

#### Fahrerassistenzsysteme im Kraftfahrzeug

Prof. Dr. phil. Klaus Bengler

Prof. Dr.-Ing. Thomas Winkle





Benefice do Tory

## 9 Übung Controllability – Beherrschbarkeit Prof. Dr.-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"





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





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





国家运输安全委员会(NTSB)的一份报告提供了事故的 详细信息。

报告显示, Uber 测试车辆以 39 英里/小时的速度相撞。碰 生前约 6 秒, 车辆的时速为 43 英里/小时。碰撞发生 前 1.3 秒, 系统已经判断出需要紧急制动以防止碰撞。根 据 Uber 的说法,测试车辆上的紧急制动干预被关闭,以 避免发生不可预测的行为。

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

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

Demnach kollidierte das Über-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 Notbremsmanöver erforderlich ist um eine Kollision zu verhindern. Laut Über waren beim Testfahrzeug Notbremseingriffe zur Vermeidung von unberechenbarem Verhalten deaktiviert.



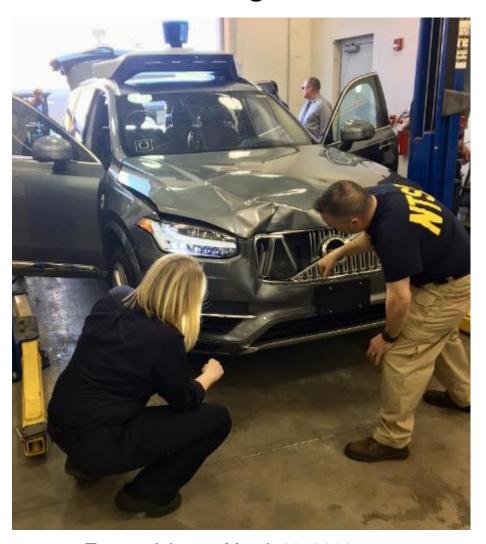
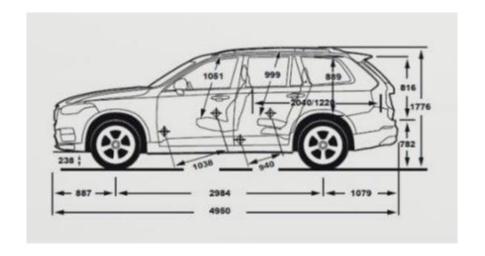


Abbildung: Police Department, Tempe, Arizona, March 18, 2018





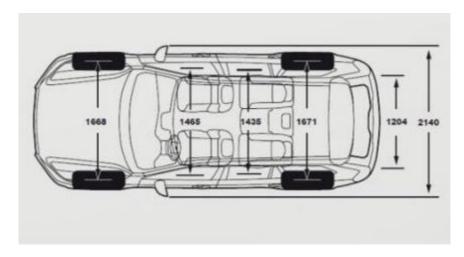


Abbildung: Volvo





Abbildung: UBER/Volvo





Abbildung: Google





Abbildung: Google









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.







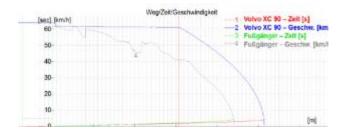
Mithilfe eines Mehrkörpermodells lässt sich der Erstkontakt der Fußgängerin mit dem geschobenen Fahrrad an der Fahrzeugfront des Volvo XC90 darstellen. 在多体模型的帮助下,可以直观地看到行人和被推自行车在沃尔沃 XC90前部的初始接触。





