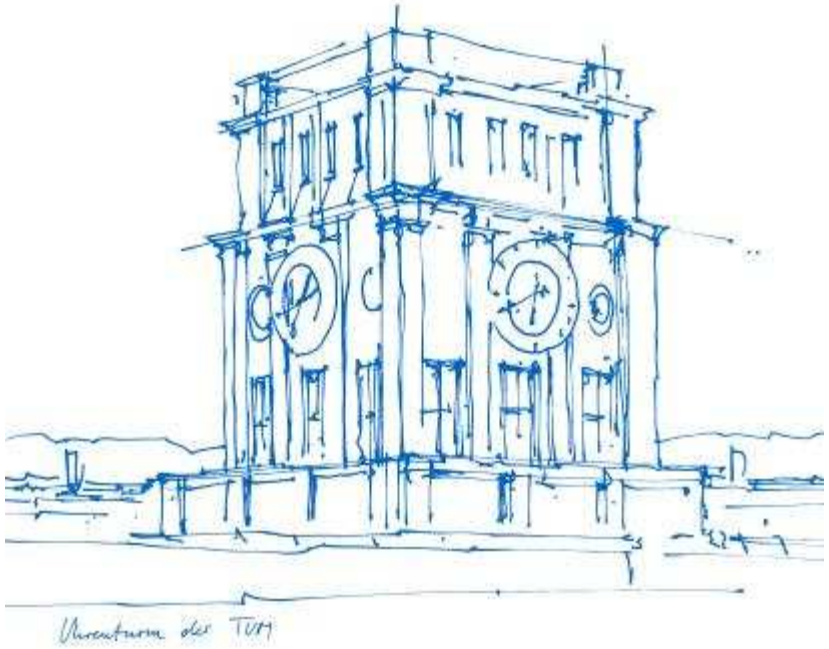
Lehrstuhl für Ergonomie
School of Engineering and Design
Technische Universität München

Fahrerassistenzsysteme im Kraftfahrzeug

Prof. Dr. phil. Klaus Bengler

Dipl. Ing. Thomas Winkle



Vorlesungsübersicht

01 Einführung 28.04.2022 – Prof. Lienkamp	**01 Einführung** 28.04.2022 – Prof. Lienkamp	**01 Übung Einführung** 28.04.2022 – Hoffmann
02 Sensorik / Wahrnehmung I 05.05.2022 – Prof. Lienkamp	**02 Sensorik / Wahrnehmung I** 05.05.2022 – Prof. Lienkamp	**02 Sensorik / Wahrnehmung I** 05.05.2022 – Prof. Lienkamp
03 Sensorik / Wahrnehmung II 12.05.2022 – Dr.-Ing. Diermeyer	**03 Sensorik / Wahrnehmung II** 12.05.2022 – Dr.-Ing. Diermeyer	**03 Übung Sensorik / Wahrnehmung II** 12.05.2022 – Schimpe
04 Sensorik / Wahrnehmung III 19.05.2022 – Schimpe	**04 Sensorik / Wahrnehmung III** 19.05.2022 – Schimpe	**04 Übung Sensorik / Wahrnehmung III** 19.05.2022 – Schimpe
05 Funktionslogik / Regelung 02.06.2022 – Dr.-Ing. Winkler	**05 Funktionslogik / Regelung** 02.06.2022 – Dr.-Ing. Winkler	**05 Funktionslogik / Regelung** 02.06.2022 – Dr.-Ing. Winkler
06 Übung Funktionslogik / Regelung 09.06.2022 – Dr.-Ing. Winkler	**06 Funktionale Systemarchitektur** 09.06.2022 – Prof. Lienkamp	**06 Aktorik** 09.06.2022 – Prof. Lienkamp
07 Deep Learning 23.06.2022 – Majstorovic	**07 Deep Learning** 23.06.2022 – Majstorovic	**07 Übung Deep Learning** 23.06.2022 – Majstorovic
08 MMI 30.06.2022 – Prof. Bengler	**08 MMI** 30.06.2022 – Prof. Bengler	**08 MMI Übung** 30.06.2022 – Prof. Bengler
09 Controllability 07.07.2022 – Prof. Bengler	**09 Controllability** 07.07.2022 – Prof. Bengler	**09 Übung Controllability** 07.07.2022 – Winkle
10 Entwicklungsprozess 14.07.2022 – Dr.-Ing. Diermeyer	**10 Entwicklungsprozess** 14.07.2022 – Dr.-Ing. Diermeyer	**10 Übung Entwicklungsprozess** 14.07.2022 – Hoffmann
11 Analyse und Bewertung FAS 21.07.2022 – Dr.-Ing. Feig	**11 Analyse und Bewertung FAS** 21.07.2022 – Dr.-Ing. Feig	**11 Übung Analyse und Bewertung FAS** 21.07.2022 – Dr.-Ing. Feig
12 Aktuelle und künftige Systeme 28.07.2022 – Prof. Lienkamp	**12 Aktuelle und künftige Systeme** 28.07.2022 – Prof. Lienkamp	**12 Aktuelle und künftige Systeme** 28.07.2022 – Prof. Lienkamp

9 Übung Controllability – Beherrschbarkeit
Dipl. Ing. Thomas Winkle

Agenda

9.1 Beispielanalyse: Fußgängerunfall “UBER self-driving vehicle”

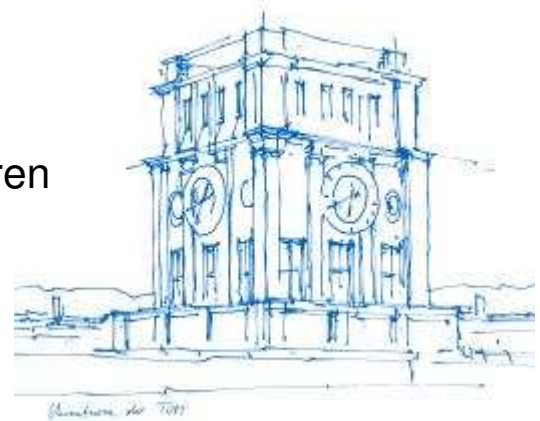
9.2 Allgemeiner Entwicklungsprozess und Freigabeprozess Controllability

9.3 Potenziell gefährliche Situationen

9.4 Beispiele für die Festlegung von Maßnahmen:

- Verletzungsrisiko?
- Controllability?
- Exposure?
- ASIL Dekomposition

9.5 Deutscher Verkehrsgerichtstag zu Automatisiertem Fahren



9 Übung
Controllability – Beherrschbarkeit / Risikomanagement

Literatur:

International Organization for Standardization (ISO), ISO 26262-3 (2018): Road Vehicles – Functional safety

Knapp, A., Neumann, M., Brockmann, M., Walz, R., Winkle, T. (2009): Code of Practice for the Design and Evaluation of ADAS, European Automobile Manufacturers Association – ACEA, www.acea.be, Brussels.

Winkle, T., Erbsmehl, C., Bengler, K. (2018). Area-Wide Real-World Test Scenarios of Poor Visibility for Safe Development of Automated Vehicles, European Transport Research Review, Journal, Springer - Verlag, Berlin, Heidelberg.

Winkle, T. (2019). Rechtliche Anforderungen an automatisiertes Fahren – Erkenntnisse aus Verkehrsgerichtstagen mit Verkehrsunfallbeispielen, Ergonomie aktuell (20) 2019, München.

Winkle, T. (2016). Development and Approval of Automated Vehicles: Considerations of Technical, Legal and Economic Risks. In: Maurer, M. (Hrsg.), Autonomous driving, Springer Verlag, Berlin, Heidelberg.

9.1 Beispielanalyse: Fußgängerunfall “UBER self-driving vehicle”

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

Abbildung: Police Department, Tempe, Arizona, March 18, 2018

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

Abbildung: Police Department, Tempe, Arizona, March 18, 2018

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

Abbildung: Police Department,
Tempe, Arizona, March 18, 2018

Detaillierte Angaben über den Unfall stellt das National Transportation Safety Board (NTSB, zu Deutsch: US-amerikanische nationale Verkehrsbehörde für Transportsicherheit) in einem Bericht zur Verfügung.

Demnach kollidierte das Uber-Testfahrzeug mit einer Geschwindigkeit von 39 mph. In etwa 6 Sekunden vor dem Aufprall fuhr das Fahrzeug mit 43 mph. Bereits 1,3 Sekunden vor dem Aufprall habe das System festgestellt, dass ein Notbrems-manöver erforderlich ist um eine Kollision zu verhindern. Laut Uber waren beim Testfahrzeug Notbremseingriffe zur Vermeidung von unberechenbarem Verhalten deaktiviert.

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

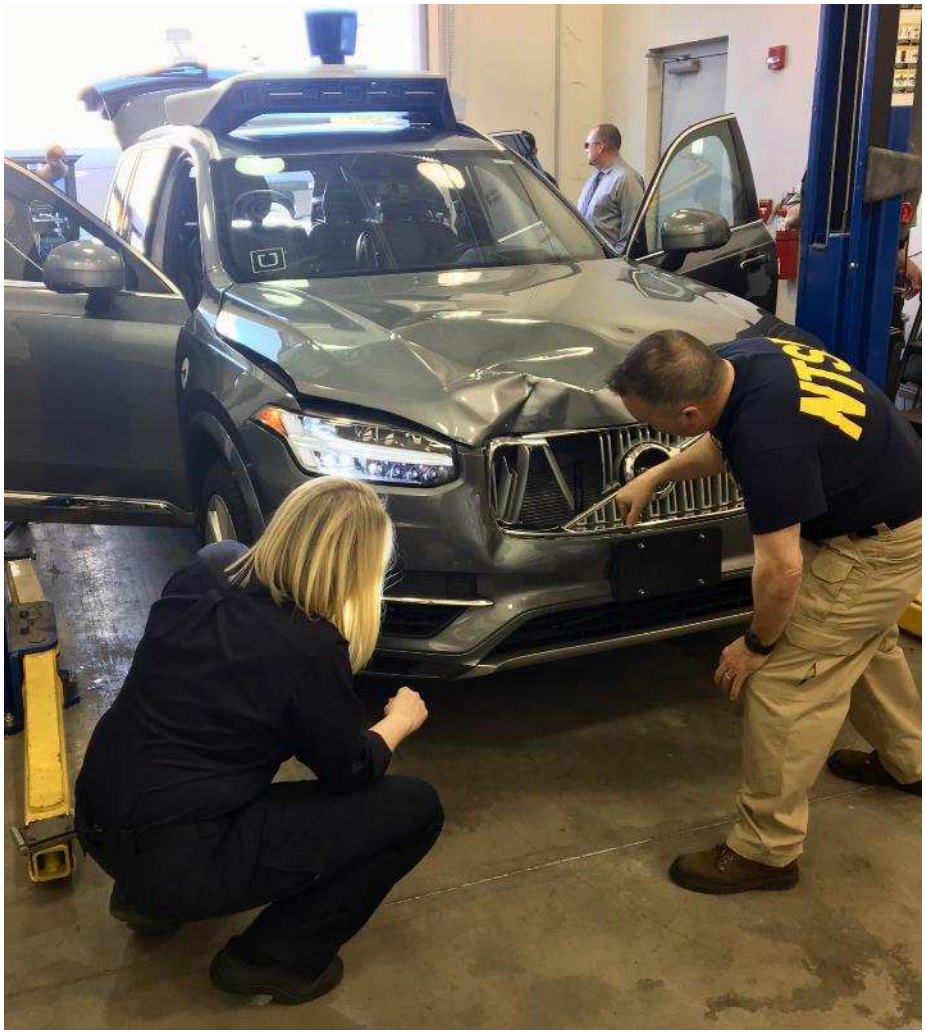
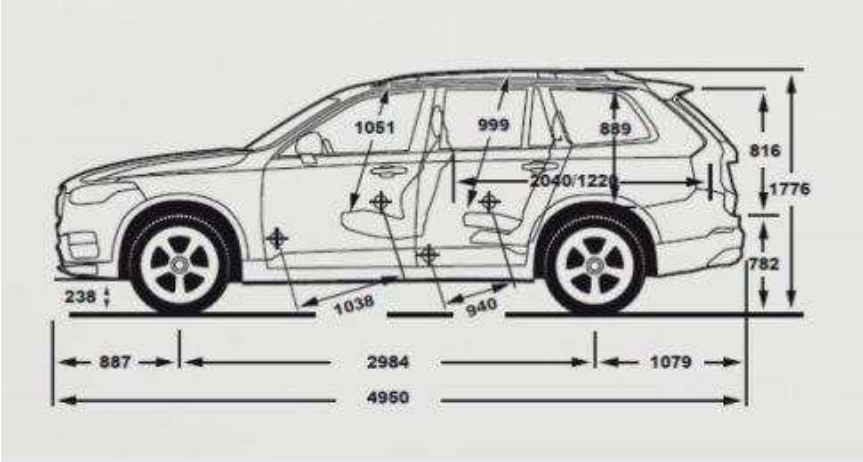


