Investigation of Safety Design Methods for Low to Medium Speed Mobility Systems in Logistics

Shota Hori [1)] Takuma Hirasawa [1)] Koji Hagiwara [1)] Shigehiro Sugihira [1)]
Yasutaka Fujiwara [1)] Masakazu Owatari [1)]

1) Advanced Powertrain Control Development Department, Second Control Development Div.
TOYOTA MOTOR CORPORATION.
1200, Mishuku, Susono, Shizuoka,410-1193 Japan
E-mail: shota_hori@mail.toyota.co.jp, Tel:055-997-2121

ABSTRACT: Currently in Japan, the aging workforce in a logistics sector and restrictions on working hours have led to the severe labor shortage problem. As one solution to this issue, the research and development of mobility equipped with autonomous driving functions for last-mile delivery are being actively explored. These mobilities are designed for a wide range of speeds, from walking speed (3 km/h) to bicycle speed (20 km/h), and there has been extensive technical discussion on this topic. However, there has been relatively less discussion regarding safety performance. In this paper, our approach is based on the safety design and quality evaluation concepts that have been previously considered for automobiles, developed the safety quality considerations for low to mid-speed (up to 20 km/h) mobility vehicles, and conduct evaluation and verification through simulations targeting operations within restricted areas, including roadways.

KEY WORDS: Autonomous Delivery, Logistics, Last Mile, Safety, Small Mobility, Micro Mobility

1. INTRODUCTION

Currently in Japan, the aging workforce in a logistics sector and restrictions on working hours have led to the severe labor shortage in logistics [(1)]. As one solution to this issue, small mobility equipped with autonomous driving functions that operate in low to medium speed ranges to realize last-mile logistics are being considered. Various studies on the autonomous driving for small mobilities have been conducted, ranging from fundamental technical discussions [(2)(3)] to the implementation of Proofs of Concept (PoC) that operate the mobilities and verify the feasibility of the service [(4)(5)].

On the other hand, there has been relatively limited discussion on the safety quality of these small mobilities, limited to investigations into safety standards for small mobilities [(6)] and risk assessments for small mobilities without autonomous driving capabilities [(7)].

In this paper, we examined the application methods of the safety and quality standards concepts that have been applied to automobiles to small mobilities that perform autonomous driving in low to medium speed ranges. Furthermore, we conducted evaluation and verification to ensure safety quality using simulations for a vast number of scenarios.

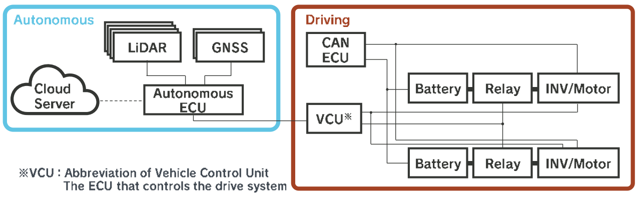

Fig. 1 Hardware Configuration

2. System Design of Small Mobility

2.1. Objectives and Applications of Small Mobility

The small mobility examined in this paper is intended for last-mile logistics applications, operating within restricted areas that include roadways. Additionally, the autonomous driving functions are designed to navigate predefined routes marked on maps, with the goal of traveling these routes to deliver goods to designated destinations. The driving environment assumes operation of electric kickboards and automobiles within restricted area roadways, adhering to speed limits of 30 km/h or below.

2.2. Hardware Design of Small Mobility

Fig. 1 illustrates an example of the hardware configuration of the mobility mentioned in this paper.

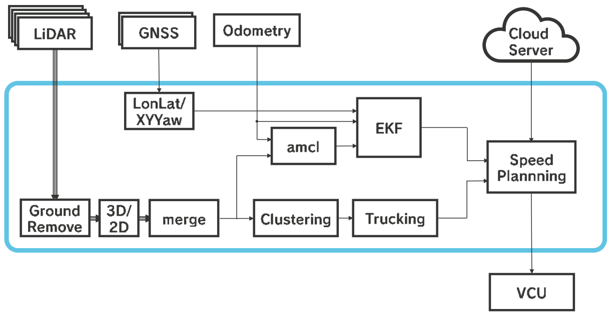

Fig. 2 Software Configuration

The drive system equipped with two in-wheel motors configured as a differential two-wheeled mechanism without steering. For autonomous driving control, a dedicated Electronic Control Unit (ECU) is provided, which utilizes four LiDAR with SPAD sensors with a horizontal field of view of 120 degrees oriented in different directions, as well as two Global Navigation Satellite System (GNSS) units to gather information on the surrounding environment and self-positioning. Furthermore, the vehicle maintains a constant internet connection, allowing it to receive instructions for autonomous driving from a cloud-based control system and transmit mobility information to fulfill its designated tasks.