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



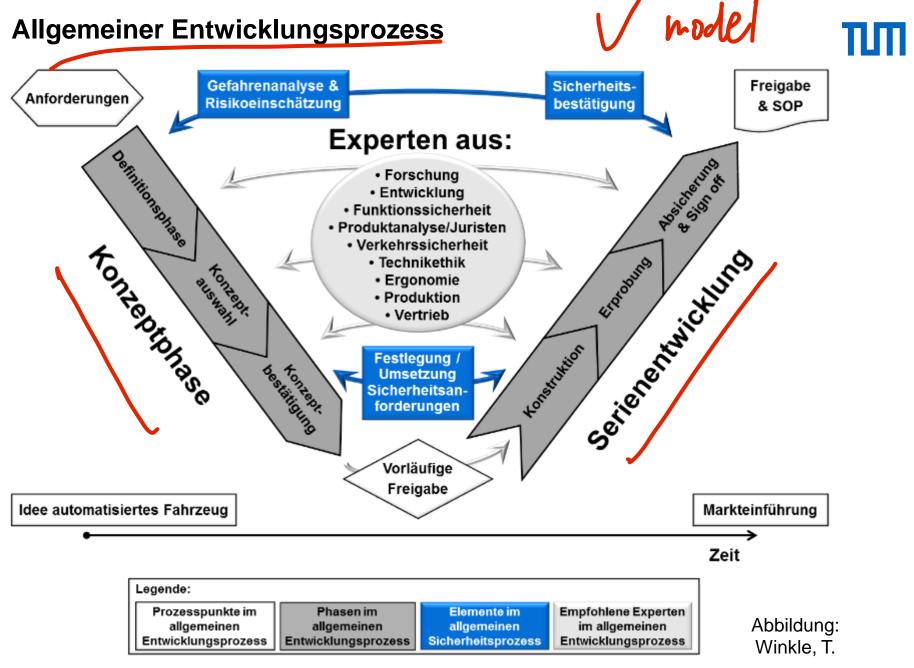


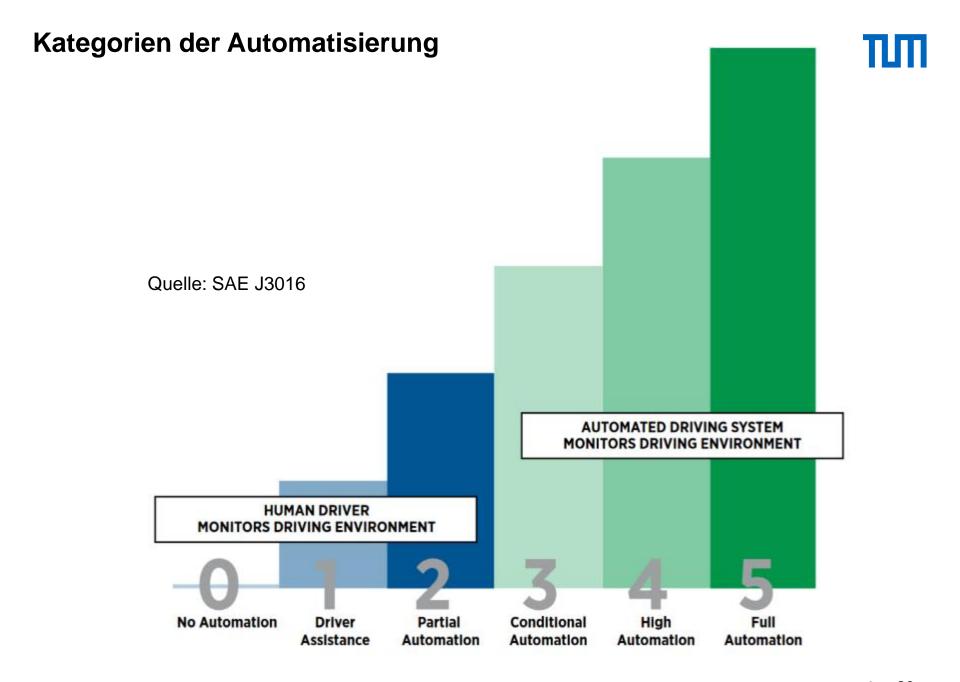
$$s = v * t = 17.8 \frac{m}{s} * 1.3 s = 23.1 m$$
$$a = \frac{v^2}{2s} = \frac{(17.8 \frac{m}{s})^2}{2 * 23.1 m} = 6.8 \frac{m}{s^2}$$

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.



# 9.2 Allgemeiner Entwicklungsprozess und Freigabeprozess Controllability





#### Kategorien der Automatisierung

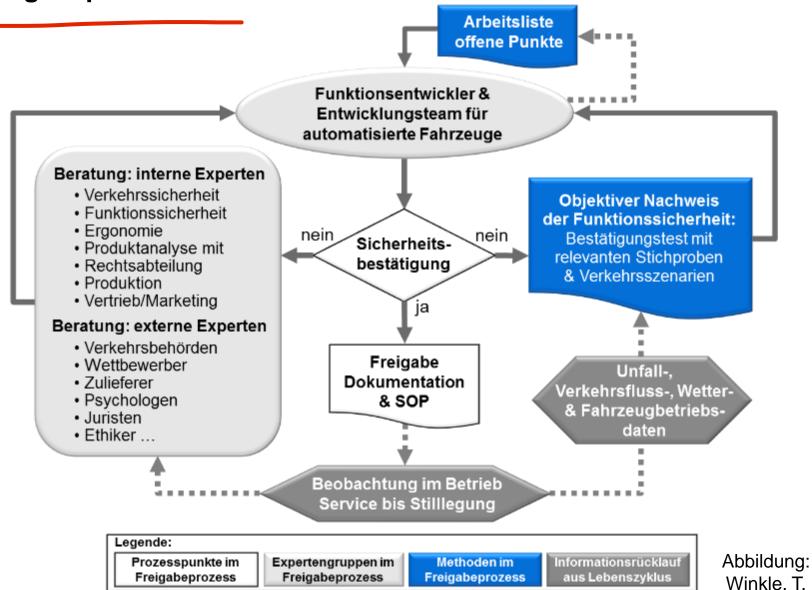


SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	Monitoring of Driving Environment	Fallback Performance of <i>Dynamic</i> <i>Driving Task</i>	System Capability (Driving Modes)
Huma	<i>n driver</i> monito	ors the driving environment				
0	No Automation	the full-time performance by the <i>human driver</i> of all aspects of the <i>dynamic driving task</i> , even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the <i>driving mode</i> -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 <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the <i>driving mode</i> -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 <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	System	Human driver	Human driver	Some driving modes
Autor	nated driving s	ystem ("system") monitors the driving environment				
3	Conditional Automation	the <i>driving mode</i> -specific performance by an <i>automated</i> 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 <i>driving mode</i> -specific performance by an automated driving system of all aspects of the <i>dynamic driving task</i> , even if a <i>human driver</i> does not respond appropriately to a <i>request to intervene</i>	System	System	System	Some driving modes
5	Full Automation	the full-time performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> under all roadway and environmental conditions that can be managed by a <i>human driver</i>	System	System	System	All driving modes

