Real-time Recursive Risk Assessment Framework for Autonomous Vehicle Operations

Wei Ming Dan Chia[1,2], Sye Loong Keoh[2,3], Anna Lito Michala[2], Cindy Goh[3]
[1]*Infocomm Technology (ICT), Singapore Institute of Technology, Singapore*
[2]*School of Computing Science, University of Glasgow, Glasgow, United Kingdom*
[3]*University of Glasgow, Singapore*
Email: Dan.Chia@SingaporeTech.edu.sg, {SyeLoong.Keoh, AnnaLito.Michala, Cindy.Goh}@glasgow.ac.uk

***Abstract* — Existing risk assessment (RA) methodology used for autonomous vehicle (AV) development and validation is insufficient for future AV operations. Existing frameworks operate based on processes such as hazard analysis and risk assessment (HARA) where risk is defined based on functional hazardous event severity and the likelihood of occurrence. This is a static process performed during the development stage and relies on prior lessons learnt and know-how. A drawback of this is the omission of potential complex environments that could occur during real-time – especially with more stringent safety requirements for AV operating at higher automation levels. Therefore, there is a need for an additional framework to further enhance the safety levels of the AV, focusing on real-time instead of static risk assessment during development. In this paper, a novel real-time recursive RA framework (ReRAF) addresses the gap by creating a novel risk representation, predictive risk number (PRN), and eventual safety levels (SLs) in the temporal and spatial domain. This approach focuses on risk assessment based on AV collision to the detected hazardous object and controllability of the AV. A dynamic recursive RA continuously captures potentially hazardous events in real-time and compares them with past occurrences to predict future safety actions. ReRAF provides a continuous improvement on the RA and acts as an additional safety layer for AV operations.**

Keywords— Autonomous vehicle, hazard analysis, risk assessment, safety framework.

I. INTRODUCTION

Autonomous Vehicles (AV) is envisioned to be the next generation of transport in the future. One of the biggest challenges in deploying AVs on the road is safety, in particular when ensuring the safe operations of AV when operating in a new environment with full automation without driver's intervention. As illustrated in TABLE I, high and full automation refers to SAE Level 4 and 5 [1] in which the Autonomous Driving System (ADS) is the de-facto responsible fallback in the occurrence of hazardous events. Unlike SAE Level 3 and below where the driver remains as the responsible fallback (similar to a driven vehicle), the safety requirements for fully automated AV with SAE Level 4 and 5 increase exponentially in terms of (1) identifying hazardous events (2) making safety decision, when a potentially hazardous event occurs.

TABLE I. SAE LEVELS AND FALLBACK RESPONSIBILITY

SAE Levels	0	1	2	3	4	5
Fallback responsibility	Driver	Driver	Driver	Driver	ADS	ADS
Automation	No	ADAS	Partial	Conditional	High	Full
Vehicle control motion	Driver	Driver and ADS	ADS	ADS	ADS	ADS
Environment monitoring	Driver	Driver	Driver	ADS	ADS	ADS

Traditional ISO 26262:2018 [2] standard has been used extensively as functional safety for Electrical/Electronics (E/E) functionality in road vehicles [3]. This standard adopts Hazard Analysis and Risk Assessment (HARA) [4] and in cases, for OEM suppliers to fulfil a targetted Automotive Safety Integrity Level (ASIL), as well as using Failure Mode Engineering Analysis (FMEA) [5] to ensure full conformance. Both HARA and FMEA results in defining safety goals for the AV or ADS. The safety goals aim to avoid hazardous events or to contain the impact of the hazard if it happens – all defined during iterative development lifecycle. The actions derived for the safety goals are important as they dictate how the vehicle reacts when a hazardous event occurs. In many cases, it is not possible to statically define all types of hazardous events in the development phase and this results in the AV being exposed to high safety risk when it encounters a new hazardous event on the road. This is further exacerbated with the driver "out of the loop" [6] and the ADS assumes the full responsibility [7] as there is no driver to assess the risk in real-time and to determine the mitigating actions. As a result, real-time risk and safety measurements (e.g. risk and safety aspects of sudden pedestrian dashing across the road) need to be considered. Without the driver in place, the existing HARA process is no longer sufficient to replace the human decision in detecting new hazardous events [8]. To address this gap, in addition to simulation and data collection during AV trials (which will only extend the boundaries of the static process), a new additional responsive framework is required to complement traditional methods. This will achieve better identification of hazardous events as well as to fulfil the coverage of Safety Of The Intended Function (SOTIF) [9] [10] by measuring the real-time operation of AV when a hazardous event emerges in a real-world setting.

