




Cite as:

M. Loba, R. Graubohm, and M. Maurer, “Showcasing Automated Vehicle Prototypes: A Collaborative Release Process to Manage and Communicate Risk,” submitted for publication.

BibTeX:

```
@inproceedings{loba_2024,
  author={{Loba}, Marvin and {Graubohm}, Robert and {Maurer}, Markus},
  title={Showcasing {Automated} {Vehicle} {Prototypes}: {A} {Collaborative} {Release} {
    Process} to {Manage} and {Communicate} {Risk}},
  year={2024},
  publisher={submitted for publication}
}
```

# Showcasing Automated Vehicle Prototypes: A Collaborative Release Process to Manage and Communicate Risk\*

Marvin Loba<sup>1</sup>, Robert Graubohm<sup>1</sup>, and Markus Maurer<sup>1</sup>

**Abstract**—The development and deployment of automated vehicles pose major challenges for manufacturers to this day. Whilst central questions, like the issue of ensuring a sufficient level of safety, remain unanswered, prototypes are increasingly finding their way into public traffic in urban areas. Although safety concepts for prototypes are addressed in literature, published work hardly contains any dedicated considerations on a systematic release for their operation. In this paper, we propose an incremental release process for public demonstrations of prototypes’ automated driving functionality. We explicate release process requirements, derive process design decisions, and define stakeholder tasks. Furthermore, we reflect on practical insights gained through implementing the release process as part of the UNICAR*agil* research project, in which four prototypes based on novel vehicle concepts were built and demonstrated to the public. One observation is the improved quality of internal risk communication, achieved by dismantling information asymmetries between stakeholders. Design conflicts are disclosed – providing a contribution to nurture transparency and, thereby, supporting a valid basis for release decisions. We argue that our release process meets two important requirements, as the results suggest its applicability to the domain of automated driving and its scalability to different vehicle concepts and organizational structures.

## I. INTRODUCTION

The widespread introduction of series vehicles equipped with automated driving systems is still pending. Yet, prototypes are gradually finding their way from proving grounds into public traffic. The operation of automated vehicles in the open-world context of urban traffic is always subject to an *inherent risk* that stems from functional and systemic causes, e.g., technical limitations and incomplete requirements. This inherent risk can be reduced but never eliminated [1]. We claim that the unavoidable existence of residual risk also applies to prototypes, which by their very nature are innovative complex systems in which safety is an emergent property.

Unfortunately, prototypes were involved in multiple accidents in previous years, e.g., involving the companies Uber, Pony.AI, or Cruise [2, III.B.]. Recall investigations after a major incident caused by a prototype from Cruise even led to the Department of Motor Vehicles in California suspending the permit for driverless test operation in October 2023 [3]. The (social) media responses following such incidents indicate the need for an open discussion on the level of risk, posed by prototypes’ operation, that is acceptable for society.

Concerning series vehicles providing automatic emergency braking, Homann [4] demanded in 2002 already that an open discussion of risk is held with suitable stakeholders in society before systems are launched on the market (freely translated from the reference to [4] by Maurer [5]). In 2016, Wachenfeld and Winner [6] stated that with the first accident caused by an automated vehicle its release will be questioned, emphasizing that the basis for a release should be designed transparently and discussed by all affected parties. In this paper, with the term “release” we refer to the granting of permission for a specific prototype operation by decision makers within an organization. This does not include certification or type approval granted by regulatory authorities, whose involvement is mandatory in certain countries in order to operate prototypes on public roads.

Challenging the basis for a release resonates with the question of what “safety” actually means. One definition common in the field is the “absence of unreasonable risk” [7, Part 1, 3.132] but Salem *et al.* [8] underpin deviating views stakeholders have on “safety” and “risk.” Regarding conceptual uncertainty, Fleischer [9] argues linguistically. Accordingly, “safety” is a common language concept, usually associated with an intuitive interpretation for each stakeholder and consensual in the expectation that automated vehicles must be “safe.” Implicit understandings may, however, only lead to a superficial consensus on the meaning individuals attribute to “safety,” suggesting that stakeholders also have divergent understandings of “safe” prototype operation. A need arising from this idea is to strengthen the communication between various domain experts involved in developing and deploying prototypes. We claim that a stakeholder-collaborative release process, which guides development, can account for this.

With this paper, we seek to accomplish two goals. First, we aim to stimulate a discussion on the level of safety to be achieved during development. With respect to series vehicles, the debate on defining safety is already underway, e.g., as “hot potato” in the focus field “safety and risk” of the German Round Table for Autonomous Driving [10]. Considering prototypes, we perceive that the debate is currently missing. But we believe that a consensus on the level of reasonable residual risk is a prerequisite for responsible authorities within an organization to be able to make conscientious decisions as to whether a prototype can be released to enter its intended operation, e.g., for demonstration purposes.

