On the UNICARagil Release Procedure

Measures for Internal and External Risk Communication

EVSAV Workshop, June 5, 2022

Robert Graubohm, TU Braunschweig

unicaragil

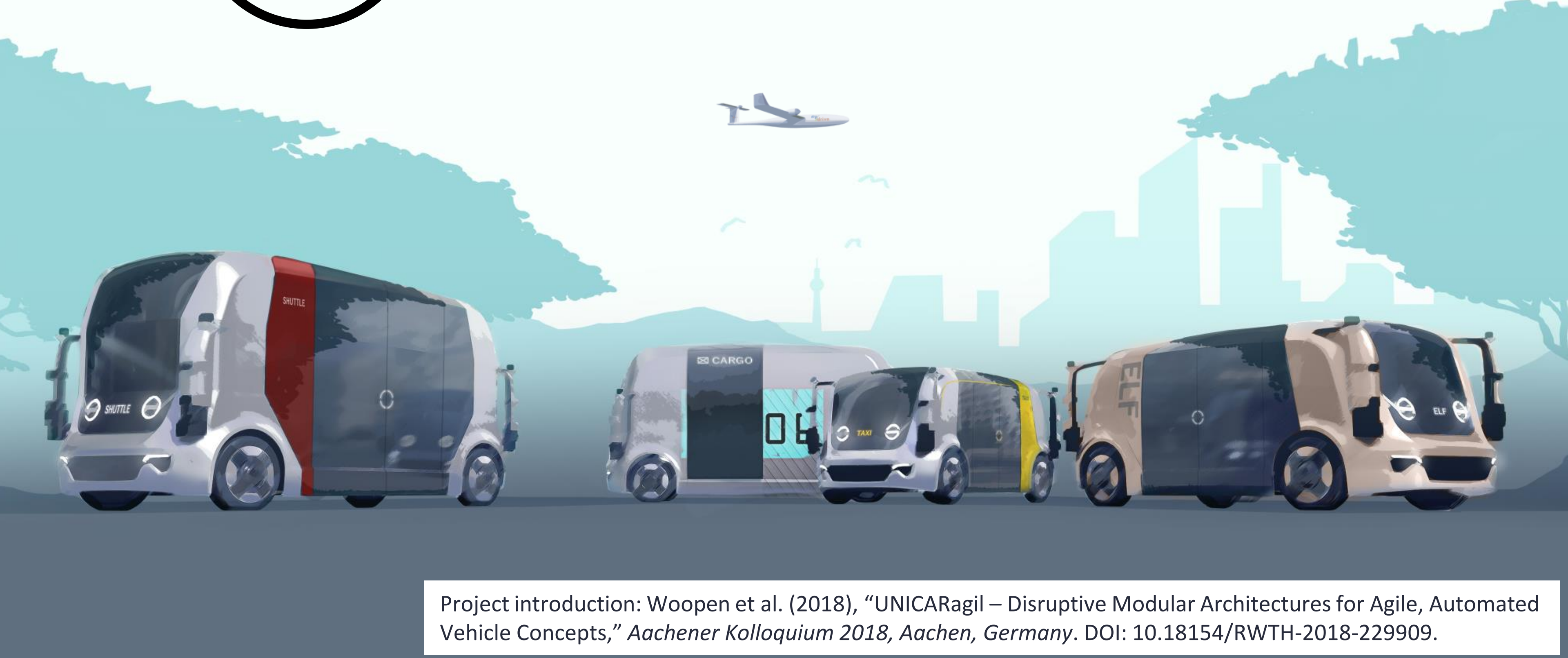
SPONSORED BY THE

Federal Ministry
of Education
and Research

unicaragil

SPONSORED BY THE

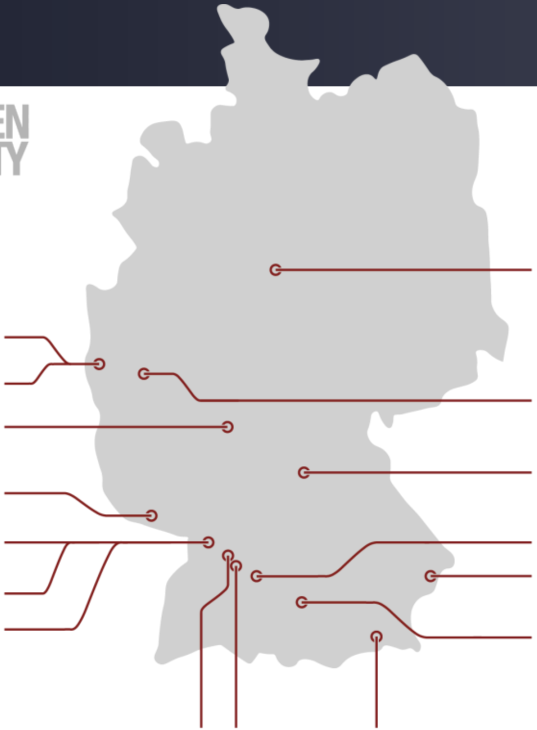
Federal Ministry
of Education
and Research



Project introduction: Woopen et al. (2018), “UNICARagil – Disruptive Modular Architectures for Agile, Automated Vehicle Concepts,” *Aachener Kolloquium 2018, Aachen, Germany*. DOI: 10.18154/RWTH-2018-229909.

The Consortium

SPONSORED BY THE
Federal Ministry
of Education
and Research



RWTH Aachen University

flyXdrive GmbH

Darmstadt Technical University

iMAR Navigation GmbH

Karlsruhe Institute of Technology

atlatec GmbH

IPG Automotive GmbH

Valeo Schalter und Sensoren GmbH

University of Stuttgart

VIRES Simulationstechnologie GmbH

Technical University of Braunschweig

Maxion Wheels Germany Holding GmbH

Schaeffler Technologies AG & Co. KG

Ulm University

University of Passau

Technical University of Munich

Prototypes' Status

Picture: unicaragil.de

What does the vehicle release process during the prototype implementation look like?