Abbildung: Police Department, Tempe, Arizona, March 18, 2018

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle



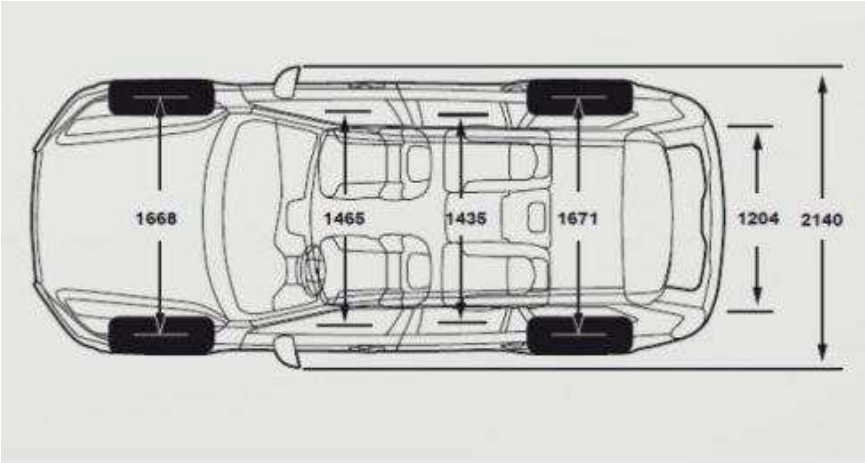


Abbildung: Volvo

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

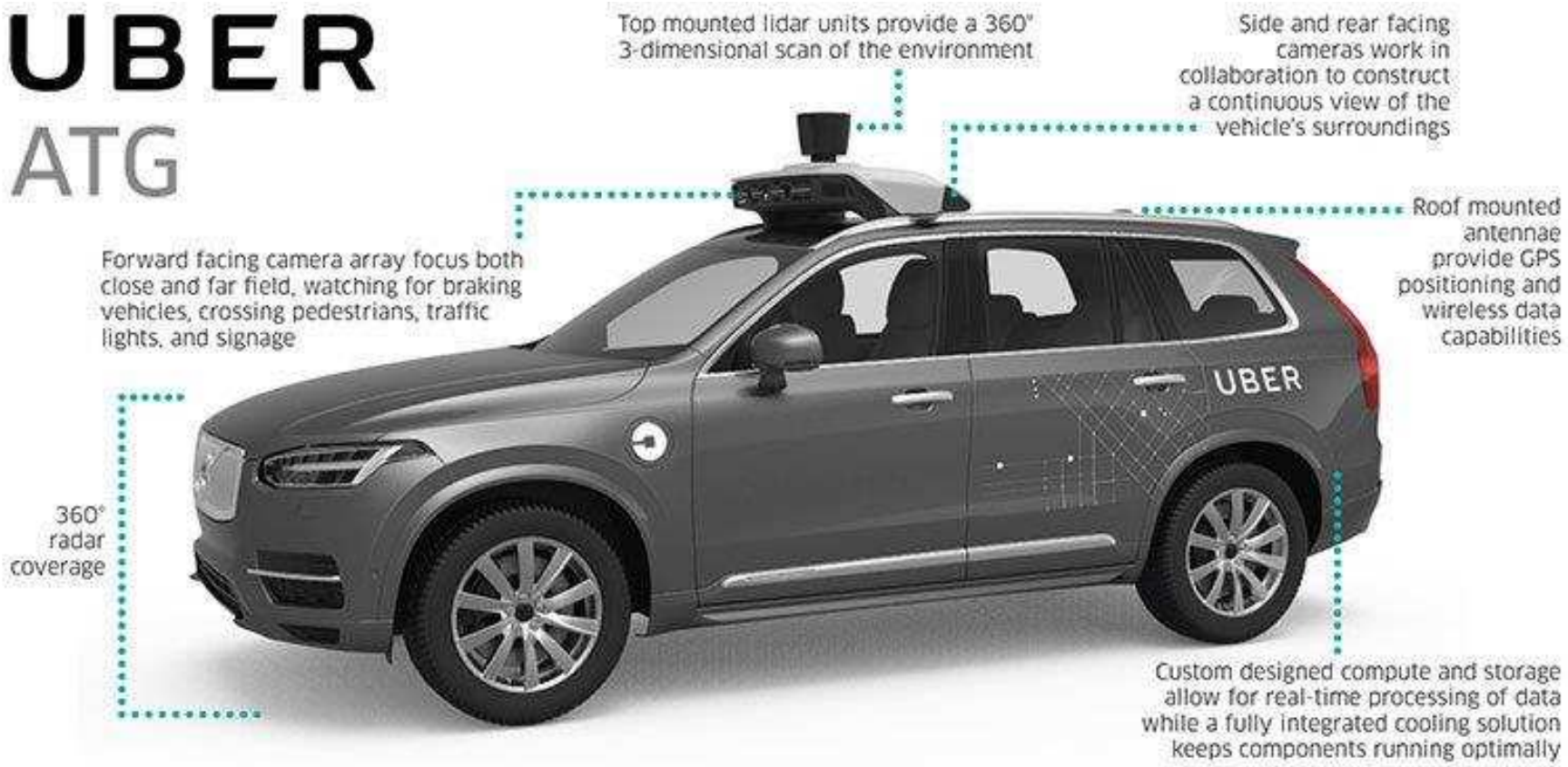


Abbildung: UBER/Volvo

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

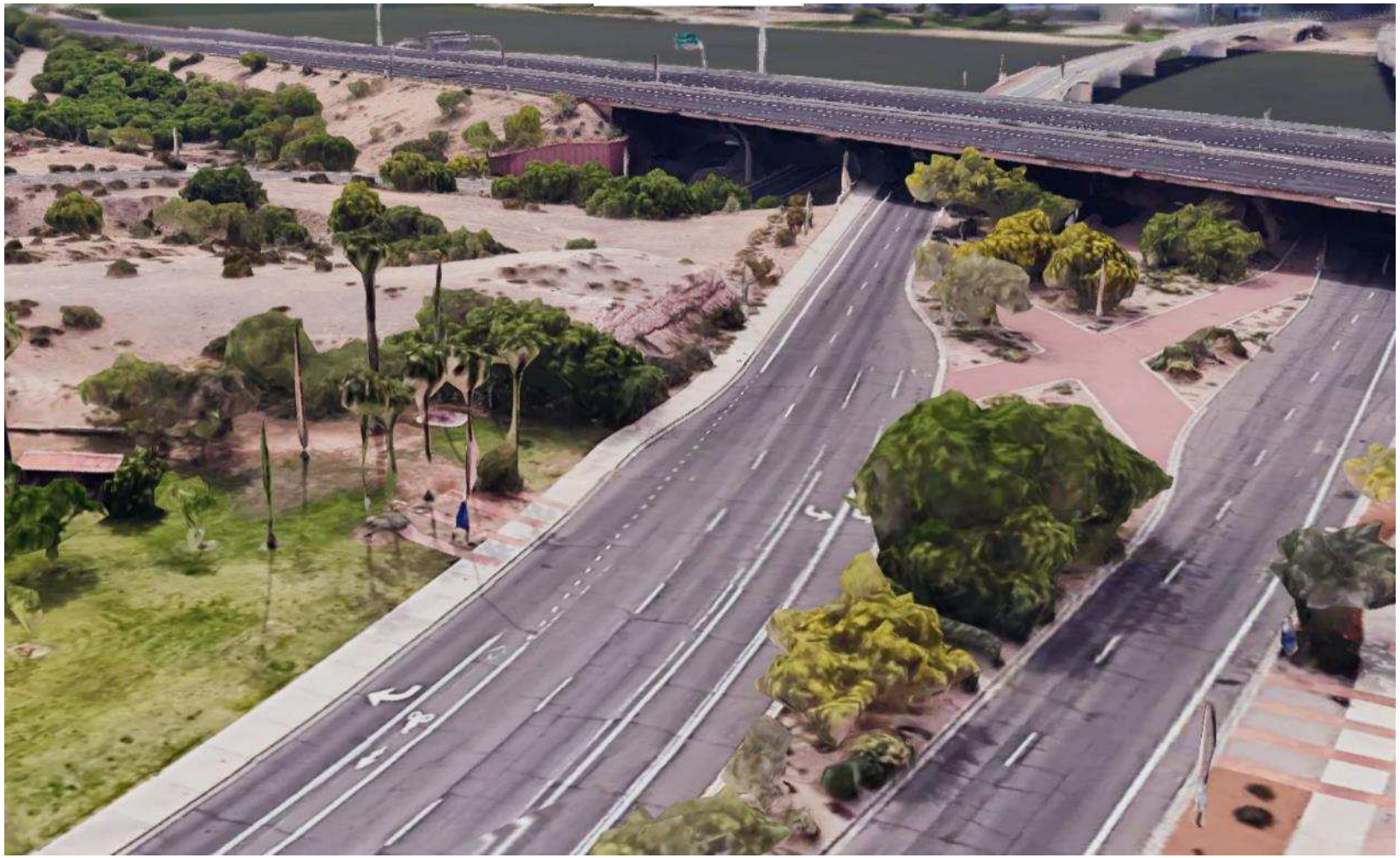


Abbildung: Google

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

Abbildung: Google

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle

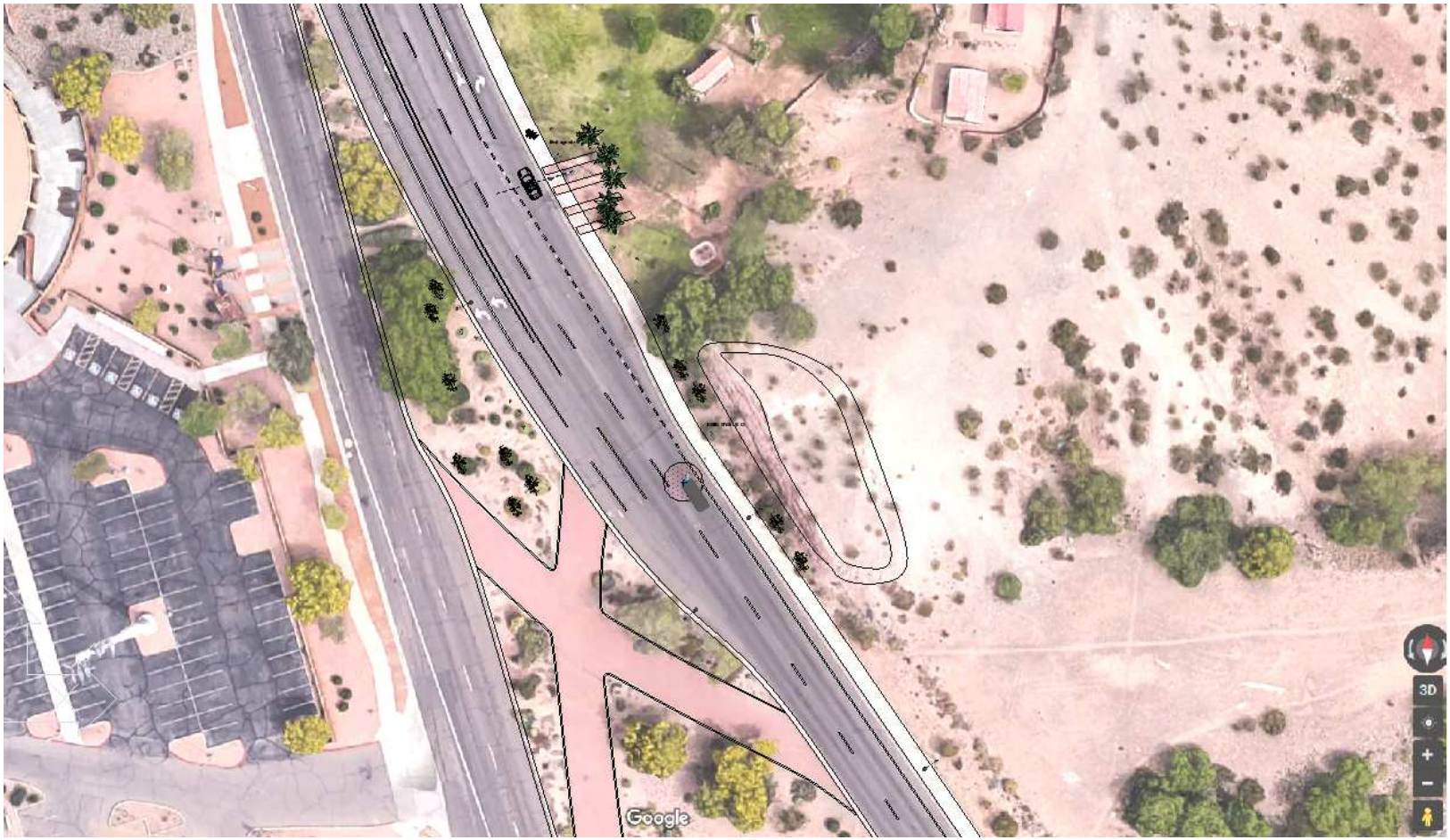
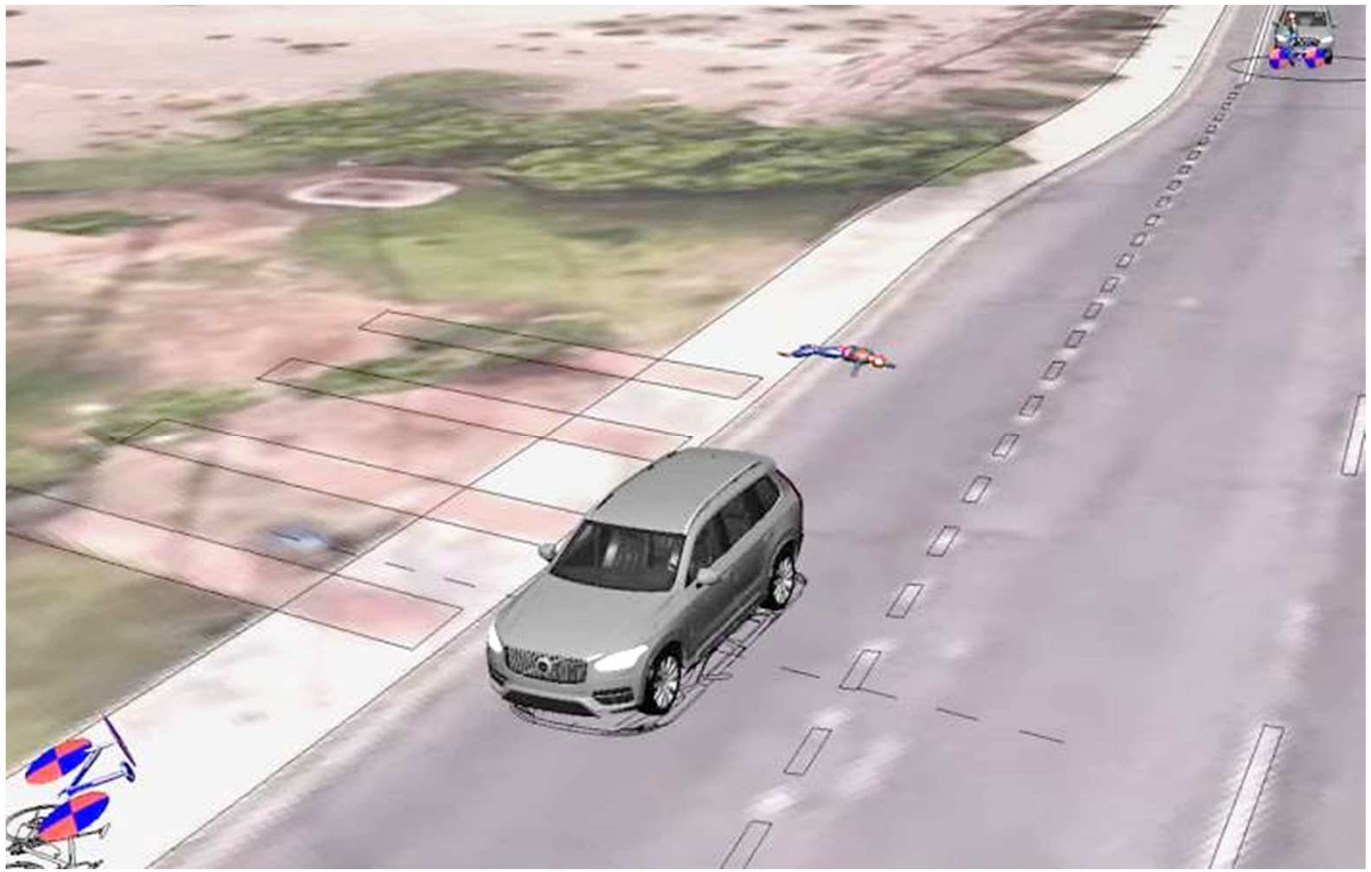


Abbildung: Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren, Ergonomie aktuell (20) 2019, München.

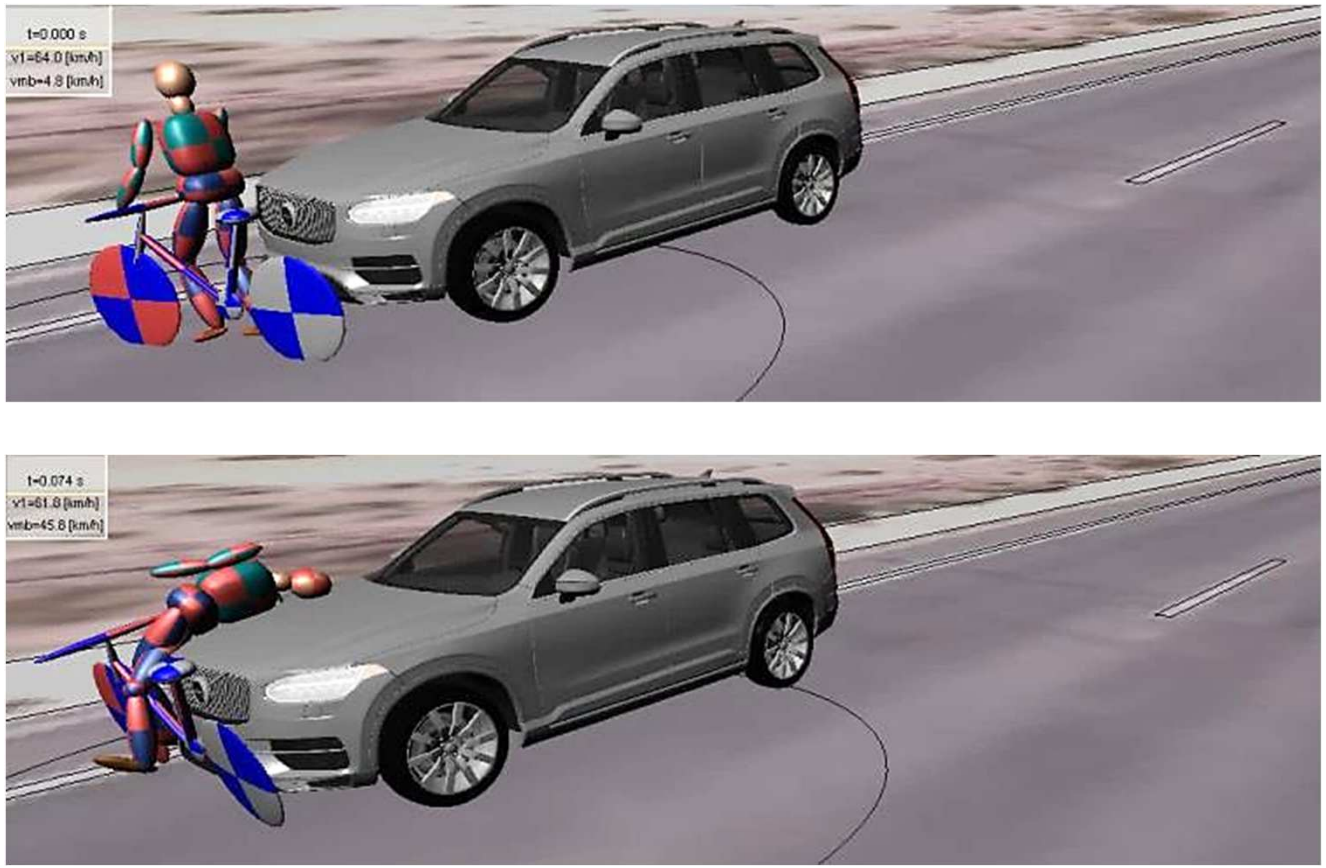
Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle



Unfallsimulation mit PC-Crash: Die Abbildung zeigt die Unfallstelle in der Simulation direkt vor der Kollision und in den Endlagen mit der aus dem Video ermittelten Fußgängergeschwindigkeit von 4,8 km/h (1,3 m/s) mit der die Fußgängerin ihr Fahrrad über die Straße schob.

