

A PRAGMATIC APPROACH TO SAFE OPERATION FOR DRIVERLESS SHUTTLES DURING DEVELOPMENT

Matthias Strauß

Christopher Pinke

Continental Autonomous Mobility Germany GmbH
Germany

Danilo da Costa Ribeiro

Wolfgang Schramm

Continental Autonomous Technologies GmbH
Germany

Paper Number 23-0072

ABSTRACT

Driverless shuttles are a modern vehicle platform designed to operate autonomously, constituting a very promising building block of future mobility solutions. At Continental, there is a long experience with these types of vehicles. In this paper, some of this experience regarding operating such vehicles during development is shared. In particular, the focus is on how a safe operation can always be ensured. To this end, a release process for such an operation, how a pragmatic safety assessment can be done and some of the peculiarities of driverless shuttles are presented.

INTRODUCTION

With recent technological advances, fully autonomous vehicles become more and more realistic. Driverless shuttles, aiming at SAE L4 autonomy, are expected to be one of the major pillars of future mobility and an ideal entry point for fully autonomous mobility solutions.

The absence of a human driver in the chain-of-effects of L4 systems changes the demands on the actual vehicle architecture and layout. Driverless shuttles, see Figure 1, are consequently designed for driverless operation without traditional instrumentation like brake pedal or steering wheel. Comparable in capacity to a small bus, the shuttles are normally capable to drive at lower speeds of up to 20 kph and are operated in private or sub-urban areas, providing first and last mile services. Notwithstanding this restricted operational design domain (ODD), they complement existing mobility solutions like taxis, busses, or trains, especially when operated in an on-demand service. Hence, shuttle systems are an ideal candidate to introduce driverless systems to a wider usage. For more information, please refer to [1], [2], or [3].



Figure 1. A driverless shuttle, developed during the CUBE activities at Continental.

Currently, driverless shuttles are operated predominantly in pilot applications. Direct feedback is retrieved from users of the service at this early stage. For recent examples see [4], [5], or [6]. In parallel, the technology matures as more and more field experience is collected. Continental has a long and successful history connected to driverless shuttles. Within the Continental Urban Mobility Experience (CUBE) activities such systems are developed and operated in Germany, USA, China, and Japan. This includes operations on public roads in mixed traffic and even pedestrian zones. Here, a deep understanding of the specifics of driverless shuttle systems has been developed, especially regarding their safety aspects and how such systems can be released for an intended use. See e.g. [7], [8], [9] as well as [10] for more information.

While established manufacturers like EasyMile [11] and Navya [12] already have a certain market penetration, recently more and more companies have focused on driverless shuttles, e.g. Zoox [13], Cruise [14] or ZF [15]. However, compared to traditional automotive business, existing shuttle systems are typically not automotive grade yet and are built on smaller scales. In addition, most deployments still require a safety operator to be on board as the technology itself is not yet capable of operating without human supervision, although this is obviously the major focus of development of shuttle manufacturers.

Due to the non-traditional design of the shuttles, also the development of such vehicles varies in some aspect from traditional vehicles. Any driverless system must fulfill the highest safety standards as a human is not available anymore as a fallback level. Established safety analysis methods like HARA [16] and FMEA [17] are often not sufficient for analyzing such complex systems.

Addressing this gap, we would like to share our approach and our insights in the field of driverless shuttles to benefit the development of safe and reliable driverless shuttle solutions. In this paper, we present a pragmatic approach regarding the safety argumentation of prototypes for driverless shuttles. The intent is to provide a general viewpoint on this topic which can serve as a guideline for the safe development and operation of such systems.

To this end, we present a generic shuttle architecture and investigate which effects the failures of the various system components can have, up to a level that is relevant for a development prototype. We expand this generic view by providing insights into a concrete prototype implementation in one of our CUBE vehicles, covering brake, battery, and steering components as well as the full chain-of-effect of autonomous driving. We elucidate measures to fulfill safety requirements based of the safety analysis.

This analysis can serve as a predecessor for more sophisticated and established methods mentioned above while enabling the operation of the prototype in a safe manner.

A RELEASE PROCESS FOR DRIVERLESS VEHICLES DURING DEVELOPMENT

Central part of operating a prototype vehicle is a defined release process. This process can vary depending on the specific development of interest. For the development of driverless shuttles, or more general highly automated vehicles, the process must cover the assessment and acceptance of all hazards posed by the system of interest, especially when trialing and operating in a public environment.

In recent years, driverless vehicle trials have been based solely on exception permits. Only recently, the worldwide first L4 law has been passed in Germany, see [18], [19], or [20], providing a solid legal basis for the development and homologation of L4 systems. However, for the application of said law in actual development activities, details still must be clarified, see [21].

The major steps of such a release process are depicted in Figure 2, following a corresponding Continental internal prototype process. It involves the clear definition of the system of interest and its intended usage, the thorough analysis of said usage and finally the approval of the intended usage. All of these steps are based on various assessment results. This process was applied during the CUBE activities and will be the frame of the content presented in the subsequent chapters.