Related Work

- Safety concepts for AV demonstrations (e.g., Ziegler et al., 2014)
- Safety argumentation for AV testing (e.g., Koopman & Osyk, 2019)
- (Unpublished) internal release procedures of vehicle manufacturers

Distinction: Project Vision vs. Experimental Vehicles

- **Project vision:**

  UNICARagil AVs for various use cases navigate automatically through mixed inner city traffic

- **Experimental vehicles:**

  Prototypes representing four use cases are tested and demonstrated on proving grounds

The release procedures discussed here are aimed at the safe operation of the prototypes during tests and demonstrations.

Safety Goals for an Urban Example Scenario

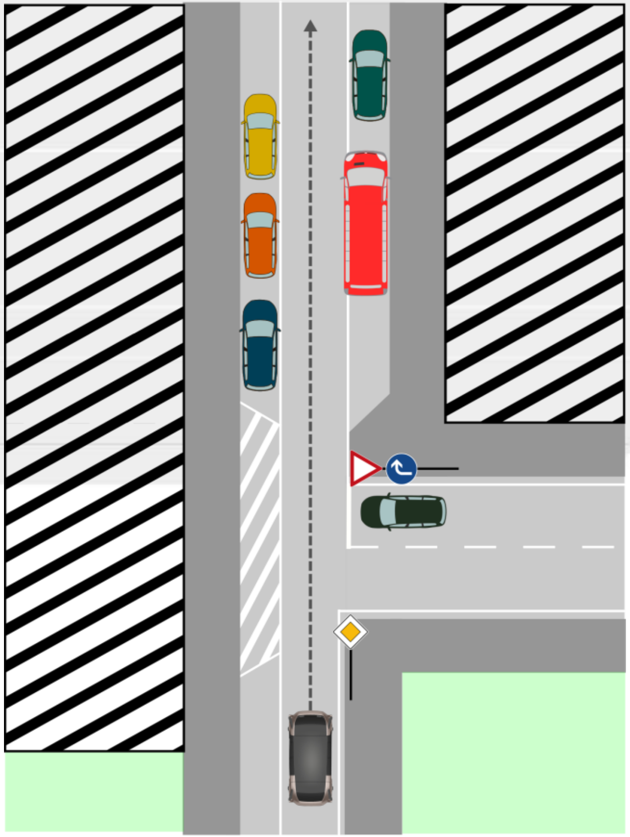
Target behavior:
Ego vehicle follows lane with adequate speed

Safety Goal Examples

SG 1 The vehicle shall move within its lane boundaries during lane following.

SG 2 The vehicle shall pass relevant objects with adequate lateral distance.

(cf. Stolte et al., 2020)

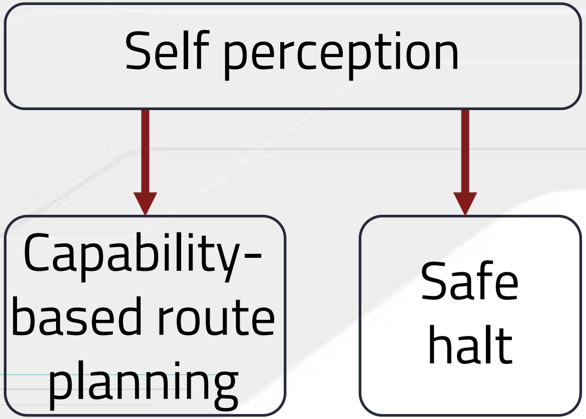


Bundesministerium
für Bildung
und Forschung

Project Specific Safety Mechanisms to Fulfill the Generic Goals

SG_1 The vehicle shall move within its lane boundaries during lane following.

SG_2 The vehicle shall pass relevant objects with adequate lateral distance.

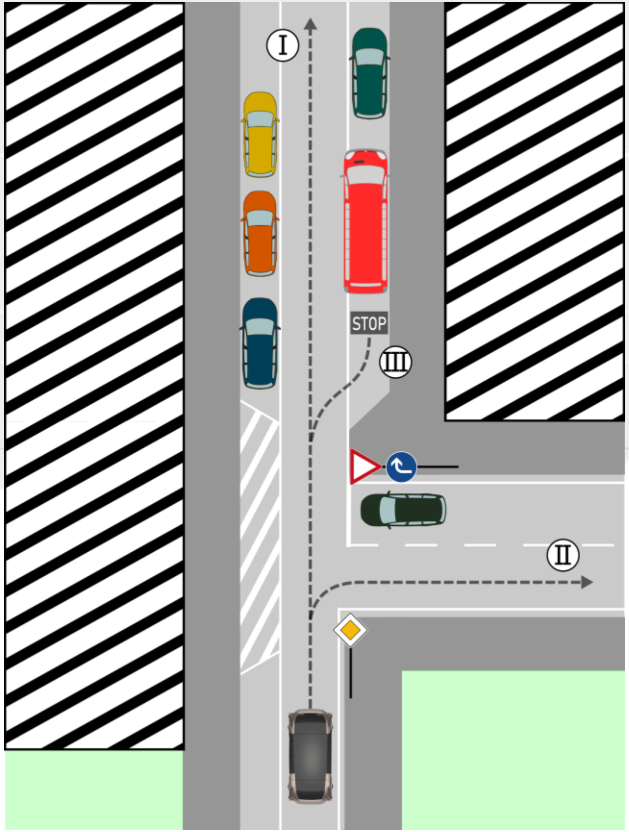


Self perception

Capability-based route planning

Safe halt

(cf. Stolte et al., 2020)



Baseline for the Prototypes‘ Release

The prototypes represent vehicles…

… built from scratch…

… designed mostly by academic institutions…

… using prototypical algorithms and hardware components…

… that will never operate in public traffic…

… that, however, not only project staff, but also externals will interact with…

… and that will drive on their own without human safety drivers.

