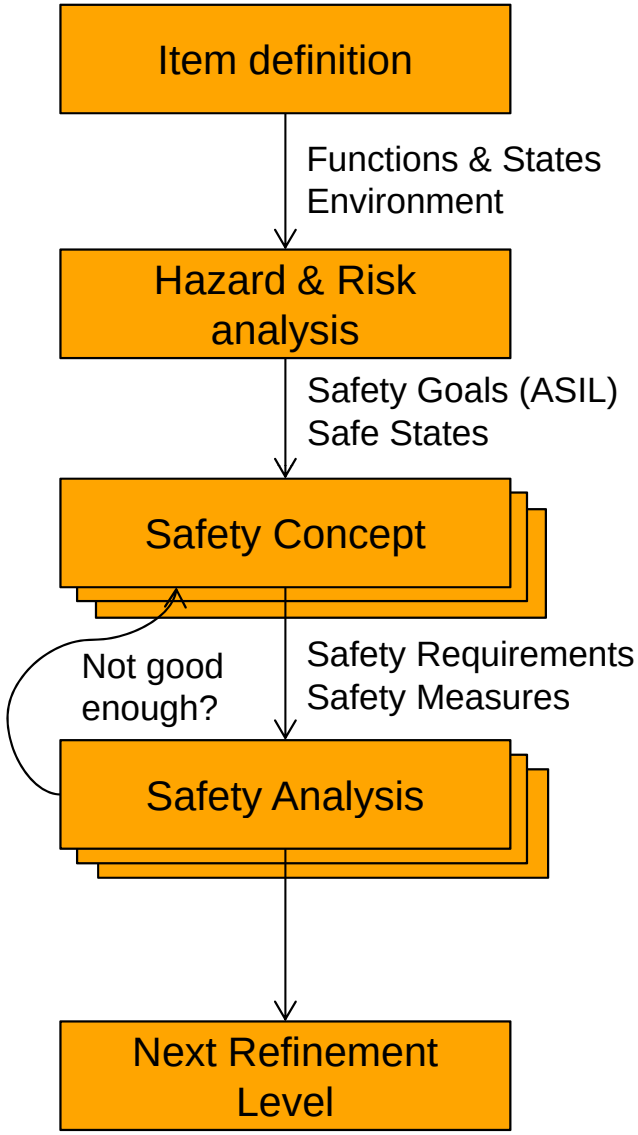
ISO 26262



ISO 26262-2:2011(E)

System Theoretic Process Analysis (STPA)

