Risk Assessment Methodologies for Autonomous Driving: A Survey

Wei Ming Dan Chia, *Member, IEEE*, Sye Loong Keoh, Cindy Goh, *Senior Member, IEEE*, and Christopher Johnson

***Abstract*— Autonomous driving systems (ADS) in recent years have been the subject of focus, evolving as one of the major mobility disruptors and being a potential candidate for deployment in urban cities due to urbanization. ADS is the system within the Autonomous Vehicle (AV) that enables automation. The different ADS technologies that enable autonomous vehicles have reached a certain maturity that no longer focus on technological deployment, but rather on the safe deployment on public roads. However, existing standards that validate functional safety and Risk Assessment (RA) may not be sufficient to tackle the increased complexity of ADS compared to traditional vehicles. This demand in ADS safety is exponentially increasing in tandem with the increase of AV automation levels. ADS are exposed to diverse environmental conditions and therefore subjected to operational risks while attempting to mimic the human driver responses. Moreover, the recent use of artificial intelligence and machine learning in the industry further shapes the way how ADS development will become in the future. This paper explains the importance of RA coverage for AV and provides a comparison and summary of existing RA methodologies. Thereafter, a recommendation of RAs for AV as potential solutions in meeting ISO 26262 and ISO/PAS 21448 standards.**

***Index Terms*— Autonomous vehicle, intelligent vehicle, risk analysis, vehicle safety management.**

I. Introduction

THE impact of Autonomous Vehicle (AV) to the transport industry is also known as the pinnacle of the fourth industrial revolution [1], [2]. AVs have been actively used by companies to showcase technological advancement and capabilities, thus demonstrating the company's technological strategy and vision of autonomous mobility [3] for the future. The intention of AV is to enhance better mobility for the elderly and disabled people [4] and to fulfil commuters' mobility demand in growing urban cities [5] without the need to build more infrastructures [6]. Furthermore, there is an increasing trend of using AV as a form of luxurious and efficient transport for the high-end market segment [7]. These motivations led vehicle original equipment manufacturers (OEMs) to invest heavily in AV development and deployment for the coming decades. Besides having to overcome their challenges with the digitalization of new business models [8], traditional vehicle OEMs will now have to create marketable solutions that lead to AV deployment in the near future. This deployment started with basic in-vehicle systems that assist the driver with more safety considerations and convenience. Features like driver-assisted systems, lane-keeping assistant, anti-collision system and eventually Advanced Driver Assisted System (ADAS) [9] mark the first success of basic ADS, which is commonly known as Society of Automotive Engineers (SAE) level 2. The SAE levels [10] defines the different degrees of vehicle automation with level 5 being the highest and level 0 with no automation. Thus, as the SAE level increases to achieve full automation, the validation of the AV or ADS becomes more complex with the use of new technology like Artificial Intelligence (AI) and machine learning.

In addition to traditional vehicle OEM manufacturers, new players have joined the market – riding on the wave of digitalization in the automotive sector. Companies in the sector of Information Technology, mobile network players, and transport start-ups have launched initiatives to develop fully self-driving vehicles from scratch [11]. Waymo and Tesla are successful examples and they have launched their own services or vehicles while others engaged in collaborative consortiums. These consortiums raised capital to develop ADS vehicles [12] for trial and deployment. To deploy AVs on public roads will require the passing of AV designated traffic rules in order to get governmental approval. Therefore, AV companies and their ecosystem partners started to search globally for countries that are ready to testbed this technology deployment with potential business cases. Thus in recent years, a global ranking of ADS readiness report was released [13], showing countries like the Netherlands and Singapore leading the level of preparedness for AVs. Such an ecosystem will attract AV owners and companies to invest in these countries and test their ADS for deployment, leading to a positive economic impact. Examples of governmental endorsement include The Netherlands taking an active role in the AV safety and legal issues with their minister announcing that a "driving license" will be required for self-driving cars [13], while Singapore announced the deployment of AV Buses in three towns (also known as districts) by 2022 in order to reduce private vehicle ownership [14]. AV Buses without the presence of the driver, will have even more risk domains to consider, such as in-vehicle security and emergency management [15], [16].

Manuscript received 6 February 2020; revised 20 February 2021; accepted 14 March 2022. Date of publication 13 April 2022; date of current version 11 October 2022. This work was supported in part by the University of Glasgow Ph.D. Scholarship. The Associate Editor for this article was A. Eskandarian. *(Corresponding author: Wei Ming Dan Chia.)*

Wei Ming Dan Chia is with the Singapore Institute of Technology, Singapore 138683 (e-mail: dan.chia@Singaporetech.edu.sg).

Sye Loong Keoh is with the School of Computing Science, University of Glasgow, Singapore 567739 (e-mail: syeloong.keoh@glasgow.ac.uk).

Cindy Goh is with the School of Engineering, University of Glasgow, Singapore 599493 (e-mail: cindy.goh@glasgow.ac.uk).

Christopher Johnson is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, Northern Ireland BT7 1NN, U.K. (e-mail: c.w.johnson@qub.ac.uk).

Digital Object Identifier 10.1109/TITS.2022.3163747

For any AV to operate on public roads, safety is the utmost key consideration for deployment. The consequence of any deviation from function safety actions or direct harm results in a non-linear fatality risk level where multiple fatalities are involved [17]. Therefore, to achieve a high level of safety for AV, a well-considered approach of Risk Assessment (RA) is needed as part of the design, verification, validation, and even beyond. This survey paper further illustrates the importance of RA coverage that includes real-time RA for AV deployment. The maturity of RA must assist the AVs in achieving the target of near-zero traffic accidents with the increasing rate of commuters in the coming decades. With the dramatic increase of software and AI component within AV development, existing standards might not be sufficient to cover the safety lifecycle of an AV development that is differentiated from typical automotive. Since AV or ADS developments are relatively new, official requirements and standardization for ADS or AV safety have yet to be strongly established [18]. Research journals, articles, and white papers have been released to educate developers while standardization is still ongoing. One of the most recent publications [19] documented how different vehicle OEM manufacturers and their tier one suppliers emphasizes the importance of safety for AV and highlighted twelve important elements (Safe operations, Operational Design Domain (ODD), Vehicle operator-initiated handover, security, user responsibility, vehicle-initiated handover, interdependency between the vehicle operators and the ADS, safety assessment, data recording, passive safety, behaviour in traffic and safe layer) that are needed to achieve a safe AV. In addition, the National Highway Traffic Safety Administration (NHTSA) has released "A Vision for Safety" report for ADS [20] as a recommended safety framework for ADS. This framework also includes twelve important elements such as System Safety, ODD, object and event detection response, fallback, traffic laws, cybersecurity, HMI, Validation methods, Crashworthiness, Post-Crash behaviour, data recording and consumer education. Therefore, the elements needed to design an ADS by the OEM are similar to the safety framework recommended by NHTSA. These elements are widely studied mostly as isolated topics, but the highest challenge is perceived as integrating them into one ADS. The integrated ADS must emphasize overall safety as the highest priority. Amid AV deployment and testing, not only existing standards are being revised, but new standards are planned in the pipeline to evolve and improve the safety aspect for ADS within the AV [18], [19], [21]. These are necessary for the landscape of vehicles automation, which are fast evolving. Existing RA methodologies may no longer be sufficient and cost-effective to address the upcoming safety demands. New RA methodologies are also needed to address vehicles that are retrofitted with ADS by detecting and preventing new hazardous events – especially if new upgrades are installed. These new RA should also consider the risk of hazardous events which may impact not only the driver but also passengers, pedestrians and even AV operators – going well beyond the existing scope of ISO 26262. Modular solutions with software modifications are perhaps needed instead of redesigning and re-validating the whole vehicle [22] with a clear legal framework addressing the responsibility of the driver, user-in-charge or operator [23].

TABLE I
SUMMARY OF SAE J3016 AUTOMATION LEVELS

Level	Name	DDT	DDT fallback	ODD
0	No Driving Automation	Driver	Driver	n/a
1	Driver Assistance	Driver and System	Driver	Limited
2	Partial Driving Automation	System	Driver	Limited
3	Conditional Driving Automation	System	Fallback-ready user (becomes the driver during fallback)	Limited
4	High Driving Automation	System	System	Limited
5	Full Driving Automation	System	System	Unlimited

In this paper, the contribution is as follows:

- Focus on the need to increase RA awareness for AV Dynamic Driving Task (DDT) fallback for higher SAE levels, while explaining the key objectives of RA to meet the ISO 26262 and ISO/PAS 21448 standards.
- Define RA coverage for AV into development and real-time operations using existing research and methodologies.
- Comparative analysis of different RA methodologies in terms of qualitative and/or quantitative approaches with unique approaches.
- An insight explanation of the importance of determinism and uncertainty in RA for AV across the different methodologies.
- Recommendation of different RA approaches either as system or component level for meeting ISO 26262 and if they contribute towards ISO/PAS 21448 standards as well.

This survey paper is organized as follows. Section II provides an overview of Automotive Standards for AV. Thereafter the importance of RA coverage is explained in Section III. This is followed by Section IV with 1) a detailed summary of the different RA methodologies and 2) a comparison of the different techniques within each methodology. The importance of determinism and uncertainty in RA are explained in Section V. Most importantly, the recommendation of RA methodologies that meet the requirements of ISO 26262 and ISO/PAS21448 are explained in Section VI. Lastly, Section VII concludes the survey paper.

II. AUTOMOTIVE STANDARD FOR AUTONOMOUS DRIVING

The rise of ADS has been one of the disrupters of the automotive industry, turning personally owned vehicles into possibilities of shared mobility. The development of ADS is defined by the SAE into 6 levels of autonomy from level 0 to level 5 [10]. Table I shows the SAE J3016 driving automation

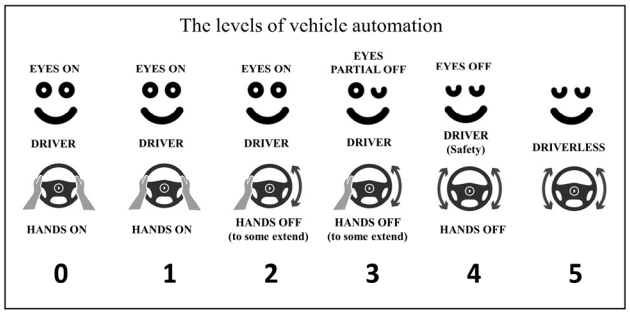

Fig. 1. A summary of the vehicle automation levels.

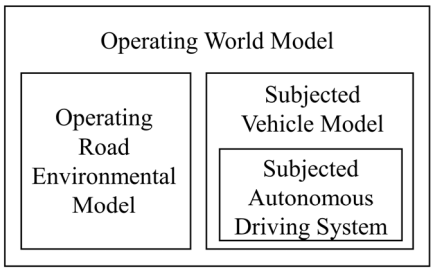

Fig. 2. Operating world model with a single subjected vehicle model and subjected autonomous driving system model.

levels, this automation taxonomy is also widely used for NHTSA [20]. Figure 1 shows another interpretation of the SAE levels by using the hands and eyes of the intended driver [23] in a simplistic manner that is easily understood by the general public. In this paper, the survey focuses on on-road AV and ADS. For off-road vehicles, other standards such as IEC/EN 61508 and ISO 13849 are added for considerations.

SAE J3016 states that automation level 0-1 can be described as a driving assistant in either longitudinal or lateral movements, while SAE level 2-5 consist of driving automation in both longitudinal and lateral approaches. The table also clearly states that the Dynamic Driving Task (DDT) can only be taken over by SAE level 2 ADS onwards but operated with limited ODD till SAE level 4. In contrast, SAE level 5 has no limits of ODD, and it is able to handle all DDT. Therefore, SAE level 5 distinguishes the rest of the SAE levels (Table I), highlighting the importance of ADS maturity at the highest level, taking over the responsibility of keeping the AV and its surroundings safe even in emergencies.