Abbildung: Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren, Ergonomie aktuell (20) 2019, München.

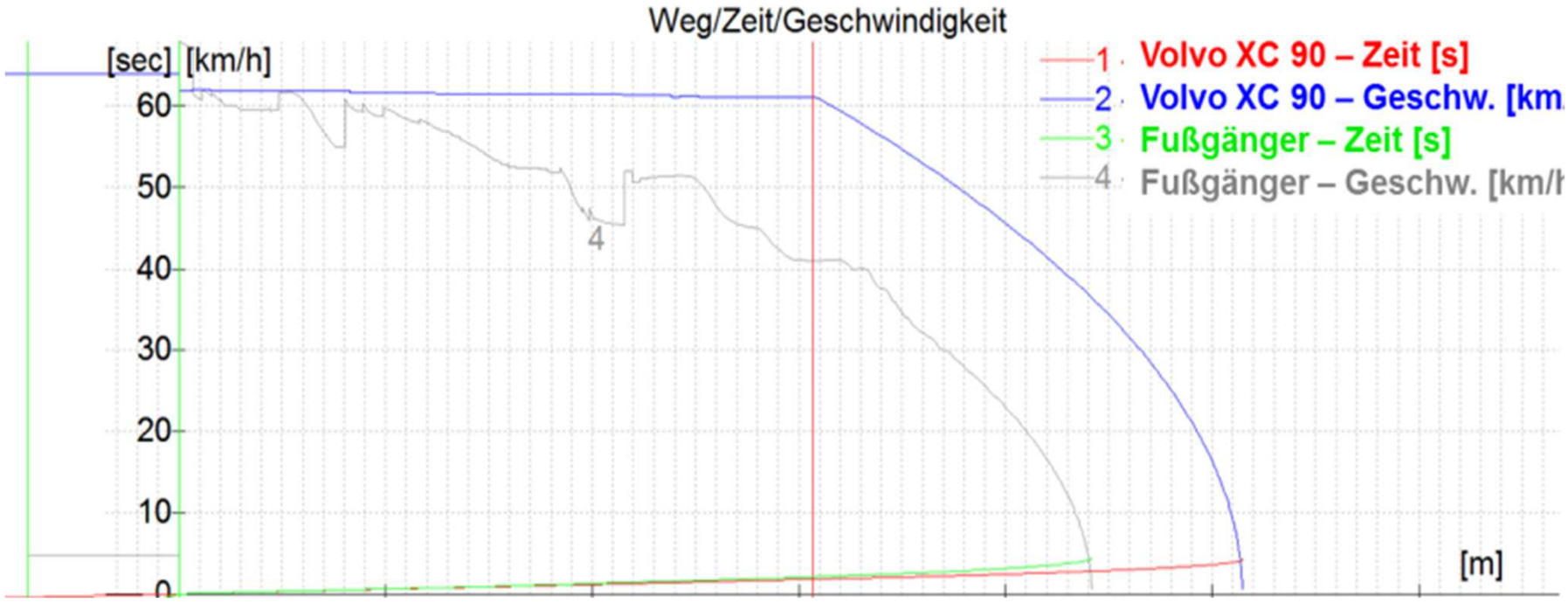
Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle



Mithilfe eines Mehrkörpermodells lässt sich der Erstkontakt der Fußgängerin mit dem geschobenen Fahrrad an der Fahrzeugfront des Volvo XC90 darstellen.

Abbildung: Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren, Ergonomie aktuell (20) 2019, München.

Beispiel Unfallanalyse:
Fußgängerunfall UBER self-driving vehicle



Die Rekonstruktion und Unfallsimulation ermöglicht die Untersuchung weiterer Annahmen mit den Entsprechenden Auswirkungen auf die Zusammenhänge von Wegen, Zeiten und Geschwindigkeiten.

Abbildung: Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren, Ergonomie aktuell (20) 2019, München.

Beispiel Unfallanalyse: Fußgängerunfall UBER self-driving vehicle

$$s = v * t = 17{,}8\ \frac{m}{s} * 1{,}3\ s = 23{,}1\ m$$

$$a = \frac{v^2}{2s} = \frac{(17{,}8\ \frac{m}{s})^2}{2 * 23{,}1\ m} = 6{,}8\ \frac{m}{s^2}$$

Unter Annahme einer Geschwindigkeit von 64 km/h (17,8 m/s) und einer sofort wirkenden Notbremsung 1,3 Sekunden vor Kollision mit einer Verzögerung von 6,8 m/s² wäre der Unfall vermieden worden.

Abbildung: Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren, Ergonomie aktuell (20) 2019, München.

9.2 Allgemeiner Entwicklungsprozess und Freigabeprozess Controllability

Allgemeiner Entwicklungsprozess

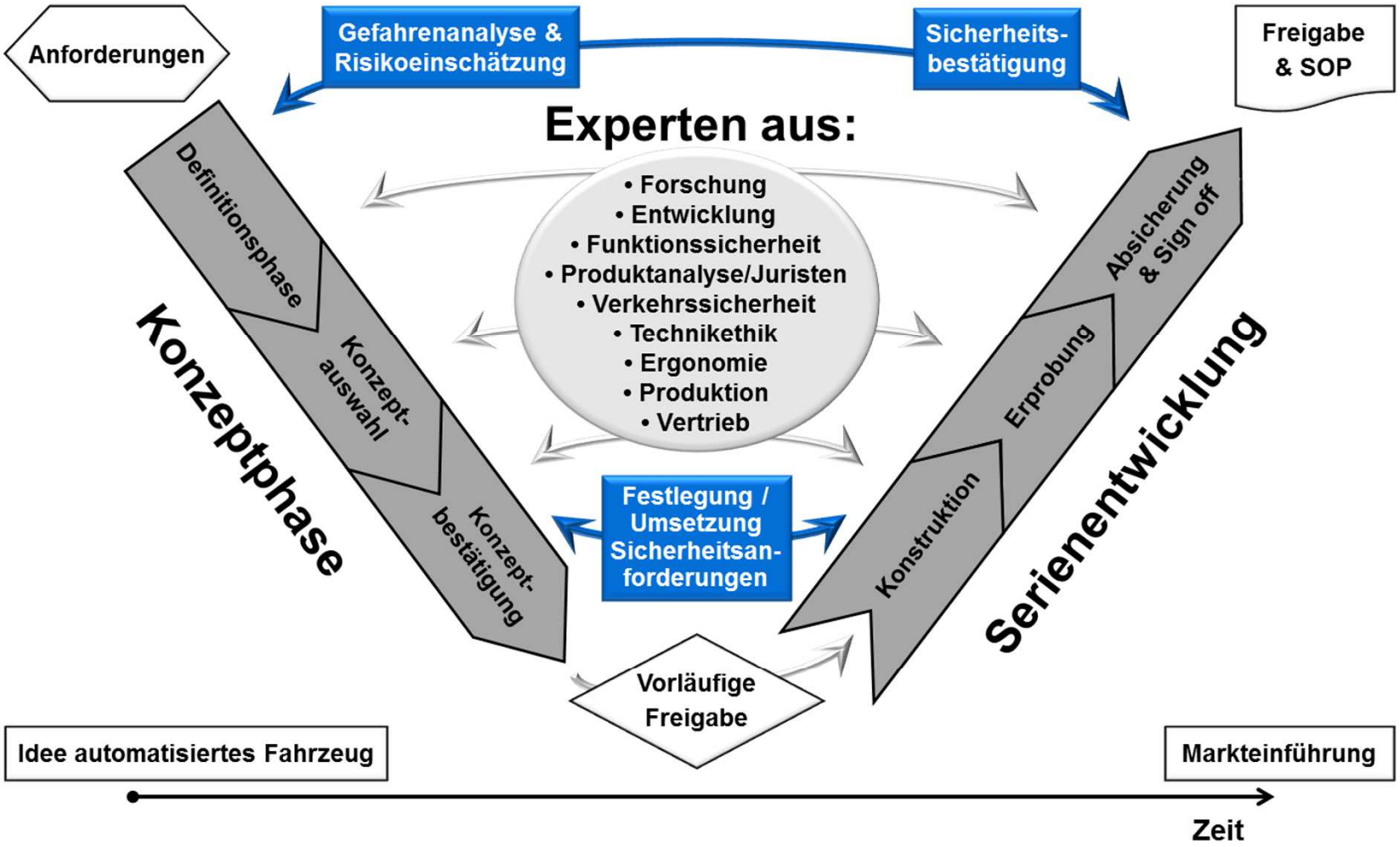
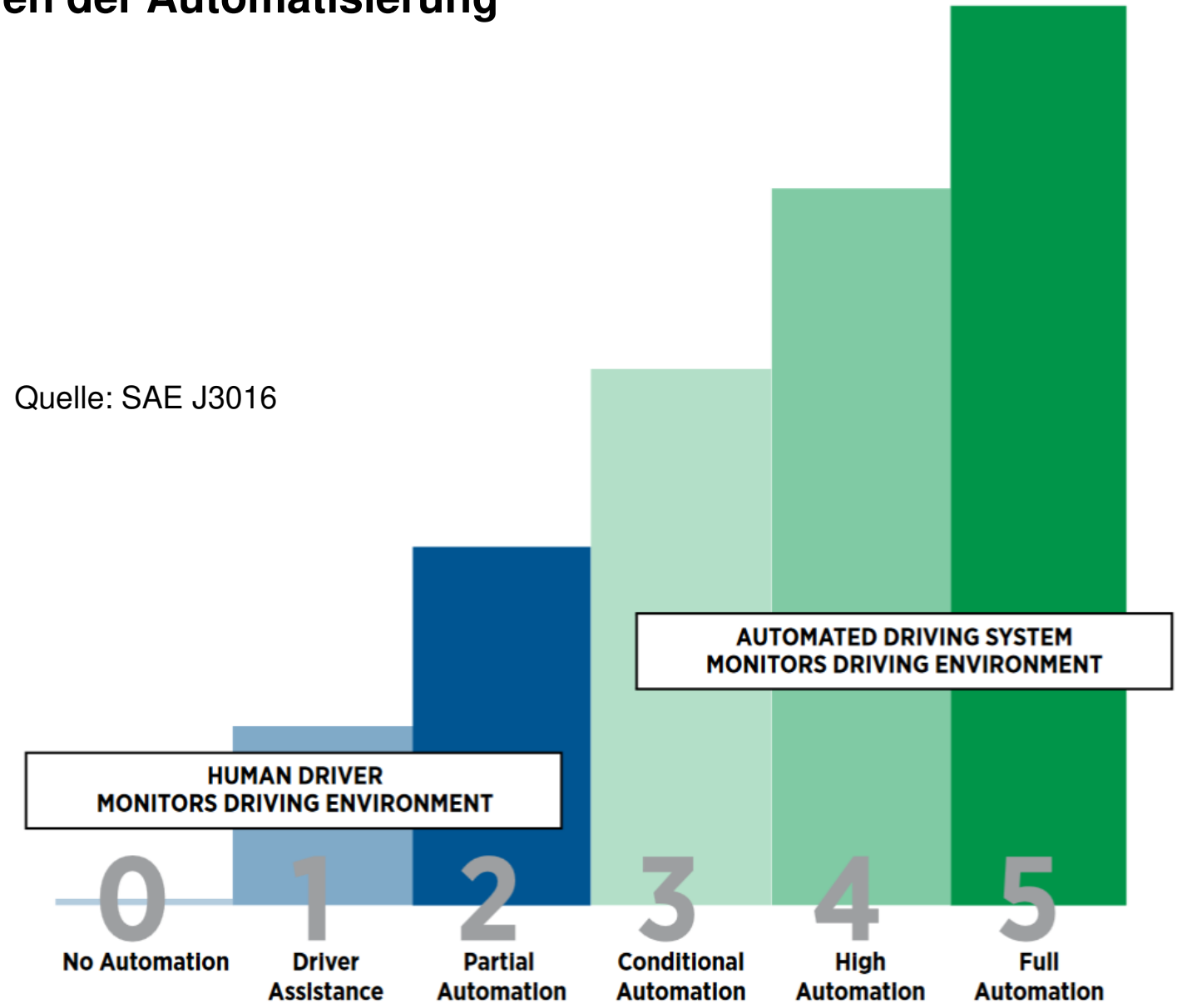