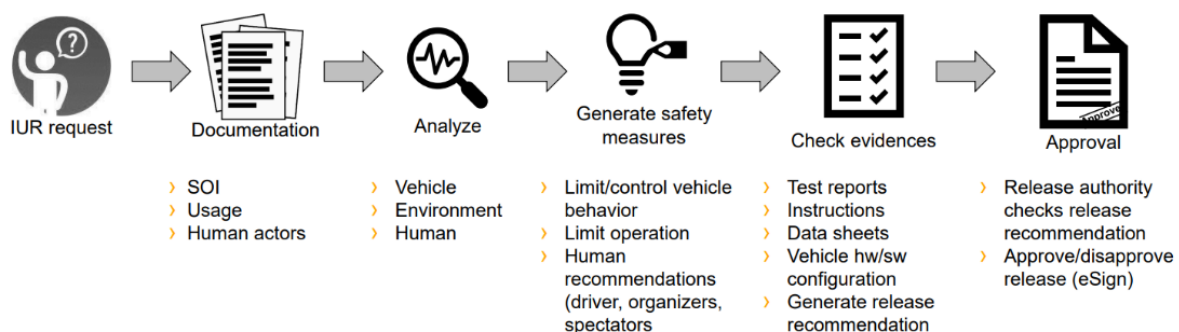


Figure 2. Exemplary Process for an intended usage release (IUR), showing the major steps towards a safe operation of the prototype vehicle.

ANALYSIS OF THE INTENDED OPERATION

An important building block to release a development system is the description of the system of interest and the intended operation. For the latter, the following topics need to be analyzed:

- System environment:
 - o What is the operational environment or domain in which the system is being used?
 - o What are the actors involved and what are their respective roles?
- System context:
 - o With which people or systems does the system interact or exchange information?
- System behavior
 - o What is the intended system behavior...
 - ...within the environment and with respect to the other traffic participants?
 - ...with respect to user interaction?

In the following, the analysis of the operational environment is limited to the intended route to keep the problem space manageable. Using modern satellite or aerial pictures, digital maps, on-site inspections, and similar data sources, valuable information about the road topology, expectable traffic participants and constraints to the operation are gathered. This information allows to split the route into smaller sections, like connecting roads and intersections or other areas of interest. This creates a sort of scenario catalogue of the intended operation. An example is given in Figure 3.



Figure 3. Aerial picture of a route (green), including route detail and extracted relevant scenario. Material taken from <https://geoportal.frankfurt.de/>.

Scenes and situations outside the route are not considered at this stage and are not part of the immediate challenge at hand.

Complexity within the operational environment and the shuttle's system functionality can be increased over time as the development of the shuttle system continues. This includes certain limitations the system has at a certain point in time. To challenge these limitations, it is then up to the development team to align on the appropriate measures. This is done together with the security and safety experts and risk owners. Measures can be manifold, e.g., performance limitations, additional supportive helping systems, external systems, or even organizational measures.

The work results from the Pegasus Project [22] are respected and considered for analysis of the operational environment and systematic identification of scenes and scenarios. One can describe the operational environment and the ODD in close alignment to the ASAM OpenX Standards [23], especially OpenDrive and

OpenScenario as well as ISO 34502 [24]. This can be done via the proposed six-layer model as described in the Pegasus Method [22]:

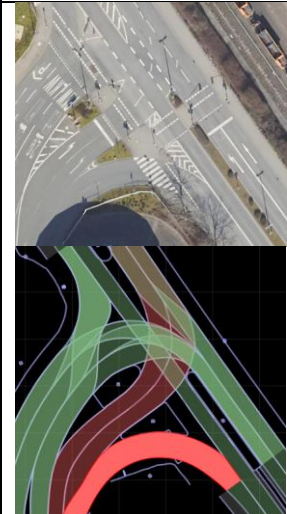
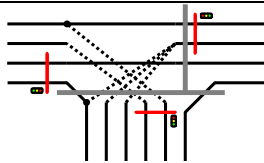
- Layer 1: Street Layer
- Layer 2: Traffic Infrastructure
- Layer 3: Temporal Modifications
- Layer 4: Moveable Objects
- Layer 5: Environment Condition
- Layer 6: Data and communication

and by abstracting the level of detail for scenario descriptions into functional, abstract, logical, and concrete scenarios.

Structuring the environment analysis into these layers helps to focus on certain topics in the team discussions with the safety engineers and the function experts. To simplify the problem space further, the route where the shuttle will be operated is sliced into smaller segments. This allows systematical identification of the road topology (Layer 1), whether the system needs to support perception of traffic infrastructure, like Traffic Signs or Traffic Lights, (Layer 2), or if there are temporal modifications like construction sites at the time of the intended operation (Layer 3). The segments are analyzed and provided to the team in form of a story board table with some easy understandable annotations.

An exemplary simplified description of one road-segment of the route storyboard from Figure 3 is shown in Table 1. With this information, the function designers, security, and safety engineers can identify hazards and hazardous situations according to the intended use. From these results, potential safety measures are derived to ensure a safe operation. These might include instructions for the safety operator, limiting the system performance, providing external support for the safety operator, controlling the environment, or others. This is described in more detail below.