This increasing demand in AV readiness and maturity towards higher levels of SAE automation generates higher demand for safety-critical requirements (especially for SAE levels 4 and 5). The consideration for risk identification, analysis and control becomes a greater area of focus. These safety-critical requirements are effectuated as a result of the ADS replacing the fallback responsibility of the driver, known as driver Out Of The Loop [24]. Thus, the AV will have to rely completely on the ADS to perform risk mitigations when hazardous events are identified and detected.

Thus higher automation levels of AV poses new challenges for commuters' safety in terms of AV deployment. These ADSs are still validated using existing standards like IEC 61508 [25] for electrical and/or electronics elements and ISO 26262 [26] for functional safety assessment. To further elaborate, ISO 26262 is derived from IEC 61508 and its objective is to address potential hazards that might be caused by failure or malfunction of safety-related components in the vehicle.

The challenge with the current ISO 26262 lies in the lack of guidance to manage violations that arise from the faults of the sensors or the processing algorithms that relates to the environment. This can happen when the AV detects a hazardous environment that operates outside the limits of the sensors or algorithms, resulting in functions not performing as intended [18]. Therefore a standardization is required to highlight potential improper function(s) and its operation limits, as mentioned in the recent release of ISO/PAS 21448 [27]. The latter specifies a development process for analysis, verification, and validation of the non-faulted scenarios and also use cases of a system. ISO/PAS 21448, also known as Safety Of The Intended Function (SOTIF), focuses on the awareness of *unknown unsafe* regions of operation compared to known unsafe and unknown safe regions. The limits of these regions can be better defined considering the Operation Design Domains (ODD) approach [7]. Therefore ISO/PAS 21448 can be summarized to address the following (especially for high levels of SAE): 1. Driver out of the loop situation, 2. the non-determinism of AI algorithms and 3. Fail-operational systems [18]. In the aspects of low SAE Levels, ISO/PAS 21448 can be seen to address risk related to external causes due to unintentional misuse and environmental factors [28]. However, the SOTIF standard does not specify the need to identify real-time RA where gaps exist between development and real-world deployment.

Therefore if AV or ADS are to be validated using ISO 26262 [21] and ISO/PAS 21448 [28], an important aspect would be to consider a proper RA coverage of the AV in terms of safety and risk. With AV or ADS operating in an environment where risk and uncertainty can occur due to human variance are considered as non-deterministic. These uncertainties and limits of operations must be converted into measurable forms of actions for the ADS, either to avoid or to improve its performance. This step can be important because it is almost impossible to consider all scenarios and causes of uncertainty during development, even by performing more tests or simulations in different scenarios. Thus, the possibility of encountering any of these unforeseen scenarios can still happen in real-life applications – due to design considerations and limitations. In Section III, we will explain further the importance of RA coverage for AV.

Before diving deep into RA coverage, approach and methodologies, a basic understanding of the taxonomy of ADS and its operating environment are essential. This information as shown in Figure 2 and Figure 3 are extracted from the ISO/PAS 21448 [27], SAE J3016 [10], [29] and ODD for AVs [30]. All transportation is labelled as an instance of an Operating World Model. Each Operating World Model consists of an Operational Road Environmental Model and the Subjected Vehicle Model. Taking AV as an example, Subjected

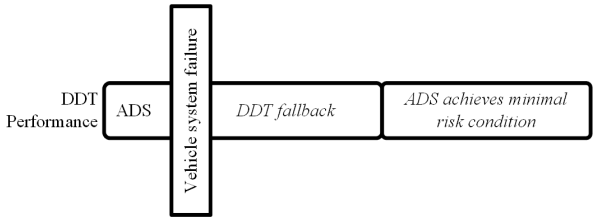

Fig. 3. SAE level 4 with ADS vehicle system failure activates DDT fallback.

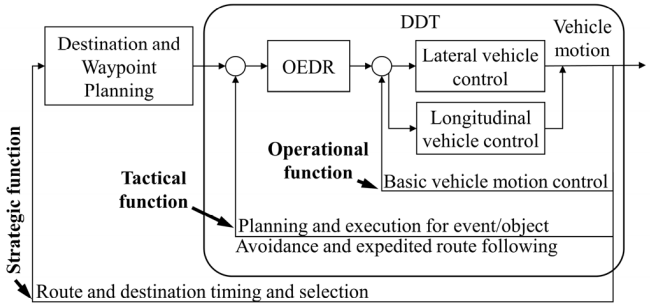

Fig. 4. Block diagram of a DDT portion in a ADS.

Vehicle Model refers to the AV and Subjected Autonomous Driving System refers to the subject ADS within the AV or Subjected Vehicle Model. However, Subjected Vehicle Model can be an AV or a normal driven vehicle. If it is a normal driven vehicle, then Subjected Autonomous Driving System will not exist.

In addition, each of the Subjected Autonomous Driving System or commonly known as ADS controls the DDT and DDT fallback of an AV. The DDT fallback falls under the responsibility of the ADS for SAE levels 4 and 5 as shown in Table I. DDT fallback occurs when a vehicle system failure has occurred, or a hazardous event is detected without any solution. As such the ADS enters into DDT fallback condition and operates with minimal risk condition. Minimal risk condition normally refers to a reduced operational performance with safety in priority. This means the AV can operate at low speed while monitoring environmental risk and monitoring its vehicle health. In normal ADS operations, as shown in Figure 4, the DDT within the ADS is guided by noting its destination and plans for upcoming waypoints. This information is further fused with object and event detection response (OEDR) to achieve vehicle motion control. The lateral and longitudinal motion control eventually determines the AV movement.

Thus the importance of OEDR, lateral and longitudinal motion denotes the importance of DDT. Since OEDR is happening in real-time, the corresponding control motion of the vehicle must be carefully mapped. In the event if the OEDR does not map to any prescribed response in terms of motion, the ADS will enter into the DDT fallback mode. During this mode, the AV will propagate with a minimal risk condition. To operate at minimal risk condition, ADS will need to rely on real-time detection or identification of risk presented in the environment.

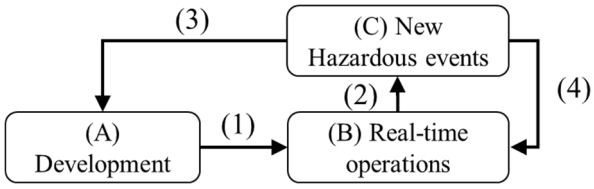

Fig. 5. RA coverage for AV.

As such, to achieve safe AV operations using RA, it is critical to identify the RA coverage of AV during development and real-time operations due to dynamic environmental changes. On top of that, the approaches for identifying risk are also different. The next sections explain how RA can be represented in different areas of coverage and approaches for AV.

III. Risk Assessment (RA) Coverage for Automotive Vehicles (AV)

The objective of RA is to identify the severity of a hazard event using OEDR and determine the mitigation control actions (hereafter known as safety actions) to prevent the event from happening or reduce its occurrence through DDT. The identification of risk from the hazardous event can derive from internal causes (vehicle level) and/or external causes (environmental level) [28]. Internal causes are related to malfunctions, faults and failures, while external causes can be due to the vehicle and environmental conditions or unintentional misuse. Therefore, to ensure sufficient coverage of RA, both development and real-time RA are needed to fulfil ISO 26262 and ISO/PAS 21448. ISO 26262 focuses on the internal causes, while ISO/PAS 21448 focuses on the environmental causes.

Figure 5 illustrates a concise overview of RA coverage for AV, which should include both product development (A) and real-time operations (B) and new hazardous events (unknown safe or unsafe) (C) can still happen during real-time operations, even though there are simulations, trial test and scenarios testing conducted. The RA coverage in this paper focuses on high automation levels 4 and 5 since the safety requirements are critical for the ADS, which do not rely on the human driver at all.

With reference to Figure 5, RA is created and planned during development (A) and are applied for real-time operations (1). However, in real-world deployment (B), it is impossible to consider all possible scenarios during development (A). Therefore, the detection (2) of new hazardous events (C) might cause unpredictable AV actions when it is supposed to react under the DDT fallback mode. At present implementation, these new hazardous events are recorded, and they require another development cycle (3) under maintenance to update and upgrade its new safety actions (if it is unknown unsafe). This reflects the potential exposed risk for every new hazardous event (C), which is not considered during development. Although there are AV trials and simulations for different scenarios, there is still a potential gap for a DDT fallback decision (4) when an unplanned new hazardous event occurs

for the AV. Therefore, in recent years, real-time coverage is also proposed [31]–[34]. To bridge this gap (4), real-time RA is needed to ascertain the necessary actions for the DDT fallback without the need to wait for the re-development loop (3) instead risk is assessed and processed in real-time for safety operations (1) – which can assist the requirement of SOTIF. This could be achieved by using the pre-mapping of safety actions for every new hazardous event detected (4). Moreover, the approach of determining RA for AV consists of 1) vehicle level approach (to detect internal vehicle causes of risk) [35] and 2) environmental level approach (to detect vehicle and environmental causes of risk) [36]. The difference in approaches is further explained in each methodology used for RA in Section IV. Therefore, to accomplish a complete coverage of RA for AV, it is required to have RA developed during product development and also for real-time operations. Within the RA, the accuracy of risk identification and the formulation of safety actions must be identified using different approaches as well.

A. Risk Assessment (RA) During Development for AV

The regulatory RA for AV development is processed under automotive standards ISO 26262 [21] part 3, starting with the safety lifecycle Hazard Analysis and Risk Assessment (HARA) [37]. With HARA process, the outcome provides a safety rating of the identified hazardous events known as Automotive Safety and Integrity Levels (ASIL). Besides HARA, which is evaluated at the vehicle level, FMEA [38] is also commonly used at the modular level of the AV. FMEA is used to determine the severity, occurrence and detection capabilities of the identified hazardous event known as failure mode with a Risk Priority Number (RPN). RPN values will reflect if the planned safety actions are sufficient for the module. Both HARA and FMEA start with identifying potential malfunction that contributes to determining its severity, probability (occurrence) and controllability classes (detection). The controllability classes include the planned safety actions when a specific malfunction occurs. Thereafter, using the ASIL classification table (shown in Table II) to provide an ASIL rating for the identified hazardous event. Within Table II severity of the identified hazardous event is guided towards one severity rating from S1 to S3, with S3 severity close to life-threatening. Meanwhile, probability E1-E4 reflect the likelihood of exposure with E3 defined as a high probability that the injury can happen. Lastly, C1-C3 denote the controllability of the system if that highlighted hazardous event would happen. This ASIL rating represents a qualitative approach towards getting a rating outcome of QM, A, B, C or D. With D being the lowest in safety rating and improvements are needed to bring up its safety levels. Different functional levels of the vehicles or AV require different safety ratings. Hence, if the safety rating of the detected hazardous event caused by a particular function does not meet the ASIL requirement, a redesign or improvement of the safety actions are necessary.

To assist the process of RA during development, other known process tools are used to 1) determine the root cause of potential identified malfunction and/or 2) determine better safety actions. These tools include hazard and operability study [39] and FMECA (extension of failure mode and effect analysis) [40], which are used extensively to meet the traditional IEC 61508 [25] requirements, while Fault Tree Analysis [41] and design failure mode and effect analysis [42] are used to meet ISO 26262 [26]. These tools are classified as qualitative approaches because they consist of systematic descriptive techniques used in identifying the root cause of the potential malfunctions. Thereafter safety actions are determined to resolve/contain the alleged root cause. The safety actions are also termed as the safety goals to achieve an overall functional safety of the AV.