Second, we aim to tackle the scarcity of published knowledge on a systematic release of prototypes and provide entities with means to prepare the basis for a release. This includes the disclosure of the risk reduction truly

\*This research was accomplished within the project “UNICAR*agil*” (FKZ 16EMO0285) and is continued within the project “AUTOtech*agil*” (FKZ 01IS22088R). We acknowledge the financial support for both projects by the Federal Ministry of Education and Research of Germany (BMBF).

<sup>1</sup>All authors are with the Institute of Control Engineering at Technische Universität Braunschweig, 38106 Braunschweig, Germany {loba, graubohm, maurer}@ifr.ing.tu-bs.de

achieved by implementation. To this end, we propose a release process that we designed and conducted as part of the research project UNICARagil. Innovative vehicle concepts were examined in the project [11]. Four prototypes (Fig. 1) representing different use cases were developed from scratch and built by a large consortium, with minimal recourse to legacy knowledge and without a fully developed and safety-assured base vehicle. Hence, the prototypes' relied on novel components that lack series integrity. As a result, a systematic release process played a key role to manage and communicate risk. The prototypes were demonstrated in driverless operation on a test track to the public in May 2023, with passengers in three prototypes.



Fig. 1. Prototypes built and demonstrated in the project UNICARagil; left to right: *autoSHUTTLE*, *autoTAXI*, *autoELF*, and *autoCARGO* [11].

It is important to clarify that this paper's focus is not on the definition of appropriate technical and organizational measures to reduce the risk for the prototypes' demonstration. Although the design and realization of the safety concept was driven by the release process and, thus, is also covered in this paper, we do not address the project-specific safety concept in depth. Rather, the safety concept represents one of multiple artifacts that form the basis of a release within the presented process framework, as detailed in section III-C.

In the remainder of this paper, first, we cover related work (section II). Then, we present the release process design and realization in detail (section III). Finally, we reflect on the release process execution, discussing the experience we gained (section IV) before concluding our paper (section V).

## II. RELATED WORK

Since insights on manufacturers' processes underlying series vehicle releases are internal to the organizations and not openly accessible, it is not feasible to orient our release process to series development procedures.

Regarding the release of prototypes a distinction is helpful, as they can exhibit different levels of maturity: On the one hand, more mature prototypes exist that operate at high frequencies in less restricted operating environments and may be considered rather as pre-series vehicles. For instance, prototypes from the company Waymo operate in fleets on public roads in selected North American cities. Waymo explains that "each change of software undergoes a rigorous release process" including simulation, closed-course tests and driving on public roads [12]. However, specific requirements/procedures for moving from testing facilities to on-road testing or omitting safety drivers are not disclosed – and especially release documents are not published.

On the other hand, prototypes in research contexts have been demonstrated in controlled environments for at least 40 years [13], [14]. Literature on such demonstrations mainly deals with technical/organizational measures, i.e., a safety concept, where human controllability acts as central risk mitigation mechanism. Controllability is either supported by actuator interfaces that provide safety drivers with an overruling capability to intervene [15]–[17] or via realizing remote stop systems [18], [19]. However, these references merely allow us to assume that an assessment of the safety concept by a decision maker (whether according implementation results in sufficient risk reduction) served as basis for approving the prototypes' operation. As presented by Nothdurft *et al.* [17] and Bagschik *et al.* [20], this assessment may be supported by an external review of a certification agency. While a reliable safety concept is a key factor for weighing a release decision, the aforementioned references are barely applicable to our work since the publications do not propose a systematic release process for prototypes.

To the best of our knowledge, the only source actually closely related to our work comes from Strauß and Pinke [21]. The authors use the example of a driverless shuttle to illustrate a release process for a specific operational context. Accordingly, the decision of a release authority is based on, among other things, extensive documentation of tests and safety measures. Yet, the authors do not address stakeholders and their interaction in detail, as they are focusing on a high-level release process chronology, the analysis of the intended operation environment, safety analyses, and details on the technical realization of the driverless shuttle prototype. We strongly encourage to get in touch with us if there is any further relevant literature that is missing from our review and helps to resolve the issues outlined in this paper.

## III. DESIGN AND REALIZATION OF A RELEASE PROCESS FOR PROTOTYPE DEMONSTRATION

In this section, we propose the release process designed and implemented in the UNICARagil project. To this end, we address requirements and associated release process design decisions (section III-A). Then, we cover involved actors and the process workflow that results from the design decisions taken (section III-B). Finally, in section III-C, we explain the creation of release modules that provide evidence for systematic risk reduction and, compiled to release documents, serve as a basis for the release for public demonstration.