Demonstration will include remote monitoring by a “safety watch”
(wireless stop switches for track marshals or escort vehicles)

Goals Regarding the Release Procedure

Project-wide **release levels** are established.

A specific release level is approved based on:

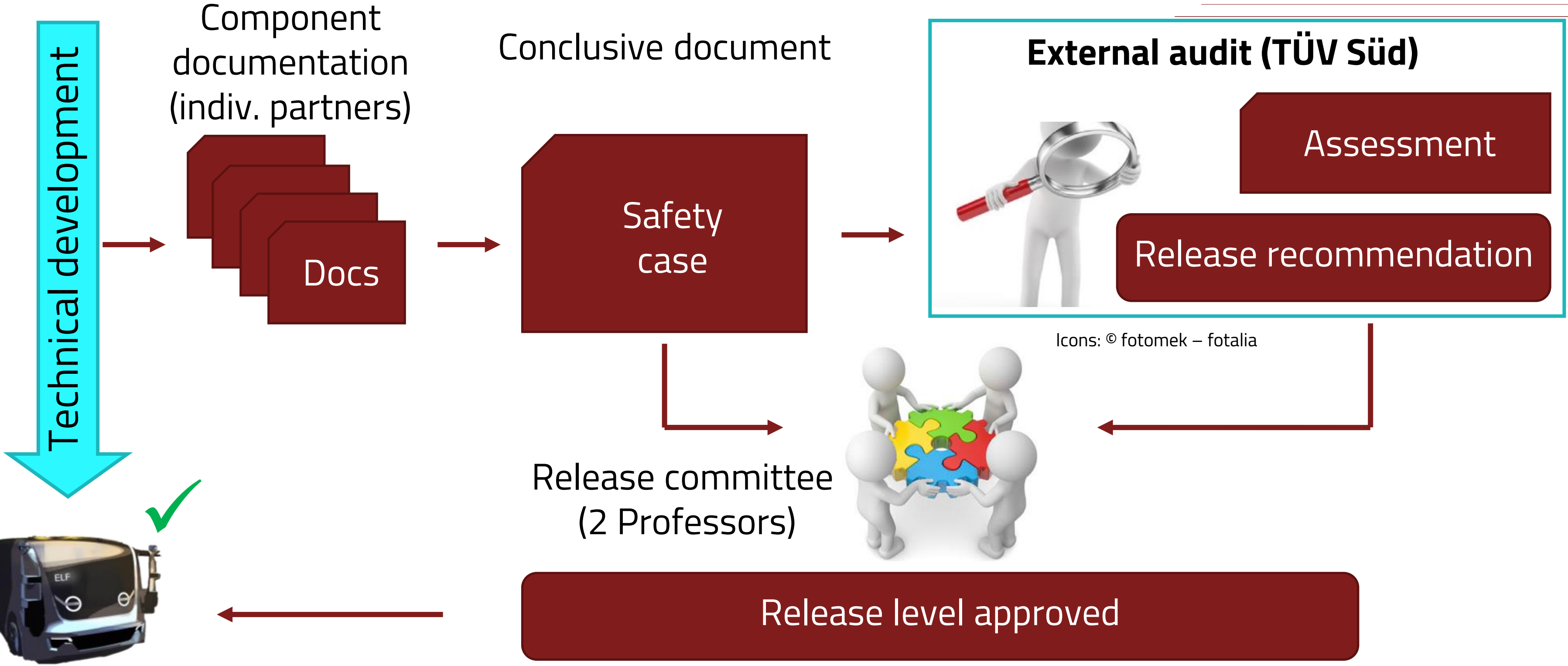
a) **appropriate documentation** of design **features** and

b) the actual vehicle **readiness**.

Thus, the following statements are characteristics of the release procedure:

- **Uncertainties** and the imminent **risks** when interacting with the vehicles are generally **known, transparent, and documented.**
- **Measures** for risk avoidance or mitigation are **specified**
- **Measures** appear to the releasing party to be **sufficient and appropriate** for the intended use
- **Implementation** of these measures is **documented**

The UNICARagil Release Procedure



Technical development

Component documentation (indiv. partners)

Docs

Conclusive document

Safety case

External audit (TÜV Süd)