Abbildung: Winkle, T.

Kategorien der Automatisierung

Quelle: SAE J3016



Kategorien der Automatisierung

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Freigabeprozess

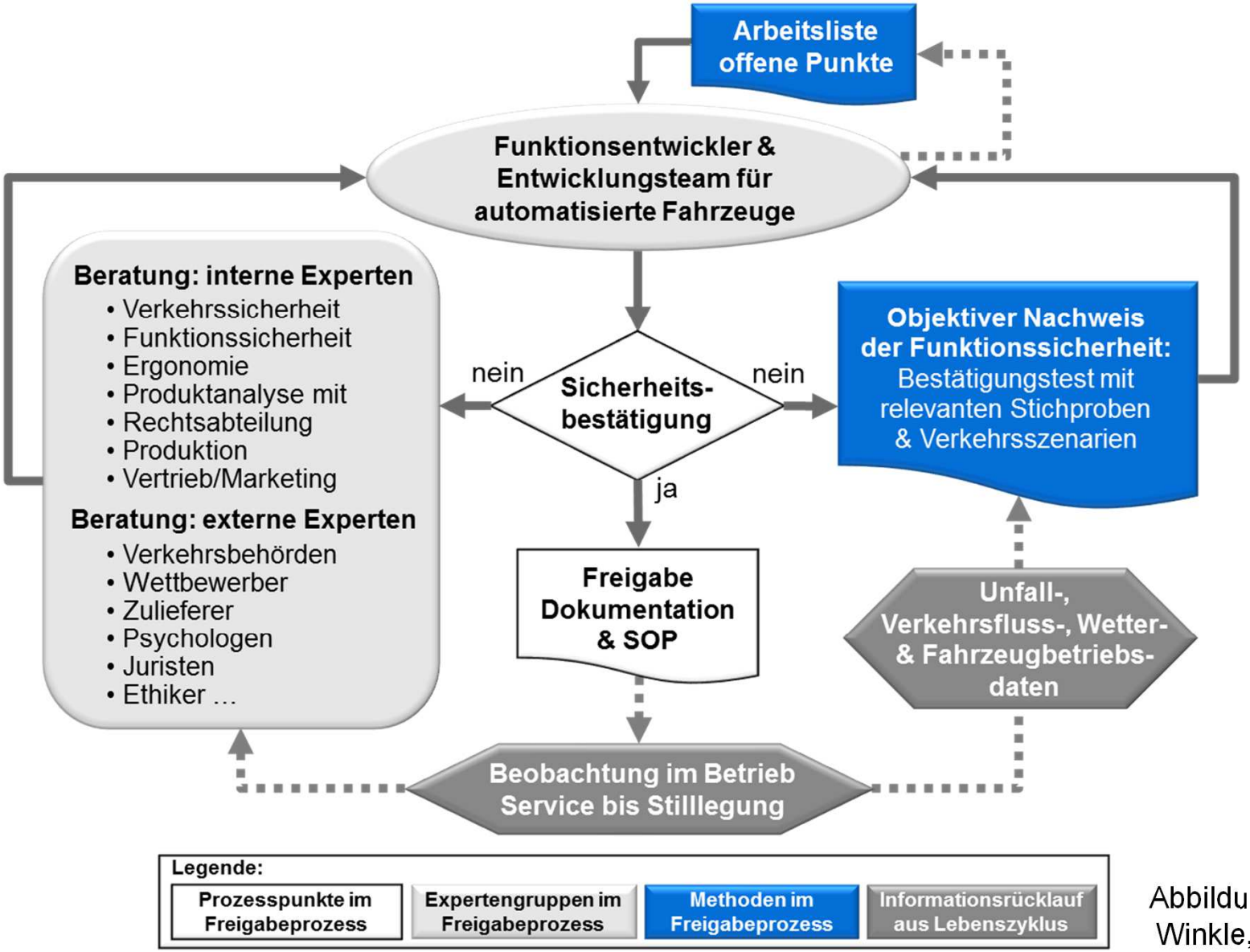


Abbildung: Winkle, T.

9.3 Potenziell gefährliche Situationen

Gefahren und Risiken aus realen Verkehrsszenarien

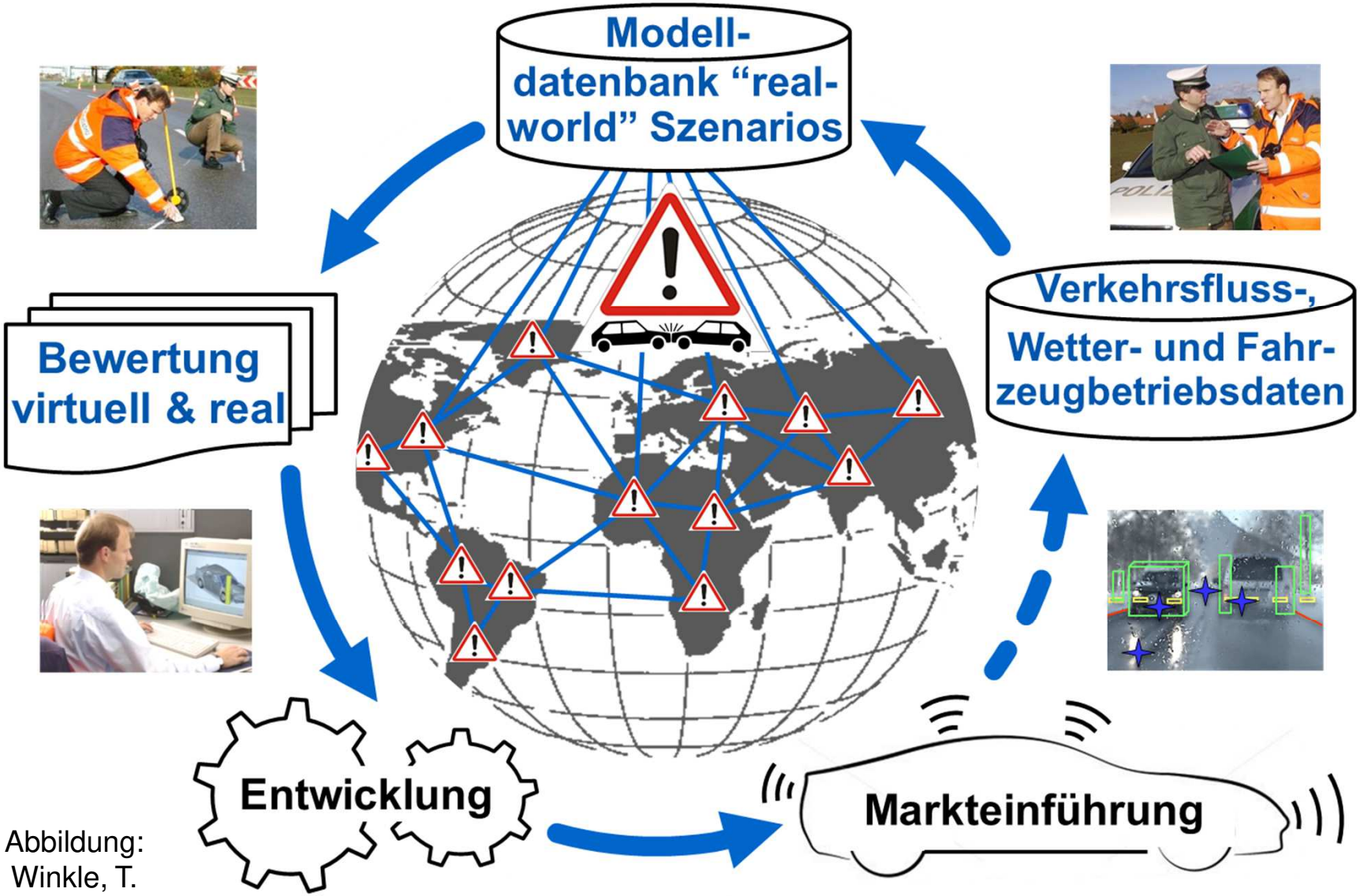


Abbildung:
Winkle, T.