TABLE II

ISO 26262 ASIL CLASSIFICATION TABLE (QM MEANS QUALITY MANAGEMENT LEVEL THAT REPRESENTS HAZARDS THAT DO NOT INDICATE ANY SAFETY REQUIREMENTS)

		Probability Class	Controllability class		
			C1	C2	C3
Severity Class	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

Besides identifying risk in the aspects of functional safety, the existing validation does not include the identification of risk in collision with hazardous events occurring in the environment. The closest reference within standards that refers to environment risk detection would be the OEDR in SAE J3016, which is deemed important for the DDT fallback and DDT operations. Thus, this highlights the need to add risk indications of a potential collision with detected hazardous environmental events. The environmental detection includes and is not limited to Vulnerable Road Users, vehicles and objects. These detections can be enhanced by the recent telemetry or communication infrastructures known as Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2X). The RA conceived during development consists of either 1) Vehicle level and/or 2) Environmental level approach. More details will be further explained in Section IV.

B. Risk Assessment (RA) During Real-Time Operations for AV

From recent works, there is an increasing interest in real-time RA. Especially since the completed RA during development is insufficient to identify all potential hazardous events during real-time AV operations. The research interest of real-time RA stems from the need to have a safety supervisor to safeguard against unpredictable behaviours of intelligent functions and justify malfunction events into parametric constraints that could be detected in real-time [43]. The concept of real-time RA serves more as an additional layer of

assurance to the existing RA framework during development. Real-time RA leans more towards the impact of the risk of collision due to the dynamic changes in the environment. Classical research that triggers the study of real-time RA using the *environmental level approach* is demonstrated by the works of Wardzinski [44]. In another example, real-time RA defines dynamic RA as a safety assurance strategy for AV in addition to traditional RA during development. This dynamic RA rates the risk level with multiple levels, which depends on the real-time environmental conditions instead of using binary representation and pre-determined risk levels [44]. This methodology requires the constant need to maintain situational awareness, identify and execute the safest possible actions after assessing the risk of any current or predicted situation. To accomplish the practical use of this methodology, challenges such as mapping of all potential scenarios must be done to ensure that there is no uncertainty present and all situation risks are assessed. These challenges triggered the work of Khastgir et. al [31], who proposed a slightly modified ASIL framework for the Dynamic Tactical Decision Marking framework for AVs. Instead of using static determination of severity, exposure and controllability ratings, the proposed framework used real-time monitoring of the different parameters guided by rule-based that maps to the corresponding severity, exposure and controllability ratings. Subsequently, a real-time ASIL rating is determined during AV operations. The latter attempts to map the environmental level approach with the vehicle level approach (malfunctions) originally used in HARA. Without detailed work of the mapping process, it is difficult to conceptualise the mechanism of how it would function in real-time. However, this research agrees that the existing static HARA fails to capture the real-time state of the system and have a bearing on the risk analysis probability. In [31], [44], an example of adding a minor quantitative approach to the traditional qualitative outcome is achieved. While in [33] a balanced approach of having both quantitative and qualitative is proposed, where Predicted Risk Number (PRN) is used as a risk figure for evaluating the vehicle and environmental aspects recursively. The PRN is formulated using control tags of vehicle operation together with risk tagging of a hazardous environmental event in the context of a potential collision from the AV. The latter is one example of a model-based RA methodology, which will be discussed in Section IV.

IV. Risk Assessment (RA) Methodologies for Autonomous Vehicles

This section compares different RA methodologies that are used and research for AVs. Table III shows the existing RA methodologies which are grouped into the process, modelling, probability, AI or cooperative based RA and they are collectively indicated if the methodology consists of vehicle and/or environment level approach. Moreover, some of these methodologies can be used for both development and real-time RA. The vehicle level approach refers to the identification of hazardous event using the functional basis of the AV or vehicle and determines risk with the possibility of malfunction. The environmental level approach refers to the triggering of detected hazardous event from the environment with the risk of collision with the AV as the primary motivation. The definition of the RA is determined to be more conclusive if it contains both qualitative and quantitative aspects. However, if the introduction of quantitative involves uncertainty, it should be addressed. These topics of determinism and uncertainty will be discussed in the later section as well as the usability of these RA methods for existing regulatory needs.

As shown in Table III, process-driven methodology [31], [32], [35]–[37], [44]–[47] tends to be more qualitative than quantitative except for [32], where it uses the frequency of incident and numeric classification toward contextual content and match its corresponding safety goals. This is done while keeping the process of HARA intact. Another observation indicates that the majority of the process-driven methodology are considered static (defined during development) except [31], [44] and [32]. In [32], a real-time update of the HARA is proposed, while in [31], a real-time ASIL determination is achieved. Process-based RA methodology performs RA based on contextual descriptions at a higher level (system) perspective. They tend to identify failures or malfunctions in functions starting from the vehicle level and extend them to environmental situations.

Model-based [48]–[50] approaches contain quantitative outcomes, while the process-based contributes more toward qualitative outcomes. Model-based methods RA includes mathematical models such as risk repulsion based on risk field theory [50] or vehicle position and slip angles of tires for collision avoidance [48]. These mathematical models provide a risk indicator to assist RA. In [49] modelling of Unified Modelling Language (UML) is used to automate the HARA process which assists ISO 26262, in this case, it has only qualitative outcomes.

The use of probability and model [51]–[53] methodology in RA provides both qualitative and quantitative outcomes. The approach of [51] places qualitative as a key driving focus, and quantitative aspects are additionally fulfilled by using probability techniques to meet the requirements of ISO26262 and SOTIF from the perspective of high level (system) approaches. Similarly, in [52], scenarios are modelled and probability functions are used to provide quantitative figures. Lastly, [53] describes a specific focus on sensor fusion techniques to improve risk management by using traffic risk assessment.

In contrast, when only probability methodology [54]–[57] is used for RA, their outcome can only be quantitative and therefore with a likely chance that the focus will be at a low level (component level). The major differentiation lies in the method of either detecting collision risk [54], [55] or collision due to occlusion [56], [57]. There is no qualitative approach for RA at high level (system-level) considerations.

In terms of AI-based methodology for RA, there are fewer references due to concerns if AI is suitable for safety-critical system design. It is evident that AI is used for decision making and predictions for the AV and ADS [67]. However, instances of AI for RA is not yet broadly studied.

TABLE III
SUMMARY OF RA METHODOLOGIES

Methodology	Research papers	Qualitative (QL) / Quantitative (QT)	Development		Real-Time
			Vehicle motion	Vehicle and Environment	Vehicle and Environment
Process	HARA/FMEA	QL	Y	N	N
	[46]	QL	Y	Y	N
	[45]	QL	Y	Y	N
	[35]	QL	Y	Y	N
	[36]	QL	Y	Y	N
	[44]	QL	Y	Y	Y
	[31]	QL	Y	Y	Y
	[32]	QT	Y	Y	Y
Mod	[48]	QT, QL	Y	P	N
	[49]	QL	Y	Y	N
	[50]	QT, QL	Y	P	P
	[33]	QT, QL	Y	Y	Y
Prob & Mod	[51]	QL, QT	Y	Y	N
	[52]	QL, QT	Y	Y	N
	[53]	QT	Y	Y	N
Prob	[54]	QT	Y	Y	Y
	[55]	QT	Y	Y	Y
	[56]	QT	Y	Y	P
	[57]	QT	Y	Y	P
AI	[58]	QT	Y	Y	Y
	[59]	QT	Y	Y	Y
	[60]	QT	Y	Y	Y
Co-operative mode	[61]	QT	Y	V2V	V2V
	[62]	QL, QT	N	V2V	V2V
	[63]	QT	Y	V2V	V2V
	[64]	QT	N	V2X	V2X
	[65]	QT	N	V2V	V2V
	[66]	QT, QL	N	V2V	V2V

Legend: Y=Yes, N=No, P=Partial, Prob: Probability, Mod: model

Lastly, cooperative mode RA methodology is an independent approach that focuses on the available data from either vehicle to vehicle (V2V) or vehicle to infrastructure (V2X). The outcomes can also reside in either vehicle or the infrastructure. The comparison of different techniques includes model-based [61], probability and model-based [62]–[64], AI-based [65] and uniquely fuzzy risk-based [66]. Among them, [62] and [66] have both qualitative and quantitative outcomes.

A. Process-Based Methodology

Both HARA and FMEA are considered process-based methodologies that use vehicle level approaches during development. If the intention is to obtain more precise malfunction identification, works such as [46] and [45] illustrate the use of the iterative refinement process in HARA to provide more detailed dimensioning and hazardous event descriptions. This provides a more concise safety goal as mitigation actions for the AV. In comparison to the works of [35], a skilled graph scenario is used to represent the relationship of the potential hazardous event to the operations of an unmanned vehicle. This provides a complete description of the scene in terms of the hazardous relationship instead of using iterative loops.

TABLE IV
RA COVERAGE USING PROCESS-BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
HARA/FMEA	QL	Y	N	N	N	-
[46]	QL	Y	Y	Iter	N	-
[45]	QL	Y	Y	Iter	N	-
[35]	QL	Y	Y	Sk	N	-
[36]	QL	Y	Y	Sc	N	-
[44]	QL	Y	Y	-	Y	DyRA
[31]	QL	Y	Y	-	Y	RASIL
[32]	QT	Y	Y	-	Y	QRN

Legend: Y=Yes, N=No, Iter: Iterative process, Sk: Skill graph, Sc: Scene, Dy: Dynamic RA, RASIL: Real-time ASIL, QRN: Quantitative Risk Norm

Other than using a skilled graph and the scene in determining the likely cause of the hazardous event mapping, [36] added the element of situational consideration to the hazardous event. This approach [36] is considered more detail compared to [35], [45], [46], but likewise, the iterative process from [46] and [45] can further refine the scene, situation and goals and values achieved. The largest difference between traditional HARA and FMEA, and research from [46] and [45] resides in the detection of malfunctions using scenarios, hazard trees and scenes, while [35] and [36] add on more complexity by defining AV operational and environmental limits or barriers as seen in [44]. This monitoring of limits is used in [44] and [31], which corresponds to real-time vehicle and environmental level detections to achieve real-time RA (which was explained in Section IIIB). Furthermore, [32] proposed a new approach known as Quantitative Risk Norm (QRN) to overcome the nature that HARA process is qualitative. QRN is a numeric figure that is dependent on the frequency of the incident within a consequence class and the incident type. The respective QRN is thereafter used to map corresponding safety goals. The comparison of different process-based RA coverage for different research can be seen in Table IV. One observation in process-based RA methodology demonstrates that the steps are purely qualitative followed by using rule-sets to define a regional status to represent severity, occurrence, controllability and eventual risk levels or ASIL rating. This risk level or ASIL rating is further used to define the need for creation/improvements of safety goals. The only exception is on [32] where figures are assigned to the qualitative description of the hazardous event and account for its frequency of incident, thereby including a quantitative element.

The only key drawback of using process-based RA methodology is the lack of quantitative measurement of risk. This could be overcome in some methodologies like probability and/or modelling methodology which considers risk as a quantitative figure.