In this paper, we propose a novel Real-Time Risk Assessment Framework (ReRAF) to complement HARA and FMEA to enhance the safety of AV. The existing HARA is performed at the vehicle level while FMEA focuses on the modular level within an AV. ReRAF is able to dynamically calculate the risk in terms of a potential collision, the controllability of the AV in terms of applied speed, braking and steering. Essentially, our framework measures the risk of collision in real-time, and then compute a Predicted Risk Number (PRN) and Safety Level (SL). The PRN is a risk number indicating possible collision of the AV with objects such as pedestrian and vehicles within its operating path, while SL is a classification of the safety levels that is mapped onto a set of recommended actions to ensure the safety of the AV. These improvements can be further classified into AV latitudinal or longitudinal control actions.

In addition, the ReRAF keeps a history of PRNs with respect to time and location of the hazardous event. This allows for recursive learning by comparing the present PRN

with the past to derive the most appropriate risk number, (known as $PRN_{weighted}$) as the true reflection of the risk of collision and subsequently determine the SL that will trigger the necessary actions on the ADS to mitigate the hazardous event. Therefore, the ReRAF framework addresses the gap caused by the driver "out of the loop" and provides better RA clarity in a real-world, real-time setting. The contributions of this paper are as follows.

- A novel framework for real-time risk assessment addressing higher autonomy needs.
- A critical evaluation of existing RA methods and their suitability for higher autonomy of AV or ADS.
- Illustration of the framework's ability through an application use case.

This paper is organized as follows: Section II presents related works on AV or ADS risk assessment and Section III describes the ReRAF in details, followed by the application use case in Section IV. We conclude the paper with future works in Section V.

II. Related work

RA is conducted using various approaches such as process-driven, dynamic processing and modelling based. In terms of developing RA for AV, traditional OEM will rely on the existing process-driven approach while the new players will attempt to use a mixture of different approaches. This Section explains some of the existing or research approaches and provides some technical comparison and reasoning for its usage.

HARA and FMEA are clear examples of process-driven RA approaches and have been used extensively for driven vehicle development lifecycle and AV development as well. HARA process focuses at the vehicle level, with proposals that use iterative loops to refine more dimensioning of the hazardous events and functional aspects [11] in a more organized approach. Riding on the same process, Stolte et al. [12] suggested an additional loop involving safety requirements and added clarity in describing the intended safety goals and safety concepts. HARA process uses severity levels in terms of probability of the hazardous event happening and controllability class to determine the ASIL level. This is similar to the RA approach used in our workplace for safety and health regulations [13] which is considered static and missed real-time hazardous events which were mentioned earlier. If the latter consists of a high severity rating, the desired control actions will be omitted which will be detrimental towards safe AV operation. In the same way, FMEA uses the severity of the hazardous event and the probability of happening to determine the value of the Risk Priority Number (RPN). The value of RPN is determined by the multiplication of the rating of the severity and probability of the identified hazardous event. If the RPN values exceed certain levels (rule-based), further control actions are required to refine the safety goals. These process-driven approaches rely heavily on existing lesson learnt and the expertise of the developers which can be an issue for new AV developers without automotive background and experiences.

Another approach known as Dynamic processing of RA was reported by Wardzinski [14] where the vehicle control system evaluates the risk of possible actions and then selects the one that is the least risky in the context of the current situation and environmental conditions. For this method to be feasible, some form of real-time processing is required. Therefore a further enhancement was suggested in Khastgir et al. [15] by adding real-time detection of hazardous events and providing a real-time ASIL to affect the decision and control for AV. However, this determination of hazardous events and thereafter real-time ASIL do not reflect the instantaneous dynamic risk and safety representative of the environment at a specific time and location [8]. The ASIL outcome only reflects the severity and likelihood occurrence of hazardous events.

The novel ReRAF, measures the risk tagging of the potential collision with the object and control tagging of the operational AV instead of using severity and probability of the hazardous event. Moreover, ReRAF occurs in real-time and performs analytical comparison over a spatial and temporal domain (which covers multiple domains of process-driven and modelling-based). The outcome provides a quantitative risk indication known as PRN and a safety representation known as SL. The recursive steps take place in learning the PRN over accumulative trips using temporal and spatial determination for the precise hazardous event. This temporal and spatial domain learning enables continuous refinement of the risk and safety representation of the AV. Another advantage of this approach entails the prevention of AV from being overly cautious during operations. For example, reducing the speed of AV operation reduces the risk figure but it must be done at a particular location and time of interest only. Otherwise, it reduces the operational level and efficiency of the AV.

