On the UNICARagil Release Procedure

Measures for Internal and External Risk Communication

EVSAV Workshop, June 5, 2022

Robert Graubohm, TU Braunschweig

SPONSORED BY THE

Federal Ministry of Education and Research
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- (Unpublished) internal release procedures of vehicle manufacturers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)
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)

Conclusive document

Safety case

Release committee (2 Professors)

Release level approved

External audit (TÜV Süd)

Assessment

Release recommendation

Icons: © fotomek – fotolia
The UNICARagil Release Procedure

Technical development

Component documentation (indiv. partners)

Docs

Conclusive document

Safety case

External audit (TÜV Süd)

Assessment

Release recommendation

Release committee (2 Professors)

Release level approved
Release Levels in UNICARagil

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

1. Technical development
2. Component documentation (indiv. partners)
3. Docs
4. Conclusive document
5. Safety case
6. Release committee (2 Professors)
7. Release level approved
8. External audit (TÜV Süd)
9. Assessment
10. Release recommendation

Graubohm: On the UNICARagil Release Procedure, IEEE IV22 EVSAV Workshop

July 14, 2022
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


Graubohm: On the UNICARagil Release Procedure, IEEE IV22 EVSAV Workshop
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.
Vehicle components:
- Dynamics modules
- Battery
- On-board communication networks
- Test driver's seat
- Vehicle structure
- Door

Additional documentation:
- Compliance with integration process
- Successful integration tests
- Description of test sites
- Operating instructions
- Test plan
The UNICARagil Release Procedure

- External audit (TÜV Süd)
- Technical development
- Component documentation (indiv. partners)
- Conclusive document
- Safety case
- Release committee (2 Professors)
- Release level approved
- Assessment
- Release recommendation

Graubohm: On the UNICARagil Release Procedure, IEEE IV22 EVSAV Workshop

July 14, 2022
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

Goal: Absence of unacceptable risk

Addressed uncertainties and risk causes

Safety requirements, safety mechanisms, and safety strategies

Solution (documentation and evidence)
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.
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


SAVE THE DATE

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

May 11, 2023, Aachen
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