Table 1.
Route-Storyboard element example

Scene and Layout	Maneuvers, Activities and Abilities	Topology and Objects	Traffic Participants
	Follow Lane: <ul style="list-style-type: none"> - Straight - Curve Stop at crosswalk Stop at stop line Follow preceding vehicle Perceive traffic light (and status) Detect TPOs (other vehicles and VRUs) TPO prediction	 Traffic sign Traffic light Crosswalk	Cars Buses Trucks Motorcycles Cyclists Pedestrians

SAFETY MANAGEMENT SYSTEM

The complexity and novelty constituted by highly automated vehicles requires more than just the functional safety analysis well established in the automotive industry. With the goal to ensure a high level of safety, not only at the development phase, but also during the vehicle's entire lifecycle a Safety Management System (SMS) was established, following [25]. Figure 4 shows an overview of the SMS in operation.

As can be seen in Figure 4, the SMS was designed to cover all the phases of the Safety Assessment activities from the development phase (starting after the system definition until the entry-into-service – EIS) until the product's end of life. According to the SMS Framework proposed by International Civil Aviation Organization (ICAO) and used widely at the aviation industry [25], the SMS has four main pillars/components: Safety Policy, Safety Risk Management, Safety Assurance and Safety Promotion. The scope of this paper is the development

activity, not the organization. Therefore, special attention will be given to Safety Risk Management and Safety Assurance only and these two components are described below in more detail.

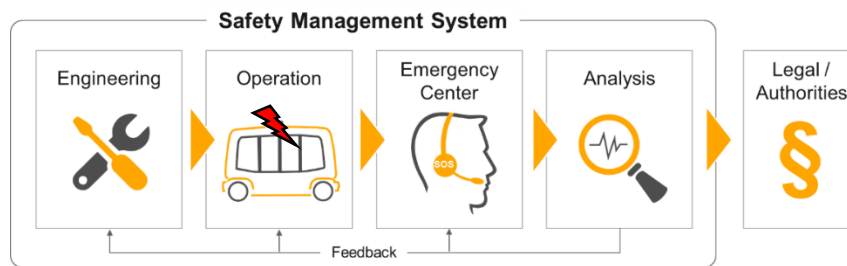


Figure 4. Overview of Safety Management System

Safety Risk Management

This SMS component’s activities take place before the entry-into-service and are responsible to ensure that the operation is safe enough to start. When the operational concept is ready, the safety analysis has the required inputs and can be carried out. It includes a top-down and a bottom-up approach.

The top-down approach is a hazard-centric analysis based on the System-Theoretic Process Analysis (STPA) [26]. This, after assessing the operation, defines the accidents (or losses, as denoted in the context of STPA) and hazards present and search for causal factors. Those could not only be triggered by technical reasons, but also from human/systems interface and specification/performance insufficiencies. Figure 5 provides a more detailed overview of the Safety causality chain used in the safety assessment.

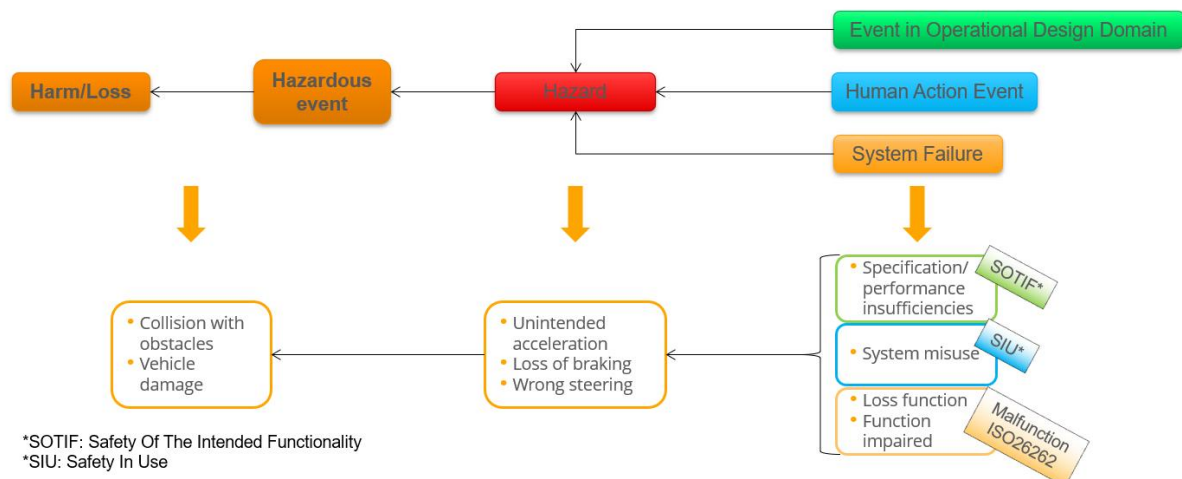


Figure 5. Safety causality chain used during safety assessment.