This proposed framework also aims to identify new hazardous events compared to a process-driven approach. These newly discovered hazardous events will surface in advance and allow AV to have sufficient time to react and these potential safety actions include the rate of increasing/decreasing speed, rate of braking and angle of steering without changing the basic operations of the AV. These adjustments are normally determined as the fine-tuning of AV performance. Although it may seem that this fine-tuning is not major in terms of the AV functional aspects but it brings a significant difference in terms of commuter experience. For example, it is not desired that braking happens abruptly when an obstruction is detected at proximity. Passenger safety will be in jeopardy if the AV is a bus full of commuters.

III. Real-Time RA framework (ReRAF)

The main objective of the ReRAF is to capture, record real-time hazardous events, subsequently compute a Predicted Risk Number (PRN) and determine the Safety Level (SL) of the AV with respect to the hazardous event. By knowing the PRN and SL in advance of the potential occurrence of the hazardous events, the ADS will be able to automatically plan for better safety goals during AV operations.

Figure 1 shows the interaction between the proposed ReRAF with the other building blocks of a typical ADS which consists of Global Navigation Satellite System (GNSS), Inertial Measurement Unit (IMU), camera and/or Lidar, drive-by-wire system and AV database. The ReRAF is an additional software module within the AV and it does not intervene with the existing design or decision making of the ADS. The ReRAF computes PRN and SL by processing information available from a standard AV on its positioning, localization,

sensor data - such as camera and Lidar as well as information of the vehicle control and its database.

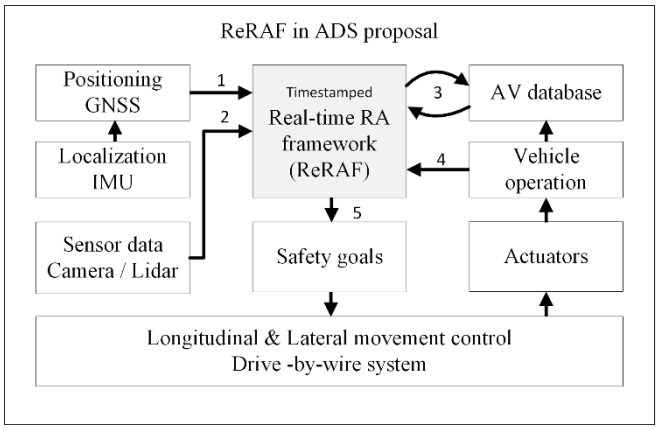

Fig. 1. Implementation of ReRAF in an ADS

A. ReRAF operational block diagram

Figure 2 illustrates the detailed operational blocks of ReRAF. The framework operates with timestamping which consists of the day, month, year, hour, minutes, seconds and milliseconds. The location and time are obtained from the vehicle's GNSS and IMU sensors. Table II denotes the notation to be used in ReRAF.

TABLE II. NOTATION OF RERAF

CT	Control Tag figure
PRN	Predictive Risk Number
$PRN_{weighted}$	Average PRN figure or occurrence
RPN	Risk Priority Number
RT	Risk Tag figure
$S\alpha$	Severity Level (S1 to S3)
SL	Safety Level.
$Sp\alpha$	Speed Levels (1.0 to 3.0)
Trip	Total number of trips that occurred at location x at a specific time t.

