Safety-configuration of Autonomous Bus in Pedestrian Zone

Qazi Hamza Jan and Karsten Berns
Robotics Research Lab, Technische Universität Kaiserslautern, 67663 Kaiserslautern, Germany

Keywords: Safety, Autonomous Bus, Pedestrian-zone, Safety Certification, Certified System, Driver-less Vehicles.

Abstract: For self-driving vehicles to be equally trusted by the community like conventional vehicles and become a pivotal part of transportation, it is crucial to guarantee the safety of such vehicles. Safety must ensure that the vehicle will not collide with other obstacles and always stop in case of system failure. The vehicle used for the safety-configuration explained in this paper is a mini-bus that can carry around 10 passengers. It is intended to drive in a pedestrian-zone, an environment that involves many pedestrians and cyclists apart from occasional vehicles in a close-fitting space. Besides the manufacturer's basic system provided to enable safety, safety certified system were added to trigger the safety at specific conditions. This includes emergency buttons, wireless safety system and configurable laser-scanners. This will allow the vehicle to stop based on physically activating the safety or automatically by laser-scanners. After various tests, the vehicle was able to brake immediately. This safety system is guaranteed not be influenced or disabled by any external system. This safety-configuration is to facilitate the entire system for safety-certification in the future.

1 INTRODUCTION

For all types of Autonomous Vehicles (AVs), safety is the paramount concernment for researchers. Redundant solutions are added to AVs to avoid any fatal crash. From present statistics in (Hicks, 2018), the crash rate of AV is lower then the human crash rate. It is justifiable to argue that there is still insufficient data to deduce that AVs are safer than human driven vehicles. Authors in (Kalra and Paddock, 2016), have statistically reasoned that AVs still need to drive several miles without failure to remain below a benchmark of failure rate. They have also argued about the number of miles required to achieve the comparison between between AVs and human crash rates. But to achieve this level of confidence, it is important to assure that the AVs are safe even in a failure-state. AVs should be capable to permanently halt after an extreme hazardous fault.

In Germany, exists pedestrian-zones in numerous parts of the city. According to the German Road Traffic Act (StVO), these zones are indicated by Traffic Calming zone signs or pedestrian marking. These areas are meant for pedestrians. Delivery and residents' vehicles are usually allowed in such zones with specific rules. Pedestrians have high priority in such zones. For an approved vehicle to drive in such a zone should be at a walking pace. Presently, the allowance of driver-less vehicles in such zones for carrying passengers along the stretch of the pedestrian-zone is under process. To enable this allowance, it is important that the vehicle must comply with the safety standards provided by the local traffic authorities.

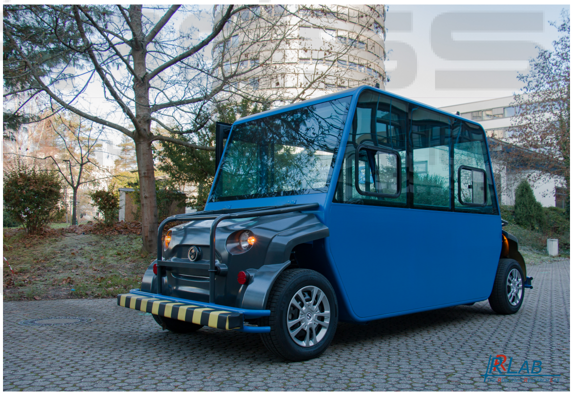


Figure 1: Driver-less bus model planned to drive in Technische Universität Kaiserslautern.

For AVs, particularly driving in pedestrian-zone, it should pass all the standard safety-related tests provided by the local traffic authorities to make certain that they will never even slightly press against any pedestrian in the case of any malfunction. It should also be taken into consideration the ludicrous behavior of the pedestrians towards the vehicle. Such behavior may include intentionally jumping in front of the vehicle or playing around the vehicle for amuse-

Jan, Q. and Berns, K.
Safety-configuration of Autonomous Bus in Pedestrian Zone.
DOI: 10.5220/0010526106980705
In *Proceedings of the 7th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2021)*, pages 698-705
ISBN: 978-989-758-513-5

ment. Here the aim is to provide safety not from perception and mapping algorithms but from the basic hardware which is always active. When either someone reaches the unsafe vicinity of the vehicle or the system crashes, then the braking must be possible. One possible scenario is when an unaware pedestrian steps in front of the vehicle and the navigation algorithm does not react timely or misses such danger. The vehicle must react to such situations. These are hard brakes that have no interference from any human error or navigation algorithms.