Assessment

Release recommendation

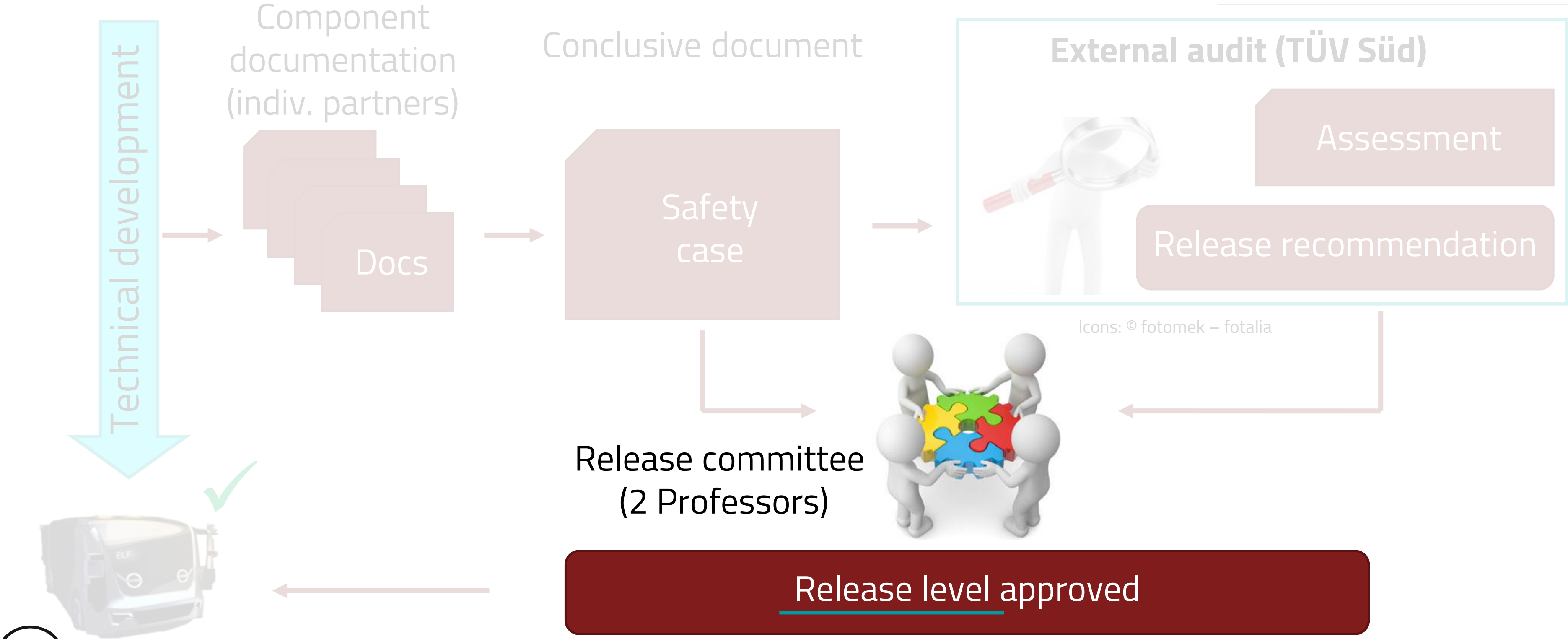
Icons: © fotomek – fotalia

Release committee (2 Professors)

Release level approved

The UNICARagil Release Procedure

Bundesministerium
für Bildung
und Forschung



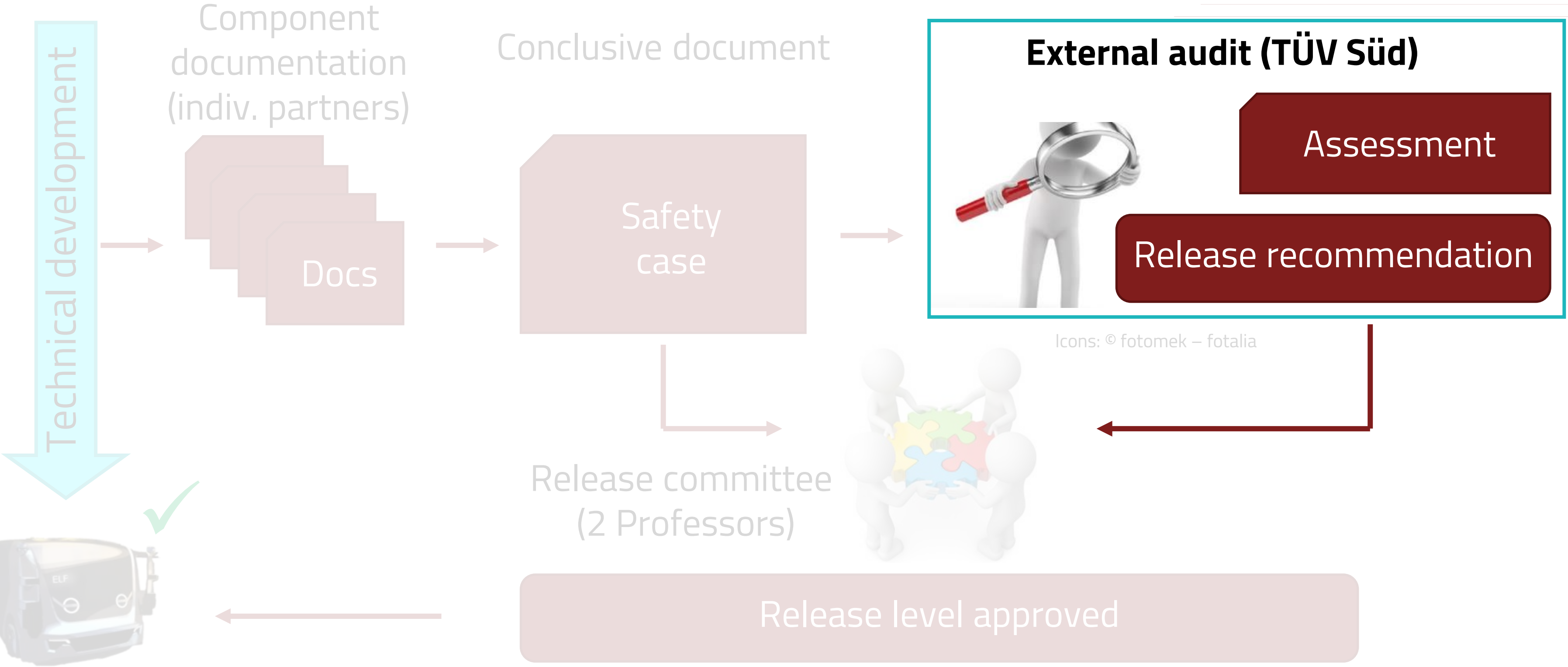
Icons: © fotomek – fotalia

Release Levels in UNICARagil

Bundesministerium
für Bildung
und Forschung

1) Release for driving with manual control on test area with reduced speed
2) Release for driving with manual control on test area
3) Release for testing functions in controlled environments involving safety drivers as a fallback
4) Release for trials of the demonstration
5) Release to demonstrate on the final event