For the scope of this paper and the generic architecture described below, a simplified bottom-up approach called “Component Failure and Effect Analysis” (CFEA) is presented. It is based on the Failure Modes and Effects Analysis (FMEA) method [17] and, as the name says, has the goal to identify the effects of some critical component failures. In this pragmatic way, however, various insights about driverless systems can already be collected. Especially, it can be applied nicely to prototype systems such as the one presented below.

After defining the causal factors for every hazard, a set of safety requirements is defined, implemented, and verified.

Safety Assurance

Considering the operation of highly automated vehicles contains a high number of unknown (and possibly unsafe) scenarios, see ISO 21448 [27], a special focus was given to the safety assurance part of the SMS. Support is provided to the people involved in the operation facing an unexpected situation, but also to learn from mistakes.

This was achieved through the establishment of an Emergency Response Plan. It created a communication channel from the people involved in the operation to an emergency team that could support and give instructions anytime. It was not limited to operators and vehicle occupants, but also applying to vulnerable road users. Additionally, any safety-critical event would be registered in a database, enabling the engineering team to mitigate any issue that caused this event. The safety assessment can then be updated, and the previously unknown hazard is now mitigated.

GENERIC DRIVERLESS SHUTTLE ARCHITECTURE

Having outlined the steps towards the operation of driverless shuttle prototypes, the basic vehicle architecture of driverless shuttles will be presented in a generic way in the following. The focus will be on the elements related to driving only, excluding higher-level functionality like environment perception or human machine interaction (HMI). The architecture consists of several key elements which are independent of the specific type and model. This is depicted in Figure 6.

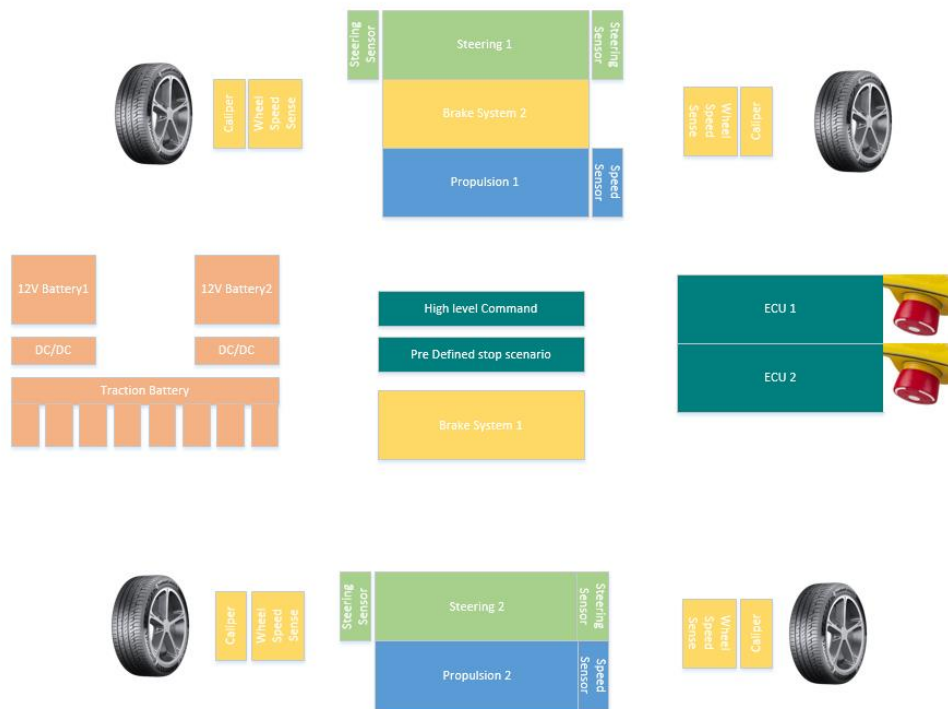


Figure 6. Generic Architecture of driverless shuttles

Obviously, most of the elements are the same as in traditional automobiles. However, without a human in the loop, there are different requirements regarding fallback levels, e.g., the redundant layout of the ECUs. Also, the supervision of the proper functionality of each element must be automatized as well. In addition, certain components must be redundant, e.g., the brake system. A somewhat special case are the emergency buttons installed inside the vehicle. They allow the passengers to trigger a Minimum Risk Maneuver in case of an emergency that the vehicle did not recognize (a so-called Emergency Stop or E-Stop).

In general, each element in the architecture can fail because of four distinct reasons: Loss of power supply, loss of communication, internal failure (mechanical or electrical), as well as a wrong action or command send to the element. Any failure of one element can induce other failures or complications in the system. Hence, the driverless system must be realized such that in each failure case for any key element, it is ensured that the vehicle reaches a safe state. For currently available commercial systems and in particular for prototype systems, it is very likely that the system cannot recover from that failure. In that case, an according mitigation must be in place. Until now a common solution is to install supervision by a human safety operator.

But even in case of human supervision, not all failures can be intercepted by the safety operator, which should be illustrated briefly in the following. In case the safety operator is standing, all failures resulting in high jerks and high longitudinal or lateral accelerations can lead to situations in which the operator may not be able to reach the emergency button to stop the vehicle. In addition, in a well-functioning system, it could be expected that the safety operator is somewhat distracted, leading to additionally increased reaction time.