For proving the AV to be safe, it should adhere to standards. These standards are a general set of rules which specifies that safety will be guaranteed in all situations. Different tests are performed based on these standards to check their effectiveness. This paper focuses on explaining the safety configuration, specifically for autonomous-bus shown in Figure 1. This bus is the first model to drive on the campus of Technische Universität Kaiserslautern. It can carry 10 passengers and is intended to drive from building to building on the university campus. Safety parameters are discussed in this paper to understand how the safety configuration should look like. This safety configuration is then extendable to other AVs by changing the safety-parameters and adding redundant systems based on the application. Different levels of safety are discussed, from the noncritical level which is safety programmed in software to the utmost critical level, i.e., directly low-level hardware in the vehicle.

The following sections are arranged as follows. Section 2 discussed the related work, Section 3 explains the concept of safety layers which was implemented for our AV. To verify the system, the structure for experiments is explained in Section 4 and the conclusion is addressed in Section 5.

2 RELATED-WORK

To test autonomous driving-related algorithms in the urban environment, many researchers are using simulation for safety purposes. The authors in (Jan et al., 2019) have used simulation for driving autonomous vehicle in a pedestrian zone. They have brought interaction strategies in the navigation of autonomous vehicles in the pedestrian zone. There is work for developing realistic pedestrians as in (Jan et al., 2020; Alghodhaifi and Lakshmanan, 2020). There are applications other than urban environment where simulations are used as in (Husemann et al., 2020). But there always remains a gap between simulation and real-world testing. It is impossible to map all the realistic behaviors in the simulations. Hence, after successfully completing tests in simulation it is then to be tested on a real vehicle. Considering the possible incongruity of software with the hardware, the system must be safe independent of any software or other interference. All these applications are required to have safe systems because there is always involvement of humans in such areas.

Authors in (Reschka, 2016) have talked about safety concept for autonomous vehicles. They have focused on Safe State which according to safety standards depends on current situation and acceptable threshold value. Acceptable level of risk must be identified with reference to ISO 26262 standards. Huang et al. (Huang et al., 2016) have given a review on testing methods for AVs. They have presented different tests such as software testing, simulation testing and AVs functional testing. They also discuss the design and system validation which which depends on functional requirements.

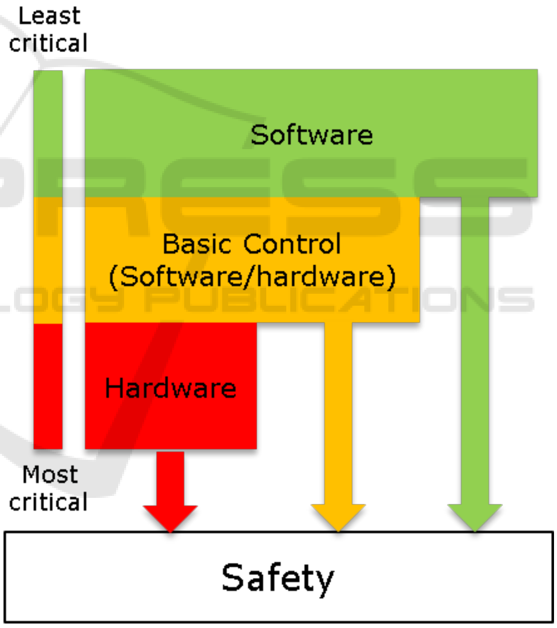


Figure 2: Representing the safety of the given system in three levels from most critical to least critical.