Copyright © 2014 SAE International. The summary table may be freely copied and distributed provided SAE International and J3016 are acknowledged as the source and must be reproduced AS-IS.

#### Freigabeprozess



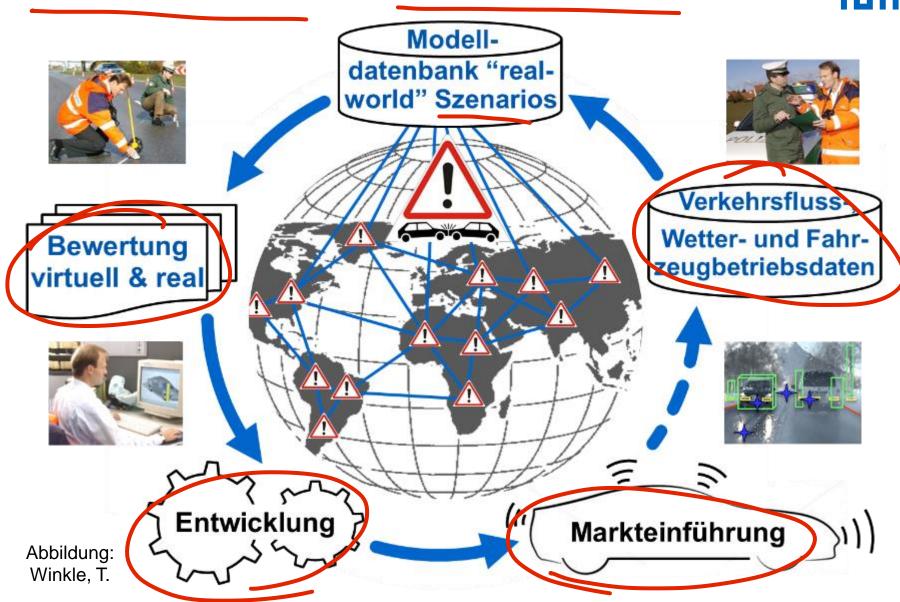




### 9.3 Potenziell gefährliche Situationen

#### Gefahren und Risiken aus realen Verkehrsszenarien





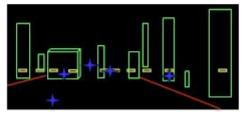
#### Lernkurve: Zunahme von verfügbaren Fahrdaten



#### Real world data / Driven miles



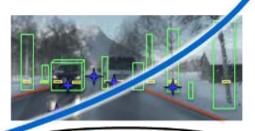
Sensor virtual assessment



Selected sensor fusion

Series

development



Real world:

Traffic-, accident-,
weather- & vehicle data

Concept phase

Levels of automation:

Passive safety

Driver only

Assisted – partial automated

Highly – fully automated

Monitoring of automated functions

New car market penetration:

Front airbag (≈100%)

Side airbag (≈100%)

Head airbag (≈50%)

ESP (≈100%)...

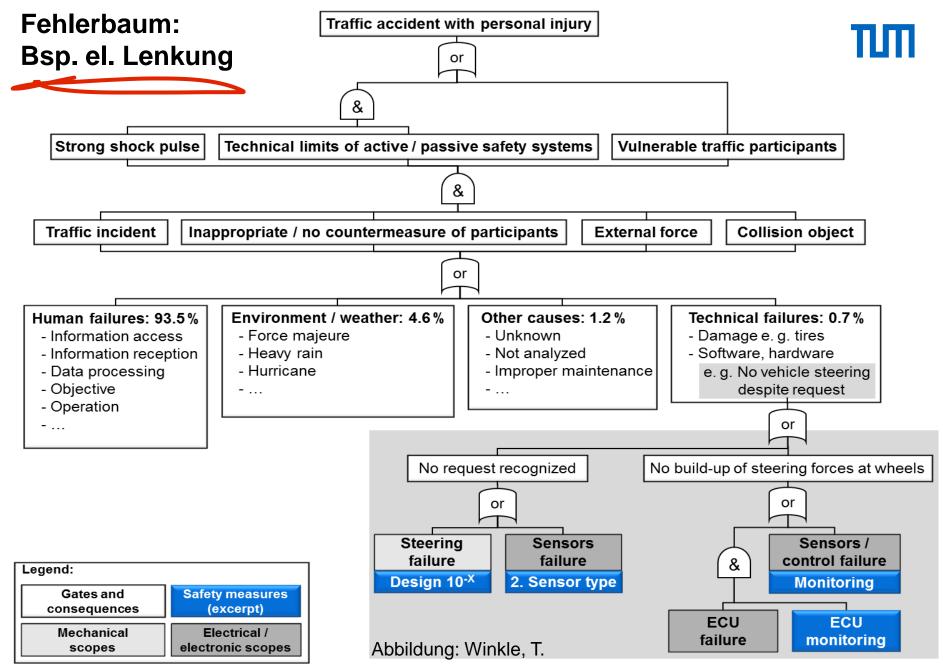
EBA (≈100%) LCA (≈10%)...