Hence, for certain failures like described above, the vehicle must reach a safe state automatically and corresponding actions must be initiated. These depend on the criticality of the failure. For driverless shuttles, the most common reaction to a failure is the E-Stop. Depending on the vehicle speed at the failure event, one can roughly distinguish three possible E-stop scenarios:

- No steering torque and decelerate to standstill with variable braking deceleration (speeds < 15kph)
- Stop in ego lane. Following a pre-defined steering angle and deceleration profile (<70 kph in inner cities)
- Stop on emergency lane (higher speeds and on highways or rural roads).

Within the scope of the FCEA, we are looking at the worst-case scenario that can result of each component failure. In addition, also on this high-level, the severity and probability of the induced hazard can be evaluated. This should be illustrated in the explicit analysis of selected components for a specific prototype in the next chapter.

APPLICATION TO A PROTOTYPE SYSTEM

In the following, some details will be provided about one specific shuttle prototype developed at Continental, the so-called CUBE-3 vehicle (see Figure 7). The intended usage of the vehicle was to operate it on routes like the one shown in Figure 3. Accordingly, the aforementioned steps towards a release of the vehicle will be briefly summarized, with a focus on the safety aspects, including the FCEA.



Figure 7. The CUBE-3 prototype vehicle.

After analyzing the route and creating the according scenario catalogue, the top-down safety analysis comprised of the analysis of the Safety-in-Use, i.e., analysis of all expected human-machine interactions, and the ODD. For the Safety-in-Use analysis, every human actor with potential contact to the operation was listed. These were, among others, safety operator and passengers. Using the STPA method, these actors were included in the vehicle's control structure and their interfaces were assessed. In this way, every possible unsafe control action was identified, and safety requirements were generated to mitigate accidents. For example, the safety operator needs a certain time to detect a hazard, make a decision, and execute it. This reaction time was used to calculate the minimal distances to objects, such that the operator can bring the vehicle to a safe state at any time. The vehicle was required to operate only within these limits. Another example considers a situation in which the vehicle actuation receives ambiguous commands or commands beyond a defined safety limit. To ensure that the safety operator has the full authority over the vehicle, a hierarchy was created in which the safety operator's commands have highest priority and overrule other commands. Also, it was ensured that the safety operator is the only one that has access to the vehicle controls next to the high-level software during operation. Corresponding documents were created with instructions for anyone interfacing the operation. These must be handed out to and respected by the involved people.

After that, the ODD was analyzed and any hazard that can occur during the vehicle operation was identified and mitigated. This included, for example, areas subject to parked vehicles and people crossing the road. The parked vehicles may obstruct the vehicle's sensors as well as the safety operator's view and may lead to pedestrians being detected very late while they are crossing the road. To mitigate this, the vehicle speed was reduced in these areas and the safety operator was instructed to pay special attention when driving through these areas. Similar measures were applied to areas in which a higher concentration of pedestrians close to the road or crossing it is expected.

After the safety assessments mentioned above, the vehicle itself was in focus. The vehicle architecture is depicted in Figure 8. The basis for the vehicle was an EasyMile EZ10 Gen2 vehicle. The EZ10 is an autonomous minibus, which has a capacity for ten people and can reach a speed of up to 20kph. The vehicle was heavily modified, keeping only lights, air conditioning, doors, air spring system and safety lasers from the original equipment. All other components, including battery, propulsion, steering, brake system, and high-level sensors were replaced. After the modifications of the vehicle (see Figure 8), it was able to drive up to 30kph. With respect to the generic driverless shuttle vehicle architecture shown above (see Figure 6), the component "ECU1" was realized using a rapid prototyping ECU manufactured by Continental. This will be referred to

simply as “ECU” in the following. For the intended usage of the vehicle, it was acceptable not to be able to continue driving in case of a failure of ECU1 and the component “ECU2” was not realized. In case of failure of ECU1, the brake system would directly trigger an emergency stop. Running mainly the high-level software, the component “High Level Commands” was realized by a PC. The component “pre-defined stop scenario” was a stop in ego lane as described above.

In the following, a brief analysis of selected components is provided according to the FCEA mentioned above, including the mitigations for identified hazards.