Martin et al. (Martin et al., 2015) have in detail talked about the certification of autonomous vehicles. They have given the process of standardizing the laws for AVs based on for National Highway Traffic Safety Administration (NHTSA) in the United States. The NHTSA includes a variety of topics from licensing of an operator to regulation for the operation of an autonomous vehicle. A safety design concept was brought in (Molina et al., 2017). They have implemented an independent module known as Autonomous Vehicle Control(AVC), which can be installed in the AV system and create a separate protection layer. It also accepts requests from a driver but still ensures the safety of the system.

In (Aeberhard et al., 2015), the researchers have tested their AVs on a German highway. They have given an overall view of their system from perception to vehicle control. They also mention to be certified they need to drive thousands of kilometers which delays the realistic requirement for their car production. To pass the functional safety standard for road vehicles, which is, ISO 26262, a thorough analysis is to be done.

UL4600 standard is discussed in (Koopman et al., 2019). They have focused on safety standards which also addresses the use of Machine learning techniques and unpredictable algorithms that are non-deterministic. It is also required to update these standards to cope with the emerging technologies. Still, it is unknown, how these standards must be applied.

It can be seen from the literature, that an independent and reliable safety system is required to stop the vehicle for different applications. Algorithms tested in a virtual environment cannot be trusted directly. Also, concrete policies should be shaped to certify such vehicles. But to facilitate the certification process, the required certification for the basic modules must be accomplished. It should follow a set of certain general rules to ensure safety let alone the safety regulations by the authorities.

3 SAFETY SYSTEM CONFIGURATION

To ensure the safety of our AV in the pedestrian zone, this section discusses in detail the safety-related configuration from the emergency-braking (hardware) to planning-algorithms (software). The configuration is divided into three different levels which can be seen in Figure 2. The bottom block shows the most critical level of safety. This is because it is independent of any external input and will always trigger safe stop in case of any self failure or activation of safety parameter. The higher limits of every non-critical layer are the lowest limit to the critical layer. All these layers are described in the following section.

The overall construction is that there is a close-loop circuit that runs through all the safety modules. These devices must be safety certified. These devices are shown in Figure 3. The orange line shows the safety circuit line. The safety circuit line is a low voltage line that is connected to relays. When this line is disrupted by any other module, it causes the motors to deactivate and in return the safety brake is activated.

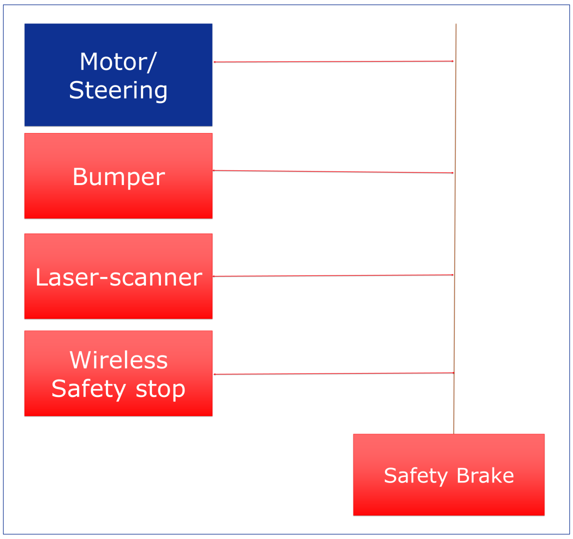


Figure 3: All the hardware module is connected to safety circuit line. This line is directly connected to the safety brake for emergency stop.

In figure 3, the circuit line in orange color is attached to all the suitable modules.

For compliance with the safety standards, the hardware must be safety certified. The details of the hardware-specific are explained in this section.

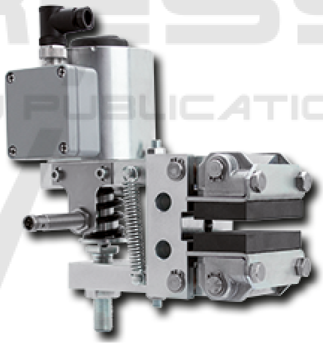


Figure 4: Brake Caliper.