The UNICARagil Release Procedure



Technical development

Component documentation (indiv. partners)

Docs

Conclusive document

Safety case

External audit (TÜV Süd)

Assessment

Release recommendation

Icons: © fotomek – fotalia

Release committee (2 Professors)

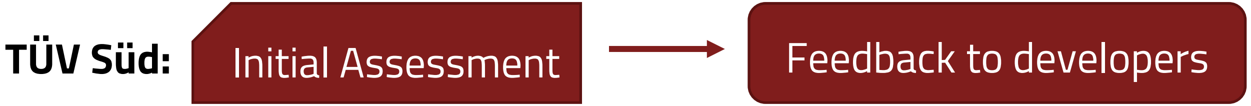
Release level approved

External audits

1) Release for driving with manual control on test area with reduced speed

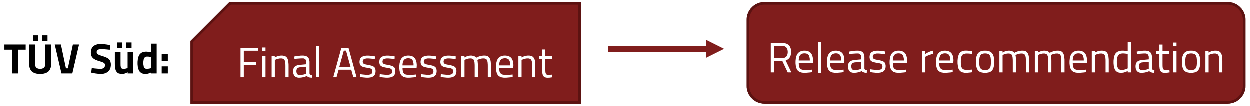
2) Release for driving with manual control on test area

3) Release for testing functions in controlled environments involving safety drivers as a fallback



TÜV Süd: Initial Assessment → Feedback to developers

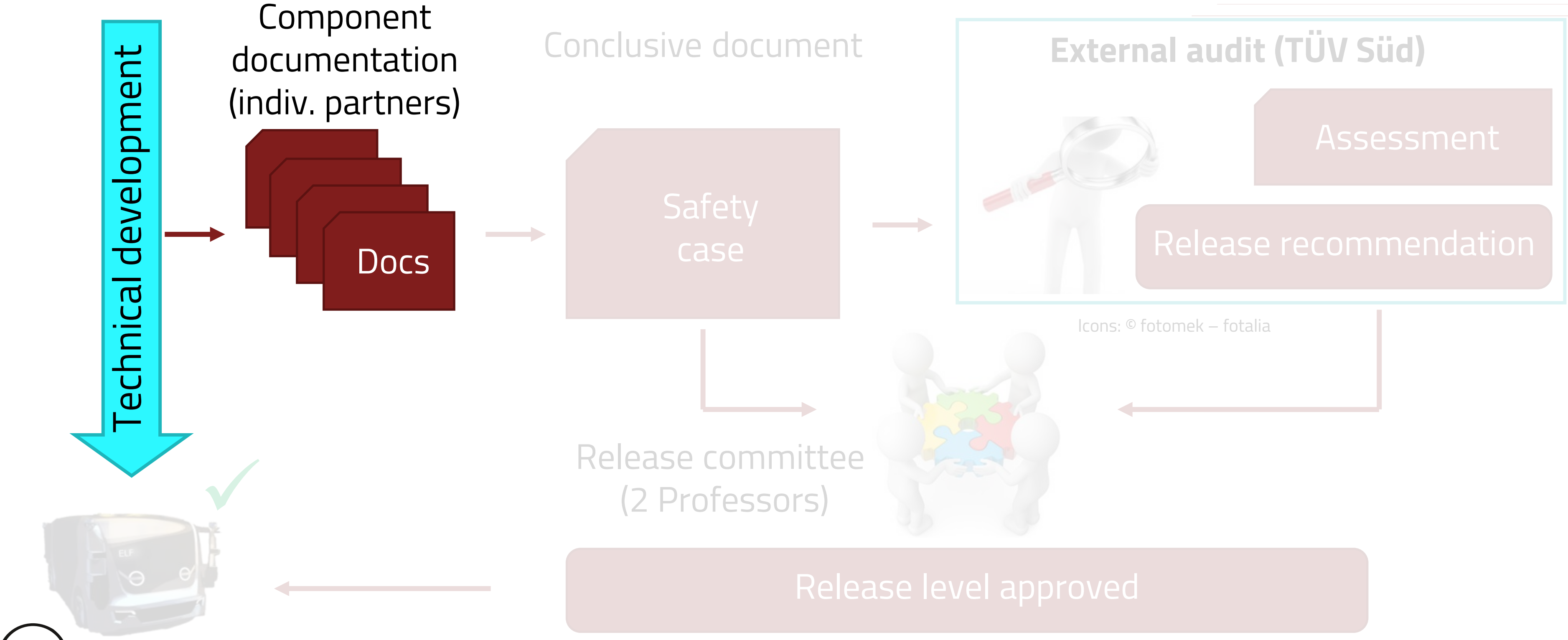
4) Release for trials of the demonstration



TÜV Süd: Final Assessment → Release recommendation

5) Release to demonstrate on the final event

The UNICARagil Release Procedure

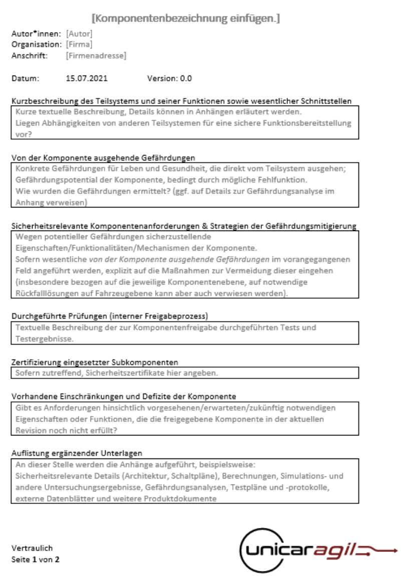


Component Documentation and Release

Uniform cover sheet for the component release, specifying

- vehicle and release level(s)
- the developers and their affiliations
- system boundaries, functionality and interfaces
- hazards posed by the component
- hazard mitigation on component level
- tests performed (component approval)
- certificates of employed subcomponents
- current limitations and deficits

The component release is signed by a professor.