### A. Requirements and Derived Process Design Decisions

For prototypes in a research project context, we consider

- knowledge asymmetry between different stakeholders,
- parallelism of top-down safety analyses and bottom-up function and component development,
- no developed and safety-assured base vehicle,
- lack of series integrity and partially short service life of novel prototypical components, and
- tension between standard-compliant concept phase activities and ongoing improvement of novel components

as major challenges for both prototype development and the establishment of a release process for their demonstration.

With respect to development processes, one widely known model for developing mechatronic systems is the V-model. While “classic” V-model schemes do not depict an iterative process character, the guideline VDI 2206 points out that several macrocycle runs can be required to achieve the final product [22]. Accordingly, prototypes can represent one kind of intermediate product that results from completing the first development cycles. However, the V-model illustrates a development context for which system-wide requirements are known at the outset and no feedback loops are required [23]. Therefore, we consider following a sequential V-model unsuitable to guide the development of innovative and complex systems. In contrast, the requirement definition for automated vehicle prototypes should be an evolutionary refinement. Hence, the release process shall allow for an agile development approach that promotes iterations in early phases, in which prototypes can be allocated.

The release process design is based on an expert-based requirement elicitation, enriched by experience of all project partners they gained from demonstrations that were successfully carried out in the past. Captured requirements (✓) and related process implications are elaborated as follows:

#### ✓ **Structured & gradual**

To enable a structured process, a strict process chronology with determined, distinct steps is mandatory. We therefore define a process workflow in advance (cf. section III-B). To account for the novelty and complexity of the development objects, we pursue a procedure that restricts the extension of the functional scope tested in operation to small steps. Hence, we foresee an incremental release, i.e., a plan for successive release stages oriented to the specified integration plan of the prototypes. Each stage definition (see *Tabelle I*) is linked to conditions under which the prototypes are allowed to operate after a release is granted.

TABLE I  
DEFINITION OF INCREMENTAL RELEASE STAGES.

Release stage <i>Operating mode*</i>	Detailed description of release stage
Stage 1 <i>Manual Operation</i>	Manual controlled rides on test sites with speeds of up to approximately 5 km/h
Stage 2 <i>Manual Operation</i>	Manual controlled rides on test sites
Stage 3 <i>Automated Operation</i>	Testing of (automated driving) functions that require safety drivers as a fallback level in a controlled environment
Stage 4 <i>Automated Operation</i>	Testing the demonstration without access for guests
Stage 5 <i>Automated Operation</i>	Public demonstration on a test track

\*The operating modes “Manual Operation” and “Automated Operation” are discussed with respect to the project context by Jatzkowski *et al.* [24].

#### ✓ **Documented**

We find that the process must document both risk and risk mitigation measures comprehensively. To obtain a reliable

basis for release approval, i.e., the assessment of reasonable residual risk by an appointed committee, we introduce the concept of profound “release documents.” Yet, to ensure safety, the prototype release approval is based both on appropriate documentation within the release documents and on the appraisal of actual “readiness” of the prototypes.

#### ✓ **Measurable**

Guaranteeing a coordinated process execution that targets systematic risk reduction constitutes another process requirement. All project participants must understand and bring about the prerequisites for “safe” operation. Maintaining a binding nature of the process by adhering to initial agreements is a decisive factor in achieving this goal. Thus, we attune compositions of “release modules” for each release stage in the concept phase of prototype development already. These modules represent documented development evidence and form the building blocks of conclusive release documents. A variety of system-wide and component-level release modules are designated in the compositions (cf. section III-C). With a predefined composition of modules, we aim to foster measurability, as lack of progress can be traced back to explicit root issues hindering release for the next stage.

#### ✓ **Accountability-driven**

Accountability is considered highly relevant to promote diligence and clarify on responsibility and, thereby, contribute to adherence to the schedule. Accordingly, roles and associated tasks need to be defined unambiguously. We encourage accountability in the process by assigning specific design and test documentation obligations on component level to individual function developers. Beyond that, function developers need to actively release the components assigned to them. These documented component releases are included as modules in release documents for the aspired release stage.

#### ✓ **Compliant & harmonized**

We strive for a process that reflects the state of the art. On the one hand, this means that the release process shall follow a thorough *Safety-by-design* paradigm. A Safety-by-Design paradigm reflects a strong focus on dealing with safety requirements, involving the conduction of hazard analyses and specification of technical solutions that meet defined safety goals at an early stage. This contrasts with the assumption that extensive testing after product development would be sufficient to guarantee safety. Hence, a focus lies on harmonizing ongoing function development on component level, which is partially rooted in early assumptions that are recorded in initial work products (Orange boxes in Fig. 2), and refined safety requirements on system level, which evolve from continuous system-wide safety analyses.