3.1 Hardware

The default hardware enables the system to brake in case of any failure. This is verified by using a safety circuit line which is then connected directly to Electromagnetic Brake Calipers. The brake model used in the vehicle of figure 1 is DH012FEM. This brake is electromagnetically released, enabling braking even on voltage failure. Figure 4 shows the model of emergency brakes. This brake is eligible to have the CSA mark, which ensures that the product is tested for applicable standards by doing rigorous testing. It has a clamping force of 1850 N which will ensure to overcome the momentum of the vehicle.

Table 1: The table shows failure/unsafe conditions.

Causes	**Status**	**E-brake and Motor**

Over speeding	$>$ 8km/h	E-Brake = enabled
		Motor = disabled

Battery	Failure	
Emergency button	Pressed	
Safety bumper	Pressed	
Door contacts	Opened (Driving)	
Laser scanners	Safety Field Interrupted)	

The instant the safety circuit line is out of power due to any of the safety module, it disables the electric motors, and safety brakes in the front and rear are enabled. The basic rule conformed with safety are defined in the Table 1.

For avoiding any disruption from other modules, the safety hardware is segregated from the rest of the hardware and software. This ensures that the safety will always be active in the base level excluding the failure from a higher level as designed in Figure. 2. This will also guarantee that any programming error from the human will never interfere with the safety of the system. By doing so, the safety certification of the modules remains valid. All the connected safety modules are explained in the following subsection.

3.1.1 Laser-scanners

For the vehicle given in Figure 1, system from SICK AG[1] is used to add other mechanisms of enabling safety. SICK system provides a flexibility in configuring the main controllers with the combination of durable sensors. These systems are specifically aimed in applications where human protection is required. Overall, SICK provides different solutions for industries which are safe and efficient. The vehicle is equipped with the following modules from SICK:

1. Main-module: Programmable for inputs and outputs.
2. Gateway: For communicating with other sensors and devices.
3. I/O Module: To get the inputs and outputs from switches and sensors.
4. Motion Control Module: To integrate the motor and steering encoders from the vehicle
5. Safety Relay: To connect the system to safety circuit line.
6. Safety Relay: Add a mechanical switch to the system
7. Safety Laser Scanners: For detection of obstacle in a particular range.

The main module have Safety Integrity Level (SIL) 3 and Safety Integrity Level, Claim Limit (SILCL) 3. These SIL specify a target level of risk reduction. These are measurements for Safety Instrument Function (SIF) performance requirements. There are four SILs defined, with SIL1 being the least and SIL4 as the highest dependable. International Electrotechnical Commission (IEC) provides the standards for a vast range of technologies that conform to international standards. IEC 61508 has classified SIL into two main classes; systematic safety integrity and hardware safety integrity. All devices having SIL certification should achieve both of these classes. The method for hardware safety integrity is to use probabilistic analysis. The probability of dangerous failure per hour(PFH) defined in IEC EN 61508 is between 0.0000001-00000001 for SIL3.

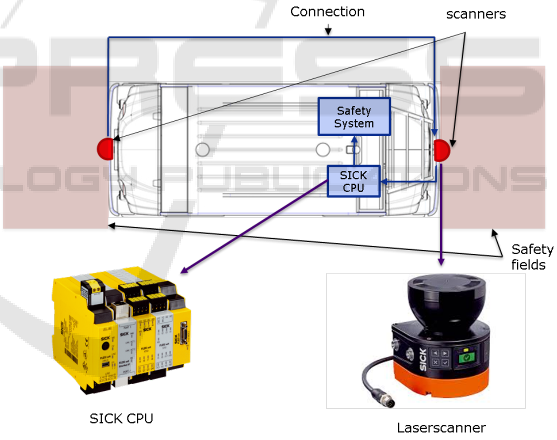


Figure 5: The figure shows the top view of vehicle with SICK system installation layout. The red semi-circle in the front and back shows the outdoorScan3 placed under the safety bumper.