B. Model-Based Methodology

We would like to firstly summarize studies using model-based methodology independently to assist the simplification

of performing HARA. In works of [49], the use of the UML model is extended for HARA process by using fault-type guide-words and an organized set of situations to determine the relevant causes. In addition, Object Constraint Language (OCL) validation checks are used to validate errors or inconsistencies, followed by mapping of table-based HARA and UML model. This method provides a framework that allows a systematic approach to document and analyse hazardous events with their root cause, thus providing an eventual clear Fault Tree Analysis [41]. UML is commonly used for software and system development for automotive [68]–[70]. This method of modelling for hazardous events and its corresponding safety response can be further extended using model-based scenarios [71] or even model-based safety analysis [72] approaches. These techniques are evident in the recent development of AV during the development lifecycle.

Other than using modelling for vehicles and scenarios, works such as [48] explored the modelling of the latitudinal and longitudinal AV controls, specifically to the path of the road and trajectory of the vehicle movement during the development process. This approach involves using (1) vehicle modelling, (2) Road Geometry modelling and eventually (3) optimization and control algorithm to achieve lane keeping for safe manoeuvring and anti-collision solution. Therefore, this method focuses on lane-keeping and collision avoidance scenarios developed during development. This is achieved by utilizing a numeric cost function to represent RA. This cost function is a qualitative measurement with the objective of optimization and control instead of the direct risk of collision with environmental aspects.

In another research [50], the longitudinal risk element is evaluated from the usage of field theory [73]. Using this method, a quantitative risk figure was obtained for collision prevention (in the case of a vehicle to vehicle). The paper introduces a unique term called "risk repulsion". Risk repulsion is said to be inversely proportionally with Time To Collision. The numeric figure is modelled with an exponential term and the figure gets larger (maximum $= 1.0$) when the rear vehicle is travelling faster than the front vehicle with reducing space between both vehicles. The components within the model take into account the difference in speed and distance between the rear and front vehicle. In this approach, the real-time crash prediction is modelled using risk repulsion.

A recent work [33] used PRN as a figure of RA using the AV control tag and risk tag to determine the indication of the risk that the AV is exposed to. This framework focuses on AV speed, steering and braking control with the severity classification, risk tag of the environmental and distance as a model to the PRN. The level of PRN then further determines the safety levels and the necessity to enhance existing safety goals. Since this framework runs in real-time repeatedly over time at specific locations, past data of PRN can be obtained to determine (during navigation and control) if the AV is going to be exposed to this risk before reaching the designated location. With the mentioned model-based RA methodology in this section, a comparison of the different techniques is summarized in Table V.

TABLE V
RA COVERAGE USING MODEL-BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
[48]	QT, QL	Y	P (R)	Cost	N	-
[49]	QL	Y	Y	UML	N	-
[50]	QT. QL	Y	P (V)	-	P (V)	RP
[33]	QT, QL	Y	Y	-	Y	PRN

Legend: Y=Yes, N=No, P(R) =Partial with Road, P(V): Partial with Vehicle, UML: Use of UML for detail modelling of hazardous events, Cost: Function cost as a form of representative RA, RP: Risk Repulsion, PRN: Predicted Risk Number

C. Probability and Model-Based Methodology

Probability and model-based RA usually consist of a mixture of qualitative and quantitative results. This section compares the different techniques used to perform RA using both model and probability-based methodology.

In [51], other than the identification of scenarios with ADS modelling, the probability of severity and occurrence of the hazardous event triggered by environmental conditions is used. The approach consists of probability spread of the potential severity rating that relates to the hazardous scenario classified and a probability segmentation of the occurrence of the hazardous event within scenarios. The final step correlates to the concept of ASIL where there will be a maximum probability for each rating. This approach evolves around the HARA process for improvements by introducing environmental modelling and probability assignment of conditions. This results in providing both qualitative and quantitative results, which gives a very good guide towards HARA improvements. This method can be implemented during the development lifecycle but may be challenging for real-time reaction due to the different scenarios with dynamic changes in the probability segmentation spread.

Besides the adaption of HARA improvements, [52] uses the probability of damage to assess the context of risk assessment. This probability of damage is dependent on the probability of collision. The probability of collision is based on the selected scenario while considering the specified behaviour of the AV. The approach also uses a model-based UML class diagram for the visualization of the Hierarchical Scenario Description Language for all the descriptive possibilities of scenarios that are being studied (which forms the qualitative aspects). The difference between this approach resides in the detailed involvement of adaptive risk analysis which considers dynamic scenarios in terms of probability of collision. In comparison, [51] focuses more on the probability of severity in terms of occurring hazardous event in scenarios. However, unfortunately, both did not have the opportunity to illustrate with realistic examples to demonstrate their approach.

In terms of RA, there are also different approaches to quantify environmental risk. One of which is demonstrated by [53],

TABLE VI
RA COVERAGE USING PROBABILITY AND MODEL-BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
[51]	QL, QT	Y	Y	Poh	N	-
[52]	QL, QT	Y	Y	P(D)	N	-
[53]	QT	Y	Y	Force	N	-

Legend: Y=Yes, N=No, Poh: Probability of occurrence of the hazardous event by quantification of the environmental conditions, P(D): Probability of Damage (due to the collision at that scenarios), Force: Equivalent forced based theory on the traffic safety field concept

using a model-based equivalent focussed on the traffic safety field concept [74]. Traffic RA is curated using the relationship of the kinetic energy of colliding objects to approximate the risk level based on the real situation. The kinetic energy is eventually translated to equivalent force to describe the traffic risk. They are still working on the risk index model as improvements and suggested to take the Relative Driving Safety Index as a reference on different scenarios. DSI is a reference used for accessing drivers behaviour which relates to safety [75]. This topic itself forms another interest in the domain of human behaviour towards AV operations which is not within the scope of this paper. This approach [53] also focuses on tracking multiple uncertainties in the situation of radar clusters or vision target object occlusion using Dempster-Shafer Theory (DST) probabilistic/evidence theory-based detection-level. This is required to achieve multi-object perception.

Table VI illustrates an overview of the different probability and model-based RA coverage that was discussed. All of which have quantitative aspects either in terms of calculating vehicle and environmental considerations or probability theory involved. In terms of coverage, all three considered both the domain of vehicle and environment during the development lifecycle. The work of [52] and [53] highlights the importance of identification of risk going into collision as a potential indicator in addition to severity, hazardous event and its occurrence.

In terms of the selected three probability and model-based methodology, the approach of [51] is an extension of the existing HARA process. While both [52] and [53] focus on the use of the risk of collision as another form of risk indicator, thus the overall approach will not be as comprehensive in terms of qualitative content.

D. Probability-Based Methodology

Probability as a form of statistics is divided into two main approaches: Bayesian or Frequentist [76]. These two approaches can also be used as probabilistic methods to perform AV or ADS RA, some recent work includes [54]–[56] and [57] research.

In both [54] and [55] the use of probabilistic collision risk is illustrated using vehicle motion and time to collision as the reference. Katrakazas *et al.* [54] proposed the use of a Dynamic Bayesian Network method for motion prediction and RA as well, which is a modified version from [77]. This method was proposed due to the intractable process if an AV was to predict all future trajectory for real-time application. Therefore, they suggested the use of interaction-aware models from DBN for RA and road interaction. Katrakazas *et al.* [54] focus on the risk of collision at the vehicle level and network level. Network level refers to the safety context of the road segment on which the AV is travelling, taking into account safe traffic and collision-prone conditions. The approach for the network-level collision was supported by basic AI classifiers such as k-Nearest Neighbour or Gaussian processes. Two of the Unique approaches of this proposal are the Collision Risk Network-level (CRN) and Collision Risk Vehicle level (CRV). Since DBN is considered as a form of spatial-temporal approach, there is a forward improvement of the current information with dependency from the past. Therefore, some basic aspect of learning from the past is applied in this approach. This approach behaves well for real-time application with learning from the past risk (which eventually can be a form of an anomaly). The only challenge is since they are time-dependent from the previous timestamp, its previous risk weight could not be formulated or determined.

In contrast, [55] uses the probability of collision risk between the vehicle and the environmental object. This is done by dividing the scene into cells and the collision risk occurs when grids are overlapped in the future prediction of the vehicle movement and the identified object. These cells represent the environment as a grid-based system which is known as Conditional Monte Carlo Dense Occupancy Tracker (CMCDOT) [78]. CMCDOT can estimate the probability of collision for each cell in the grid. The mentioned approach in this context explains the use of time-based propagation as well. Thus, it fits well for real-time usage.

Other than the probability of collision risk, occlusion within a scene can also cause risk or accidents. The work of [56] and [57] adopts this approach. Occlusion determines the possibility of collision due to objects that are blocked in a normal field of view. In both pieces of research, a precise or intersection map must be provided as a baseline requirement. This method of risk assessment can also be classified at the traffic macro level rather than from a single AV point of view. In particular, [56] uses probabilistic RA to justify object occlusions due to sensors' limitation on unseen areas (e.g., a radar only sees object A in front of moving object B, blocking the radar detection which can become a high collision risk if the object B decides to move towards the radar). This risk covers over Cartesian space and represents an algorithm that performs for both observed and unobserved regions at urban intersections. This risk can be used for route planning or control to prevent collisions.

In comparison, [57] uses a probability-based technique to identify the highest probable chance of an occluded vehicle that enters into the mathematically defined occluded region with boundary representations. The probabilistic collision risk

TABLE VII
RA COVERAGE USING PROBABILITY-BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
[54]	QT	Y	Y	-	Y	CRV&CRN
[55]	QT	Y	Y	-	Y	CMCDOT
[56]	QT	Y	Y	-	P	Cartesian
[57]	QT	Y	Y	-	P	BDY

Legend: Y=Yes, N=No, P=Partial, CRV&CRN: Collision risk vehicle and collision risk network, Cartesian: Risk over Cartesian space, BDY: Determine the probability of emerging vehicle from the occluded boundary.

estimation is then defined based on the speed probability of the emerging vehicle entering the boundary of interest into the sight of the AV. As mentioned, these two methods, [56] and [57], rely on the availability of map information and proper road information. The real-time process of determining occluded vehicles and thereafter the risk of collision is probable but computationally intensive for each scene. The experiment conducted by [57] in three different scenarios also provided better confidence in the mentioned approach. However, it is not mentioned if it is done during real-time or the scene was pre-developed during the development lifecycle. Therefore, we consider this work as partially meeting real-time RA.

E. Artificial Intelligence (AI) Based Methodology

The use of AI, machine learning (ML) and deep learning (DL) based methodology for RA is an emerging topic within safety-critical engineering. In recent years, AI has been used in risk assessment in the medical field [79], analysis of the risk of groundwater contamination [80] or even financial credit risk [81]. This has increased the applications of AI usage in the context of RA for Autonomous Systems as well [82]. Recently the use of AI, especially deep learning, has been pervasive in the domain of AV [67]. Therefore it is difficult to avoid AI approaches in the aspects of AV development. The safety aspect of ML in highly automated driving is trending, but the challenge of handling uncertainty reduces the confidence in a real-world approach. For example, a use case was studied to justify its impact of measuring risk to ensure safe operations [83] of highly automated driving (SAE Levels 4 and 5), especially during DDT fallback mode. In that study, it emphasised on the importance of developers' knowledge within the AI and the importance of uncertainty calculation plus blackbox testing. In addition, the use of assurance case approach is recommended to obtain a systematic analysis of the root cause to mitigate risk and the importance of run-time (we refer to real-time) measures or risk to check against the developed decisions. We will contribute and address some of these topics in Section V in terms of the effects of determinism and uncertainty toward risk. In conjunction with our interest in using AI in RA, specific studies of ML impact on safety in Automotive Software is also analyzed based on ISO 26262 in Salay *et al.* [84].