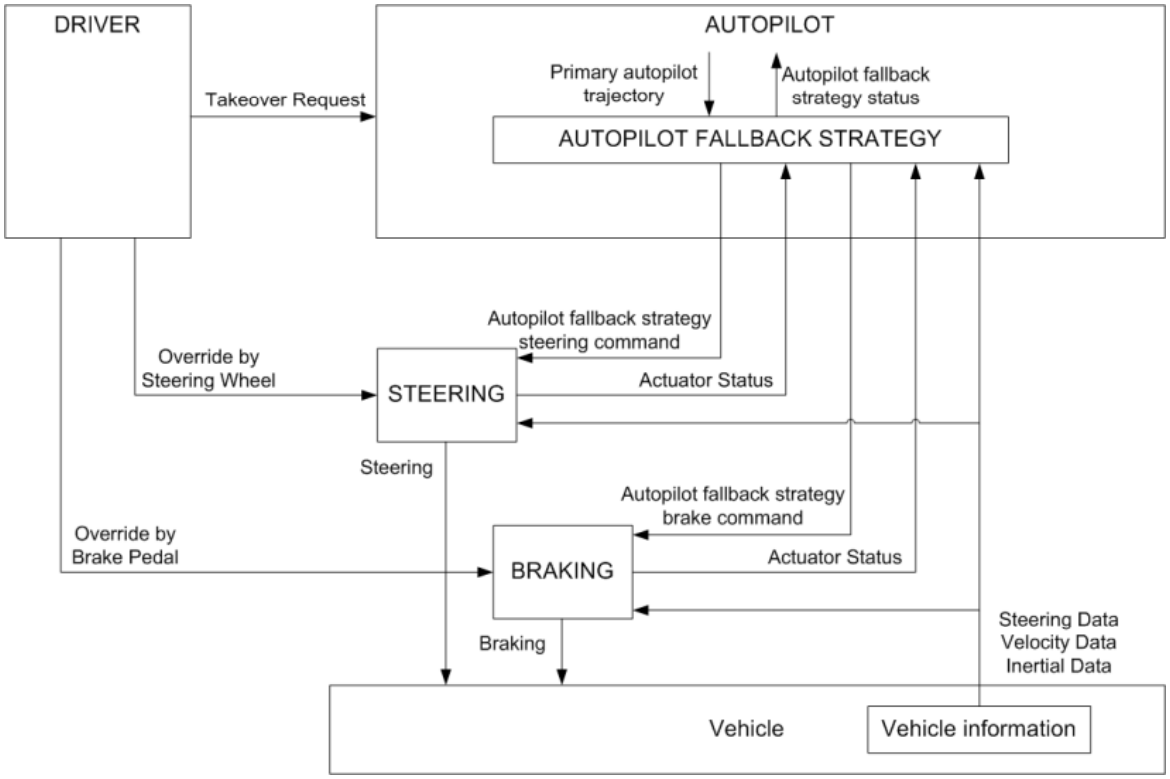
- Define and describe the system
  - ISO 26262 – Item definition
  - STPA – Control Structure
- Hazard and risk analysis
  - ISO 26262 – Hazard and risk analysis
  - STPA – Hazard Analysis and identify unsafe control actions
- Functional Safety Concept
  - ISO 26262 – Derive safety requirements from the safety goals and allocate them to the system
  - STPA – Design safety into the system (eliminate or control potential unsafe control actions)



STPA Control Structure and Hazards

- Identify the hazards with the hazard and risk analysis (ISO 26262 Part 3)

- Create the control structure



ID	Safety Goal	ASIL
SG-01	The autopilot shall avoid unintended steering requests during manual mode.	ASIL D
SG-02	The autopilot shall avoid no steering requests.	ASIL D
SG-03	The autopilot shall avoid steering requests with wrong values	ASIL D