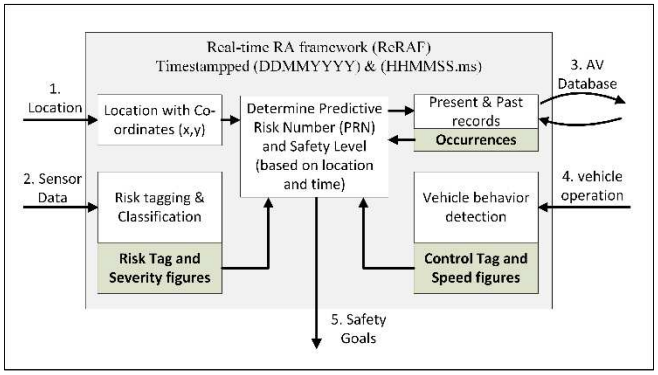

Fig. 2. Operational blocks of the ReRAF

ReRAF focuses on four factors, namely Severity level ($S\alpha$), Risk Tag figure (RT), Control Tag figure (CT) and Speed ($Sp\alpha$) to determine the PRN and SL. $S\alpha$ and RT are determined based on AV's sensor data such as Lidar scan or camera images. ReRAF uses the existing real-time object detection and classification methodologies to determine the $S\alpha$ and the RT within the sensor field of view. $S\alpha$ is derived based on the expected severity of the collision with respect to the types of objects involved, while RT is computed based on the distance of the obstructing object to the AV. For example, if a human is detected, $S\alpha$ will be higher, while if a small piece of rock (that does not hinder the drivability on the pathway) is detected on the road, the $S\alpha$ will be small. The CT represents the detected AV controls such as the reaction and intensity of braking and steering actions that took place in reacting to the hazardous event. While $Sp\alpha$ of the AV is used as an amplification factor. Therefore, high CT represents the high values of uncontrolled AV behaviour. The details are further explained in Section III-C with an application use case illustrated in Section IV.

The ReRAF determines PRN based on $S\alpha$, RT, CT and $Sp\alpha$ at that particular time and location which form a tuple data to be stored in the AV database. To identify the occurrence of these hazardous events over a period of time, a weighted PRN is used. The $PRN_{weighted}$ represents the average PRN over the total number of trips that occurred in that particular location and time. This $PRN_{weighted}$ is also stored in the AV database and updated over time. The determination of $PRN_{weighted}$ forms the recursive aspect of the ReRAF.

Therefore, during real-time ReRAF operation, the information is timestamped in milliseconds and the previous records are retrieved to perform a comparison of the present PRN with the $PRN_{weighted}$. If a large delta exists, improvement of safety actions will be triggered based on SL. This will be further explained in Section III-E. The triggering of safety goals improvements can be automated based on the determined SL.

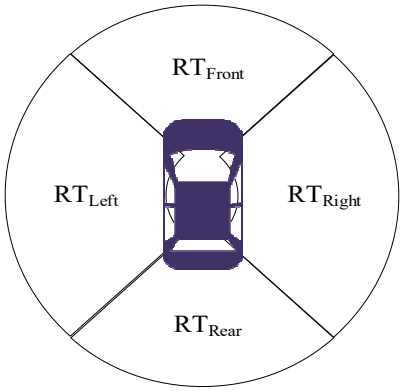

Fig. 3. Segregation of 360° view for risk regions

B. Ego vehicle 360° view risk tagging figure (RT) in segregation zones

To cover the detection of risk and safety aspects of the complete environment, the AV needs to segregate its surrounding environment into a minimum of four critical zones: front, rear, left and right sensing. All four zones should have their individual RT. Therefore, the determination of PRN uses the present risk indicated in TABLE III, as the zonal area for RT. One of the main advantages of this approach is the ability to pre-determine the RT independently from the speed of the AV. This pre-determination of RT indicates the risk of collision with any identified object in the surrounding environment. These RT can be used for the ADS as a pre-warning risk of collision. The segregation of zones can be illustrated in Fig. 3. They are represented as RT_{Front}, RT_{Rear},

RT_{Left} and RT_{Right}. All four regions can have their RT continuously tagged in real-time as shown in TABLE III.

TABLE III. RISK TAG FIGURE (RT) ASSOCIATED WITH THE DIRECTION OF TRAVEL

Direction of travel	Next intended direction	Present risk	Forecasted risk	Background risk
Forward	Left turn	RT_{Front}	RT_{Left}	RT_{Right}, RT_{Rear}
Forward	Right turn	RT_{Front}	RT_{Right}	RT_{Left}, RT_{Rear}
Forward	Changing to next left lane	RT_{Front}	RT_{Front}, RT_{Left}	RT_{Right}, RT_{Rear}
Forward	Changing to next right lane	RT_{Front}	RT_{Front}, RT_{Right}	RT_{Left}, RT_{Rear}
Reverse	Parking	RT_{Rear}	RT_{Rear}, RT_{Left}, RT_{Right},	RT_{Front}
Stop	Stop	All regions	All regions	NA

When an RT level is high in a particular zone, a hazardous event is flagged and recorded in that specific time and location. This RT level (present risk) can be identified in which specific region the hazard occurs when the AV is in operation (forward, reverse, stop). For example, when the AV is moving forward, the present risk is RT_{front} while having RT_{Left} or RT_{Right} as a background risk. If the AV approaches a potential hazard in the forward direction of travel, the RT_{front} will increase as it goes nearer. Likewise, when a high RT_{Left} occurs, this represents a hazardous event that has occurred at the left of the AV. Therefore if the ADS decides to make a left turn, the RT_{Left} can be used as an advance risk indicator. In another example, if RT_{Rear} is high, then it is not advisable for the AV to reverse until the RT_{Rear} drops. Thus the different RTs as shown in TABLE III act as a prediction for the next direction of travel. A summary of the different possible scenarios is provided in TABLE III. Background risk represents the associated RT in non-intended direction of travel. TABLE III shows some of the possible combinations of RT (in terms of zone(s)) in accordance with the intended travel of AV as the main consideration.