2.3. Small Mobility Software Design

Fig. 2 illustrates an example of the software architecture of the mobility in this paper. The onboard software is broadly divided into an autonomous driving controller and a vehicle drive controller. The autonomous driving controller section receives inputs from four LiDAR sensors' signals, GNSS positioning information, and wheel speed data to perform self-position estimation, comprehensive surrounding recognition, and speed planning.

Due to the processing power of vehicle-mounted systems, it is necessary to reduce a computational load on the ECU for the LiDAR point cloud measurements, thus the 3D point cloud is converted to 2D scan for use. For self-position estimation, the LiDAR component utilizes Adaptive Monte Carlo Localization (amcl) [8], while the GNSS component uses Real Time Kinematic (RTK) GNSS [9] to convert latitude and longitude information into a planar Cartesian coordinate system. The absolute positions and orientations derived from these are then integrated with wheel speed using an Extended Kalman Filter (EKF) [10] to enable operation both indoors and outdoors.

As for surrounding recognition, clustering and tracking are performed on the 2D scan to estimate the speed of clusters and predict potential collisions.

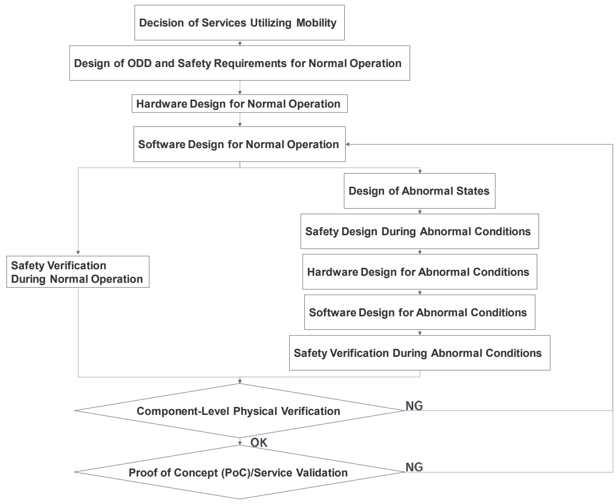

Fig. 3 Safety Design Process

3. Small Mobility Safety Design

The low-to-mid speed mobilities targeted in this study operate at higher speeds than low-speed mobility used for tasks such as indoor delivery (up to approximately 3 km/h), reaching medium speeds of up to approximately 20 km/h within restricted areas, including roadways and indoor environments. However, they do not operate at high speeds like automobiles. Therefore, directly applying the autonomous driving quality standards designed for low-speed mobility vehicles and automobiles to these vehicles is not considered optimal. Consequently, for the logistics service assumed in this study, we designed and verified hardware and software to ensure safety under both normal and failure conditions through a process illustrated in Fig. 3.

3.1. Safety Functions Under Normal Operations

As safety functions under normal operations, the system that described in the previous section, utilizes 360-degree 2D point clouds obtained from LiDAR sensors to perceive the surrounding environment. Using this capability, the mobility implements "collision avoidance," "pedestrian-priority stopping at crosswalks," and " obstruction avoidance before starting".

Furthermore, regarding these functionalities, we conducted a safety verification process based on the flow of defining quality standards, Operational Design Domain (ODD) analysis, identifying unsafe scenarios, and verifying quality standards. That process referencing the Autonomous Driving Safety Evaluation Framework Ver 3.0 [11] and ISO34502 [12]. Additionally, for the validation of safety under normal operations, we examined scenarios for "collision avoidance," "pedestrian priority stopping at crosswalks," and "obstruction avoidance before starting". In this paper, we described verification using collision avoidance as an example from these scenarios.