The main module does all the processing of connected input/output devices. The connection can be either through Gateway, I/O module, Motion control module, or laser-scanner. The configuration is done in Safety Designer (SD) software which is a certified tool provided by the SICK. SD software provides all connection and configuration handling for modules such as input/outputs, motion controllers, and laser-scanners. The installation layout of the scanner and SICK processing unit can be seen in Figure 5. Both the scanners are connected in a line-

[1] https://www.sick.com/de/en

configuration with the main-module through Gateway to get the safe inputs/outputs. Each laser-scanner is configured separately to provide the required signals to the main-module

1. *Main-module:* The main-module processes all the signals from the input and output. These input and output signals could be from input/output modules or laser-scanners. The processing is done based on the valid configuration saved in its system plug. In the SD software, the main-module has a logical editor, where, all the logic is implemented based on the requirements.

2. *Safety Laser Scanner:* For laser-scanner, the outdoorScan3[2] is used. The outdoorScan3 is certified for use in an outdoor environment. It has a rugged design with extra shockproof. It can be used in slightly unfavorable weather conditions like rain, snow, and fog. It has SIL2 and SILCL2. In the event of a fault, the safety output via the network becomes logic 0. This is detected by the main module and the system enables the safety of the vehicle.

   The laser-scanner offers to create protective and warning fields. These fields are configurable shapes in the area of measurement of the scanner, which when detects an obstacle within the limits of that shape, disables the safe/unsafe outputs(depending on the field) from the scanner. This is very useful because there exists different stopping distances at different velocities for vehicles. It can be programmed to monitor 8 fields simultaneously. The characteristics of configurable fields are:

   (a) Warning field: For functional use only with a range of 40m.

   (b) Protective Field: For detection and protection with a range of 4m.

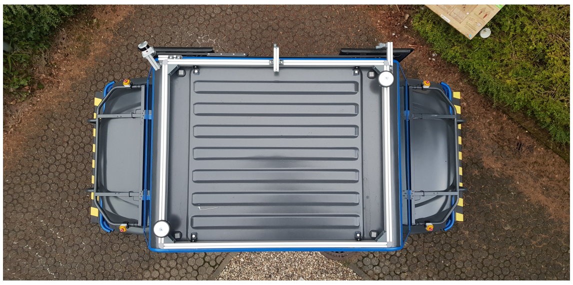


Figure 6: This is the top view of the vehicle at a close-fitting corner. The shape of field must be changed to avoid static obstacles otherwise it would always go to a stop position.

128 monitoring cases can be set in the laser-scanner. The relevant field-sets can be assigned to every monitoring cases, and activated based on input provided to the laser-scanner. For the scenario in this paper, the monitoring cases can be seen in Section. 4. Specific monitoring cases is active based the values set from the encoder reading. Two encoders are used on from the motor for speed measurement and the other from the steering. The more the speed is, the more stopping distance and, hence the larger the field is created. This kind of design will enable the vehicle not to collide at variable speeds and different steering angles.

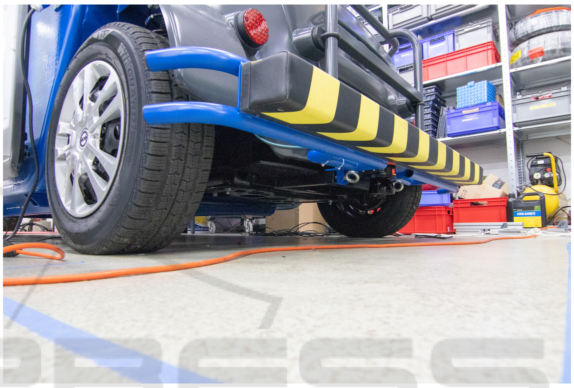


Figure 7: The safety bumper is shown in yellow and black strip. Bumper placement for safe stop is place at the front and rear.

As for the case of speed only, it is important to change the field shape to a pertinent steering. This is due to the following reasons:

(a) It becomes critical when steering the vehicle. As the vehicle has a double-Ackermann steering which can implies that both front and rear wheels steer symmetrically. For this reason, it is expected to have a smaller turning radius. Protective fields must be designed such that it is intercepted timely by the pedestrians walking alongside of the vehicle on a curve.

(b) Another explanation for designing the fields is demanded at narrow turns. This can be seen in Figure 6. As the narrow turn approaches, the fields must shape in a way that avoids the inclusion of obstacles like bushes or other structures. Otherwise, the vehicle will always go to a safety-stop state.