Lernkurve: Zunahme von verfügbaren Fahrdaten

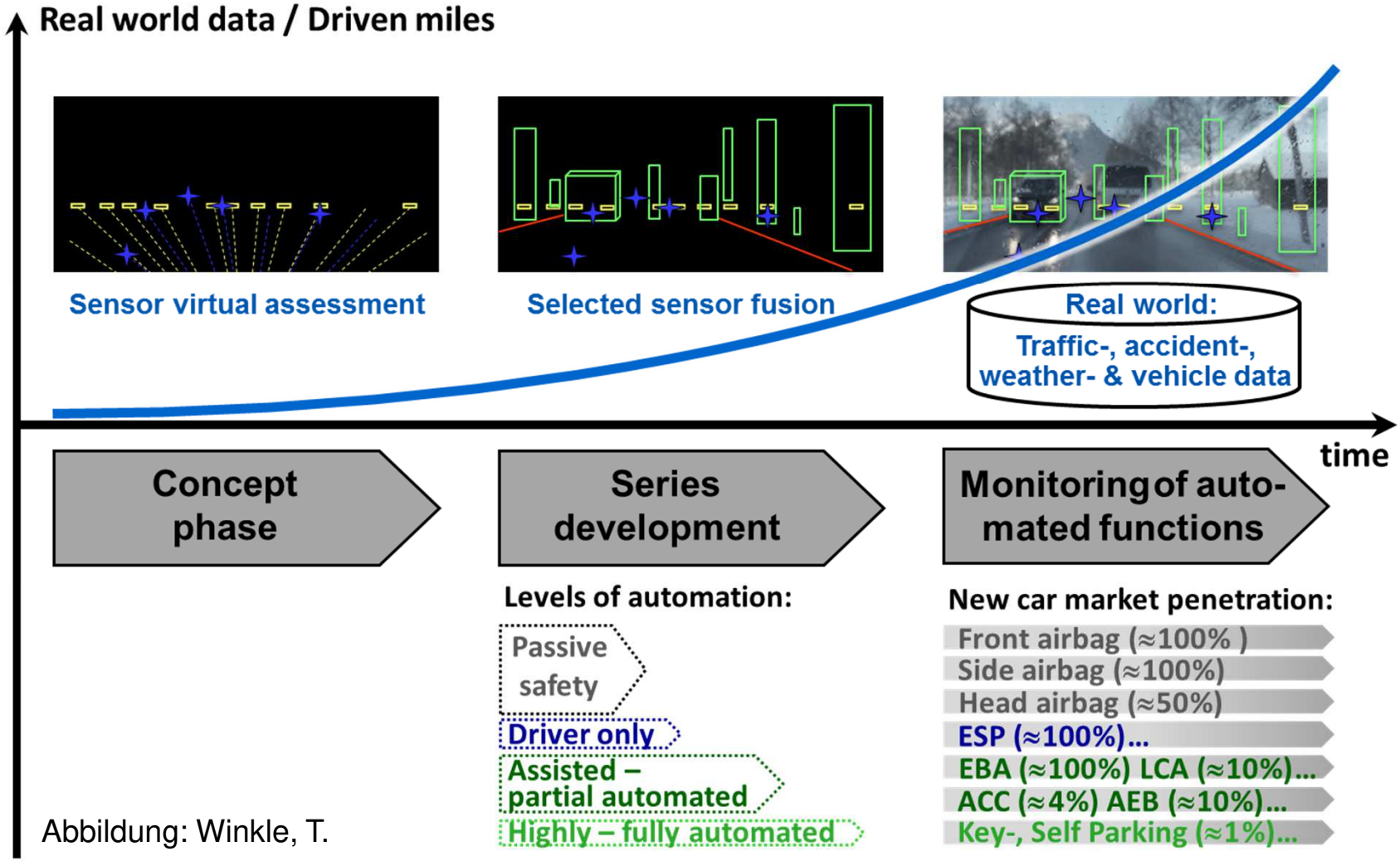


Abbildung: Winkle, T.

Fehlerbaum: Bsp. el. Lenkung

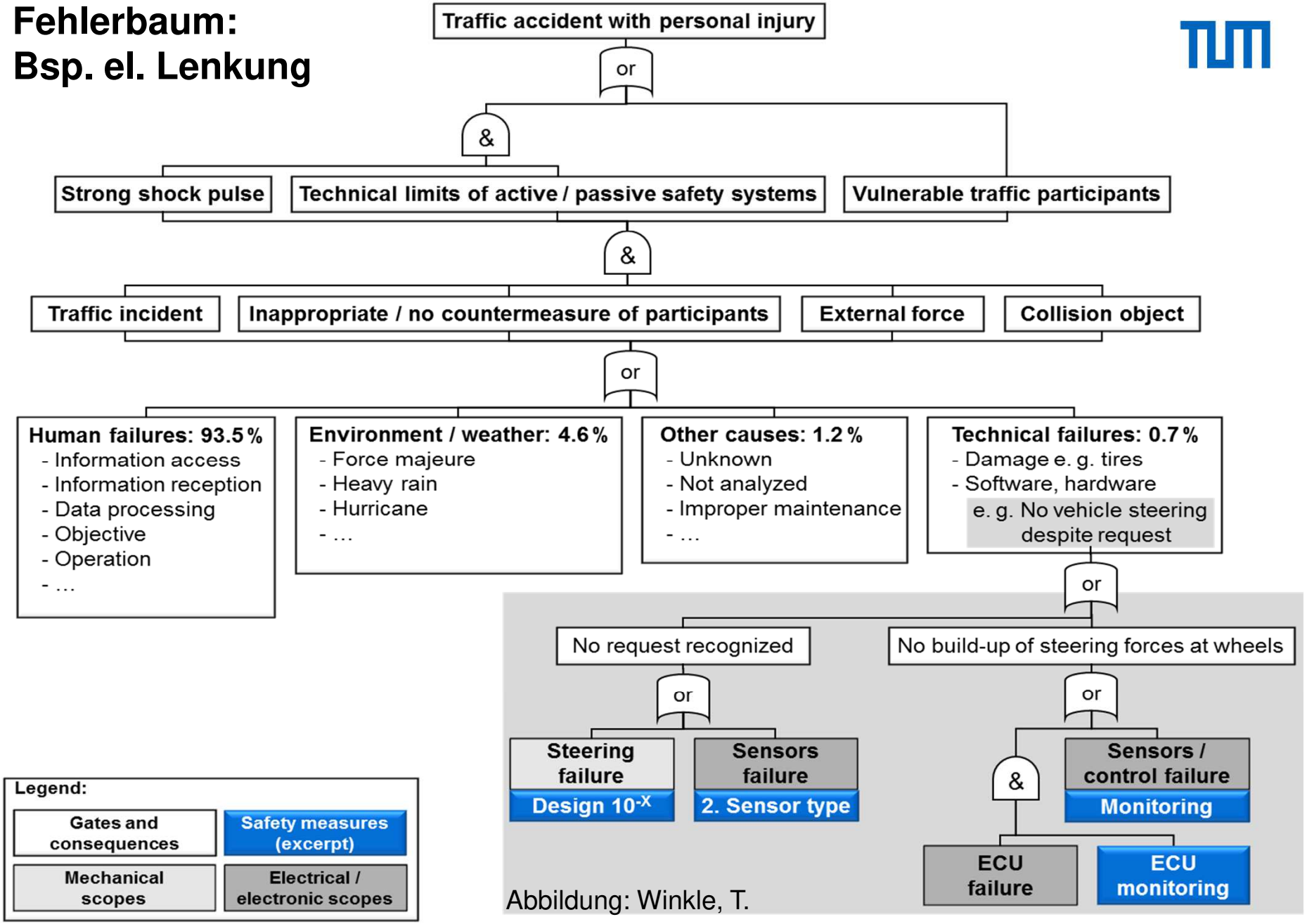
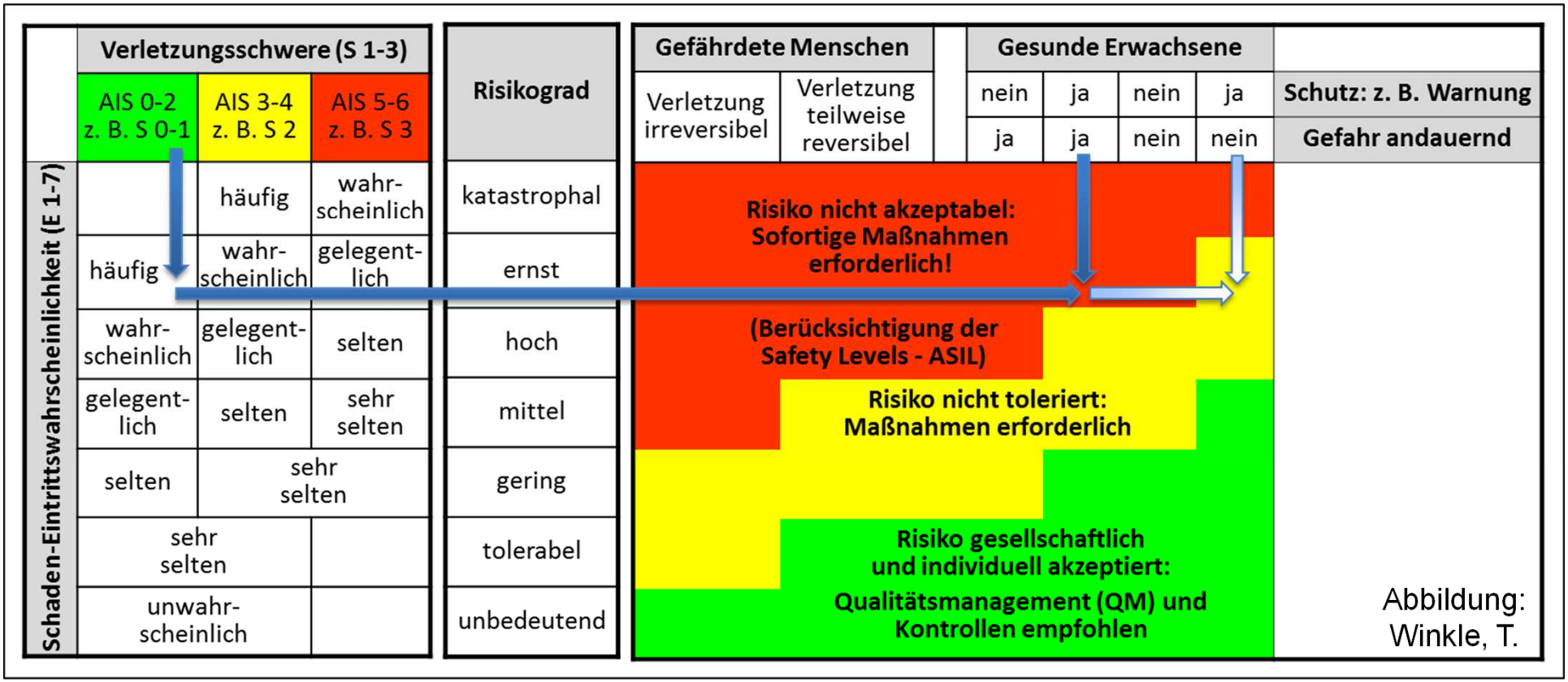


Abbildung: Winkle, T.