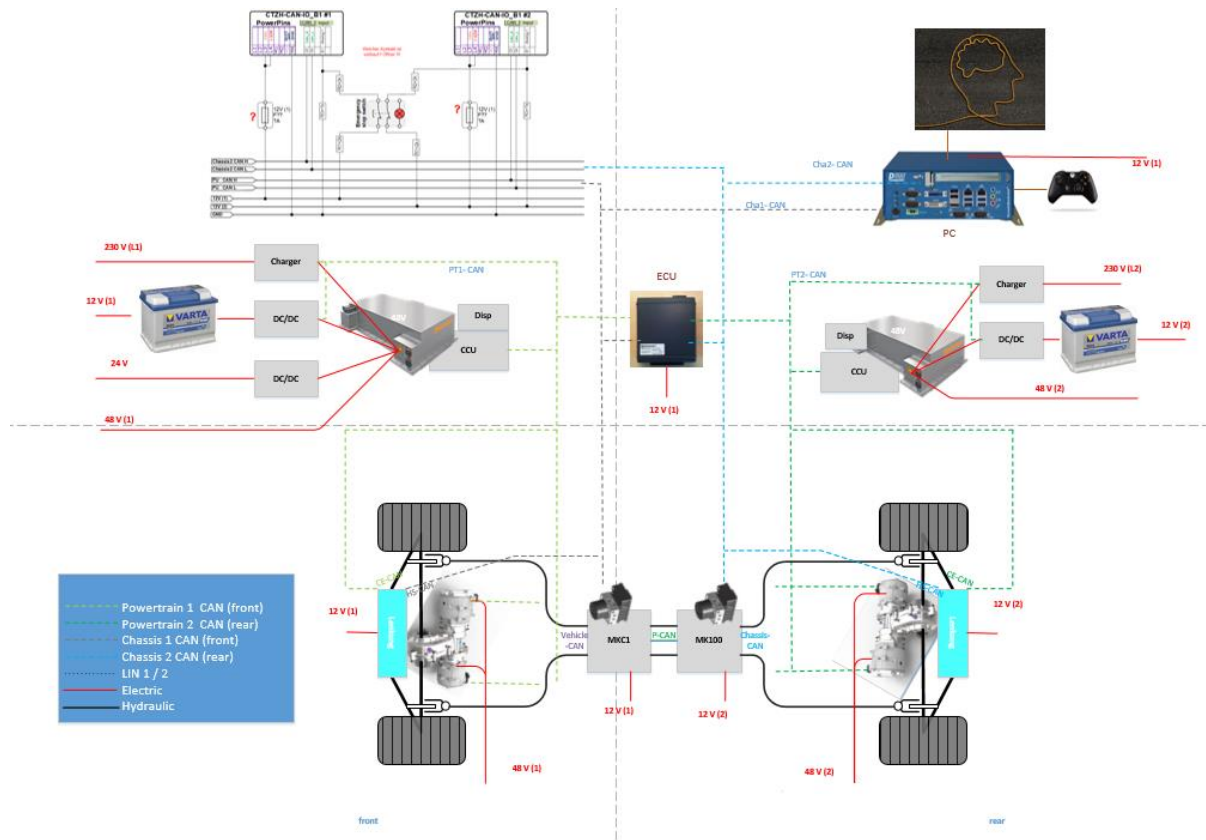


Figure 8. E/E architecture of the CUBE-3 prototype vehicle.

Main Brake System

The main brake system is the MKC1 of Continental, having three main roles: Deceleration of the vehicle, providing anti-lock braking (ABS) or traction control interfaces (TCS) as well as supervision of vehicle commands send to the brake system. Regarding the latter, in case there are any failures in timing, checksum, or the values itself, the brake system can degrade the shuttle system and bring the vehicle to a stop automatically. Using a hydraulic brake system brings the vehicle to a safe stop and standstill, which cannot be guaranteed just by braking with electric motors. For electrical engines, in comparison, there is a chance that the vehicle even gets faster or starts driving backwards if there is a failure in the fallback control loop.

Secondary Brake System

The secondary brake system is the Continental MK100, and it is the fallback system for the main brake system. Assuming that the fallback level is not active very often, not the whole functional range is needed. For example, TCS could be disabled in a degraded mode. But basic functions like ABS or Electronic Brakeforce Distribution (EBD) are still needed, as otherwise the vehicle could get unstable during emergency maneuvers with high decelerations. Also, regular self-tests are required for the fallback level as otherwise there is the risk of a sleeping failure.

Another requirement for the fallback brake system is that it should be able to deliver higher decelerations than in normal driving mode. This results from the detection time of the failure. If a deceleration is requested and the first brake system fails, the shuttle will still be moving, and consequently further decrease the distance to the object it is braking for. With that also the required deceleration to stop in front of the object increases. For example, if the maximum deceleration in the driving mode is 3.5m/s^2 the fallback level should at least reach 5m/s^2 . In addition, the maximum jerk and pressure build up time play a big role in such a scenario.

Steering

In the CUBE-3 vehicle, two steering systems were integrated, one on the front and one on the rear axle. Both are designed the same way, such that they can reach the same steering angle. In that way, the vehicle is already equipped with a redundant steering system. Nevertheless, there are failure modes which are different to simple “loss of steering”: Self-steering and misalignment. The latter typically has a mechanical reason, which can be regarded as quite improbable, as steering systems are designed in a very safe way. And in addition, the misalignment is assumed to be only very small in that case.

On the other hand, self-steering is a very dangerous failure case. The available driving path is in most cases very narrow and most of the time there is oncoming traffic to be expected, e.g., in inner cities. Hence, already a deviation of 1,5m to the target track can lead to severe incidents. With an assumed lateral acceleration of $6,5 \text{ m/s}^2$, 1,5m are reached within 0,7s. This is clearly below the reaction time of a safety operator. Anyway, even an immediately started emergency brake maneuver could not prevent a crash in this situation.