On the other hand, this refers to the application of standards in the field, e.g., vehicle-wide hazard analyses are guided by processes of the safety standards ISO 26262 [7] and ISO 21448 [25]. External supervision supports compliance and increases confidence in the safety assurance activities. Consequently, the process involves an independent certification agency with competence for respective audits evaluating the compliance with these standards.





The development based thereon is followed by (sub-)system integration and test case execution. As indicated by a “rationale” element, the currently approved release stage determines permissible test operation conditions. After testing, function developers describe the implementation and submit the related documentation to the safety engineers.

Parallel to the function developers’ activities, vehicle-wide safety analyses are continued by the safety engineers. These analyses allow to concretize the safety concept and associated work products continuously, resulting in an evolving safety documentation. The generation of underlying release modules is detailed in section III-C. The refined safety concept acts as a basis for evaluating the ongoing implementation. Safety engineers examine the implementation documentation at component level that is provided by the function developers. They check if sufficient proof is furnished that defined safety requirements served as basis of implementation and that those requirements are verified by testing. If a mismatch, i.e., deficient requirement fulfillment, is revealed, function developers are mandated to review their documentation and implementation. Otherwise, function developers issue a component release, contributing to the aggregated components release documentation.

The certification agency collaborates with both the function developers (“*Accompany Tests*”) and safety engineers (“*Review Safety Assurance Activities*”). The agency’s recommendation for or against a release is captured in a review documentation that is also included in the release documents.

When a release document is compiled, it can be reviewed by a release committee. Depending on an assessment of the residual risk, this committee decides whether a release can be issued for the targeted release stage and the associated operating conditions. Approval of the final release stage ends the process by permitting the demonstration. Previous release stages address the use of the prototypes throughout advancing prototype construction and testing of their automated driving functionality, as illustrated in [Tabelle I](#).

### C. Evidence for the Prototypes’ Safety Assurance

Fig. 3 shows the schematic release document composition for public demonstration and one of the UNICARagil prototypes named *autoELF*. There are two main aggregation points for a multitude of release modules, with the relationship modeled by logical aggregation ( $\text{—}\diamond$ ). The first is the system-wide safety documentation and the second is the components release documentation, contributed by safety engineers and function developers, respectively.

#### System-wide safety documentation

As indicated by the generalization relationship ( $\text{—}\triangleright$ ), except for the operating instructions, all release modules contributing to the system-wide documentation can be associated with matching ISO 26262 work products (highlighted in italics in this paragraph): A *safety plan* (cf. [7, Part 2, 6.4.6]) functions as coordination instrument for the safety assurance activities. A system description (*item definition*, cf. [7, Part 3, 5]) allows to perform the *hazard analysis and risk assessment* (cf. [7, Part 3, 6]). Functional safety requirements are derived from

resulting safety goals and captured in the *functional safety concept* (cf. [7, Part 3, 7]). Technical safety requirements can be elicited and allocated to components that need to fulfill these requirements. The associated *technical safety concept* (cf. [7, Part 4, 6]) comprises the technical safety requirements and enables to deduce test cases systematically (cf. [7, Part 4, 7–8]). Based on all of the previously explained work products, a *safety case* (cf. [7, Part 2, 6.4.8]) is prepared, with the absence of unreasonable risk being the top-level claim, backed by a structured argument about how the gathered development evidence supports this claim.

When it comes to identifying hazards, an approach to conduct the initial hazard identification was developed in the project context by Graubohm *et al.* [27]. Considering vehicle dynamic and boarding scenarios representative for the intended operational scope was decisive in order to identify hazards. Coupling these representative operational scenarios with possible component malfunctions enabled us to derive hazardous scenarios and assess the associated risk.

In order to assess this risk, we introduced the concept of RSIL (Research Safety Integrity Level, see [Tabelle II](#)), targeting a qualitative delimitation of levels that constitute the risk potential of hazardous scenarios. This classification aims to provide an indicator of the “priority” with which hazardous scenarios, respectively safety requirements derived from them, need to be addressed by development effort during implementation. The underlying assumption is that conscientious development according to the categorization results in an overall risk reduction to a reasonable threshold. As series integrity cannot be assumed for the prototype realization in the project, no list of prescribed methods for dealing with systematic faults, e.g., with regard to testing hardware and software, or random hardware faults, e.g., permissible failure rates, are linked to the RSILs, in contrast to ASIL (Automotive Safety Integrity Level [7, Part 1, 3.6]) recommendations provided by the ISO 26262 standard.

TABLE II  
DEFINITION OF RESEARCH SAFETY INTEGRITY LEVELS.