ACC (≈4%) AEB (≈10%)...

Key-, Self Parking (≈1%)...

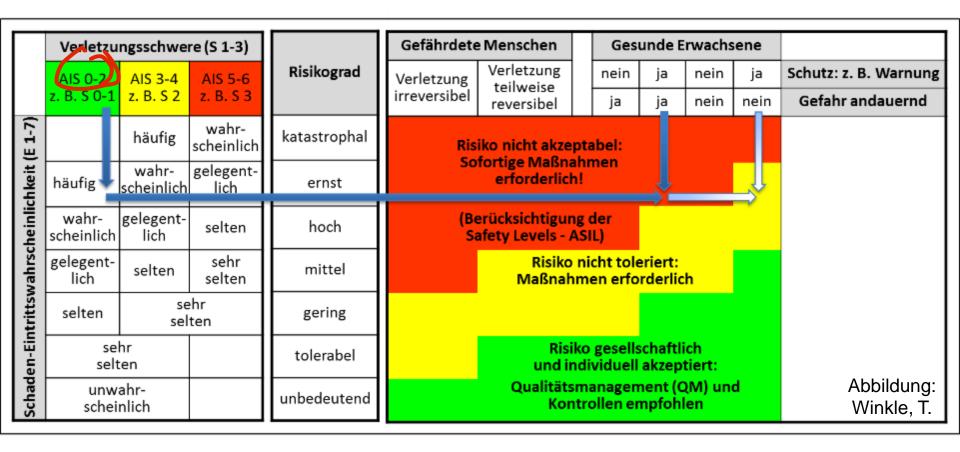
Abbildung: Winkle, T.

time





#### 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, <a href="http://www.nhtsa.gov">http://www.nhtsa.gov</a>

"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: 汽车安全完整性等级(ASIL)简介

Rückruf: 前向防撞、自适应巡航控制、车速控制、油门踏板

经销商: 菲亚特克莱斯勒有限责任公司菲亚特克莱斯勒有限责任公司,NHTSA 运动编号:14V293000,报告接收日期:2014 年 6 月 4 日:2014年6

月4日, http://www.nhtsa.gov

"当可选的自适应巡航控制系统启动后,驾驶员临时踩下加速踏板以提高(覆盖)车辆的设定速度,使其超过巡航控制系统本身的速度,在再次松开加速踏板后,车辆可能会继续短暂加速"。

Übung: 汽车安全完整性等级(ASIL)简介

Rückruf: 避免前向碰撞, 激活碰撞缓解制动系统

经销商:本田汽车公司,NHTSA 运动编号: 15V301000,报告接收日期: May 20, 2015, http://www.nhtsa.gov

"在某些驾驶条件下,碰撞缓解制动系统(CMBS)可能会错误地将某些路边物体(如金属栅栏或金属护栏)理解为障碍物,并意外地应用制动器。如果 CMBS 在行驶过程中意外施加紧急制动力,则会增加发生碰撞的风险"。

# Figures: Honda Motor Company

#### 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 RLX

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 (Hrsq.): Autonomous Driving. Springer Berlin Heidelberg, 2016, S. 599

#### Übung:

Einstufung eines Automotive Safety Integrity Level (ASIL)



Severity Exposure		Controllability			
		C1	C2	<b>C</b> 3	
	E1				
C4	E2				
S1	E3				
	E4				
	E1				
00	E2				
S2	E3				
	E4				
	E1				
00	E2				
S3	E3				
	E4				

Quellen: ADAS Code of Practice, ISO 26262

## Kategorisierung der Verletzungsschwere: Severity (S0 - S3)



Class	S0	S1	S2	<b>S</b> 3
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	<b>S</b> 3
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)