The risk of AI approaches if being used alone, can increase the appearance of non-determinism with increased risk, especially if developers lack an inherent understanding of the requirements it uses to create decision making [85]. As such, DL might learn unsafe behaviours which were not intended in the first place. Therefore, AI and DL methodology might require more real-time testing and validation as compared to classical approaches such as process, probability and model-based. It is critical to note that the stochastic approach for AI or DL has its challenges for a safety-critical system. The key recommended approach normally includes a deterministic, non-deterministic, hybrid model like probability and model-based approaches or even AI with probability-based approaches that brings down the uncertainty levels. Even so, higher efforts of deliberate proof must be obtained for AI-based safety-critical systems to justify their deterministic outcome. In this section, some approaches to AI for RA are discussed and compared in terms of RA coverage and usability. Our key focus resides in AI for RA, while we omit the discussion of AI applications for AV, which can be seen in [67].

Feth *et al.* [58] and [59] demonstrated the use of DL as a form of RA. While Feng *et al.* [60] proposed the use of multiple Deep Neural Network (DNN) to capture uncertainty in classification which most AI(DL)-based RA might miss out on. The purpose of [58], [59] are similar to previous research that use either time to collision and/or occlusion to measure risk, while in [60] the focus is to quantify uncertainty specific to the Lidar sensor of the AV. The deep learning approaches used between [58] and [59] are also different. The former uses deep Convolutional Neutral Network (CNN) [86] while the latter uses Deep Predictive Model (a modification from Bayesian inference Convolution Long Short-Term Memory [87]). Feng *et al.*, on the other hand, uses a combination of ResNet8 [88], [89], Faster RCNN [90] and eventually Bayesian Neural Networks [91] to capture uncertainty risk.

Feth *et al.* [58] use CNN on the captured front scene and divide them into 3 sections: normal, caution and warning section. The sections labelled are of regression in nature and not classification. The author intends to reduce the operational process needs of CNN to provide an end-to-end paradigm to provide risk directly from the camera input. To obtain a risk figure, the image is then inputted to a Risk Metric Calculator tool [92]. The Risk Metric Calculator divides the scene into grid boxes and measures the amount of unoccupied box. With more unoccupied boxes, the risk is lower as it measures between the AV and its surrounding.

In [59], Bayesian ConvLSTM is used as a form of Deep Predictive Model (DPM) as an elevated approach from CNN in [58]. The approach is similar in getting the risk of collision using vision-based deep learning techniques. This is a predictive approach that incorporates temporal information during decision making, multi-modal information about the environment and also information about the uncertainty inherent to the task. The modelling of uncertainty is based on theoretical insights from [91] which is used in the DPM.

TABLE VIII
RA COVERAGE USING AI (DL)-BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
[58]	QT	Y	Y	-	Y	RM
[59]	QT	Y	Y	-	Y	DPM
[60]	QT	Y	Y	-	Y	Uncertainty

Legend: Y=Yes, N=No, DPM: Deep Predictive Model that uses Bayesian ConvLSTM, RM: risk metric

TABLE IX
RA COVERAGE USING COOPERATIVE MODE BASED METHODOLOGY

Research papers	Qualitative (QL) / Quantitative (QT)	Development			Real-Time	
		Vehicle motion	Vehicle and Environment	Unique approaches	Vehicle and Environment	Unique approaches
[61]	QT	Y	V2V	-	V2V	MPC
[62]	QL, QT	N	V2X	-	V2X	CRB
[63]	QT	Y	V2V	-	V2V	HC
[64]	QT	N	V2X	-	V2X	GCR
[65]	QT	N	V2X	-	V2X	PCA-BP
[66]	QT	N	V2X	-	V2X	FRB

Legend: Y=Yes, N=No, MPC: Use of model predictive control to measure risk using radar and V2V information. CRB: Contextual risk-based approach HC: Human-Centric active safety (co-driver), GCR: Global Collision Risk FRB: Fuzzy risk-based approach

The main objective is to improve vehicle safety by predicting future vehicle collisions in time to activate driver warning systems to recognize and anticipate dynamic catastrophic events beyond the immediate time horizon.

Lastly, [60] used ResNet 8 [88] to pre-process the Lidar images to detect small vehicles that occupy small grid cells, followed by Faster-RCNN pipeline to generate the bird's eye view 3D region proposals, followed by the use of Bayesian Neural Networks as the intermediate layers to extract uncertainties. Furthermore, to classify uncertainty into epistemic or aleatoric, Entropy (SE) and Mutual Information (MI) techniques are used. As compared to the generic approach where neural networks are used to train and detect an object, uncertainties are typically not considered. The interesting result demonstrates that epistemic uncertainty is related to vehicle detection accuracy while aleatoric is influenced by the vehicle distance and occlusion. This research outcome provides a baseline for consideration of DNN usage for AV risk uncertainty. Uncertainty is a major topic for the safety-critical system when AI/ML/DP approaches are used. This topic will be discussed later in Section V.

F. Cooperative Model-Based Methodology

Cooperative mode is an evolution of the existing Vehicular Ad-hoc Network (VANET) in early 2000. VANET started as a mobile ad-hoc network connection between vehicles that utilize the IEEE 802.11p standard. Thereafter with the start of DSRC/V2V, it has slowly evolved to new names like V2X [93]. In recent years due to the growth of cellular 5G, V2X has also been integrated into the 5G bandwagon and renamed as Cellular -V2X (C-V2X) [94]. With the reduction in access times and increase in bandwidth within 5G, the original intention of VANET has increased its interest in safety-critical topics such as risk factors. Initially, the purpose of VANET was to provide entertainment features, internet connections to vehicles and telematics functions. Moreover, with the limitations of the AV sensors, the AV have challenges in looking ahead and around the corner, therefore the use of the infrastructure-based system such as V2X or C-V2X can be helpful to assist the AV in planning. This is exceptionally true in the case of highly automated driving where the total reliance on efficiency and safety lies in the ADS decision making and algorithm design with timely information with low latency. Therefore the use of an infrastructure-based system to assist AV's DDT fallback requirement for SAE levels 4 and 5 can be critical in terms of safety.

The generic understanding of cooperative mode for AV shows that infrastructure information can be transmitted to the AV (or connected vehicles) and then be used to manage risk on top of operational needs. Specifically, [61]–[65] and [66] are compared in terms of approaches that contribute to risk identification or assessment. In our description, V2V is equivalent to the concept of VANET.

From the listed studies, there are mixtures of modelling and/or probability, AI and fuzzy risk-based approaches as shown in Table IX. In the case of modelling, [61] used a Model Predictive Control (MPC), which is also a known modelling technique that involves the optimization of a performance index concerning future control sequence and using a predicted output signal based on a process model [95]. In this architecture, all the information from V2V is then fused with sensors and radars, providing location and motion estimation. These results are then passed to the rule-based multi-traffic prediction block. This block uses MPCs to make predictions for both latitudinal and longitudinal aspects. The outcome can then be computed as a collision RA and the result will be a probability figure.

In addition to modelling, the hybrid use of modelling and probabilistic approach is seen in [62]–[65] and [66]. Demmel *et al.* [64] proposed a Global RA using V2V and infrastructures, where [61] and [63] focus on V2V only. In this research [64], every vehicle is translated into its risk estimation based on two distinct components: collision probability and severity of the collision. For example, if the Lidar sensor data shows that there is a risk with detected obstacle or risk of collision with the front vehicle that applies sudden braking, both can be analyzed using the above-mentioned methodology. In the case where multiple sensors are used, a further global collision risk can also be determined at the vehicle level. The global collision risk figure takes the maximum risk figure among each of these measured sensor sources.

At the macro level, if all the AV share their perceived risk values, the identified scenario for the whole driving context can create an average risk estimator known as augmented collision risk – which is the average of all individual local vehicles to establish this risk figure. This average risk value is similar to the approach used by Fitzgerald *et al.* [96]. The latter demonstrates that using V2V relays and passing of information from one vehicle to another (in this case, risk figures) allows the eventual host vehicle to have additional warning time by notification of risk figure while moving towards a hazardous event.

Other modelling and probabilistic approaches like Thayananthan and Shaikh, [62] proposed a unique use of contextual risk-based decision approach. The approach consists of a simple probability distribution known as risk values of all the detected parameters collected from V2V, such as lane information, road conditions, traffic congestions, weather, speed and time. Their probability is determined in the form of table indexes. The contextual content is matched with probabilities figures like a rule-based system.

Similarly, using the model and probability approach, [63] used human modelling and probability to mimic the human-centric active safety control that focuses on the intervention moment based on prior research findings in [97]. This moment occurs when an intervention point is crossed, which represents the probability of vehicle collision can occur. This intervention moment is the best trade-off between maximum collision risk and predicted human reaction time and acts as a baseline of safety in the AV that mimics human intervention in terms of 1) active safety and 2) reaction time of safety actions.

The use of AI in Cooperative mode RA methodology is also a recent inclusion in Zhao *et al.* [65], stating the specific use of Principal Component Analysis (PCA) to de-correlate the feature in the infrastructure traffic data set and recombine them into a set of linearly independent features. Thereafter a Back-Propagation Neural Network is used to train the predictive model. In order to predict the driving risk of a vehicle, their results are then compared with the typical Support Vector Machine (SVM) approach. The comparison showed an improvement in terms of 3-8 percentage points across the different number of testing records. The inclusion of PCA also contributes 1-2 percentage points among the improvement mentioned.

Lastly, [66] demonstrates the use of a fuzzy risk-based decision method for cooperative based RA methodology. The concept proposed is an extension from [12] by using vehicle context parameters such as lane, weather, time, traffic, road and speed together with driver's attitude such as age and experience to determine risk. This risk is based on different weights used for the vehicle context and driver attitude multiplied by the impact. The extension includes the further classification of the traffic and speed into low, medium and high risk, improvement of mapping function formation, clearer determination of the weights to vehicle contextual parameters, threat and driver's attitude. Further proof was done to verify the proposed concept.

With reference to Table IX, [66] and [65] proposed risk prediction and decision metrics which are not entirely for AV but they have included methods that can be useful for risk associating with V2V information and V2X approaches. While [66] illustrates the importance of environmental conditions by using other vehicle information to look ahead, and [65] uses PCA-BPNN to predict traffic accidents from the information gathered from all vehicles (which can be a fleet of AVs). In terms of RA coverage, the nature of Cooperative modes depends on the real-time information obtained between vehicles. Therefore, the classification of these approaches all can function in real-time. However, in [61] and [63], the focus of risk management remains more on the vehicle than the infrastructure level compared to the others. In summary, it is important to note that the mentioned V2X approaches do not provide any reflective risk control for vehicle motion for this section.

TABLE X
DETERMINISM AND UNCERTAINTY IN RA METHODOLOGIES

RA methodology	Qualitative (QL) or Quantitative (QT)	Determinism			Uncertainty	
		Deterministic	Non-Deterministic	Stochastic	Aleatoric	Epistemic
Process,	QL	Yes	No	No	NA	NA
Model	QL & QT	Yes	No	No	NA	NA
Model + Probability	QL & QT	Yes	Yes	Yes	Yes	No
Probability	QT	No	Yes	Yes	Yes	No
AI-based	QT	No	Yes	Yes	Yes	Yes

V. IMPORTANCE OF DETERMINISM AND UNCERTAINTY IN RISK ASSESSMENT

With the different RA methodologies addressed in section IV, it is important to address the different outcomes that each methodology brings towards safety in terms of RA. The different outcomes can be addressed firstly in terms of qualitative, quantitative, determinism and type of uncertainty involved. Table X shows that different RA methodologies result in different determinism and uncertainty. For the case of process-based methodology, the outcomes are descriptive, which are evident in the iterative loops of the HARA process in [46] and [47], skill graph implementation to assist the detailing of the hazardous event [35] and more descriptive details of the scene in [36] in assisting RA activities. They are mostly deterministic, and based on the given description, there is only one definite outcome if the input or the malfunction is the same. Whereas in the case of RA that involves model-based methodology in [48]–[50], they have a hybrid mix of both qualitative (QL) and quantitative (QT) outcomes. Although having both QL and QT, the outcome and approach remain deterministic since its modelling of the original descriptive process are modelled into an automated process like [49] and some QT in terms of risks are represented by cost figures in [48]. In these aspects, a sole model-based approach does not have any non-deterministic outcomes or uncertainties.