RSIL	Definition of the respective RSIL	ASIL Reference
RSIL 0	A conscientious execution of safety assurance activities is considered sufficient to control the risk. There is no need for additional measures.	QM
RSIL 1	Risk is classified as <i>very low</i> . Appropriate technical or organizational measures must be defined, implemented, and tested to address the risk.	ASIL A
RSIL 2	Risk is classified as <i>low</i> . Appropriate technical or organizational measures must be defined, implemented, and tested to address the risk.	ASIL B
RSIL 3	Risk is classified as <i>high</i> . Appropriate technical or organizational measures must be defined, implemented, and tested to address the risk.	ASIL C
RSIL 4	Risk is classified as <i>very high</i> . Appropriate technical or organizational measures must be defined, implemented, and tested to address the risk.	ASIL D

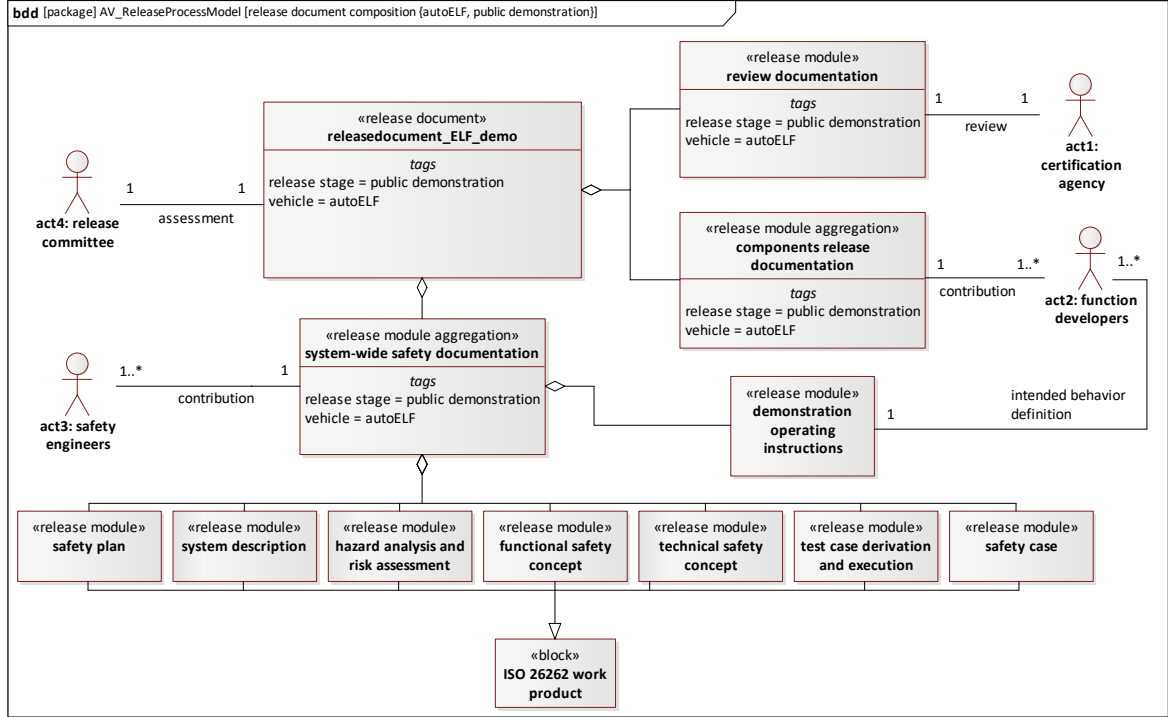


Fig. 3. SysML block definition diagram representing an exemplary release document composition (release stage: public demonstration, prototype: *autoELF*).

Regarding the safety concept, Stolte *et al.* [28] discuss the linking of identified hazards and emerging safety goals with project-specific safety mechanisms in detail. It is worth mentioning that prototypical safety functions that were investigated in the project, such as the function “safe halt,” (cf. [29]) implemented for demonstration purposes, could not contribute to the safety concept. On the contrary, these functions had to be considered as causes of malfunctioning behavior, possibly leading to additional safety requirements.

From a technical perspective, the safety concept in the project relied heavily on redundancies and fallback strategies in case of undesirable component behavior. Defining organizational measures to deal with safety requirements is highly important for prototypical on-road testing and demonstrating in a controlled environment, as it partially accounts for the lack of component integrity. Examples for organizational measures correspond to controlling the operational design domain, for instance via the definition of possible encounter traffic or preventing access of external persons to the driving corridors of the prototypes. Additionally, one instrument we found to be essential for the design of a resilient safety concept in the project was a “safety watch.” A radio emergency stop system allowed human track marshals to stop a prototype immediately. Besides functional requirements, non-functional aspects like mechanical safety or electromagnetic compatibility were also addressed in the safety concept. Relevant test cases for the verification and validation of safety requirements involved simulation as well as executing fault injection and demonstration scenario tests.