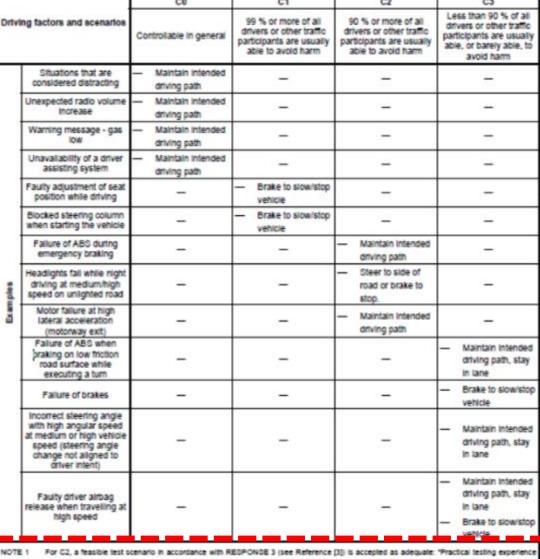
Dabei wird die Controllability im Code of Practice und in der ISO 26262 von C0 - C3 kategorisiert. Hier die Klassen C0 - C3 des ADAS Code of Practice:

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



Class of controllability (see Table 3)

Verweis auf ADAS Code of Practice (siehe Folie 4)

NOTE 1 For C2, a feasible test scenario in accordance with RESPONDE 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-oriteria 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.



		C0	C1	C2	C3	
Examples	Situations that are considered distracting	<ul> <li>Maintain intended driving path</li> </ul>	1	_	-	
	Unexpected radio volume increase	<ul> <li>Maintain intended driving path</li> </ul>	_	_	_	
	Warning message - gas low	<ul> <li>Maintain intended driving path</li> </ul>	_	_	_	
	Unavailability of a driver assisting system	<ul> <li>Maintain intended driving path</li> </ul>	_	-	_	
	Faulty adjustment of seat position while driving	-	<ul> <li>Brake to slow/stop vehicle</li> </ul>	-	_	
	Blocked steering column when starting the vehicle	-	<ul> <li>Brake to slow/stop vehicle</li> </ul>	ı	_	
	Failure of ABS during emergency braking	ı	-	<ul> <li>Maintain intended driving path</li> </ul>	_	
	Headlights fail while night driving at medium/high speed on unlighted road	-	_	<ul> <li>Steer to side of road or brake to stop.</li> </ul>	_	
	Motor failure at high lateral acceleration (motorway exit)	-	-	<ul> <li>Maintain intended driving path</li> </ul>	-	
	Failure of ABS when braking on low friction road surface while executing a turn	-	_	_	Maintain intended driving path, stay in lane	
	Failure of brakes	-	-	-	<ul> <li>Brake to slow/stop vehicle</li> </ul>	
	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	
TE	ITE 1 For C2 a feasible test scenario in accordance with RESPONSE 3 (see Reference (3)) is accented as adequate: "Practical testing experience					



### Risiko Controllability Beispiele

Quelle:

ISO 26262: 2018

Teil 3



## Kategorisierung der Eintrittswahrscheinlichkeit: Exposure: (E1 - E4)

Class	E1	<b>E2</b>	<b>E</b> 3	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."

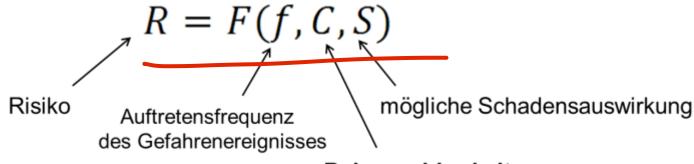
NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [3]) is accepted revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 2 for the test, a level of controllability of 85 % (with a level of confidence of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



Das ASIL Modell – Automotive Safety Integrity Level



Beherrschbarkeit

In der ISO 26262 wird vereinfacht angenommen: f=E

Auftretenswahrscheinlichkeiten und Controllability werden in Klassen eingeteilt



Bestimmung des Automotive Safety Integrity Level (ASIL)

		C1	C2	C3
	E1	QM	QM	QM
<b>S</b> 1	E2	QM	QM	QM
31	E3	QM	QM	Α
	E4	QM	Α	В
	E1	QM	QM	QM
<b>S2</b>	E2	QM	QM	Α
32	E3	QM	Α	В
	E4	Α	В	С
	E1	QM	QM	Α
S3	E2	QM	А	В
33	E3	А	В	С
	E4	В	С	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



### **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



### **ASIL Dekomposition**

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

正确的分解可以用一个非常简单的数学公式来表示, 其中适用以下协议:

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 
$$C(D)$$
 + 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



### **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.

#### ASIL 分解 必须牢记,ASIL A(D)并不等同于 ASIL A。这意味着

- 如果分解后的元素使用了相同的部件或软件,则必须对从属误差进行分析,以发现系统误差。
- 结构的硬件指标以及可能导致违反安全目标的随机硬件错误在整体功能上保持一致!
- 必须证明分解元素具有足够的独立性。

#### ASIL 分解或监测

何时是分解,何时是监控?

在分解的情况下,必须根据安全目标对两个元件进行冗余设计。例如,如果电压/电流/转矩/……过高,主计算机和安全计算机必须能够相互独立地切 换到安全状态。

在监控过程中,诊断程序只会告知主计算机有问题,但只有主计算机才能将系统切换到安全状态!