STPA Unsafe Control Actions

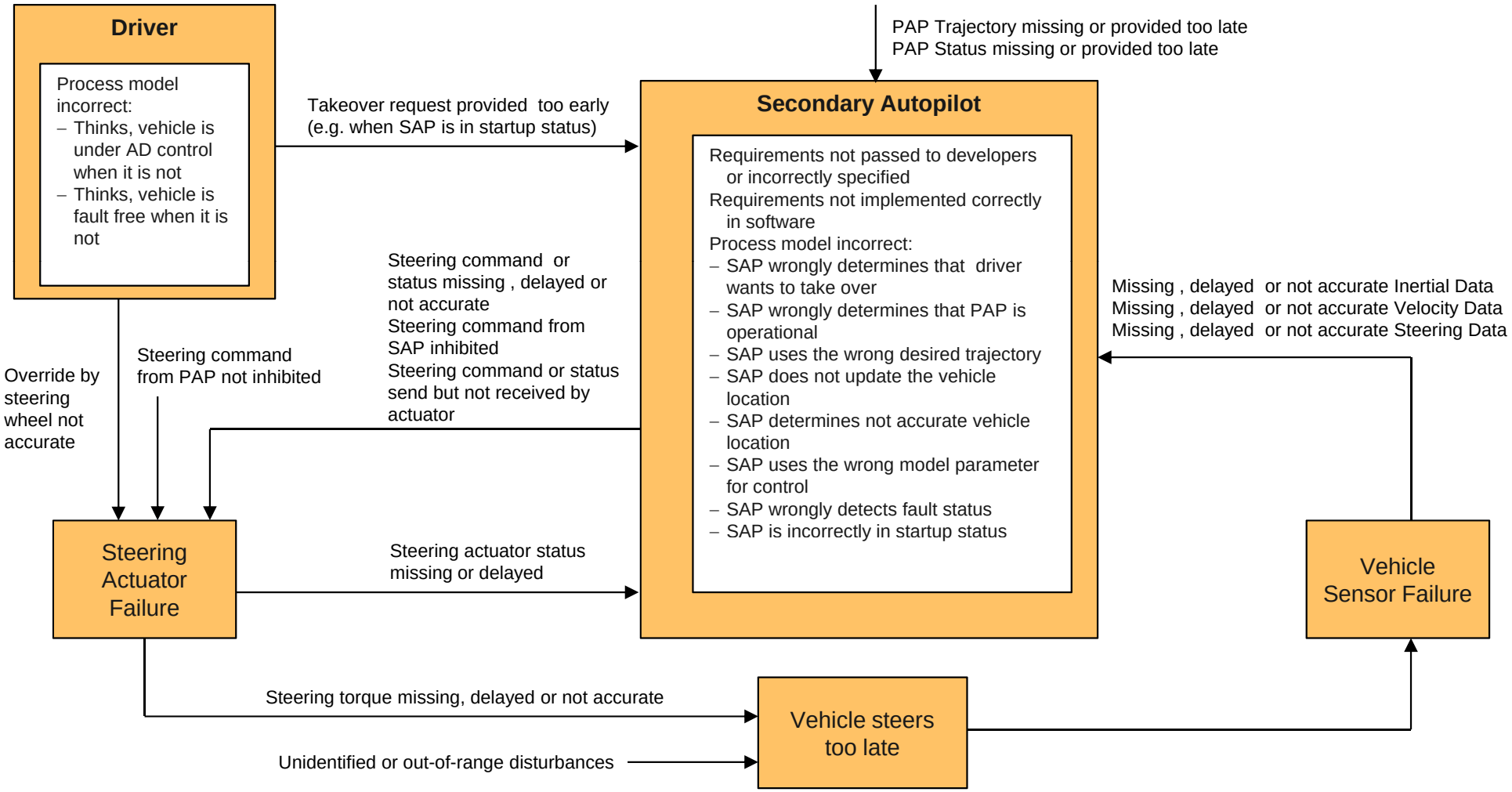
› Identify unsafe control action and map to hazards

Control Action	Action required but not provided		Unsafe action provided		Incorrect Timing/Order		Stopped too soon /Applied too long	
	Description	Safety Goal	Description	Safety Goal	Description	Safety Goal	Description	Safety Goal
Steering Command from autopilot fallback strategy to Steering	**UCA01** Vehicle does not steer while following safety path trajectory and lateral movement is required	SG-02 ASIL D	**UCA02** Vehicle steers, but following safety path trajectory and lateral movement is not required	SG-01 ASIL D	**UCA03** Vehicle steers too early while following safety path trajectory and lateral movement is required	SG-03 ASIL D	**UCA05** Vehicle stop to steer while following safety path trajectory and lateral movement is required	SG-03 ASIL D
					UCA04 Vehicle steers too late while following safety path trajectory and lateral movement is required	SG-03 ASIL D	**UCA06** Vehicle continue with a stuck value to steer while following safety path trajectory and lateral movement is required	SG-03 ASIL D

STPA Causal Factors

Causal Factors for Unsafe Control Action UCA04:
Vehicle steers too late while following safety path trajectory and lateral movement is required

AD Automated Driving
PAP Primary Autopilot
SAP Secondary Autopilot



Conclusion

- STPA is a systematic top down approach to eliminate the unsafe control actions that could lead to hazardous states
- STPA drives the earliest design decisions and is therefore a usefull addition to the tools in the ISO26262 concept phase
- System redundancy adds more interactions into the system but will not eliminate the unsafe control actions by itself
- Next steps should consider unsafe interactions of control actions between multiple controllers (Driver, Autopilot 1&2)

Thank you
for your attention!