Complementary to the safety concept, operating instructions for testing and demonstration were prepared, con-

taining, e.g., detailed descriptions of (incident) procedures and roles. With the operating instructions, we aimed to reasonably calibrate the trade-off between demonstration scope, e.g., complexity of the demonstrated functionality, and risk for operation. The instructions included the routes for the prototypes’ demonstrations, which were planned based on an assessment of the prototypes’ capabilities and limitations.

#### Components release documentation

On the function developers’ side, various release modules had to be contributed at the component level. As an example, for release stages requiring automated operation developers had to document component releases for environment perception, behavior planning, and motion control. These and other modules shown in Fig. 4 represent functional architecture elements common in a sense-plan-act control scheme and, thus, were deemed necessary for releasing prototypes and using them in automated operation mode.

Besides component releases for shared components, prototype-specific components and functions led to differentiated compositions for the respective release documents. For instance, the *autoELF* was designed to provide the use case of an autonomous family vehicle. To achieve the necessary accessibility for impaired and/or older family members, the prototype *autoELF* was equipped with (an actuated) lift platform that allowed for boarding the *autoELF* barrier-free. Hence, the release module “boarding assistance (lift)” was required from the developers to compile the components release documentation for the prototype *autoELF* – as can be seen in Fig. 4 for the release stage *public demonstration*.

Correspondingly, the composition of release modules primarily resulted from architectural considerations with respect

to the functions required for the prototype operation that was foreseen for the release stage. Component release documents were based on a project-wide template to nurture consistency and coherence of the function developers' documentation. Accordingly, function developers had to describe the component's functions including their interfaces and subsystem boundaries, implemented fallback mechanisms, and known limitations. Also, developers had to clarify on hazards caused by the component, safety-relevant component requirements, and derived mitigation strategies. Furthermore, component level tests had to be recorded. Traceability between top-down and bottom-up considerations was fostered, as the technical safety concept explicitly linked technical safety requirements to the corresponding component release documentation.

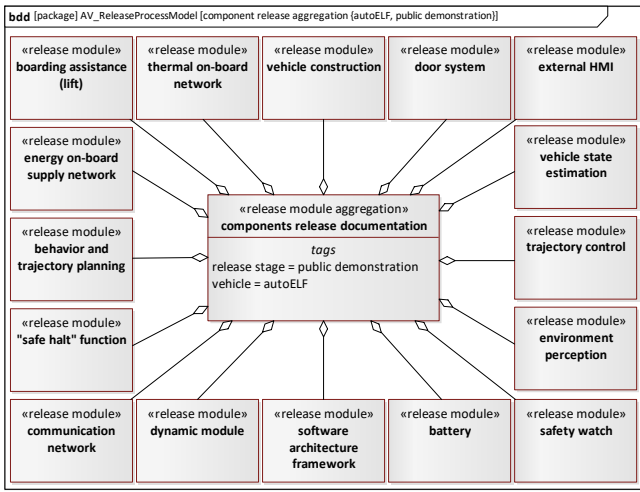


Fig. 4. SysML block definition diagram representing the composition of an example component release documentation by various release modules (release stage: public demonstration, prototype: *autoELF*).

#### IV. DISCUSSION

Operationalizing the release process in a specific project context led to valuable insights. We observed that assigning documentation obligations promoted accountability and timely contributions. This was vital because there is a strong dependency of the release progress on the contributions provided by function developers: If component releases were pending, release documents could not be compiled and operation according to the next release stage was prevented.

While the prototypes were largely based on the same architecture and shared platforms, they also featured individual functions. The presented process takes these differences into account, in particular via the modularity provided by prototype-specific compositions of required component releases. The successful process execution suggests not only the general applicability of the process, but also the potential of scalability of a common process for the systematic release of prototypes, even if they are based on diverse concepts.

The release process led to increased transparency. We dispelled knowledge asymmetries concerning performance limitations and the implementation status. Harmonization documents like operating instructions promoted internal communication quality, as they served as drivers of design

decisions both for the development and the demonstration setting. Although posing a burden to developers, extensive documentation enabled close monitoring of the safety concept's realization, allowing us to reveal potential deficits in advance and impede realizing design decisions based thereon that could have led to hazardous prototype behavior. So, while preparing a release decision by disclosing the risk reduction actually achieved by implementation was the main goal when conceptualizing the release process, sensitizing the developers to safety-relevant considerations also had a risk-reducing effect during prototype development.

Project partners, who focused on function development or on system safety respectively, worked closely together to ensure the fulfillment of safety requirements. This close collaboration revealed, among other things, that developers of specific domains might have divergent understandings when considering "safety" in an implementation context. Thereby, the process highlighted the relevance of a debate about the definition of "safety" but also could show that a process tailored to nurture internal communication contributes to the harmonization of stakeholder-individual understandings.