### **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:

- 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.
- 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.
- Die Einführung des Fahrmodusspeichers durch § 63a StVG wird begrüßt. Zur Aufklärung von Delikten ist darüber hinaus iedenfalls 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 f
 ür Verkehrswissenschaft - e.V. service@deutscher-verkehrsgerichtstag.de Baron-Voght-Str. 106 a | 22607 Hamburg Telefon: (040) 89 38 89 | Fax: (040) 89 32 92

www.deutscher-verkehrsgerichtstag.de organisation@deutscher-verkehrsgerichtstag.de BIC/SWIFT: PBNKDEFF Steuer-Nummer: 17/411/01528

Konto 295 795 208 | BLZ 200 100 20 IBAN: DE06 2001 0020 0295 7952 08

#### **EMPFEHLUNG**

#### Arbeitskreis II

Automotistorios Fehron (Straffochtliche Fragori)



Setherful in Shakowakani in Zusannanhang milihodh and vaka forrelistation Patron wird auch durch des Stoff und Ontranspeldispeltemecht gewähnlicht. Vor diesem Hintegrund engenent der Arbeits werz.

- Die durch hoch, und veilbeitenteilseintes Fehren aufgewertinen neuen Fragerindungen sind auf der Grundlags des bied ungen Stationite zu iseen. Es bedaff keines Stotiken stellsechts, Derzeit ist auch ein Unternehmensstratiocht inswed richt erforderlich.
- Die bereits erlolgte frühtzeitige Richaffung eines Rahmens für das automatisierte Fahren hüherer Stalen wied ausdrücklich begrußt. Die dezeitige gesetzliche Regelung der
- Deutscher Verkehrsgerichtstag 2019: Strafrechtliche Fragen
- 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. <a href="http://www.acea.be/uploads/publications/20090831\_Code\_of\_Practice\_ADAS.pdf">http://www.acea.be/uploads/publications/20090831\_Code\_of\_Practice\_ADAS.pdf</a>



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. <a href="http://link.springer.com/content/pdf/10.1007%2F978-3-662-45854-9\_28.pdf">http://link.springer.com/content/pdf/10.1007%2F978-3-662-45854-9\_28.pdf</a>

**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. <a href="http://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8">http://link.springer.com/content/pdf/10.1007%2F978-3-662-48847-8</a> 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/

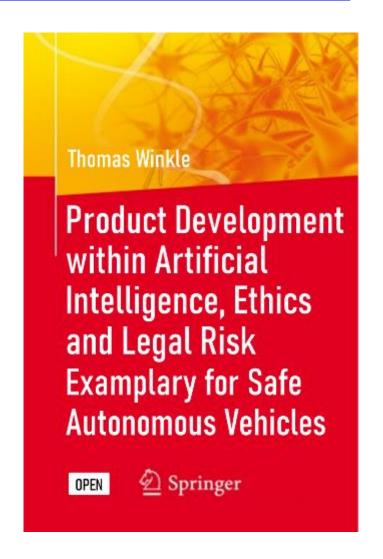
Winkle, T., Erbsmehl, C., Bengler, K. (2018): Area-Wide Real-World Test Scenarios of Poor Visibility for Safe Development of Automated Vehicles, European Transport Research Review, Journal, Springer - Verlag, Berlin, Heidelberg. <a href="https://etrr.springeropen.com/track/pdf/10.1186/s12544-018-0304-x">https://etrr.springeropen.com/track/pdf/10.1186/s12544-018-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



**Winkle, T. (2022):** Product Development within Artificial Intelligence, Ethics and Legal Risk – Exemplary for Safe Autonomous Vehicles.

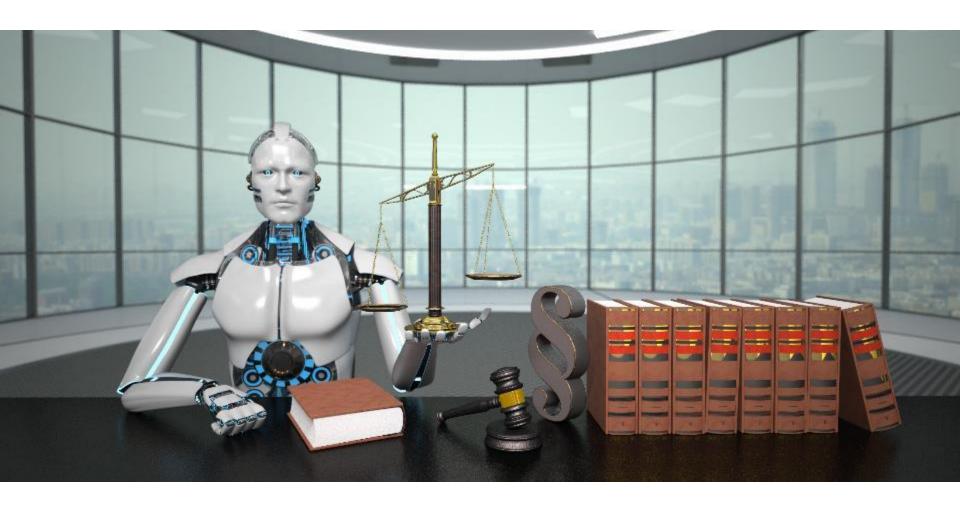
Springer - Verlag, Berlin, Heidelberg.