3.1.2 Safety Bumpers

The safety bumpers are used as last resort for safety stop. These are active collision cushions which have

[2] https://www.sick.com/de/en/opto-electronic-protective-dev ices/safety-laser-scanners/outdoorscan3/c/g503552

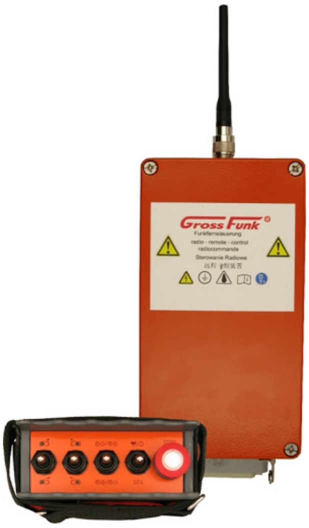


Figure 8: Grossfunk wireless safety switch for activation of safety in the vehicle.

safety switch-off function. This is directly connected to the safety circuit line. The position of the safety bumper can be seen in Figure 7.

3.1.3 Wireless Safety Stop

For redundancy in activating of safety stop, a wireless safety stop is installed directly with the safety line circuit. The component used is from Grossfunk. This has a wireless remote and receiver which is securely transmits data. It is activated when either the button is pressed or the remote goes out of range. During the initial operation and testing of the vehicle, the vehicle will always be under direct sight of a human operator, so in case of emergency he/she can activate the wireless stop.

3.1.4 Motor

Two 15kW motors are installed for the front and rear wheels. These motors are controlled by motor-controllers that take commands from the basic control discussed in Section 3.2. The motors are deactivated in case of emergency brakes. It has IP54 protection. It also has a thermal sensor and encoder for feedback to the motor-controller. These motors are powerful enough to drive the vehicle up to 40 km/h.

3.2 Basic Control

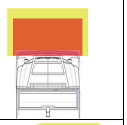
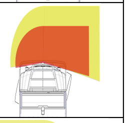
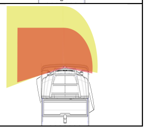
The basic control between our software and hardware is manufactured by Kompairobotics[3]. Our system can communicate with the basic control through Ethernet to a jetson where their architecture is active. All the basic configurations can be set in this architecture. This includes velocity, steering, and other input/output commands. It has a watchdog mechanism between the low-level controller and all CAN devices. If there is any dysfunction or no velocity command is received then the emergency stop is activated.

3.3 Software

Safety is also taken into account from our autonomous navigation architecture known as Robust bEhAvior-based ConTrolfor Off-road Navigation (REACTiON) (Wolf et al., 2018). This is the least critical in terms of safety but it is considered to react first to a situation. REACTiON takes into consideration the vehicle kinematics and based on that it autonomously drives the vehicle. It does all the path-planning and avoids the static and dynamic obstacles. This is done in order to avoid the activation of safety brakes repeatedly.

The architecture has a safety module which creates virtual bumpers from the same front and rear laser-scanner shown in Figure 5. The velocity decreases based on activation of these bumpers. Normal vehicle brakes are activated once the size of the bumper becomes less then the threshold.

Table 2: The table shows the different monitoring cases and the required fields.

Monitoring Case	Description	Fields
Driving straight	When driving straight the fields are perfect square	
Turning right	At full steering towards right	
Turning left	At full steering towards left	

4 EXPERIMENTS AND RESULTS

Due to the nature of the experiment, it is not possible to show the results in the paper. Since the experiments were related explicitly to hardware testing. But to explain the formation of the protective and warning fields, the vehicle turning radius is discussed and the relevant created fields are shown in the Table 2.

[3] https://kompairobotics.com/robot-kompai/

Table 3: Chosen speed, steering angles and relevant monitoring case numbers. The numbers inside the table present the monitoring cases which are assigned as MCXXX to the laser-scanner.