Involving a certification agency added great value. The feedback on accompanied tests and the review of evidence we provided increased overall confidence in the safety measures. Our system-wide safety analyses were found to align with established standards and processes to an adequate degree. Yet, although a release recommendation represents an indicator for appropriate measures taken to reduce risk, an external assessment should not be the sole reason for release. Release documents must still be thoroughly reviewed<sup>3</sup> by the release committee to avoid potential confirmation bias.

We encountered a trade-off in defining release modules that are required for a release stage. A demand too great slows down development progress since more effort, which is required to release prototypes in an early phase, leads to delayed testing of new functions. If the demand is too low, the release process fails to serve its purpose. Release documents will then provide insufficient evidence that adequate risk-reducing mechanisms have been implemented and tested. One approach that has proven helpful is to consult the system architecture to aid the determination of functional components required for the operation in question. However, ways to establish traceability between release modules and a prototype's architecture are still subject to our research. In our future work, we intend to investigate following questions:

- To what extent can formerly released components be reused in a related context, i.e., how to deal with legacy release documentation/implementation?
- During operation, what triggers call an already-granted release on component or vehicle level into question?
- How do we, aided by architectural considerations, promote the tracing of triggers to affected release modules?
- What are suitable means of representing the risk potential of hazardous scenarios in a research context?

<sup>3</sup>The process execution in the project yielded around 700 pages long release documents per prototype for the public demonstration.



- What are consequences of system modifications for the prototype operation formerly approved?
- How to prepare requirements and test cases to have advanced knowledge about necessary regression tests?

## V. CONCLUSION

While automated vehicle prototypes are already operating in urban environments on a daily basis, there is hardly any literature on a systematic release for prototypes. Based on our experience from the project UNICARagil, we aim to narrow this gap. Hence, we presented a release process for prototypes' demonstration that involves coordinated stakeholder collaboration. The process follows a Safety-by-Design paradigm and targets challenges of prototype development and deployment in a research context.

In this paper, we argued the suitability of the process to reveal the achieved risk reduction. According to gained knowledge, we deem coherent release documents, enriched by all actors and prepared adequately, as an appropriate basis for a prototype release decision. It became apparent that a close supervision of function development by safety engineers helps uncover deficits and design conflicts.

The process execution has shown that a common understanding of "safety" among all those involved in development supports the release of prototypes. While the release process poses a procedural framework to prepare the basis for a release and drive the development process in a safety-oriented manner, release parties also must be able to deduce when they can assess residual risk exposed in release documents as tolerable. Thus, there is a need to lead a debate on the safety level during development (i.e., for the use of prototypes) which we want to initiate with this paper. As part of the AUTotech.agil project, we will investigate the stated research needs and aim to advance the presented process.

We thank Sonja Luther and Niklas Braun for proofreading, Torben Stolte for his contributions to the presented work, and Udo Steiniger for his valuable input in the course of a contracted review of the safety concept in the project.