https://link.springer.com/book/10.1007/978-3-658-34293-7



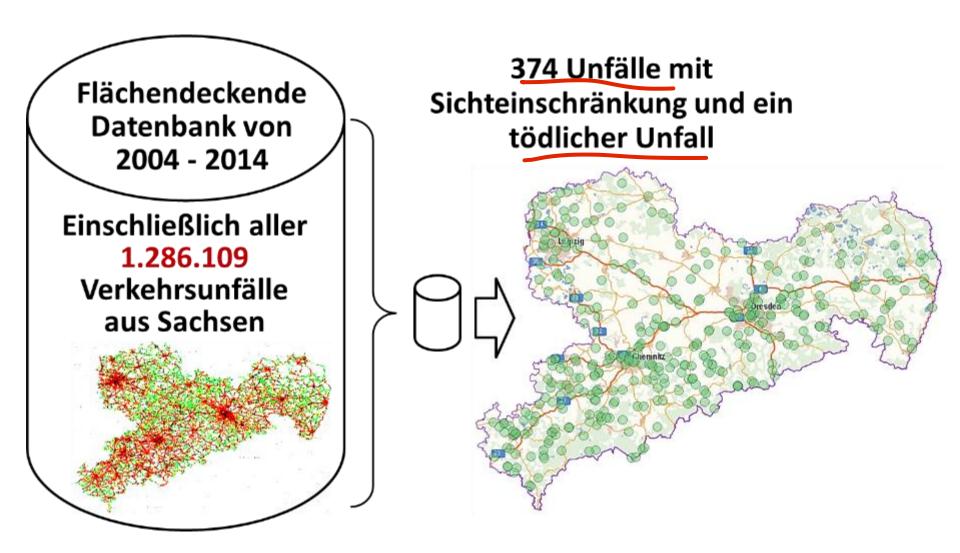
# Product development within Artificial Intelligence, ethics and the associated liability risk





## Flächendeckende Analyse von 1.286.109 Verkehrsunfällen mit Relevanz für automatisiertes Fahren







## Fußgänger sichtbar (vor Gegenverkehr)





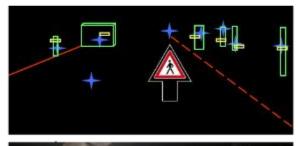


Maschinelle Wahrnehmung

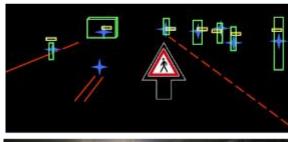
Mensch und Maschine

## Fußgänger nicht sichtbar (hinter Gegenverkehr)













### Weiteres Beispiel: Tödlicher Verkehrsunfall: Fahrer bewusstlos mit Herzinfarkt



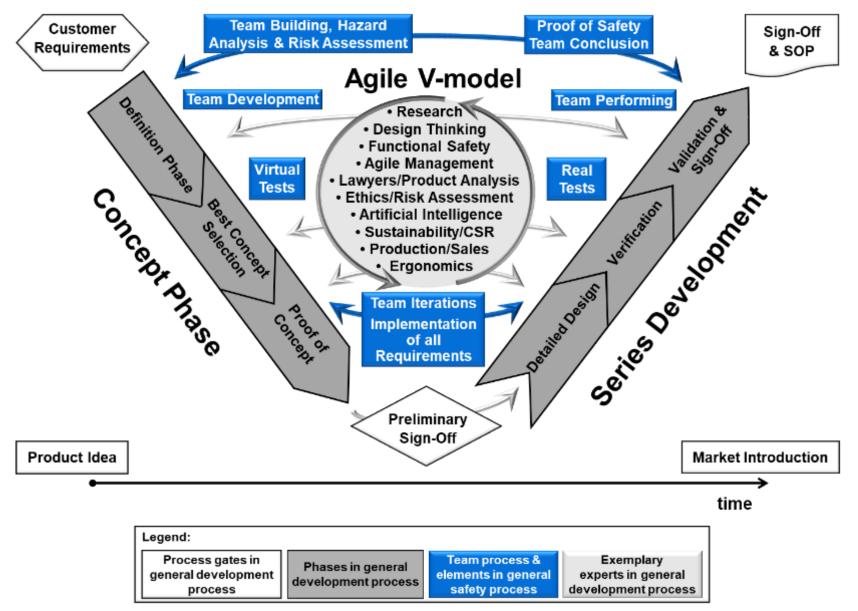
### Beispiel: Tödlicher Verkehrsunfall: Fahrer bewusstlos mit Herzinfarkt