Beispiel: Risikoeinstufung für entsprechende Maßnahmen



9.4 Beispiele für die Festlegung von sicherheitserhöhenden Maßnahmen

Übung: Einstufung eines Automotive Safety Integrity Level (ASIL)

Rückruf: Forward Collision Avoidance, Adaptive Cruise Control, Vehicle Speed Control, Accelerator Pedal

Hersteller: Fiat Chrysler Limited Liability Company LLC, NHTSA Campaign Number: 14V293000, Report Receipt Date: June 4, 2014, http://www.nhtsa.gov

"When optional adaptive cruise control was activated and the driver temporarily pressed the accelerator pedal to increase (override) vehicle's set speed more than the cruise control system would on its own, the ***vehicle could continue to accelerate briefly after the accelerator pedal was released again****."*

2014 Dodge Durango

2014 Jeep Grand Cherokee

Figures: Fiat Chrysler

Quelle: Winkle, Thomas: Development and Approval of Automated Vehicles: Considerations of Technical, Legal and Economic Risks. In: Maurer, Markus; Gerdes, J. Christian; Lenz, Barbara; Winner, Hermann (Hrsg.): Autonomous Driving. Springer Berlin Heidelberg, 2016, S. 589

Übung: Einstufung eines Automotive Safety Integrity Level (ASIL)

Rückruf: Forward Collision Avoidance, Activation of Collision Mitigation Braking System

Hersteller: Honda Motor Company, NHTSA Campaign Number: 15V301000, Report Receipt Date: May 20, 2015, http://www.nhtsa.gov

"In certain driving conditions, the Collision Mitigation Braking System (CMBS) ***may incorrectly interpret certain roadside objects such as metal fences or metal guardrails as obstacles and unexpectedly apply the brakes.*** *If the CMBS unexpectedly applies emergency braking force while driving, there is an increased risk of a crash."*

2014, 2015 Acura MDX

2014, 2015 Acura RLX

Figures: Honda Motor Company

Quelle: Winkle, Thomas: Development and Approval of Automated Vehicles: Considerations of Technical, Legal and Economic Risks. In: Maurer, Markus; Gerdes, J. Christian; Lenz, Barbara; Winner, Hermann (Hrsg.): Autonomous Driving. Springer Berlin Heidelberg, 2016, S. 599

Übung:
Einstufung eines Automotive Safety Integrity Level (ASIL)

Severity	Exposure	Controllability C1	C2	C3
S1	E1			
	E2			
	E3			
	E4			
S2	E1			
	E2			
	E3			
	E4			
S3	E1			
	E2			
	E3			
	E4			

Quellen: ADAS Code of Practice, ISO 26262

Kategorisierung der Verletzungsschwere: Severity (S0 - S3)

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (informative)	AIS 0 Damage that cannot be classified safety related, e.g. bumps with the infrastructure	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5 and 6

Abbreviated Injury Scale (AIS) in der ISO 26262

Code	Injury Description	ISO
AIS 0	**no injuries**	**S0**
AIS 1	**light injuries** such as skin-deep wounds, muscle pains, whiplash, etc.	**S1**
AIS 2	**moderate injuries** such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures, etc.	**S1**
AIS 3	**severe but not life-threatening injuries** such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing, etc.	**S2**
AIS 4	**severe injuries (life-threatening, survival probable)** such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing	**S2**
AIS 5	**critical injuries (life-threatening, survival uncertain)** such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding	**S3**
AIS 6	**extremely critical or fatal injuries** such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities), etc.	S3

Risikobewertung - Controllability Einstufung (Anhang A.3.4)

Dabei wird die Controllability im Code of Practice und in der ISO 26262 von C0 - C3 kategorisiert. Hier die Klassen C0 - C3 des ADAS Code of Practice:

Class	C0	C1	C2 *	C3
Description (informative)	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Definition	Distracting	More than 99% of average drivers or other traffic participants are usually able to control the damage.	More than 85% of average drivers or other traffic participants are usually able to control the damage.*	The average driver or other traffic participant is usually unable, or barely able, to control the damage.

Abbildung: Categorisation of Controllability for risk assessment

ADAS Code of Practice A.3.4, S. A44

ISO 26262:2018 Risikobewertung – Klassen der Controllability Beispiele

Driving factors and scenarios		Class of controllability (see Table 3) C0	C1	C2	C3
		Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm
Examples	Situations that are considered distracting	— Maintain intended driving path	—	—	—
	Unexpected radio volume increase	— Maintain intended driving path	—	—	—
	Warning message - gas low	— Maintain intended driving path	—	—	—
	Unavailability of a driver assisting system	— Maintain intended driving path	—	—	—
	Faulty adjustment of seat position while driving	—	— Brake to slow/stop vehicle	—	—
	Blocked steering column when starting the vehicle	—	— Brake to slow/stop vehicle	—	—
	Failure of ABS during emergency braking	—	—	— Maintain intended driving path	—
	Headlights fail while night driving at medium/high speed on unlighted road	—	—	— Steer to side of road or brake to stop.	—
	Motor failure at high lateral acceleration (motorway exit)	—	—	— Maintain intended driving path	—
	Failure of ABS when braking on low friction road surface while executing a turn	—	—	—	— Maintain intended driving path, stay in lane
	Failure of brakes	—	—	—	— Brake to slow/stop vehicle
	Incorrect steering angle with high angular speed at medium or high vehicle speed (steering angle change not aligned to driver intent)	—	—	—	— Maintain intended driving path, stay in lane
	Faulty driver airbag release when travelling at high speed	—	—	—	— Maintain intended driving path, stay in lane — Brake to slow/stop vehicle

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted as adequate: "Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven. This is appropriate evidence of the rationale for a C2-estimate.

NOTE 2 For C1 a test to provide a rationale that 99 % of the drivers "pass" the test in a certain traffic scenario might not be feasible because a huge number of test subjects would be necessary as the appropriate evidence for such a rationale.

NOTE 3 As no controllability is assumed for category C3, it is not relevant to have appropriate evidence of the rationale for such a classification.

Verweis auf ADAS Code of Practice (siehe Folie 4)

Risiko Controllability Beispiele

		C0	C1	C2	C3
Examples	Situations that are considered distracting	— Maintain intended driving path	—	—	—
	Unexpected radio volume increase	— Maintain intended driving path	—	—	—
	Warning message - gas low	— Maintain intended driving path	—	—	—
	Unavailability of a driver assisting system	— Maintain intended driving path	—	—	—
	Faulty adjustment of seat position while driving	—	— Brake to slow/stop vehicle	—	—
	Blocked steering column when starting the vehicle	—	— Brake to slow/stop vehicle	—	—
	Failure of ABS during emergency braking	—	—	— Maintain intended driving path	—
	Headlights fail while night driving at medium/high speed on unlighted road	—	—	— Steer to side of road or brake to stop.	—
	Motor failure at high lateral acceleration (motorway exit)	—	—	— Maintain intended driving path	—
	Failure of ABS when braking on low friction road surface while executing a turn	—	—	—	— Maintain intended driving path, stay in lane
	Failure of brakes	—	—	—	— Brake to slow/stop vehicle
	Incorrect steering angle with high angular speed at medium or high vehicle speed (steering angle change not aligned to driver intent)	—	—	—	— Maintain intended driving path, stay in lane
	Faulty driver airbag release when travelling at high speed	—	—	—	— Maintain intended driving path, stay in lane — Brake to slow/stop vehicle

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted as adequate: *Practical testing experience

Quelle:
ISO 26262: 2018
Teil 3

Kategorisierung der Eintrittswahrscheinlichkeit: Exposure: (E1 - E4)

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Definition of duration/ probability of Exposure (informative)	Not specified	< 1% of average operating time	1% - 10% of average operating time	> 10% of average operating time

Quellen: ADAS Code of Practice, ISO 26262

Verweis in der ISO 26262:2018 auf ADAS Code of Practice

* Zu C2:

Verweis auch in der zweiten Auflage der ISO 26262-3:2018, Part 3 Concept phase, auf den RESPONSE 3 ADAS Code of Practice:

* *"For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted as adequate: "Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven.*
This is appropriate evidence of the rationale for a C2-estimate."

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted
revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 2
for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for h
appropriate evidence of the rationale for a C2-estimate.

NOTE 2 For C1 a test to provide a rationale that 99 % of the drivers "pass" the test in a certain traffic scena
number of test subjects would be necessary as the appropriate evidence for such a rationale.

NOTE 3 As no controllability is assumed for category C3, it is not relevant to have appropriate evidence of the

Gefahrenanalyse und Risikobewertung (Anhang A.3)

Das ASIL Modell – Automotive Safety Integrity Level

$$R = F(f, C, S)$$

- R: Risiko
- f: Auftretensfrequenz des Gefahrenereignisses
- C: **Beherrschbarkeit**
- S: mögliche Schadensauswirkung

mit $f = \lambda \cdot E$

- λ: Ausfallrate des Systems
- E: Auftretenswahrscheinlichkeit der Fahrsituation

In der ISO 26262 wird vereinfacht angenommen: $f = E$

Auftretenswahrscheinlichkeiten und Controllability werden in Klassen eingeteilt

Gefahrenanalyse und Risikobewertung (Anhang A.3)

Bestimmung des Automotive Safety Integrity Level (ASIL)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

- QM: Quality Management; Keine Anforderung zur Erfüllung der ISO 26262
- ASIL-A: Niedrige Sicherheitsanforderungen
- ASIL-D: Hohe Sicherheitsanforderungen

vgl. Anhang A.3.5, S. A45

Gefahrenanalyse und Risikobewertung (Anhang A.3)

ASIL Dekomposition

Die ASIL-Dekomposition ist in Kapitel 9 – ASIL der ISO 26262 beschrieben.

Definition der Dekomposition in Kapitel 1:

"apportioning of safety requirements redundantly to sufficiently independent elements (1.32), with the objective of reducing the ASIL (1.6) of the redundant safety requirements that are allocated to the corresponding elements"

Deutsche Übersetzung:

Redundante Aufteilung der Sicherheitsanforderungen auf ausreichend unabhängige Elemente – vor dem Hintergrund der Reduzierung der ASIL Einstufungen der redundanten Sicherheitsanforderungen – die auf die entsprechenden Elemente zugewiesen werden.

vgl. ISO 26262 Kap. 9

Gefahrenanalyse und Risikobewertung (Anhang A.3)

ASIL Dekomposition

Die **richtige** Dekomposition lässt sich durch eine ganz einfache mathematische Formel wiedergeben, in der folgende Vereinbarungen gelten:

QM (X) wird ersetzt durch 0

ASIL A(X) wird ersetzt durch 1

ASIL B(X) wird ersetzt durch 2

ASIL C(X) wird ersetzt durch 3

ASIL D(X) wird ersetzt durch 4

vgl. ISO 26262

ASIL Dekomposition

Die Summe der dekomponierten Elemente muss gleich dem Wert der ursprünglichen Einstufung sein.

Diese Umrechnungen sind korrekt:

$ASIL_{neu1} + ASIL_{neu2} = ASIL_{alt}$

$ASIL\ C_{(D)} + ASIL\ A_{(D)} = ASIL\ D$

$3 + 1 = 4$

$ASIL\ D = ASIL\ C_{(D)} + ASIL\ A_{(D)}$

$4 = 3 + 1$

$ASIL\ C = ASIL\ A_{(C)} + ASIL\ A_{(C)} + ASIL\ A_{(C)}$

$3 = 1 + 1 + 1$

vgl. ISO 26262

ASIL Dekomposition

Grundsätzlich ist berücksichtigen, dass beispielsweise ein ASIL A(D) keinesfalls einem ASIL A entspricht. Das bedeutet:

- Wenn für die dekomponierten Elemente gleiche Teile bzw. gleiche Software verwendet werden sollten, dann müssen die abhängigen Fehler analysiert werden um systematische Fehler aufzudecken.