C. *Severity (S_α), risk tag figures (RT), speed (Sp_α), control tag figures (CT) and occurrence indicators ($PRN_{weighted}$)*

As mentioned in Section A, the ReRAF uses S_α, RT, CT and Sp_α and occurrence indicators to obtain the PRN and SL while $PRN_{weighted}$ is obtained over accumulated occurrences of PRN at that particular location and time.

RT is triggered by detected objects and provides a certain range of values that corresponds to the distance of the AV to the object. The further the object is to the AV, the lower the RT. The set of values indicated in TABLE IV are intended for illustration purpose.

The detection method can be achieved by using any known deep learning vision approach. For example, YoloV3[16], YoloV4 [17] and EfficientDet [18] and ASFF [19] which provide resolutions to object detection such as bounding boxes and object classification.

As shown in Fig. 4, we adopted YoloV3 to perform object detection. If the bounding boxes are within the region of detection, the RT process will start while S_α will be determined by the object classification method. TABLE IV further illustrates the potential guidance for RT and S_α using a rule-based approach for object detection. The overall processing time of the RT depends on the frame per second of the capturing image sensors. In terms of image aspects, a typical 15 frames per second is expected and the RT processing will take typically 200ms.

TABLE IV. RISK TAG FIGURE AND SEVERITY RATINGS

Severity (S_α)	Risk Tag description	Risk Tag figure (RT))
S1 level ($S_\alpha = 1.0$) Such as small non-living objects	Detected objects in the region of interest (RT increases when the object is closer to the AV)	04 (>50 meters)
		06 (26 – 50 meters)
		08 (11 – 25 meters)
		10 (5-10 meters)
		20 (< 5 meters)
S2 level ($S_\alpha = 2.0$) An object that will hinder the drivability	Detected objects in the region of interest (RT increases when the object is closer to the AV)	04 (>50 meters)
		06 (26 – 50 meters)
		08 (11 – 25 meters)
		10 (5-10 meters)
		20 (< 5 meters)
S3 level ($S_\alpha = 3.0$) Such as human and(or) large object that will obstruct vehicle	Detected objects in the region of interest (RT increases when the object is closer to the AV)	04 (>50 meters)
		06 (26 – 50 meters)
		08 (11 – 25 meters)
		10 (5-10 meters)
		20 (< 5 meters)

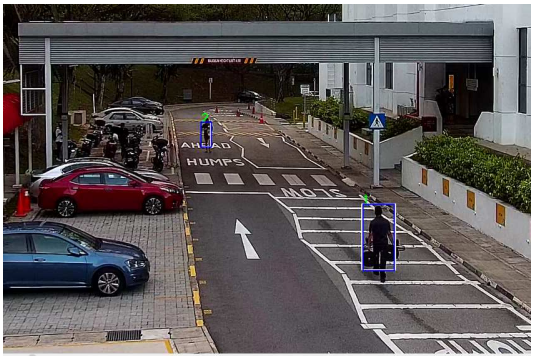

Fig. 4: Pedestrian detection using YoloV3 achieve in 15 FPS

The CT is a measurement of the sudden events that occur when an AV is in operation. This includes triggering safety actions from the AV. The CT gives a higher number when there are more sudden manoeuvres of the AV. There is an amplification factor in relation to Sp_α. This is illustrated in TABLE V. In terms of vehicle data, the information is available every 5 milliseconds via CAN data of the vehicle and the processing will take typically 100 milliseconds. The set of values indicated in TABLE V are intended for illustration purposes.

TABLE V. CONTROL TAG FIGURE AND SPEED

Spα	Condition (i.e)	CT
Speed level 1 (Spα =1.0) Speed is less than 40 km/h	Gradual slowing down and/or no slight steer	0.2
	Low (intermittent) braking and/or no slight steer	0.4
	Sudden braking and/or no slight steer	0.6
	Sudden braking with steering	0.8
	Sudden brake and oversteering	1.0
Speed level 2 (Spα =2.0) Speed is between 40-80 km/h	Gradual slowing down and/or no slight steer	0.2
	Low (intermittent) braking and/or no slight steer	0.4
	Sudden braking and/or no slight steer	0.6
	Sudden braking with steering	0.8
	Sudden brake and oversteering	1.0
Speed level 3 (Spα =3.0) Speed is more than 80 km/h	Gradual slowing down and/or no slight steer	0.2
	Low (intermittent) braking and/or no slight steer	0.4
	Sudden braking and/or no slight steer	0.6
	Sudden braking with steering	0.8
	Sudden brake and oversteering	1.0