## REFERENCES

- [1] M. Maurer, "Elektronische Fahrzeugsysteme – Jahresbericht: Akademisches Jahr 2017/2018," Tech. Rep., Ed.: Gerrit Bagschik.
- [2] M. Wansley, "Regulating driving automation safety," *Emory Law Journal*, vol. 73, 2024.
- [3] California State Transportation Agency – Department of Motor Vehicles, *Order of Suspension (Cruise LLC)*, [Online]. Available: <https://s3.documentcloud.org/documents/24080715/gm-cruise-order-of-suspension-driverless-testing.pdf>, 2023.
- [4] K. Homann, *Wirtschaft und gesellschaftliche Akzeptanz: Fahrerassistenzsysteme auf dem Prüfstand*, Presentation, Uni-DAS e.V. Workshop Fahrerassistenz, Walting, Germany, 2002.
- [5] M. Maurer, "Elektronische Fahrzeugsysteme – Jahresbericht: Akademisches Jahr 2017/2018," Tech. Rep., Ed.: Inga Jatzkowski.
- [6] W. Wachenfeld and H. Winner, "The Release of Autonomous Vehicles," in *Autonomous driving: Technical, legal social aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 425–449. DOI: 10.1007/978-3-662-48847-8\_21.
- [7] *Road vehicles — Functional safety*, International Organization for Standardization Standard 26262, 2018.
- [8] N. F. Salem *et al.*, "Safety and Risk – Why Their Definitions Matter," in *Handbook Assisted Automated Driving*, Winner, Hermann, and Dietmayer, Klaus and Eckstein, Lutz and Jipp, Meike and Maurer, Markus and Stiller, Christoph, Ed., 4th ed., unpublished, Wiesbaden, Germany: Springer Vieweg.
- [9] T. Fleischer, *Safety and Acceptance — A View of Two Mysteries*, Presentation, Oberseminar IfR Braunschweig, virtual, 2023.
- [10] M. Maurer, *Das inhärente Risiko autonomer Straßenfahrzeuge*, Presentation, Braunschweig Mobility Days – Autonom und Digital, Fachtagung »Autonomes Fahren und Stadtstruktur«, Braunschweig, Germany, 2023.
- [11] R. van Kempen *et al.*, "AUTotech.agil: Architecture and Technologies for Orchestrating Automotive Agility," in *32nd Aachen Colloq. Sustain. Mobility*, 2021, pp. 1–49. DOI: 10.18154/RWTH-2023-09783.
- [12] Waymo LLC, "Waymo Safety Report," Tech. Rep., 2021.
- [13] E. Dickmanns and A. Zapp, "Autonomous High Speed Road Vehicle Guidance by Computer Vision," *IFAC Proceedings Volumes*, vol. 20, no. 5, Part 4, pp. 221–226, 1987, 10th Triennial IFAC Congress on Automatic Control - 1987 Volume IV, Munich, Germany.
- [14] C. Thorpe, M. Hebert, T. Kanade, and S. Shafer, "Vision and Navigation for the Carnegie-Mellon Navlab," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 10, no. 3, pp. 362–373, 1988.
- [15] C. Thorpe, T. Jochem, and D. Pomerleau, "Automated Highways and the Free Agent Demonstration," in *Robot. Res. Y. Shirai and S. Hirose, Eds.*, London: Springer London, 1998, pp. 246–254. DOI: 10.1007/978-1-4471-1580-9\_23.
- [16] J. Ziegler *et al.*, "Making Bertha Drive—An Autonomous Journey on a Historic Route," *IEEE Intelligent Transportation Systems Magazine*, vol. 6, no. 2, pp. 8–20, 2014. DOI: 10.1109/MITS.2014.2306552.
- [17] T. Nothdurft *et al.*, "Stadtпилот: First fully autonomous test drives in urban traffic," in *14th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Washington, DC, USA: IEEE, 2011, pp. 919–924. DOI: 10.1109/ITSC.2011.6082883.
- [18] A. Broggi *et al.*, "Extensive Tests of Autonomous Driving Technologies," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 3, 2013. DOI: 10.1109/TITS.2013.2262331.
- [19] Q. Jan and K. Berns, "Safety-configuration of Autonomous Bus in Pedestrian Zone," in *Proc. 7th Int. Conf. Veh. Technol. Intell. Transport Syst.*, 2021. DOI: 10.5220/0010526106980705.
- [20] G. Bagschik, M. Steimle, T. Stolte, and M. Maurer, "Afas – Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Bundesautobahnen: AP2 – Final Report," Tech. Rep., 2019. DOI: 10.2314/GBV:1662494076.
- [21] M. Strauß and C. Pinke, "A Pragmatic Approach to Safe Operation for Driverless Shuttles During Development," in *27th Int. Technical Conf. Enhanced Saf. Veh.*, 2023.
- [22] *Design methodology for mechatronic systems*, VDI Guideline 2206, Verein Deutscher Ingenieure, Düsseldorf, Germany, 2004.
- [23] J. Schäuffele and T. Zurawka, *Automotive Software Engineering*. Warrendale, PA, USA: SAE Int., 2016.
- [24] I. Jatzkowski *et al.*, "Integration of a Vehicle Operating Mode Management into UNICARagil's Automotive Service-oriented Software Architecture," in *30th Aachen Colloq. Sustain. Mobility*, Aachen, Germany, 2021, pp. 595–614. DOI: 10.24355/dbbs.084-202110271613-0.
- [25] *Road vehicles — Safety of the intended functionality*, International Organization for Standardization Standard 21448, 2022.
- [26] N. F. Salem *et al.*, "Risk Management Core—Toward an Explicit Representation of Risk in Automated Driving," *IEEE Access*, vol. 12, 2024. DOI: 10.1109/ACCESS.2024.3372860.
- [27] R. Graubohm, T. Stolte, G. Bagschik, and M. Maurer, "Towards Efficient Hazard Identification in the Concept Phase of Driverless Vehicle Development," in *IEEE Intell. Veh. Symp. (IV)*, Las Vegas, NV, USA: IEEE, 2020, pp. 1297–1304. DOI: 10.1109/IV47402.2020.9304780.
- [28] T. Stolte *et al.*, "Towards Safety Concepts for Automated Vehicles by the Example of the Project UNICARagil," in *29th Aachen Colloq. Sustain. Mobility*, 2020, pp. 1561–1594. DOI: 10.24355/dbbs.084-202011171557-0.
- [29] S. Ackermann, "Safe Halt as Fail-safe Concept for Automated Driving Systems," Ph.D. dissertation, Technische Universität Darmstadt, Darmstadt, Germany, 2023.