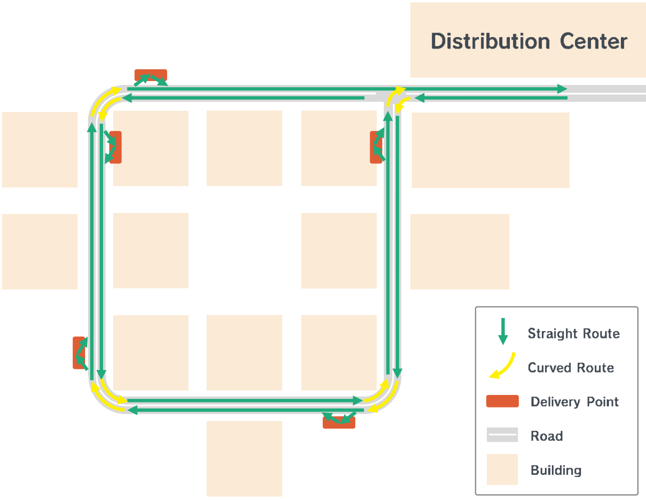

Fig.4 Map of the target area

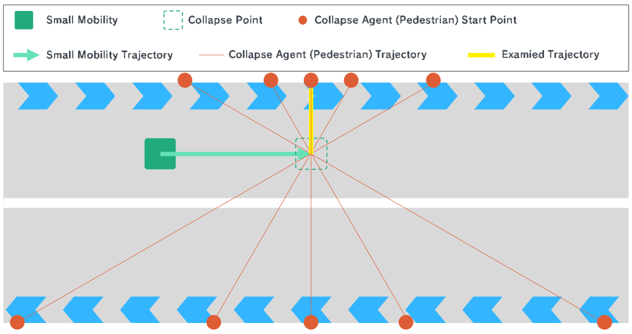

Fig.5 Straight road of the target area

Dash out Target (Pedestrian)			Small Mobility				Enviroment
Approach Angle[deg]	Size[m]	Max Velocity [km/h]	Max Velocity [km/h]	Distance to Collapse Point[m]	Trjectiory Offset[m]	Initial Velocity [km/h]	Road Width[m]
±30	0.5×0.15	3.6	8	25	0	0	3.5
±60	0.3×0.1	7.2					
±90							
±120							
±150							

Table.1 Scenario Configuration

First, we defined quality standards for the collision avoidance. Its safety standard is that the mobility must be able to stop before collision with a collision target approaching either along its path or towards the vehicle body.

Next, for ODD analysis, we assumed an autonomous delivery service using a mobility within a restricted area. A map of the target area and the drivable regions are shown in Fig.4. The traffic participants in this area include automobiles, bicycles and electric kickboards, and pedestrians.

In actual verification, unsafe scenarios are considered for each type of traffic participant; however, in this paper, we focused on unsafe scenarios involving pedestrians. Roads in the assumed area consist of roadways, bicycle lanes, and sidewalks shown in Fig.5, and within the area, all straight roads are uniform. While pedestrians generally walk on sidewalks, we assumed that scenarios where pedestrians dash out from the boundary between sidewalks and bicycle lanes in specific areas such as crosswalks, resulting in collisions with the mobility vehicle, are the most unsafe. Regarding such dash-outs, as mentioned earlier, the safety functions under normal operations are implemented using a rule-based method; thus, the determination of whether to stop is based on the relative positions between the mobility and pedestrians. Therefore, referring to Fig.4, we conducted verification by dividing the movement paths of pedestrians and the mobility vehicle into straight and curved paths. Fig.5 illustrates a case where the movement paths of the mobility vehicle and pedestrians intersect in straight lines. This unsafe scenario is defined as parameters in Table 1, and in this verification, a total of 40 patterns as shown in the Table 1 were identified. Additionally, these parameters were selected to accommodate a wide range of scenarios by adjusting the parameter ranges and increments when verification scenarios change. For example, by varying the road width, the distance to the collision point, and the initial velocity, it is possible to simulate dash-out patterns from multiple blind spots. Furthermore, while there are 40 pedestrian path patterns for collision safety involving straight paths, applying similar examinations to "collision avoidance," "pedestrian priority stopping at crosswalks," and "obstruction avoidance before starting" results in a total of 1,700 patterns identified.