In contrast, RA methodology that involves probability has some form of uncertainty in real-world modelling. Even though probability provides quantitative outcomes but the uncertainty that relates beyond the limits or uncaptured vehicle or environmental conditions should be considered, otherwise an unknown risk can occur even if the probability can be extremely low. For example, if probabilities are defined within known limits of the sensor, there should be probabilities considered for outside the limits of the sensor as uncertainty as well. In [51]–[53], quantitative figures are given as forms of the probability of occurrence, damage or equivalent forced based theory to estimate risk, uncertainty is taken care of as forms of unconsidered scenarios [52], error rate [51] or uncertainty in multi-target detection [53]. These approaches have their uncertainty classified as aleatoric since modelling techniques have been used in their approach which removes epistemic uncertainty.

When probability techniques are used in RA methodology, most of the approaches consist of the risk of collision [54], [55] or occlusions [56], [57]. Occlusion naturally takes care of the uncertainty using boundary methods [57] or sensor limits [56]. These limits prevent the lack of knowledge from making the stochastic uncertainty epistemic. The stochastic probability approach is also popular for AV predictive control in uncertain environments [98], [99].

In recent times of popular AI approaches, AI DL are also used for RA with examples in [58], [59]. Similarly to the probability approach, if the AI-approach is used alone (end-to-end) and does not have a guiding principle from modelling techniques, the uncertainty places a certain amount of risk. However, the uncertainty in AI can contain two kinds of problems since the accuracy of prediction or classification is very much dependent on the training dataset. The problem includes 1) the inaccuracy of the results due to insufficient dataset and 2) the lack of data set, which shows the lack of knowledge. The inaccuracies can be a form of uncertainty due to random outcomes within a classification of possible scenarios. This can be termed as Aleatoric uncertainty. While in the case of lack of data that leads to uncertainty, this can be classified as Epistemic uncertainty. Thus, without a secondary model, for example, a rule-based system to validate its outcome can incur unwanted risk. The training data can also include wrong references, which might lead to unwanted responses. These unwanted responses might also lead to risk-related outcomes, which are at times referred to as error rates. Therefore, as of current end-to-end AI DL approaches are discouraged for safety-critical systems.

Therefore, AI, especially DL have uncertainties included, and they are needed to be addressed as part of the results. In most studies, these are classified as the error rate of the AI process. In [58], the uncertainty is verified by comparing with the ground truth while using a risk metric to map the CNN results into figures. While in [59], the uncertainty used in DPM is classified as stochastic forward passes. Therefore Feng *et al.* [60] work is a reference where the uncertainty is identified and represented in an interaction aware of the AV and its potential occlusion.

It is also important to note that for process and model-based RA methodology, the approach focuses on known malfunctions and does not contain unknowns, which leads to uncertainty. Moreover, in real-world operations, uncertainty does occur. Therefore, it purely implies that the coverage of RA consideration must be sufficient for real-world operations. With most of these processes and model RA methodology implemented only during development with a team of experts' skill in the art, occurrences of missing safety mitigations in real-time operations can still happen if a hazardous situation occurs. It is impossible to expect perfect safety mitigations in real-time (using only development considerations for RA) and eventually fall back on the driver to mitigate or prevent accidents. Thus, the requirement of real-time RA coverage becomes a definite must when SAE Levels increases to Levels 4 and 5. Since the DDT fallback must have a complete real-time risk assessment of the AV and the environment, all uncertainty must be accounted for. This relates to the coverage of SOTIF in terms of the design of ODD and its operating limits requirement as well.

On the other hand, probability and AI-based RA methodology give better coverage of the situation with quantitative outcomes, but the occurrence of a hazardous event cannot be ascertained when uncertainty exists. Therefore, the safety actions cannot be decided with certainty. However, it is still sufficient to indicate the level of risk (to which the AV is subjected to its environment) and result in safety actions to reduce the AV performance. Therefore, in most cases, a mixture of RA methodology approaches is recommended with enhanced RA coverage (in both development and real-time), which will help increase AV operations' safety.

VI. Recommendation of RA Methodology

It is important before any recommendation to highlight the key requirements of the standards for AV. In terms of the safety of the AV, ISO 26262 and ISO/PAS 21448 are the two outstanding standards that relate to AV testing and validation. ISO 26262 is based on functional safety for all automotive vehicles, while ISO/PAS 21448 is more centred around AV performance limitations of the intended behaviour. The definition is listed in full as follows:

- Functional safety is defined as "absence of unreasonable risk due to hazards cause by *malfunctioning* behaviour of E/E Systems" (ISO 26262-1, Def 1.51)
- Safety of the Intended Functionality is defined as the absence of unreasonable risk due to hazards caused by *performance limitations of the intended behaviour* or by reasonable foreseeable misuse by the user (ISO.PAS 21448, Def 3.5)

As such, it is important to note that ISO 26262 have processes such as HARA to guide *malfunction* (M) identification normally known as internal causes of the vehicle that affect operations. While ISO/PAS 21448 refers to performance limitations that can be linked to triggering event analysis [28] that indicates the limitation of performance. Within SOTIF, it is also required to know if the intended function has design coverage for known safe/unsafe and unknown safe/unsafe regions from the triggers of boundary conditions. This is true in real-life software development where boundary conditions are not taken care of as a possible outcome that may lead

TABLE XI
RECOMMENDATION OF RA METHODOLOGY

Methodology	Research papers	Development		Real-Time	ISO 26262	ISO/PAS 21448
		Vehicle motion	Vehicle and Environment	Vehicle and Environment		
Process	HARA/FMEA	Y	N	N	S	N
	[46]	Y	Y	N	S	N
	[45]	Y	Y	N	S	N
	[35]	Y	Y	N	S	N
	[36]	Y	Y	N	S	N
	[44]	Y	Y	Y	S	Y
	[31]	Y	Y	Y	S	Y
	[32]	Y	Y	Y	S	Y
Mod	[48]	Y	P	N	S	Y
	[49]	Y	Y	N	S	N
	[50]	Y	P	P	C	Y
	[33]	Y	Y	Y	S	Y
Prob & Mod	[51]	Y	Y	N	S	Y
	[52]	Y	Y	N	C	Y
	[53]	Y	Y	N	C	Y
Prob	[54]	Y	Y	Y	C	Y
	[55]	Y	Y	Y	C	Y
	[56]	Y	Y	P	C	Y
	[57]	Y	Y	P	C	Y
AI	[58]	Y	Y	Y	C	Y
	[59]	Y	Y	Y	C	Y
	[60]	Y	Y	Y	C	Y
Co-operative mode	[61]	Y	V2V	V2V	C	Y
	[62]	N	V2V	V2V	S	Y
	[63]	Y	V2V	V2V	C	Y
	[64]	N	V2X	V2X	C	Y
	[65]	N	V2V	V2V	C	Y
	[66]	N	V2V	V2V	S	Y

Legend: Y=Yes, N=No, C=Component, S=System, P=Partial

to unknown unsafe conditions. Based on the stated considerations, a consolidated list of different RA methodologies for AV is individually rated (refer to Table XI) in adherence to the respective standards. Based on the diversity of topics listed, it is almost impossible to identify one method that could cover both standards in full. In theory, one could also state that a topic that contributes (reflected as Y in Table XI) to ISO/PAS 21448 can also be a component (reflected as C in Table XI) contribution for ISO 26262. However, an approach that consists of system-level contribution (reflected as S in Table XI) for ISO 26262 may not meet the needs of ISO/PAS 21448 as the boundary conditions are not stated or properly defined in the testing and validation plan. Thus, the identification of these boundaries requires a rule-based or model-based system in terms of qualitative or numeric figures from quantitative outcomes. It is also of interest in SOTIF if the non-determinism or stochastic uncertainty is defined with clarity within its limits of operations.

Table XI identifies the studies in Section IV against the requirements of both ISO 26262 and ISO/PAS 21448. They are referenced against RA coverage if they can be implemented during development and/or real-time operations. From the process-based methodology perspective, using malfunction is perfect for ISO 26262 but if the malfunctions do not identify the limits of intended behaviour, then it does not fulfil the requirement of ISO/PAS 21448. With exceptions of [31], [32] and [44], they demonstrated with the inclusion of real-time RA and limits of intended behaviour (note that having a Y for ISO/PAS 21448 only indicates that it contributes to the standard and it does not imply full validation of the AV relying on that method). In the case of modelling, probability and AI-based methodology generally contribute to the ISO/PAS 21448 as long as they have detection or triggers based on the vehicle and environment conditions. Only in the case of [49], where the limits of operations are not identified. The rest of the approach contains quantitative figures where boundary conditions are defined, thus meeting ISO/PAS 21448.

TABLE XII
KNOWN AND UNKNOWN SAFE/UNSAFE REGIONS

Functional/ Triggers	Safe	Unsafe
Known Boundary	• RA coverage for Development • Deterministic	• RA coverage for Development • Deterministic
Unknown	• RA coverage for Real-time • Non-deterministic • Stochastic	• RA coverage for Real-time • Non-deterministic • Stochastic

In the case of cooperative mode for RA, the situation is a bit more complex. If the risk indicators are produced from the perspective of the AV or vehicle with more contextualization, it is related to ISO 26262 [62] at the system level. If the focus is purely on the risk of collision, they reside more on the component level. The risk of collision belongs to a trigger-based event that can support the identification of functional limits. Therefore, that contributes to the ISO/PAS 21448.

Besides, meeting standards, it is also important to distinguish malfunctions or triggers and if they belong to which four quadrants of known safe, known unsafe, unknown safe and unknown unsafe regions as shown in Table XII. It can be assumed that known safe/unsafe regions are typically covered by RA coverage during development. It is also possible and optional for real-time RA to discover known unsafe if a specific trigger or malfunction occurs not according to design in real-time as a form of redundancy check.

If a system can capture new hazardous events during its operation, it is then able to identify unknown safe/unsafe situations. For that to happen, RA coverage for real-time needs to take place. If there is no real-time RA, then the boundary of the unknown safe/unsafe (Boundary, Table XII) must be clearly defined in the SOTIF domain for RA to be conceived during development. These regions are also illustrated in Table XII.

In retrospective, it is also important to note that the functionality of an AV can be deterministic, but environmental detection cannot be perfect in the real-world, thus the presence of non-deterministic and uncertainty. Therefore, it is aligned that even with live trials and simulations for different scenarios of AV operations, it is still insufficient to guarantee safety at one hundred percent. Therefore, a real-time RA approach can help to resolve this in the long run. Having real-time RA

TABLE XIII
SUMMARY OF DIFFERENT SURVEYS FOR AV

Domain for Autonomous Vehicle (AV)	Reference
Scenario-based Safety Assessment	[100]
Deep Learning Techniques	[67]
Motion, planning and control techniques	[101]
Motion prediction and RA for intelligent vehicles	[102]
Application of functional safety using ISO26262	[21]

coverage fulfils the ISO/PAS 21448 requirements while taking care of uncertainty.

To assist the reader in terms of exploration towards different research approaches and articles for AV, the listed survey papers are documented in Table XIII for reference.