Therefore, two safety features were implemented, one regarding the self-steering and one regarding the maximum steering gradient. The self-steering detection feature checks whether the steering sensors deliver valid data and whether the actual steering angle is close to the requested one. On the other hand, the steering angle gradient is limited, with the limitation also being supervised. Both supervisions are capable of directly triggering a full stop of the vehicle. With that, the reaction time of the driver is taken out of the loop.

48 Volt Power Supply

The CUBE-3 vehicle has been equipped with two 48V power supplies. In that way that the vehicle is capable to apply engine torque even if one battery fails. As the intended vehicle speeds are below 30 kph and it was operated only on normal inner-city roads, a safe stop in case one battery fails was an acceptable safety requirement. As it is not a critical failure if one 48V power supply fails, a moderate deceleration was chosen to stop the vehicle.

Propulsion

The propulsion system of the CUBE-3 vehicle consists of two engine packages. Every engine package consists of two Belt Driven Starter Generators (BSGs) with 7kW each, as well as a differential. The maximum acceleration of the vehicle, however, was limited to $3,5 \text{ m/s}^2$ to protect standing passengers. Every propulsion system was connected to its own 48V Battery system, which in turn allowed the continuation of the mission if one 48V system fails, as described above.

DC-to-DC converters

The vehicle was equipped with automotive-grade DCDC converters. These are controllable via CAN and can transform energy from 12V to 48V and from 48V to 12V. They have an own supervision and shut off the DCDC functionality if a failure was detected on one of the board nets, while still communicated this error on CAN. In that way, a redundant information on the state of the 48V board nets (one from the battery and one from the DCDC converters) was available. In addition, there was also redundant information on the state of the 12V board nets, one from the DCDC converters and one from the Brake System. Whenever there was a failure in the board nets or a mismatch of information, a soft stop was triggered.

12 Volt power supply

Most of the actuation and computation devices are feed by 12V. To achieve redundancy, two 12V batteries were installed in the vehicle. This is rather a brute-force method, but sufficient for the scope of this prototype. A long-term solution would be to use only one battery and in addition install a supervision, which would decouple the battery from the board net in case it drains too much current.

High Level command and supervision (PC + ECU)

Within the software stack running the vehicle there was a distinction between high- and low-level software. The high-level software contains object detection, environmental modelling, prediction, vehicle maneuver and motion planning. The lower-level software consists of control algorithms and vehicle interface handling. The lower-level software was again split into two parts, one executed on the PC for the vehicle control algorithms and one running on the ECU to safeguard the actuator commands and to ensure correct interface handling.

In case of an error in the vehicle commands from the PC, these were overwritten, and a brake and steer straight command was sent to the actuators. This was very meaningful, because in case of high acceleration, high deceleration or high steering requests, the movement of the cabin becomes so severe that the safety operator would not be able to push the emergency button.

Also, the actuators had safety mitigations. If the commands sent from the ECU were corrupted, the steering was set to inactive (and with that steering straight) and the brake system was building up brake pressure.

In any of these cases, a recording was triggered, covering at least the last sixty seconds. The recording was then analyzed, and the incident was discussed by the engineering team with the safety experts in a safety management meeting, as defined in the SMS mentioned above.

Emergency buttons

The two emergency buttons are read-in in a redundant way by two ECUs. To be safe against shortcuts, the emergency stop button voltage was set to be 8V. As soon as it would drop below 5V or increase above 11V an emergency stop was triggered.

Door System

The door system, originating from busses, was designed to stay closed when a failure occurs. While a bus has more than one door which can serve as emergency exit, this is not valid in the case of the shuttle. Therefore, the doors were equipped with an emergency button, which disabled the whole door.

On the other hand, it is possible that this emergency button is pressed during normal operation. Therefore, a safety mechanism was implemented which triggers a soft stop of the vehicle in that case.

With these analysis results at hand, the CUBE-3 vehicle was successfully released and operated. Similar steps were performed for other prototype systems at Continental, covering different use cases as well as different vehicle platforms.

CONCLUSIONS AND PERSPECTIVES

In this paper, it was outlined how prototypes of driverless shuttles can be used during development, either towards a complete shuttle system or also for specific components or functions thereof. We argued that a certain release process should be installed in order to safely prepare and operate such prototypes. We presented a generic view on driverless shuttles in terms of their basic architecture. A safety assessment was then performed using one specific prototype vehicle developed and operated at Continental as a hands-on example. Here, we combined both top-down and bottom-up analysis steps to provide a pragmatic way to release such a vehicle. For the bottom-up analysis, we present a pragmatic approach called Component Failure and Effect Analysis (CFEA).

The considerations presented here should not substitute existing and established methods but should complement those within the scope of advanced engineering or development activities in general, in which sometimes a pragmatic approach delivers more value in a faster way. The results presented here may well be used as baseline for further developments, such that driverless shuttles become more and more mature in the near future.