### V-Modell mit Integration von Agilem Projektmanagement

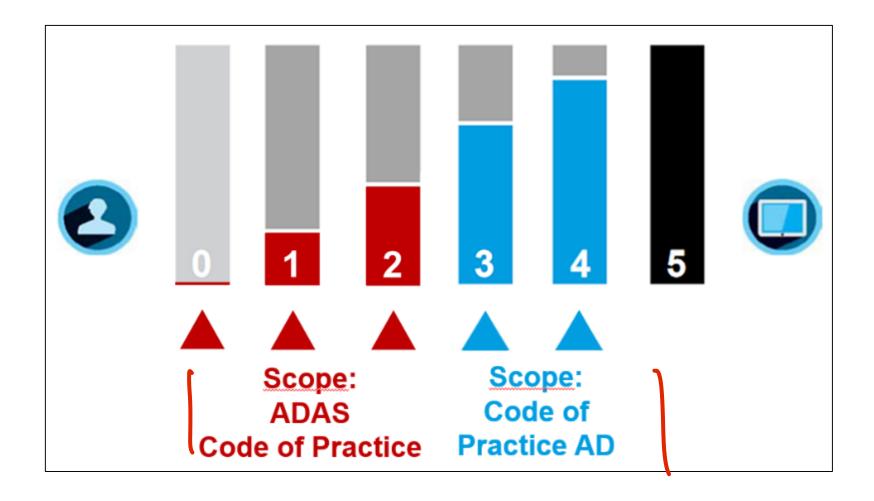




9- 59

### Automatisierungsstufen und Hauptanwendungsbereiche Code of Practice





## Unfalldatenschreiber zur Sensorerkennung des UBER Unfalls: Erste Erkennung eines Objekts 5,6 Sekunden vor Kollision



Time in [s] before impact	Speed in [mph]	Speed in [km/h]	Sensor classification and path prediction	Further incidents and more details
- 5.6	44	70.8	<u>Classification</u> : <b>Vehicle - by Radar</b> <u>Path prediction</u> : None - not on the path of the Volvo	Radar recognizes first detection and estimates its speed
- 5.2	45	72.4	Classification: Unknown Object - by Lidar Path prediction: Static, not on path	Lidar recognizes first detection of an unknown object, no speed determined
- 4.2	45	72.4	Classification: Vehicle - by Lidar Path prediction: In left lane	No tracking history, vehicle predicted as traveling in left lane
- 3.9	45	72.4	<u>Classification</u> : Vehicle - by Lidar <u>Path prediction</u> : In left lane	Tracking history, vehicle predicted as traveling in left lane
- 3.8 until - 2.7	45	72.4	Classification: alternated several times between vehicle and unknown - by Lidar Path prediction: alternated between static and left lane, not considered on path of the Volvo	At each change objects tracking history is unavailable and object's path predicted as static. When classification remains same, ADS predicts path traveling in left lane

Unfalldatenschreiber zur Sensorerkennung des UBER Unfalls:

Sichere Erkennung eines Objekts im Fahrschlauch 1,2 Sekunden vor Kollision

Time in [s] before impact	Speed in [mph]	Speed in [km/h]	Sensor classification and path prediction	Further incidents and more details
- 5.6	44	70.8	<u>Classification</u> : Vehicle - by Radar <u>Path prediction</u> : None - not on the path of the Volvo	Radar recognizes first detection and estimates its speed
- 5.2	45	72.4	Classification: Unknown Object - by Lidar Path prediction: Static, not on path	Lidar recognizes first detection of an unknown object, no speed determined
- 4.2	45	72.4	Classification: Vehicle - by Lidar Path prediction: In left lane	No tracking history, vehicle predicted as traveling in left lane
- 3.9	45	72.4	Classification: Vehicle - by Lidar Path prediction: In left lane	Tracking history, vehicle predicted as traveling in left lane
- 3.8 until - 2.7	45	72.4	Classification: alternated several times between vehicle and unknown - by Lidar Path prediction: alternated between static and left lane, not considered on path of the Volvo	At each change objects tracking history is unavailable and object's path predicted as static. When classification remains same, ADS predicts path traveling in left lane
- 2.6	45	72.4	<u>Classification</u> : <u>Bicycle - by Lidar</u> <u>Path prediction</u> : Static, not on path	Changed classification of object, no tracking history
- 2.5	45	72.4	<u>Classification</u> : Bicycle - by Lidar <u>Path prediction</u> : Not on the path	ADS predicts the bicycle path as traveling in the left lane
- 1.5	44	70.8	<u>Classification</u> : <u>Unknown - by Lidar</u> <u>Path prediction</u> : Static, partially on the path of the Volvo	Changed classification, ADS generates a motion plan around object, maneuver to the right
- 1.2	43	69.2	Classification: Bicycle - by Lidar Path prediction: Volvo travel lane	Again changed classification, no tracking history, hazard situation, action suppression begins
-0.2	40	64.4	<u>Classification</u> : Bicycle - by Lidar <u>Path prediction</u> : Volvo travel lane	An acoustic warning has been generated to indicate controlled deceleration has been initiated.
-0.02	39	62.8		Vehicle operator takes control of the steering wheel -> deactivating ADS
Impact				
1.8	37	59.5	-	Safety driver brakes
3,1	0	0	Final Position	