D. *Use of database and occurrence to determine $PRN_{weighted}$*

The occurrence figures that contribute to $PRN_{weighted}$ are automatically recorded by the ReRAF into the AV database. The determination of the $PRN_{weighted}$ is considered as a recursive process since it is continuously updated over a period of time with increasing occurrences. A sample of the described data is listed in TABLE VI. The ReRAF records are timestamped with location-based information to provide PRN, $PRN_{weighted}$, SL, using Sα, RT, CT and Spα. The ReRAF module will determine in real-time the SL at each waypoint or by a fixed distance determined by the ADS. The current PRN determined at the time (t_X) and location (latitude and longitude, obtained from GNSS) shall be compared with the previously computed $PRN_{weighted}$. If the present PRN has a large delta compared to $PRN_{weighted}$ from the AV database, evaluation of safety goals will be triggered with the dependency on the calculated SL (more will be illustrated in Section IV). Using ReRAF, the AV will be able to know if more aggressive safety actions are required for the present operation and future runs over the same route and time.

In addition, during each maintenance cycle of the AV, the owner of the AV fleet can decide if it is necessary to improve the safety aspects of AV operations, by modifying the corresponding safety goals needed for decision making. The validation of this improvement can be validated via simulation for the specific location using scenarios recorded in the AV database.

E. *Derivation of the predictive risk number (PRN), weighted predictive risk number ($PRN_{weightaged}$) and safety levels (SL)*

As part of the ReRAF, PRN is calculated as shown in Equation (1). The corresponding SL is then determined by the PRN levels as shown in TABLE VII. An average $PRN_{weighted}$ as shown in Equation (2) is derived for comparison with the present PRN figure. If the present PRN is lesser than $PRN_{weighted}$, this indicates the situation has improved against the hazardous event either from a better vehicle behaviour represented by CT or the hazardous event risk has lowered, represented by RT. The number of times the AV uses the same location and time is recorded as the number of trips. The overall processing time of PRN is expected to be 300 milliseconds based on initial evaluation.

TABLE VI. SAMPLE OF DATABASE INFORMATION FROM RERAF

Time (HHMMSS.mS)	Location (latitude, longitude)	SL	PRN	$PRN_{weighted}$	Sα	RT	Spα	CT
113801.020	1.301355, 103.783635	4	4.8	3.2	3	4	1	0.4
113801.040	1.301519, 103.783514	4	1.6	1.6	1	8	1	0.2
113802.000	1.301682, 103.783356	4	1.6	1.6	1	8	1	0.2
113802.020	1.301763, 103.783291	1	21.6	3.2	3	6	2	0.6

$$PRN = S_\alpha \times RT \times Sp\alpha \times CT \quad (1)$$

$$PRN_{weighted} = \sum_{1}^{Trips} \frac{PRN_{trip}}{Trips} \quad (2)$$

TABLE VII. SAFETY LEVEL RATING

SL	PRN	Actions
1	>20	Safety actions are immediate.
2	10-19	Safety actions need to be planned.
3	5-10	Safety actions to be considered.
4	<5	No actions needed

IV. APPLICATION USE CASE

The operation of ReRAF is demonstrated in this section using an application use case as an example.

A. *First trip to Location A at specific time t*

Figure 5 Illustrates the hazardous event detected in real-time at Location A, at time *t* (18 hours 38 minutes 10.1 seconds). In this situation, a pedestrian (detected as a traffic violation) suddenly dashes across the road 10 meters away from the AV travelling at 60 km/hour. The AV decides to perform sudden braking with steering as a result of its default emergency handling.

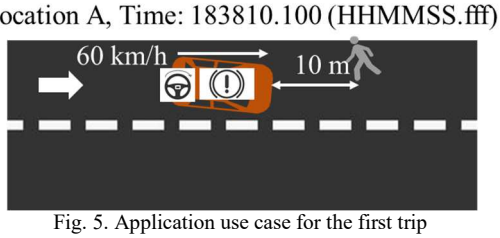

Fig. 5. Application use case for the first trip

By applying the ReRAF framework and based on TABLE IV, S_α = 3, RT = 10, TABLE V, Sp_α = 2, CT=0.8. Using Equation (1), PRN = S_α x RT x Sp_α x CT = 48. Therefore based on TABLE VII, SL is classified as 1. As this is the first occurrence, $PRN_{weighted}$ = 0. Since PRN is greater than $PRN_{weighted}$ and SL is 1, this information will be sent to the ADS to perform safety actions in real-time. The safety actions include sudden braking and steering if emergency handling has not been triggered prior. Subsequently, $PRN_{weighted}$ will be updated using Equation (2). PRN, $PRN_{weighted}$, SL, S_α, RT, CT and Sp_α will be stored in the AV database reference to location A and time t, as shown in TABLE VIII. The mapping of safety actions to the values of PRN and SL is accomplished before the operations of the AV.