[Komponentenbezeichnung einfügen.]

Autor*innen: [Autor]
Organisation: [Firma]
Anschrift: [Firmenadresse]

Datum: 15.07.2021 Version: 0.0

Kurzbeschreibung des Teilsystems und seiner Funktionen sowie wesentlicher Schnittstellen

Kurze textuelle Beschreibung, Details können in Anhängen erläutert werden.
Liegen Abhängigkeiten von anderen Teilsystemen für eine sichere Funktionsbereitstellung vor?

Von der Komponente ausgehende Gefährdungen

Konkrete Gefährdungen für Leben und Gesundheit, die direkt vom Teilsystem ausgehen; Gefährdungspotential der Komponente, bedingt durch mögliche Fehlfunktion.
Wie wurden die Gefährdungen ermittelt? (ggf. auf Details zur Gefährdungsanalyse im Anhang verweisen)

Sicherheitsrelevante Komponentenanforderungen & Strategien der Gefährdungsmitigierung

Wegen potentieller Gefährdungen sicherzustellende Eigenschaften/Funktionalitäten/Mechanismen der Komponente.
Sofern wesentliche *von der Komponente ausgehende Gefährdungen* im vorangegangenen Feld angeführt werden, explizit auf die Maßnahmen zur Vermeidung dieser eingehen (insbesondere bezogen auf die jeweilige Komponentenebene, auf notwendige Rückfalllösungen auf Fahrzeugebene kann aber auch verwiesen werden).

Durchgeführte Prüfungen (interner Freigabeprozess)

Textuelle Beschreibung der zur Komponentenfreigabe durchgeführten Tests und Testergebnisse.

Zertifizierung eingesetzter Subkomponenten

Sofern zutreffend, Sicherheitszertifikate hier angeben.

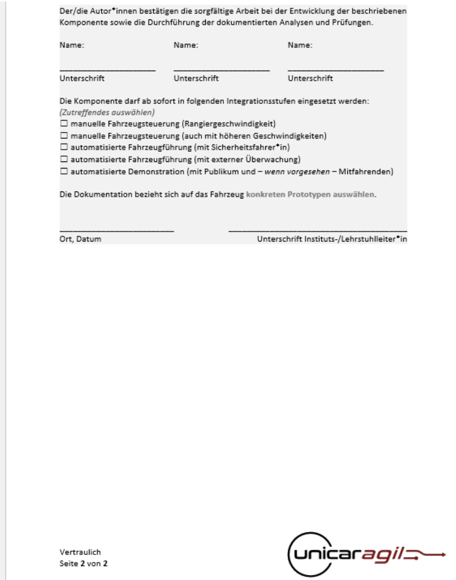
Vorhandene Einschränkungen und Defizite der Komponente

Gibt es Anforderungen hinsichtlich vorgesehenen/erwarteten/zukünftig notwendigen Eigenschaften oder Funktionen, die die freigegebene Komponente in der aktuellen Revision noch nicht erfüllt?

Auflistung ergänzender Unterlagen

An dieser Stelle werden die Anhänge aufgeführt, beispielsweise:
Sicherheitsrelevante Details (Architektur, Schaltpläne), Berechnungen, Simulations- und andere Untersuchungsergebnisse, Gefährdungsanalysen, Testpläne und -protokolle, externe Datenblätter und weitere Produktdokumente

Vertraulich
Seite 1 von 2



Der/die Autor*innen bestätigen die sorgfältige Arbeit bei der Entwicklung der beschriebenen Komponente sowie die Durchführung der dokumentierten Analysen und Prüfungen.

Name: Name: Name:

______________________ ______________________ ______________________
Unterschrift Unterschrift Unterschrift

Die Komponente darf ab sofort in folgenden Integrationsstufen eingesetzt werden:
(Zutreffendes auswählen)
☐ manuelle Fahrzeugsteuerung (Rangiergeschwindigkeit)
☐ manuelle Fahrzeugsteuerung (auch mit höheren Geschwindigkeiten)
☐ automatisierte Fahrzeugführung (mit Sicherheitsfahrer*in)
☐ automatisierte Fahrzeugführung (mit externer Überwachung)
☐ automatisierte Demonstration (mit Publikum und – *wenn vorgesehen* – Mitfahrenden)

Die Dokumentation bezieht sich auf das Fahrzeug konkreten Prototypen auswählen.