VII. CONCLUSION

This survey adds to the knowledge of RA methodologies for AV. It presents the importance of RA coverage for development and real-time operations. The justification of RA coverage is due to the requirement of ISO 26262 and ISO/PAS 21488 that covers risks related to internal causes such as malfunction of the AV and external causes such as environment to the AV. The increased focus in RA is also due to the increasing safety needs of the ADS during DDT fallback for highly automated driving. With the driver out of the loop, the ADS need to be aware of its surrounding to operate in a minimal risk situation in case of DDT fallback. The review of RA methodologies in this paper is divided into different approaches for comparison and highlights their unique approaches and if they are qualitative or quantitative. The individual methodology also classified if they can be implemented during development or real-time RA coverage as well as malfunctions for vehicles and/or the ability to trigger events for hazardous environmental detection. In addition, the importance of determinism and uncertainty is highlighted in the context of risk. Lastly, recommendations for the different RA methodologies are proposed if they fit the requirements of ISO 26262 and ISO/PAS 21448.

REFERENCES

[1] S. Wells, A. Whittington, and R. Talwar, "The fourth industrial revolution," *Training J., Mag.*, pp. 30–32, Jul. 2017.

[2] A. Turner. *Waymo and Other Self-Driving Car Makers Powering a 3.7 Trilli Shift*. Accessed: Dec. 6, 2019. [Online]. Available: https://www.afr.com/technology/waymo-and-other-selfdriving-car-makers-powering-a-37-trillion-shift-20190131-h1apqt

[3] A. P. T. Möller, D. Pinner, and A. Tschiesner, "Reserve a seat—The future of mobility is arriving early," McKinsey Company, Germany, Tech. Rep., 2018.

[4] C. D. Harper, C. T. Hendrickson, S. Mangones, and C. Samaras, "Estimating potential increases in travel with autonomous vehicles for the non-driving, elderly and people with travel-restrictive medical conditions," *Transp. Res. C, Emerg. Technol.*, vol. 72, pp. 1–9, Nov. 2016, doi: 10.1016/j.trc.2016.09.003.

[5] K. Hidaka and T. Shiga, "Forecasting travel demand for new mobility services employing autonomous vehicles," *Transp. Res. Proc.*, vol. 34, pp. 139–146, Jan. 2018, doi: 10.1016/j.trpro.2018.11.025.

[6] U. Nations. (2019). *World Urbanization Prospects 2018 Highlights*. [Online]. Available: https://population.un.org/wup/Publications/Files/WUP2018-Highlights.pdf

[7] T. A. Litman, "Autonomous vehicle implementation predictions," in *Implications for Transport Planning Victoria Transport Policy Institute*. Victoria, BC, Canada: Victoria Transport Policy Institute, Oct. 2019. [Online]. Available: https://www.vtpi.org/avip.pdf

[8] A. Athanasopoulou, W. A. G. A. Bouwman, F. A. Nikayin, and G. A. de Reuver, "The disruptive impact of digitalization on the automotive ecosystem: A research agenda on business models, platforms and consumer issues," in *Proc. 29th Bled eConf. Digit. Economy*, 2016, p. 4.

[9] P. Planing, *Innovation Acceptance The Case of Advanced Driver-Assistance Systems*. Wiesbaden, Germany: Springer, 2014.

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

[11] A. Herrmann, *Autonomous Driving: How The Driverless Revolution Will Change the World*. Bingley, U.K.: Emerald Publishing, 2018.

[12] CBINSIGHTS. *40+ Corporations Working on Autonomous Vehicles*. CBINSIGHTS. [Online]. Available: https://www.cbinsights.com/research/autonomous-driverless-vehicles-corporations-list/

[13] KPMG. (2019). *Autonomous Vehicles Readiness Index*. Assessing Countries Preparedness for Autonomous Vehicles. [Online]. Available: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf

[14] C. N. Asia, "Commentary: Driverless vehicles can reshape Singapore, but do consider the human elements," Channel News Asia, Singapore, Tech. Rep., 2017.

[15] M. Azad, N. Hoseinzadeh, C. Brakewood, C. R. Cherry, and L. D. Han, "Fully autonomous buses: A literature review and future research directions," *J. Adv. Transp.*, vol. 2019, pp. 1–16, Dec. 2019, doi: 10.1155/2019/4603548.

[16] A. O. Salonen, "Passenger's subjective traffic safety, in-vehicle security and emergency management in the driverless shuttle bus in Finland," *Transp. Policy*, vol. 61, pp. 106–110, Jan. 2018, doi: 10.1016/j.tranpol.2017.10.011.

[17] (2018). *FHWA-SA-18-032, Guide for Scalable Risk Assessment Methods for Pedestrains and Bicyclists*. [Online]. Available: http://safety.fhwa.dot.gov

[18] A. Takacs, D. A. Drexler, P. Galambos, I. J. Rudas, and T. Haidegger, "Assessment and standardization of autonomous vehicles," in *Proc. IEEE 22nd Int. Conf. Intell. Eng. Syst. (INES)*, Jun. 2018, pp. 185–192, doi: 10.1109/INES.2018.8523899.

[19] M. S. M. Wood *et al.*, "Safety first for automated driving," Connected Automated Driving.eu, EU, Tech. Rep., 2019.

[20] NHTSA. (2017). *Automated Driving Systems: A Vision for Safety 2.0*. Ann Arbor, MI, USA. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[21] M. A. Gosavi, B. B. Rhoades, and J. M. Conrad, "Application of functional safety in autonomous vehicles using ISO 26262 standard: A survey," in *Proc. SoutheastCon*, Apr. 2018, pp. 1–6, doi: 10.1109/SECON.2018.8479057.

[22] C. B. S. T. Molina, J. R. D. Almeida, L. F. Vismari, R. I. R. Gonzalez, J. K. Naufal, and J. B. Camargo, "Assuring fully autonomous vehicles safety by design: The autonomous vehicle control (AVC) module strategy," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2017, pp. 16–21, doi: 10.1109/DSN-W.2017.14.

[23] N. P. Qc. *Automated Vehicles Scottish Law Commission, Public Law*. Scottish Law Commission. Accessed: Dec. 12, 2019. [Online]. Available: https://www.lawcom.gov.U.K./project/automated-vehicles/

[24] 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, Switzerland: Springer, 2017, pp. 387–416.

[25] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, document IEC 61508, 2010.

[26] *Road Vehicles Functional Safety*, document ISO 26262, 2018. [Online]. Available: https://www.iso.org/standard/68383.html

[27] *Road Vehicles Safety of the Intended Functionality*, document ISO/PAS 21448, 2019.

[28] O. M. Kirovskii and V. A. Gorelov, "Driver assistance systems: Analysis, tests and the safety case. ISO 26262 and ISO PAS 21448," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 534, no. 1, 2019, Art. no. 012019, doi: 10.1088/1757-899X/534/1/012019.

[29] *Surface Vehicle Recommended Practice*, SAE, Warrendale, PA, USA, Jun. 2018.

[30] K. Czarnecki, *Operational Design Domain for Automated Driving Systems Taxonomy of Basic Terms*. Waterloo, ON, Canada: Univ. of Waterloo, Waterloo Intelligent Systems Engineering (WISE) Lab, 2018.

[31] 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 *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–6, doi: 10.1109/ITSC.2017.8317868.

[32] F. Warg *et al.*, "The quantitative risk norm—A proposed tailoring of HARA for ADS," in *Proc. 50th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2020, pp. 86–93, doi: 10.1109/DSN-W50199.2020.00026.

[33] W. M. Dan Chia, S. Loong Keoh, A. L. Michala, and C. Goh, "Real-time recursive risk assessment framework for autonomous vehicle operations," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Apr. 2021, pp. 1–7.

[34] D. Wang, W. Fu, Q. Song, and J. Zhou, "Potential risk assessment for safe driving of autonomous vehicles under occluded vision," *Sci. Rep.*, vol. 12, no. 1, p. 4981, Mar. 2022, doi: 10.1038/s41598-022-08810-z.

[35] G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, "Identification of potential hazardous events for an unmanned protective vehicle," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2016, pp. 691–697.

[36] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, "Defining and substantiating the terms scene, situation, and scenario for automated driving," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 982–988, doi: 10.1109/ITSC.2015.164.

[37] I. Clifton and A. Ericson, *Hazard Analysis Techniques for System Safety*, 2nd ed. Hoboken, NJ, USA: Wiley, 2016.

[38] S. Khaiyum, B. Pal, and Y. S. Kumaraswamy, *An Approach to Utilize FMEA for Autonomous Vehicles to Forecast Decision Outcome*. Cham, Switzerland: Springer, 2014, pp. 701–709.

[39] *Hazard and Operability Studies (HAZOP Studies) Application Guide*, document IEC 61882, 2016.

[40] *Failure Modes and Effects Analysis (FMEA and FMECA)*, document IEC 60812, 2018.

[41] *Fault Tree Analysis*, document IEC 61025, 2006.

[42] *Surface Vehicle Standard (R) Potential Failure Mode and Effects Analysis in Design (DFMEA), Potential Failure Mode Effects and Analysis in Manufacturing and Assmebly Process (Process FMEA)*, SAE, Warrendale, PA, USA, 2009. [Online]. Available: https://www.sae.org/standards/content/j1739_200901/

[43] R. Adler, P. Feth, and D. Schneider, "Safety engineering for autonomous vehicles," in *Proc. 46th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshop (DSN-W)*, Jun. 2016, pp. 200–205, doi: 10.1109/DSN-W.2016.30.

[44] A. Wardziński, "Safety assurance strategies for autonomous vehicles," in *Computer Safety, Reliability, and Security*, M. D. Harrison and M.-A. Sujan, Eds. Berlin, Germany: Springer, 2008, pp. 277–290.

[45] T. Stolte, G. Bagschik, A. Reschka, and M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1848–1855.

[46] F. Warg, M. Gassilewski, J. Tryggvesson, V. Izosimov, A. Werneman, and R. Johansson, "Defining autonomous functions using iterative hazard analysis and requirements refinement," in *Computer Safety, Reliability, and Security*, A. Skavhaug, J. Guiochet, E. Schoitsch, and F. Bitsch, Eds. Cham, Switzerland: Springer, 2016, pp. 286–297.

[47] T. Stolte, G. Bagschik, A. Reschka, and M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle," presented at the IEEE Intell. Vehicles Symp. (IV), Redondo Beach, CA, USA, Jun. 11–14, 2017.

[48] H. M. Fahmy, M. A. A. El Ghany, and G. Baumann, "Vehicle risk assessment and control for lane-keeping and collision avoidance at low-speed and high-speed scenarios," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4806–4818, Jun. 2018, doi: 10.1109/TVT.2018.2807796.

[49] K. Beckers, M. Heisel, T. Frese, and D. Hatebur, "A structured and model-based hazard analysis and risk assessment method for automotive systems," in *Proc. IEEE 24th Int. Symp. Softw. Rel. Eng. (ISSRE)*, Nov. 2013, pp. 238–247.

[50] B. Wu, Y. Yan, D. Ni, and L. Li, "A longitudinal car-following risk assessment model based on risk field theory for autonomous vehicles," *Int. J. Transp. Sci. Technol.*, vol. 10, no. 1, pp. 60–68, Mar. 2021, doi: 10.1016/j.ijtst.2020.05.005.

[51] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle, and W. Damm, "Identification and quantification of hazardous scenarios for automated driving," in *Model-Based Safety and Assessment*, M. Zeller and K. Höfig, Eds., Cham, Switzerland: Springer, 2020, pp. 163–178.