TABLE VIII: DATABASE WITH THE RERAF VALUES AFTER THE FIRST TRIP

Time (HHMMSS. mS)	Location (latitude, longitude)	SL	PRN	PRN weighted	S_α	RT	Sp_α	CT
113810.100	A	1	48	48	3	10	2	0.8

B. *Second trip to Location A at time t*

With the AV navigating a second trip to Location A, taking into account the ReRAF values stored in the AV database, the AV plans a safety action by reducing the operating speed from 60 km/hour to 40 km/hour when it is close to Location A at time *t* (shown in Fig 6). This reduction in operating speed will allow more braking distance and thus more reaction time for the AV when a pedestrian dashes across Location A at the same time *t* again. With ReRAF operating in real-time recursively, the figures in the AV database as shown in TABLE VIII will be updated to TABLE IX. The new PRN of 4.8 will reflect the reduction in operating speed for the second trip and since it is smaller than $PRN_{weighted}$ in TABLE VIII and SL is 4, no additional safety actions are required.

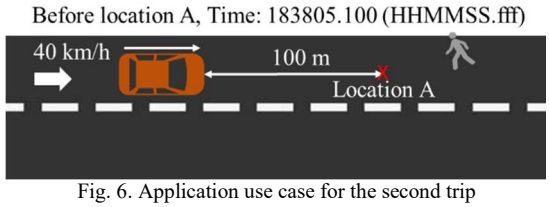

Fig. 6. Application use case for the second trip

TABLE IX. DATABASED WITH THE RERAF VALUES AFTER THE SECOND TRIP

Time (HHMMSS. mS)	Location (latitude, longitude)	SL	PRN	PRN weighted	S_α	RT	Sp_α	CT
113810.100	A	4	4.8	26.4	3	4	2	0.2

This application use case demonstrates the usability of the ReRAF to trigger safety actions depending on the values of PRN, $PRN_{weighted}$ and SL. PRN gives the instantaneous risk number at that specific location and time while $PRN_{weighted}$ provides an average PRN figure of that location over the same period of time. $PRN_{weighted}$ can be used as a reference for other AV vehicles as well. Since ReRAF operates real-time and at a precise location and specific period of time, any advance safety action implemented is not broadly used for all location and at all time, thus this optimizes the operation of the AV (to prevent being over-conservative) and apply safety actions only when it is hazardous events are identified.

From utilizing ReRAF in a temporal and spatial domain in terms of the AV operations, over a period of time assists the AV in predicting advanced safety reactions to avoid potential hazardous events. ReRAF approach focuses on the risk of collision within the environment and the instantaneous operation of the AV while existing HARA and FMEA methods focus on the potential hazardous events caused by malfunction systems during development. Thus identifying the key differences in approaches and propose that ReRAF to be implemented in addition to existing HARA and FMEA.

V. CONCLUSION

In this paper, a novel ReRAF has been developed. The proposed framework acts as an additional layer of RA for safer AV operations. ReRAF provides PRN and SL in the temporal and spatial domain in real-time situations. PRN and SL are uniquely formulated based on RT, S_α, Sp_α and CT determined from the framework which is stored in the AV database (both local and remote). These PRNs and SLs are used to trigger the ADS for safety action improvements while $PRN_{weighted}$ can be used to predict future safe AV operations via a recursive process. Unlike traditional HARA which focuses on functional hazardous events' severity and the likelihood of occurrence for risk assessment, ReRAF uses real-time recursive risk assessment based on AV collision to the detected hazardous object and controllability of the AV. This paper illustrates the purpose, importance and design of this framework, demonstrated with an application use case. The next steps are to simulate, perform test trials and validate ReRAF in scenarios where PRN is known to be high.

ACKNOWLEDGEMENT

We are thankful to MooVita Pte Ltd for their collaboration to explore, perform trials and fine tune the proposed ReRAF framework with their AV development team. This work is sponsored in part by Ignition Grant from Singapore Institute of Technology and with kind support from the University of Glasgow Ph.D. Scholarship for 1st Author.