	Speed (km/h)					
Steering angles (degrees)	0	1	2	3	5	8
-22	-220	-221	-222	X	X	X
-15	-150	-151	-152	-153	X	X
-10	-100	-101	-102	-103	-105	X
-5	-50	-51	-52	-53	-55	X
0	00	01	02	03	05	08
5	50	51	52	53	55	X
10	100	101	102	103	105	X
15	150	151	152	153	X	X
22	220	221	222	X	X	X

The discrete speeds are chosen from 0 *km/h* to 8 *km/h*. Lower speeds are mostly selected because the vehicle is expected to drive more at lower speeds. For our case, the maximum threshold of highest driving speed was 8 *km/h*. In case the vehicle reaches this speed, SICK will enable safety brakes because it is never expected to reach such speeds in a pedestrian zone. The maximum steering the vehicle is able to achieve is 22°. 5° angle of interval is selected for every chosen speed. The Monitoring cases in the laser-scanner are assigned base on the table. 3 for every speed and steering angle. X in Table 3 implies that monitoring case for such a sequence of speed and steering is not preferred since high steering is unsuitable at high speeds, especially in a pedestrian zone.

For fields at a particular steering, the turning radius of the vehicle was found by the following equation:

$$R = \sqrt{(l/2)^2 + l^2 cot^2 \alpha}$$

The equation was taken from (Bhavesh K.Gohil, 2018), where R is the turning radius, l is the distance from front wheel to rear wheel. and α is the steering angle. After taking the dimensions of the bus and maximum steering angle, it was noted that the turning radius for the vehicle in Figure 1 is 4.2m. This is shown in figure. 9. Based on the values from the steering encoders, the associated fields are activated. This field is made not larger then the outer and inner turning radius of the vehicle. As mentioned in the section 3.1.1, this is important when the vehicle reaches a sharp corner. Figure 10 shows similar situations with protective and warning fields. It can be seen that the bushes are not taken as an obstacle of turning in the other direction and the vehicle can easily turn without safety brake activation.

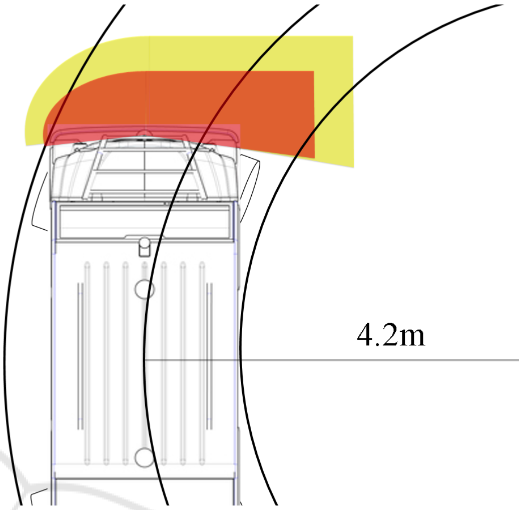


Figure 9: The figure shows the protective field in red and warning field in yellow for speed of 1km/h with full right steering. The turning radius for this vehicle is 4.2m.

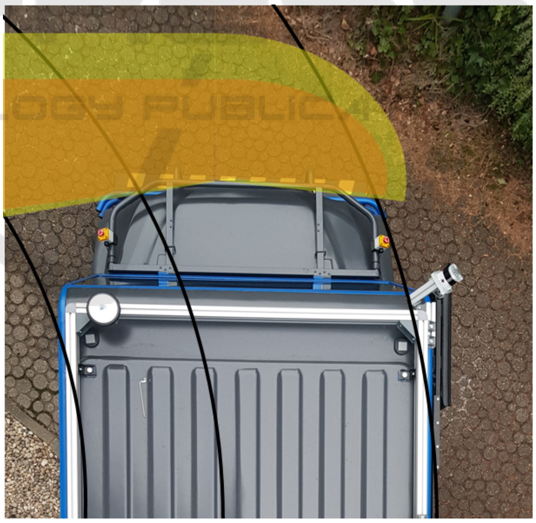


Figure 10: The figure show the perpective view of the vehicle from image 6. The shape of the fields are such that it turns in at the corner without enabling the safety brakes.