3.2. Safety Functions During Failure Conditions

For safety during failure conditions, the system is designed from three primary functions to prevent the unsafe state even in the event of a single hardware failure: “stopping via safety scanners”, “redundant main and sub Vehicle Control Units (VCU) configuration”, and “brakes that operate during power loss through a combination of VCU output and relays”. These measures ensure safety is maintained when normal operation fails. Additionally, the design references ISO 3691-4[13] and implement a Failure Modes and Effects Analysis (FMEA) with 230 items applied to the normal system, resulting in the hardware configuration illustrated in Fig.6.

First, stopping via safety scanners. Two safety scanners are installed at the front and rear. When an obstacle enters the monitored range, an emergency stop is triggered to avoid a collision.

Next, the redundant VCU configuration consists of two VCUs (main and sub) that monitor each other. Both VCUs can issue brake commands, and the various sensors monitored by the VCUs ensure that even in the event of a VCU failure, the unsafe state can be avoided.

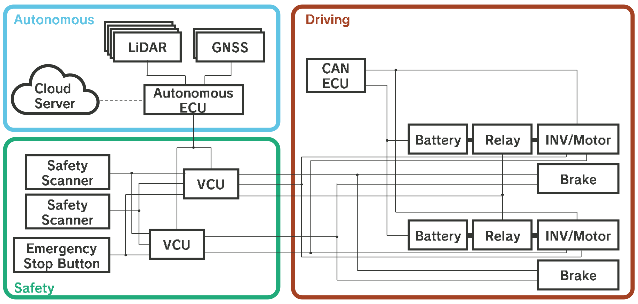

Fig.6 Hardware Configuration with failure safety

Finally, the brakes actuated by VCU output utilize a combination of relays and VCU outputs, enabling the brakes to engage even in the event of a power loss.

4. Small Mobility Safety Design

In this chapter, we conducted a verification of the safety design proposed in the preceding chapter.

4.1. Safety Functions Under Normal Operations

Regarding safety under normal operations, we considered evaluating the scenarios defined in the previous chapter against quality standards. Verification processes that involve interactions with other entities, as previously mentioned, tend to generate an extensive number of patterns. Therefore, by conducting verifications using a lightweight 2D simulation, we were able to rapidly iterate the development cycle and perform successive improvements. We carried out verification on a total of 1,700 patterns including "collision avoidance," "pedestrian-priority stopping at crosswalks," and "obstruction avoidance during starting," confirming that the system can appropriately stop in response to foreseeable and avoidable events.

Finally, we presented the results of the verification of the simulation's validity in Fig.7. In this verification, we specifically examined unsafe collision avoidance patterns with minimal distance margins prior to collision, namely the patterns represented by the yellow lines in Fig,5. We replicated the same scenarios tested in the simulation using the actual machine and a crash test dummy . The results indicated that under the field tested, there was approximately a 280 [ms] difference between the simulation and the actual machine in the time taken to recognize a pedestrian and issue a stop command. Additionally, regarding the execution, there were a 200[ms] delay introduced to replicate the actual machine in the simulation and approximately a 302 [ms] delay in the actual machine, resulting in a difference of about 100 [ms]. Consequently, a total delay of approximately 380 [ms]

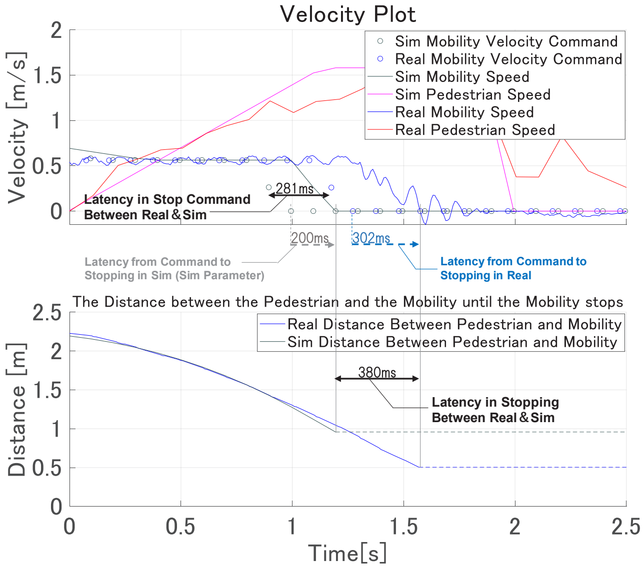

Fig.7 Result of Simulation and Field Testing

occurs between the simulation and the actual device when stopping the mobility system.