__________________________ ____
Ort, Datum Unterschrift Instituts-/Lehrstuhlleiter*in

Vertraulich
Seite 2 von 2

Partner Documentation for the First Release Levels

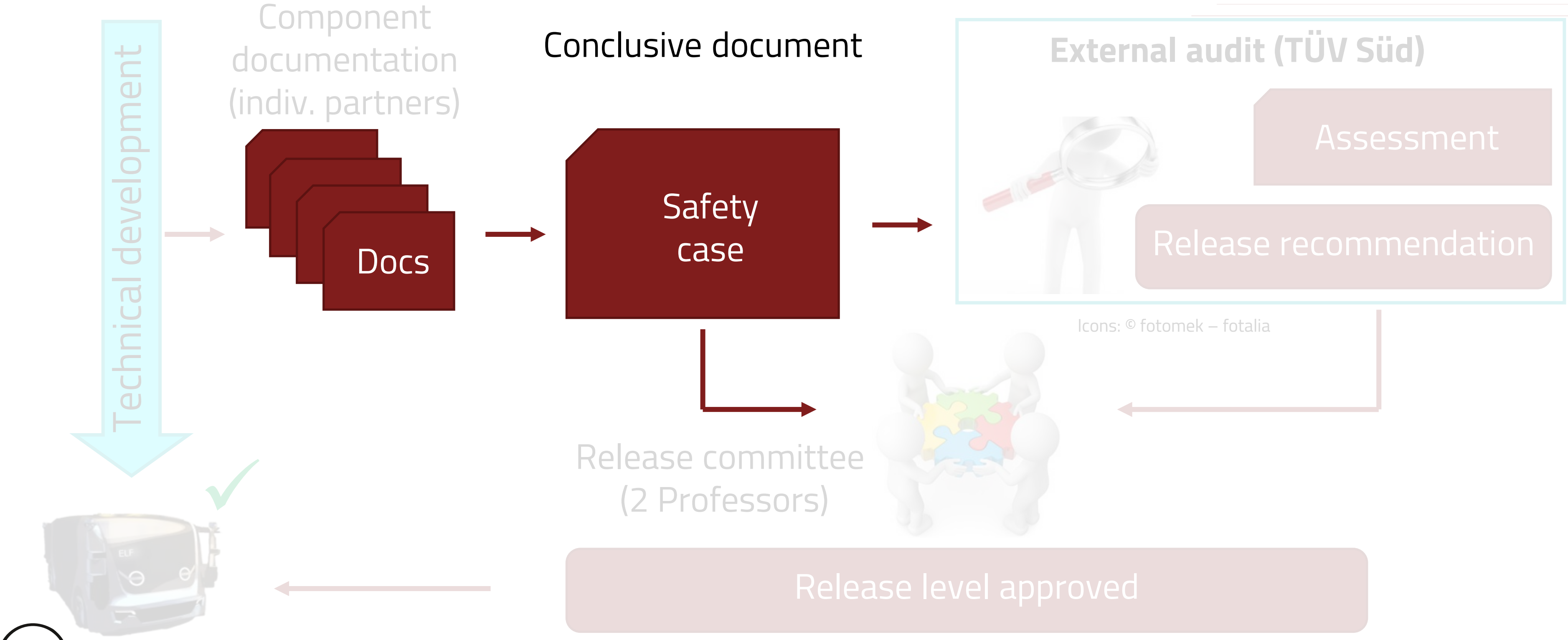
Vehicle components:

- Dynamics modules
- Battery
- On-board communication networks
- Test driver's seat
- Vehicle structure
- Door
- Control interfaces
- On-board power supply
- Thermal management
- Electronic mirrors
- Headlights
- Driver intervention capability

Additional documentation:

- Compliance with integration process
- Successful integration tests
- Description of test sites
- Operating instructions
- Test plan

The UNICARagil Release Procedure



Technical development

Component documentation (indiv. partners)

Docs

Conclusive document

Safety case

External audit (TÜV Süd)

Assessment

Release recommendation

Icons: © fotomek – fotalia

Release committee (2 Professors)

Release level approved

Structure of the Conclusive Documentation

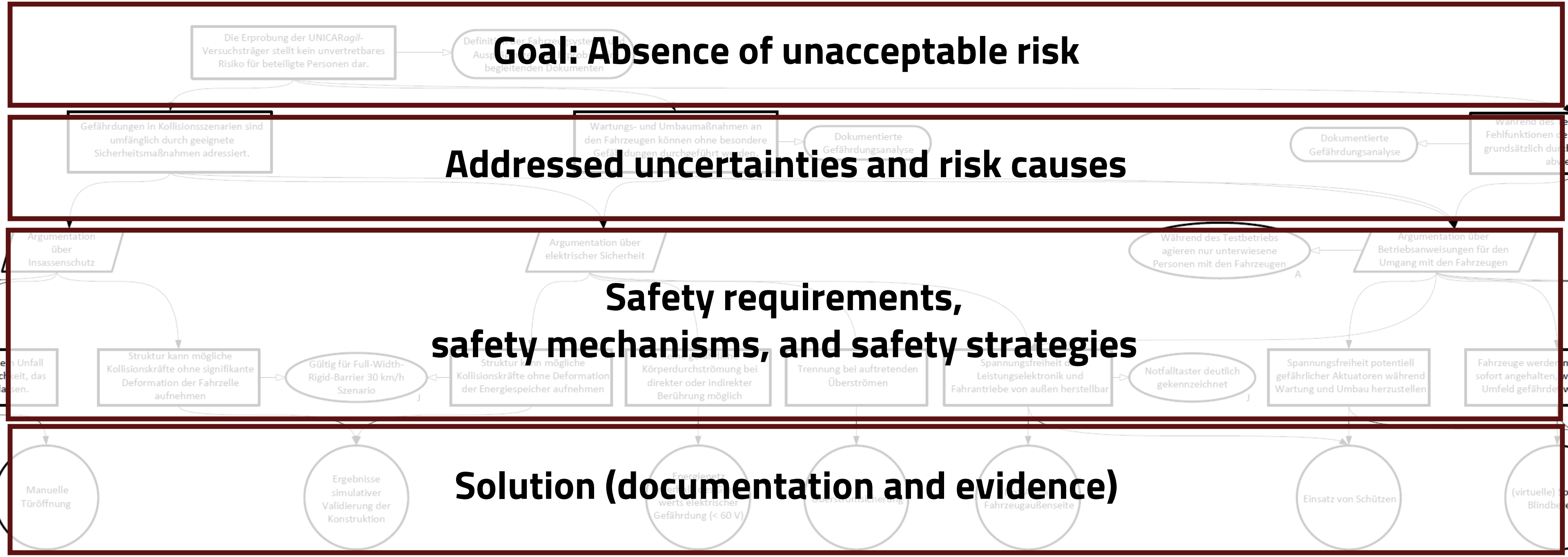
- Approval of the release committee (signature fields) for a specific vehicle and release level
- Project context and introduction
- Explanation of the release level and listing of the enclosed component documentations
- System-wide safety case (safety argument for the release level and disclosure of causes of risks)
- Partner documentations