REFERENCES

- [1] ERTRAC Working Group: "Connectivity and Automated Driving", *Connected, Cooperative and Automated Mobility Roadmap*, European Road Transport Research Advisory Council (ERTRAC), 2022.
- [2] Department for Transport and Department for Business, Energy & Industrial Strategy: Centre for Connected and Autonomous Vehicles, *Connected & Automated Mobility 2025: Realising the benefits of self-driving vehicles in the UK*, Crown, 2022.
- [3] U.S. Department of Transportation, *Automated Vehicles 3.0: Preparing for the Future of Transportation 3.0*, 2018.
- [4] Rhein-Main-Verkehrsverbund Servicegesellschaft mbH, „Probefahrt in die Zukunft,“ 2022. [Online]. Available: <https://www.probefahrt-zukunft.de/>.
- [5] Verkehrsbetriebe Hamburg-Holstein, „RealLabHH: Hamburg testet die Mobilität von Morgen,“ 2021. [Online]. Available: <https://vhhbus.de/reallabhh-reallabor-hamburg/>.
- [6] W. Davis, „Toyota e-Palette autonomous vehicles to be rolled out 'within the next few years',“ 2021. [Online]. Available: <https://www.drive.com.au/news/toyota-e-palette-autonomous-vehicles-to-be-rolled-out-within-the-next-few-years/>.

- [7] A. Hartmannsgruber, J. Seitz, M. Schreier, M. Strauss, N. Balbierer und A. Hohm, „CUBe: A Research Platform for Shared Mobility and Autonomous Driving in Urban Environments,“ in *IEEE Intelligent Vehicles Symposium*, Paris, 2019.
- [8] C. Pinke, A. Hohm und M. Grießer, „Industrialized technology building blocks for on-demand autonomous shuttles in urban and sub-urban use cases enabling mass-market scales, affordability, automotive reliability and safety,“ in *27th ITS World Congress*, Hamburg, 2021.
- [9] F. Lotz, R. Grewe und C. Pinke, „A “Common Core” Architecture as an Enabler for Cross-Platform Autonomous Driving,“ in *Apringer ATZ - Automatisiertes Fahren 2022*, Wiesbaden, 2022.
- [10] Continental, „Autonomous in Continental's and EasyMile's Robo-Taxi at the International Motor Show (IAA),“ 2019. [Online]. Available: <https://www.continental.com/en/press/press-releases/robo-taxi/>.
- [11] I. Lunden, "EasyMile raises \$66M for its autonomous people-and-goods shuttles," 2021. [Online]. Available: <https://techcrunch.com/2021/04/28/easymile-raises-66m-for-its-autonomous-people-and-goods-shuttles/>.
- [12] Business Wire, „Navya Sells 8 Self-Driving Shuttles in the US to Autonomous Mobility Provider Beep,“ 2022. [Online]. Available: <https://www.businesswire.com/news/home/20220911005052/en/>.
- [13] Freethink Team, „Inside Zoox: The robot vehicle totally changing transportation,“ [Online]. Available: <https://www.freethink.com/series/hard-reset/autonomous-vehicle>.
- [14] A. J. Hawkins, „Cruise starts pre-production of its autonomous shuttle thanks to \$5 billion from GM,“ 2021. [Online]. Available: <https://www.theverge.com/2021/6/15/22534945/gm-credit-cruise-autonomous-vehicle-origin-production>.
- [15] Sustainable Bus Editorial Team, „ZF autonomous shuttle presented in UK,“ [Online]. Available: <https://www.sustainable-bus.com/news/zf-autonomous-shuttle-presented-uk/>.
- [16] ISO 26262:2011 Road vehicles - Functional safety, 2018.
- [17] AIAG; VDA, FMEA Handbook, 2019.
- [18] German Federal Government, *Straßenverkehrsgesetz (StVG) (German Road Traffic Act)*, 2021.
- [19] German Ministry for Transportation and Digital Infrastruktur, „Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung - AFGBV),“ 2022. [Online]. Available: <https://ec.europa.eu/growth/tools-databases/tris/index.cfm/de/search/?trisaction=search.detail&year=2021&num=344&dLang=DE>.
- [20] German Federal Government, „FAQ Autonomous Driving,“ [Online]. Available: <https://www.bundesregierung.de/breg-en/news/faq-autonomous-driving-1916398>.
- [21] German Federal Motor Transport Authority, „Erprobungsgenehmigung gemäß § 1i StVG in Verbindung mit § 16 AFGBV,“ 2022. [Online]. Available: https://www.kba.de/DE/Themen/Typgenehmigung/Autonomes_automatisiertes_Fahren/Erprobungsgenehmigung/erprobungsgenehmigung_node.html.
- [22] Pegasus Project, „Pegasus,“ [Online]. Available: <https://www.pegasusprojekt.de/en/>.
- [23] Association of Standardization of Automation and Measuring Systems, „ASAM Homepage,“ [Online]. Available: <https://www.asam.net/>.

- [24] ISO 34502:2022 Road vehicles - Test scenarios for automated driving systems - Scenario based safety evaluation framework, 2022.
- [25] International Civil Aviation Organization (ICAO), Safety Management Manual (SMM) - Doc 9859 AN/474, 2013.
- [26] N. G. Leveson und J. P. Thomas, „STPA Handbook,“ March 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
- [27] ISO 21448:2022 Road vehicles - Safety of the intended functionality, 2022.