- Die Hardware Metriken für die Architektur und auch die zufälligen Hardwarefehler, die zu einer Verletzung des Sicherheitszieles führen könnten bleiben für die Gesamtfunktion identisch!

- Für die dekomponierten Elemente muss eine ausreichende Unabhängigkeit gezeigt werden.

vgl. ISO 26262

ASIL Dekomposition oder Überwachung

Wann handelt es sich um eine Dekomposition und wann um eine Überwachung?

Bei der Dekomposition müssen beide Elemente bezogen auf das Sicherheitsziel redundant ausgelegt sein. So müssen beispielsweise der Hauptrechner und der Sicherheitsrechner bei zu hoher Spannung/zu hohem Strom/zu hohem Drehmoment/… unabhängig voneinander in den Safe State schalten können.

Bei einer Überwachung teilt die Diagnose dem Hauptrechner lediglich mit, dass etwas nicht in Ordnung ist – jedoch nur der Hauptrechner kann das System in einen „Safe State“ überführen!

vgl. ISO 26262

9.5 Deutscher Verkehrsgerichtstag zu Automatisiertem Fahren

Deutscher Verkehrsgerichtstag 2019: Strafrechtliche Fragen

EMPFEHLUNG

Arbeitskreis II

Automatisiertes Fahren (Strafrechtliche Fragen)

Sicherheit im Straßenverkehr im Zusammenhang mit hoch- und vollautomatisiertem Fahren wird auch durch das Straf- und Ordnungswidrigkeitenrecht gewährleistet. Vor diesem Hintergrund empfiehlt der Arbeitskreis:

1. Die durch hoch- und vollautomatisiertes Fahren aufgeworfenen neuen Fragestellungen sind auf der Grundlage des bisherigen Strafrechts zu lösen. Es bedarf keines Sonderstrafrechts. Derzeit ist auch ein Unternehmensstrafrecht insoweit nicht erforderlich.

2. Die bereits erfolgte frühzeitige Schaffung eines Rahmens für das automatisierte Fahren höherer Stufen wird ausdrücklich begrüßt. Die derzeitige gesetzliche Regelung der Pflichtenstellung des Fahrzeugführers beim hoch- und vollautomatisierten Fahren (§ 1b StVG) ist, trotz mancher Bedenken – z.B. hinsichtlich des Spannungsverhältnisses von Abwendungsbefugnis und Wahrnehmungsbereitschaft – bezüglich ihrer praktischen Handhabbarkeit, grundsätzlich ausreichend. Die weitere Klärung obliegt der Judikatur und Rechtsdogmatik.

3. Die Einführung des Fahrmodusspeichers durch § 63a StVG wird begrüßt. Zur Aufklärung von Delikten ist darüber hinaus jedenfalls für hoch- und vollautomatisierte Fahrzeuge die dafür erforderliche Unfall- und Ereignisdatenspeicherung vorzusehen. Inhalt und Umfang der für die Unfallrekonstruktion zu speichernden Daten sind zu vereinheitlichen; die zu einer Speicherung führenden Ereignisse und die Schnittstellen sind zu standardisieren. Die Daten müssen jedenfalls auch im Fahrzeug gespeichert werden und aus ihm auslesbar sein.

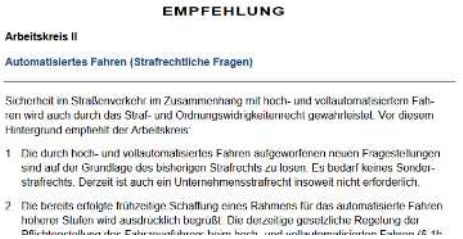
4. Um eine effektive Verfolgung von Delikten zu gewährleisten, empfiehlt sich die geeignete Kennzeichnung der maximal möglichen Automatisierungsstufe des Fahrzeugs.

Deutscher Verkehrsgerichtstag
- Deutsche Akademie für Verkehrswissenschaft - e.V.
Baron-Voght-Str. 106 a | 22607 Hamburg
Telefon: (040) 89 38 89 | Fax: (040) 89 32 92

www.deutscher-verkehrsgerichtstag.de
service@deutscher-verkehrsgerichtstag.de
organisation@deutscher-verkehrsgerichtstag.de
Steuer-Nummer: 17/411/01528

Postbank Hamburg
Konto 295 795 208 | BLZ 200 100 20
BIC/SWIFT: PBNKDEFF
IBAN: DE06 2001 0020 0295 7952 08

Deutscher Verkehrsgerichtstag 2019: Strafrechtliche Fragen



EMPFEHLUNG

Arbeitskreis II

Automatisiertes Fahren (Strafrechtliche Fragen)

Sicherheit im Straßenverkehr im Zusammenhang mit hoch- und vollautomatisiertem Fahren wird auch durch das Straf- und Ordnungswidrigkeitenrecht gewährleistet. Vor diesem Hintergrund empfiehlt der Arbeitskreis:

1. Die durch hoch- und vollautomatisiertes Fahren aufgeworfenen neuen Fragestellungen sind auf der Grundlage des bisherigen Strafrechts zu lösen. Es bedarf keines Sonderstrafrechts. Derzeit ist auch ein Unternehmensstrafrecht insoweit nicht erforderlich.

2. Die bereits erfolgte frühzeitige Schaffung eines Rahmens für das automatisierte Fahren höherer Stufen wird ausdrücklich begrüßt. Die derzeitige gesetzliche Regelung der

1. Die durch hoch- und vollautomatisiertes Fahren aufgeworfenen neuen Fragestellungen sind auf der Grundlage des bisherigen Strafrechts zu lösen. Es bedarf keines Sonderstrafrechts. Derzeit ist auch ein Unternehmensstrafrecht insoweit nicht erforderlich.
2. Die bereits erfolgte frühzeitige Schaffung eines Rahmens für das automatisierte Fahren höherer Stufen wird ausdrücklich begrüßt. Die derzeitige gesetzliche Regelung der Pflichtenstellung des Fahrzeugführers beim hoch-u nd vollautomatisierten Fahren(§ 1b StVG) ist, trotz mancher Bedenken – z.B. hinsichtlich des Spannungsverhältnisses von Abwendungsbefugnis und Wahrnehmungsbereitschaft – bezüglich ihrer praktischen Handhabbarkeit, grundsätzlich ausreichend. Die weitere Klärung obliegt der Judikatur und Rechtsdogmatik.
3. Die Einführung des Fahrmodusspeichers durch § 63a StVG wird begrüßt. Zur Aufklärung von Delikten ist darüber hinaus jedenfalls für hoch- und vollautomatisierte Fahrzeuge die dafür erforderliche Unfall- und Ereignisdatenspeicherung vorzusehen. Inhalt und Umfang der für die Unfallrekonstruktion zu speichernden Daten sind zu vereinheitlichen; die zu einer Speicherung führenden Ereignisse und die Schnittstellen sind zu standardisieren. Die Daten müssen jedenfalls auch im Fahrzeug gespeichert werden und aus ihm auslesbar sein.
4. Um eine effektive Verfolgung von Delikten zu gewährleisten, empfiehlt sich die geeignete Kennzeichnung der maximal möglichen Automatisierungsstufe des Fahrzeugs

Weitere Literaturquellen

Chiellino, U., Winkle, T., Graab, B., Ernsberger, A., Donner, E., Nerlich, M. (2010): Was können Fahrerassistenzsysteme im Unfallgeschehen leisten? In: Zeitschrift für Verkehrssicherheit 3/2010, TÜV Media GmbH, S. 131-137, Köln

Donner, E., Winkle, T., Walz, R., Schwarz, J. (2007): Response3 – Code of Practice für die Entwicklung, Validierung und Markteinführung von Fahrerassistenzsystemen (ADAS). In Technischer Kongress 2007, Verband der Automobilindustrie (VDA), S. 231-241, Sindelfingen.

International Organization for Standardization (ISO), ISO 26262-3 (2018): Road Vehicles – Functional safety

Knapp, A., Neumann, M., Brockmann, M., Walz, R., Winkle, T. (2009): Code of Practice for the Design and Evaluation of ADAS, Preventive and Active Safety Applications, eSafety for road and air transport, European Commission Integrated Project, Response3, European Automobile Manufacturers Association – ACEA, Brussels. http://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf

Matthaei, R., Reschka, A., Rieken, J., Dierkes, F., Ulbrich, S., Winkle, T., Maurer, M. (2015): Autonomes Fahren, In: Winner, H., Hakuli, S., Lotz, F., Singer, C., (Hrsg.), Handbuch Fahrerassistenzsysteme, 3. Auflage, S. 1146-1168, Vieweg Teubner, Wiesbaden.

Winkle, T. (2015): Entwicklungs- und Freigabeprozess automatisierter Fahrzeuge: Berücksichtigung technischer, rechtlicher und ökonomischer Risiken. In: Maurer, M., Gerdes, C., Lenz, B., Winner, H., (Hrsg.), Autonomes Fahren - Technische, rechtliche und gesellschaftliche Aspekte. Springer - Verlag, Berlin, Heidelberg.
http://link.springer.com/content/pdf/10.1007%2F978-3-662-45854-9_28.pdf

Winkle, T. (2015): Sicherheitspotenzial automatisierter Fahrzeuge: Erkenntnisse aus der Unfallforschung. In: Maurer, M., Gerdes, C., Lenz, B., Winner, H., (Hrsg.), Autonomes Fahren - Technische, rechtliche und gesellschaftliche Aspekte. Springer - Verlag, Berlin, Heidelberg.
http://link.springer.com/content/pdf/10.1007%2F978-3-662-45854-9_17.pdf

Winkle, T. (2016): Development and Approval of Automated Vehicles: Considerations of Technical, Legal and Economic Risks. In: Maurer, M., Gerdes, C., Lenz, B., Winner, H., (Hrsg.), Autonomous driving – technical, legal and social aspects. Springer - Verlag, Berlin, Heidelberg.
http://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8_28.pdf

Winkle, T. (2016): Safety Benefits of Automated Vehicles: Extended Findings from Accident Research for Development, Validation and Testing. In: Maurer, M., Gerdes, C., Lenz, B., Winner, H., (Hrsg.), Autonomous driving – technical, legal and social aspects. Springer - Verlag, Berlin, Heidelberg.
http://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8_17.pdf

Winkle, T. (2019): Rechtliche Anforderungen an automatisiertes Fahren – Erkenntnisse aus Verkehrsgerichtstagen mit Verkehrsunfallbeispielen, Ergonomie aktuell (20) 2019, München.
https://www.lfe.mw.tum.de/downloads/

Winkle, T., Erbsmehl, C., Bengler, K. (2018): Area-Wide Real-World Test Scenarios of Poor Visibility for Safe Development of Automated Vehicles, European Transport Research Review, Journal, Springer - Verlag, Berlin, Heidelberg.
https://etrr.springeropen.com/track/pdf/10.1186/s12544-018-0304-x