The primary cause of the significant discrepancy in the time taken to issue the stop command was likely due to a velocity estimation of the collision target, which incurred errors by assuming an ideal shape for the collision target. Based on these results, at least a 400 [ms] delay is required to accurately estimate the safety margin for the 2D simulator .

4.2. Safety Functions During Failure Conditions

Regarding safety during failure conditions, like automobiles, functional testing using Hardware-in-the-Loop Simulation (HiLS) and software unit testing were conducted as necessary to ensure the implementation quality of failure safety. Since the same process used in a general vehicle development (14) was applied, detailed descriptions are omitted in this paper.

5. Summary

In this paper, we proposed a method for applying the concepts of safety and quality standards, which have been applied to automobiles, to small mobilities operating in low to medium-speed ranges for autonomous driving. Additionally, we conducted verification of the quality standards for autonomous driving functions using 2D simulations and actual devices, confirming that idealized 2D simulation-based verification still presents some challenges in the recognition of collision objects.

ACKNOWLEDGMENT

REFERENCES

(1) Ministry of Land, Infrastructure, Transport and Tourism., "[Current Situation and Issues Surrounding Logistics.] *Buturyu wo torimaku genzyo to kadai (in Japanese)*" Ministry of Land, Infrastructure, Transport and Tourism., https://www.mlit.go.jp/road/ir/ir-council/buturyu_douro/pdf01/03.pdf (accessed October 4, 2024).

(2) W. Xu and F. Zhang, "FAST-LIO: A Fast, Robust LiDAR-Inertial Odometry Package by Tightly-Coupled Iterated Kalman Filter," in IEEE Robotics and Automation Letters, vol. 6, no. 2, pp. 3317-3324, April 2021, doi: 10.1109/LRA.2021.3064227

(3) C.Chen et al. ," DeepDriving: Learning Affordance for Direct Perception in Autonomous Driving",Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2015, pp. 2722-2730

(4) Uber. "Bringing the future to today: making robot delivery a reality." Uber. https://www.uber.com/en-JP/blog/so-funakoshi/ (accessed October 4, 2024).

(5) Council on Social Capital Development. "[New Mobility and Road Space.] *arata na mobility to doro kukan (in Japanese)*" Ministry of Land, Infrastructure, Transport and Tourism. https://www.mlit.go.jp/policy/shingikai/content/001595749.pdf (accessed October 4, 2024).

(6) Markis, A.et al. ,"Safety of Mobile Robot Systems in Industrial Applications.", In Proceedings of the ARW OAGM Workshop 2019, Steyr, AT, USA, 9–10 May 2019; pp. 26–31.

(7) Hishikawa, T. et al., "Safety evaluation of personal mobility vehicles and pedestrians under mixed traffic flow using traffic simulation." Asian Transp. Studies 2022

(8) S. Thrun et al., *Probabilistic Robotics*, The MIT Press, 2005.

(9) H. Namie, "[The Principle and the Practice of the RTK-GPS] *RTK-GPS no genre to ouyou (in Japanese)*" ,GPS International Symposium '01 CGSIC/IISC 3rd Asia-Pacific Regional Meeting, Tutorial Lecture Materials, pp.21-38, February 2001.

(10) T. Moore and D. Stouch, *A Generalized Extended Kalman Filter Implementation for the Robot Operating System*, Springer, 2014.

(11) S. Sato et al., *[Safety Evaluation Framework for Autonomous Driving Ver 3.0] Jidounten no anzensei hyouka framework (in Japanese)*, Japan Automobile Manufactures Association, Inc, 2022.

(12) International Organization for Standardization, *ISO 34502:2022*, International Organization for Standardization, 2022.

(13) International Organization for Standardization, *ISO 3691-4:2020*, International Organization for Standardization, 2020.

(14) T. Yamaguchi, T. Kaga, " An application of model checking to the development of engine control software" in Proceedings of the JSAE Annual Congress,Vol.115, No.13, p.13-18 (2013)