5 CONCLUSION

This paper has described the safety configuration of the Driver-less bus shown in Figure 1. This driverless bus is meant for driving autonomously in a pedestrian-zone. The most important feature when driving in such zones is the safety of the people and environment. Hence, it is essential that the vehicle is totally safe even during a malfunction or any glitch in the system. This ensures that the vehicle should stop in any case to avoid collision with the people or environment. On the other hand, the vehicle should also stop when someone is trying to compellingly mess-around the vehicle. The hardware used for safety is safety certified to fulfill the requirements of safety certification. By performing the tests, the vehicle was able to stop at different speeds without colliding with the obstacle by forging the system manually in all possible ways.

The process of safety certification for autonomous vehicles is not defined explicitly. It varies according to application and country. But to achieve the certification in a later stage it is important to use and follow the standard types of equipment that are already certified to ease the validation process.

REFERENCES

Aeberhard, M., Rauch, S., Bahram, M., Tanzmeister, G., Thomas, J., Pilat, Y., Homm, F., Huber, W., and Kaempchen, N. (2015). Experience, results and lessons learned from automated driving on germany's highways. *IEEE Intelligent transportation systems magazine*, 7(1):42–57.

Alghodhaifi, H. and Lakshmanan, S. (2020). Simulation-based model for surrogate safety measures analysis in automated vehicle-pedestrian conflict on an urban environment. In *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2020*, volume 11415, page 1141504. International Society for Optics and Photonics.

Bhavesh K.Gohil, Nilesh G. Joshi, H. B. P. P. B. K. (2018). Optimization of steering system for four wheel vehicle. *IEEE Technology and Society Magazine*, 6(8):52–62.

Hicks, D. J. (2018). The safety of autonomous vehicles: Lessons from philosophy of science. *IEEE Technology and Society Magazine*, 37(1):62–69.

Huang, W., Wang, K., Lv, Y., and Zhu, F. (2016). Autonomous vehicles testing methods review. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pages 163–168. IEEE.

Husemann, J., Wolf, P., Vierling, A., Berns, K., and Decker, P. (2020). Towards high-quality road construction: Using autonomous tandem rollers for asphalt compaction optimization. In ”Osumi, Hisashi”, F. H. T. K., editor, *Proceedings of the 37th International Symposium on Automation and Robotics in Construction (ISARC)*, pages 90–97, Kitakyushu, Japan. International Association for Automation and Robotics in Construction (IAARC).

Jan, Q. H., Kleen, J. M. A., and Berns, K. (2020). Self-aware pedestrians modeling for testing autonomous vehicles in simulation. In *VEHITS*, pages 577–584.

Jan, Q. H., Klein, S., and Berns, K. (2019). Safe and efficient navigation of an autonomous shuttle in a pedestrian zone. In *International Conference on Robotics in Alpe-Adria Danube Region*, pages 267–274. Springer.

Kalra, N. and Paddock, S. M. (2016). Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability? *Transportation Research Part A: Policy and Practice*, 94:182–193.

Koopman, P., Ferrell, U., Fratrik, F., and Wagner, M. (2019). A safety standard approach for fully autonomous vehicles. In Romanovsky, A., Troubitsyna, E., Gashi, I., Schoitsch, E., and Bitsch, F., editors, *Computer Safety, Reliability, and Security*, pages 326–332, Cham. Springer International Publishing.

Martin, J., Kim, N., Mittal, D., and Chisholm, M. (2015). Certification for autonomous vehicles. *Automative Cyber-physical Systems course paper, University of North Carolina, Chapel Hill, NC, USA*.

Molina, C. B. S. T., De Almeida, J. R., Vismari, L. F., Gonzalez, R. I. R., Naufal, J. K., and Camargo, J. (2017). Assuring fully autonomous vehicles safety by design: The autonomous vehicle control (avc) module strategy. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 16–21. IEEE.

Reschka, A. (2016). Safety concept for autonomous vehicles. In *Autonomous Driving*, pages 473–496. Springer.

Wolf, P., Ropertz, T., Berns, K., Thul, M., Wetzel, P., and Vogt, A. (2018). Behavior-based control for safe and robust navigation of an unimog in off-road environments. In *Commercial Vehicle Technology 2018*, pages 63–76. Springer.