REFERENCES

[1] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE, 2018. [Online]. Available: https://www.sae.org/standards/content/j3016_201806/

[2] *Surace Vehicle Recommended Practice (r) Considerations for ISO 26262 ASIL Hazard Classification*, SAE, 2018.

[3] M. A. Gosavi, B. B. Rhoades, and J. M. Conrad, "Application of Functional Safety in Autonomous Vehicles Using ISO 26262 Standard: A Survey," in *SoutheastCon 2018*, 19-22 April 2018 2018, pp. 1-6, doi: 10.1109/SECON.2018.8479057.

[4] S. Khastgir, S. Birrell, G. Dhadyalla, H. Sivencrona, and P. Jennings, "Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems," *Safety Science,* vol. 99, pp. 166-177, 2017/11/01/ 2017, doi: https://doi.org/10.1016/j.ssci.2017.03.024.

[5] *IEC 60812 Failure modes and effects analysis (FMEA and FMECA)*, IEC, IEC, 2018.
[6] H. Martin, K. Tschabuschnig, O. Bridal, and D. Watzenig, "Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?," in *Automated Driving: Safer and More Efficient Future Driving*, D. Watzenig and M. Horn Eds. Cham: Springer International Publishing, 2017, pp. 387-416.
[7] N. Merat *et al.*, "The "Out-of-the-Loop" concept in automated driving: proposed definition, measures and implications," *Cognition, Technology & Work,* vol. 21, no. 1, pp. 87-98, 2019/02/01 2019, doi: 10.1007/s10111-018-0525-8.
[8] F. Warg *et al.*, "The Quantitative Risk Norm - A Proposed Tailoring of HARA for ADS," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 29 June-2 July 2020 2020, pp. 86-93, doi: 10.1109/DSN-W50199.2020.00026.
[9] T. Á, D. A. Drexler, P. Galambos, I. J. Rudas, and T. Haidegger, "Assessment and Standardization of Autonomous Vehicles," in *2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES)*, 21-23 June 2018 2018, pp. 000185-000192, doi: 10.1109/INES.2018.8523899.
[10] O. M. Kirovskii and V. A. Gorelov, "Driver assistance systems: Analysis, tests and the safety case. ISO 26262 and ISO PAS 21448," *IOP Conference Series: Materials Science and Engineering,* vol. 534, no. 1, p. <xocs:firstpage xmlns:xocs=""/>, 2019, doi: 10.1088/1757-899X/534/1/012019.
[11] F. Warg, M. Gassilewski, J. Tryggvesson, V. Izosimov, A. Werneman, and R. Johansson, *Defining Autonomous Functions Using Iterative Hazard Analysis and Requirements Refinement*. 2016, pp. 286-297.
[12] T. Stolte, G. Bagschik, A. Reschka, and M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle," presented at the IEEE Intelligent Vehicles Symposium (IV), Redondo Beach, CA, USA, June 11-14, , 2017.
[13] S. S. Online, "Workplace Safety and Health Act - Workplace Safety and Heath (risk Management) Regulations," no. S 141/2006, Workplace Safety and Heath (risk Management) Regulations, p. 5, 2007. [Online]. Available: https://sso.agc.gov.sg/SL/WSHA1920-RG8#xv-.
[14] A. Wardziński, "Safety Assurance Strategies for Autonomous Vehicles," in *Computer Safety, Reliability, and Security*, Berlin, Heidelberg, M. D. Harrison and M.-A. Sujan, Eds., 2008// 2008: Springer Berlin Heidelberg, pp. 277-290.
[15] S. Khastgir, H. Sivencrona, G. Dhadyalla, P. Billing, S. Birrell, and P. Jennings, "Introducing ASIL inspired dynamic tactical safety decision framework for automated vehicles," in *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, 16-19 Oct. 2017 2017, pp. 1-6, doi: 10.1109/ITSC.2017.8317868.
[16] J. Redmon and A. Farhadi, "YOLOv3: An Incremental Improvement," *ArXiv,* vol. abs/1804.02767, 2018.
[17] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: Optimal Speed and Accuracy of Object Detection," *ArXiv,* vol. 2004.10934v1, 2020.
[18] M. Tan, R. Pang, and Q. V. Le, "EfficientDet: Scalable and Efficient Object Detection," *ArXiv,* vol. 1911.09070v7, 2019.
[19] S. Liu, D. Huang, and Y. Wang, "Learning Spatial Fusion for Single-Shot Object Detection," *ArXiv,* vol. 1911.09516v2, 2019.