Safety Case: Causes of Risks

- Unpredictability of potentially dangerous vehicle behavior (e.g., control interface or actuator failures)
- Uncertainty about consequences of a collision for occupants
- Uncertainty about the behavior of persons in the vehicle environment
- Uncertainty about operating modes of the vehicle (mode confusion, mode awareness, …)
- Possibility of electrical hazard (during operation, due to collisions, or during maintenance)
- Possibility of trapped occupants due to faults in the “door” system
- Possibility of insufficient monitoring or lack of adequate intervention options during operation

Safety Case: Safety Argument

Bundesministerium
für Bildung
und Forschung



Goal: Absence of unacceptable risk

Addressed uncertainties and risk causes

**Safety requirements,
safety mechanisms, and safety strategies**

Solution (documentation and evidence)

Die Erprobung der UNICAR*agil*-Versuchsträger stellt kein unvertretbares Risiko für beteiligte Personen dar.

begleitenden Dokumenten

Gefährdungen in Kollisionsszenarien sind umfänglich durch geeignete Sicherheitsmaßnahmen adressiert.

Wartungs- und Umbaumaßnahmen an den Fahrzeugen können ohne besondere Gefährdungen durchgeführt werden.

Dokumentierte Gefährdungsanalyse

Dokumentierte Gefährdungsanalyse

Fehlfunktionen

grundsätzlich

Argumentation über Insassenschutz

Argumentation über elektrischer Sicherheit

Während des Testbetriebs agieren nur unterwiesene Personen mit den Fahrzeugen

A

Argumentation über Betriebsanweisungen für den Umgang mit den Fahrzeugen

Struktur kann mögliche Kollisionskräfte ohne signifikante Deformation der Fahrzelle aufnehmen

Gültig für Full-Width-Rigid-Barrier 30 km/h Szenario

J

Kollisionskräfte ohne Deformation der Energiespeicher aufnehmen

Körperdurchströmung bei direkter oder indirekter Berührung möglich

Trennung bei auftretenden Überströmen

Leistungselektronik und Fahrantriebe von außen herstellbar

Notfalltaster deutlich gekennzeichnet

J

Spannungsfreiheit potentiell gefährlicher Aktuatoren während Wartung und Umbau herzustellen

Fahrzeuge werden sofort angehalten,

Manuelle Türöffnung

Ergebnisse simulativer Validierung der Konstruktion

werts elektrischer Gefährdung (< 60 V)

Fahrzeugaußenseite

Einsatz von Schützen

(virtuelle)

Internal Risk Communication Effects

The project partners

- have an idea of remaining risks and dangers,
- are aware that integrity and safety of controllers and actuators are far from series standards,
- know about the fallback measures of a release level,
- reviewed the documented restrictions for tests going along with a release level, and
- consider their component‘s potential safety impact systematically throughout the development.

External Risk Communication Effects

A published release documentation emphasizes UNCIARagil's dedication towards safety already in the design stage of AVs.

The documentation also discloses

- the knowledge of remaining risks and dangers,
- the basis for release decisions by the project,
- responsibilities and accountabilities of individual partners, and
- the established release procedure.

Conclusion

Our release procedure establishes

- five release levels,
- documented component-oriented hazard analyses,
- disclosure of the key deficiencies that motivate a human fallback,
- external auditing before release for demonstration, and
- a sound basis for risk assessment.

As a result, the release document is a hundreds of pages long comprehensive record of all established safety measures.

References

- P. Koopman & B. Osyk, "Safety Argument Considerations for Public Road Testing of Autonomous Vehicles," SAE Int. J. Adv. & Curr. Prac. in Mobility 1(2):512-523, 2019, doi: 10.4271/2019-01-0123.
- T. Stolte et al., "Towards Safety Concepts for Automated Vehicles by the Example of the Project UNICARagil," in 29th Aachen Colloq. Automobile and Engine Technology 2020, pp. 1561-1594, doi: 10.24355/dbbs.084-202011171557-0.
- T. Woopen et al., "UNICARagil - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts," in 27th Aachen Colloq. Automobile and Engine Technology 2018, pp. 663–694, doi: 10.18154/RWTH-2018-229909.
- J. Ziegler et al., "Making Bertha Drive—An Autonomous Journey on a Historic Route," IEEE Intell. Transp. Syst. Mag. 6(2):8-20, 2014, doi: 10.1109/MITS.2014.2306552.

SAVE THE DATE

final event

Presentations and live demonstrations of our project results on connected and automated driving

May 11, 2023, Aachen

Picture: unicaragil.de

Bundesministerium
für Bildung
und Forschung

Thank you for your attention.

Robert Graubohm

TU Braunschweig, Institute of Control Engineering (IfR)

Email: graubohm@ifr.ing.tu-bs.de

Web: http://www.ifr.ing.tu-bs.de

unicaragil

SPONSORED BY THE
Federal Ministry
of Education
and Research