[52] D. Wittmann, M. Lienkamp, and C. Wang, "Method for comprehensive and adaptive risk analysis for the development of automated driving," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–7, doi: 10.1109/ITSC.2017.8317791.

[53] X. Zheng, B. Huang, D. Ni, and Q. Xu, "A novel intelligent vehicle risk assessment method combined with multi-sensor fusion in dense traffic environment," *J. Intell. Connected Vehicles*, vol. 1, no. 2, pp. 41–54, Dec. 2018, doi: 10.1108/JICV-02-2018-0004.

[54] C. Katrakazas, M. Quddus, and W.-H. Chen, "A new integrated collision risk assessment methodology for autonomous vehicles," *Accident Anal. Prevention*, vol. 127, pp. 61–79, Jun. 2019, doi: 10.1016/j.aap.2019.01.029.

[55] P. Ledent, A. Paigwar, A. Renzaglia, R. Mateescu, and C. Laugier, "Formal validation of probabilistic collision risk estimation for autonomous driving," in *Proc. IEEE Int. Conf. Cybern. Intell. Syst. (CIS) IEEE Conf. Robot., Autom. Mechatronics (RAM)*, Nov. 2019, pp. 433–438, doi: 10.1109/CIS-RAM47153.2019.9095806.

[56] M.-Y. Yu, R. Vasudevan, and M. Johnson-Roberson, "Occlusion-aware risk assessment for autonomous driving in urban environments," *IEEE Robot. Autom. Lett.*, vol. 4, no. 2, pp. 2235–2241, Apr. 2019, doi: 10.1109/LRA.2019.2900453.

[57] M. Lee, M. Sunwoo, and K. Jo, "Collision risk assessment of occluded vehicle based on the motion predictions using the precise road map," *Robot. Auto. Syst.*, vol. 106, pp. 179–191, Aug. 2018, doi: 10.1016/j.robot.2018.05.005.

[58] P. Feth, M. N. Akram, R. Schuster, and O. Wasenmüller, *Dynamic Risk Assessment for Vehicles of Higher Automation Levels by Deep Learning*. Cham, Switzerland: Springer, 2018, pp. 535–547.

[59] M. Strickland, G. Fainekos, and H. B. Amor, "Deep predictive models for collision risk assessment in autonomous driving," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2018, pp. 4685–4692.

[60] D. Feng, L. Rosenbaum, and K. Dietmayer, "Towards safe autonomous driving: Capture uncertainty in the deep neural network for lidar 3D vehicle detection," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 3266–3273.

[61] D. Shin, B. Kim, J. Seo, and K. Yi, "Effects of wireless communication on integrated risk management based automated vehicle," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 1767–1772, doi: 10.1109/ITSC.2015.287.

[62] V. Thayananthan and R. Shaikh, "Contextual risk-based decision modeling for vehicular networks," *Int. J. Comput. Netw. Inf. Secur.*, vol. 8, no. 9, pp. 1–9, Sep. 2016.

[63] D. Shin, B. Kim, K. Yi, A. Carvalho, and F. Borrelli, "Human-centered risk assessment of an automated vehicle using vehicular wireless communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 667–681, Feb. 2019, doi: 10.1109/TITS.2018.2823744.

[64] S. Demmel *et al.*, "Global risk assessment in an autonomous driving context: Impact on both the car and the driver," *IFAC-PapersOnLine*, vol. 51, no. 34, pp. 390–395, 2019, doi: 10.1016/j.ifacol.2019.01.009.

[65] H. Zhao, T. Mao, H. Yu, M. Zhang, and H. Zhu, "A driving risk prediction algorithm based on PCA -BP neural network in vehicular communication," in *Proc. 10th Int. Conf. Intell. Hum.-Mach. Syst. Cybern. (IHMSC)*, Aug. 2018, pp. 164–169.

[66] R. A. Shaikh and V. Thayananthan, "Risk-based decision methods for vehicular networks," *Electronics*, vol. 8, no. 6, p. 627, Jun. 2019, doi: 10.3390/electronics8060627.

[67] S. Grigorescu, B. Trasnea, T. Cocias, and G. Macesanu, "A survey of deep learning techniques for autonomous driving," *J. Field Robot.*, vol. 37, no. 3, pp. 362–386, 2020, doi: 10.1002/rob.21918.

[68] A. Alebrahim, *Bridging the Gap Between Requirements Engineering and Software Architecture*. Duisburg, Germany: Springer, 2016.

[69] A. Nyßen and P. Könemann, "Model-based automotive software development using Autosar, UML, and domain-specific languages," in *Proc. Embedded World Conf.*, Nuremberg, Germany, 2013.

[70] AutoSAR. (2016). *Modeling Guidelines of Basic Software EA UML Model Release 4.3.0*. [Online]. Available: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_TR_BSWUMLModelModelingGuide.pdf

[71] J. Bach, S. Otten, and E. Sax, "Model based scenario specification for development and test of automated driving functions," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2016, pp. 1149–1155.

[72] M. Tlig *et al.*, "Autonomous driving system: Model based safety analysis," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2018, pp. 2–5, doi: 10.1109/DSN-W.2018.00012.

[73] D. Ni, "A unified perspective on traffic flow theory—Part I: The field theory," in *Proc. ICCTP*, Jul. 2011, pp. 4227–4243.

[74] J. Wang, J. Wu, and Y. Li, "The driving safety field based on driver–vehicle–road interactions," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 2203–2214, Aug. 2015, doi: 10.1109/TITS.2015.2401837.
[75] T. Ôzkan and T. Lajunen, "Person and environment: Traffic culture," in *Handbook of Traffic Psychology*, B. E. Porter, Ed., San Diego, CA, USA: Academic, 2011, pp. 179–192.
[76] J. Patterson and A. Gibson, *Deep Learning*, 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc, 2017.
[77] S. Lefevre, "Risk estimation at road intersections for connected vehicle safety applications," Laboratoire d'informatique de Grenoble, Saint-Martin-d'Hères, France, Tech. Rep., 2012.
[78] L. Rummelhard, A. Negre, and C. Laugier, "Conditional Monte Carlo dense occupancy tracker," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 2485–2490, doi: 10.1109/ITSC.2015.400.
[79] P. Ferroni *et al.*, "Risk assessment for venous thromboembolism in chemotherapy-treated ambulatory cancer patients: A machine learning approach," *Med. Decis. Making*, vol. 37, no. 2, pp. 234–242, Feb. 2017, doi: 10.1177/0272989X16662654.
[80] F. Sajedi-Hosseini *et al.*, "A novel machine learning-based approach for the risk assessment of nitrate groundwater contamination," *Sci. Total Environ.*, vol. 644, pp. 954–962, Dec. 2018, doi: 10.1016/j.scitotenv.2018.07.054.
[81] N. Bussmann, P. Giudici, D. Marinelli, and J. Papenbrock, "Explainable AI in fintech risk management," *Frontiers Artif. Intell.*, vol. 3, p. 26, Apr. 2020, doi: 10.3389/frai.2020.00026.
[82] A. Delaborde, "Risk assessment of artificial intelligence in autonomous machines," presented at the 1st Int. Workshop Evaluating Prog. Artif. Intell. (EPAI) Conjunct. With (ECAI), Santiago de Compostela, France, 2020. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03009978
[83] S. Burton, L. Gauerhof, and C. Heinzemann, *Making the Case for Safety of Machine Learning in Highly Automated Driving*. Cham, Switzerland: Springer, 2017, pp. 5–16.
[84] R. Salay, R. Queiroz, and K. Czarnecki, "An analysis of ISO 26262: Using machine learning safely in automotive software," 2017, *arXiv:1709.02435*.
[85] C. Johnson, "The increasing risks of risk assessment: On the rise of artificial intelligence and non-determinism in safety-critical systems," in *Proc. 26th Saf.-Crit. Syst. Symp.*, Feb. 2018, pp. 1–15.
[86] Y. LeCun, "Deep learning & convolutional networks," in *Proc. IEEE Hot Chips 27 Symp. (HCS)*, Aug. 2015, pp. 1–95.
[87] X. Shi, Z. Chen, H. Wang, D.-Y. Yeung, W.-K. Wong, and W.-C. Woo, "Convolutional LSTM network: A machine learning approach for precipitation nowcasting," presented at the 28th Int. Conf. Neural Inf. Process. Syst., Montreal, QC, Canada, vol. 1, 2015.
[88] S. Li, J. Jiao, Y. Han, and T. Weissman, "Demystifying ResNet," 2016, doi: 10.48550/ARXIV.1611.01186.
[89] K. He, X. Zhang, S. Ren, and J. Sun, "Identity mappings in deep residual networks," 2016, doi: 10.48550/ARXIV.1603.05027.
[90] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 6, pp. 1137–1149, Jun. 2017, doi: 10.1109/TPAMI.2016.2577031.
[91] Y. Gal, "Uncertainty in deep learning," Dept. Eng., Univ. Cambridge, Cambridge, U.K., 2016.
[92] P. Feth, "A tool for the development and comparison of approaches for the dynamic risk assessment of active safety systems," in *Commercial Vehicle Technology*. Wiesbaden, Germany: Springer, 2018, pp. 387–399.
[93] S. U. Bhover, A. Tugashetti, and P. Rashinkar, "V2X communication protocol in VANET for co-operative intelligent transportation system," in *Proc. Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Feb. 2017, pp. 602–607, doi: 10.1109/ICIMIA.2017.7975531.
[94] 5GAA. (Jan. 22, 2019). *Timeline for Deployment of C-V2X (V2V/V2I)*. [Online]. Available: https://5gaa.org/wp-content/uploads/2019/01/5GAA_White-Paper-CV2X-Roadmap.pdf
[95] P. E. Orukpe, "Model predictive control fundamentals," *Nigerian J. Technol. (NIJOTECH)*, vol. 31, no. 2, pp. 139–148, 2012. [Online]. Available: https://www.ajol.info/index.php/njt/article/viewFile/123569/113097
[96] E. Fitzgerald and B. Landfeldt, "A system for coupled road traffic utility maximisation and risk management using VANET," in *Proc. 15th Int. IEEE Conf. Intell. Transp. Syst.*, Sep. 2012, pp. 1880–1887.
[97] D. Shin, K. Park, and M. Park, "Effects of vehicular communication on risk assessment in automated driving vehicles," *Appl. Sci.*, vol. 8, no. 12, p. 2632, 2018. [Online]. Available: https://www.mdpi.com/2076-3417/8/12/2632
[98] A. Carvalho, Y. Gao, S. Lefevre, and F. Borrelli, "Stochastic predictive control of autonomous vehicles in uncertain environments," in *Proc. 12th Int. Symp. Adv. Vehicle Control (AVEC)*, Tokyo, Japan, 2014.
[99] L. Changchun, A. Gray, L. Chankyu, J. K. Hedrick, and P. Jiluan, "Nonlinear stochastic predictive control with unscented transformation for semi-autonomous vehicles," in *Proc. Amer. Control Conf.*, Jun. 2014, pp. 5574–5579.
[100] S. Riedmaier, T. Ponn, D. Ludwig, B. Schick, and F. Diermeyer, "Survey on scenario-based safety assessment of automated vehicles," *IEEE Access*, vol. 8, pp. 87456–87477, 2020, doi: 10.1109/ACCESS.2020.2993730.
[101] B. Paden, M. Čáp, S. Z. Yong, D. Yershov, and E. Frazzoli, "A survey of motion planning and control techniques for self-driving urban vehicles," *IEEE Trans. Intell. Vehicles*, vol. 1, no. 1, pp. 33–55, Jun. 2016, doi: 10.1109/TIV.2016.2578706.
[102] S. Lefèvre, D. Vasquez, and C. Laugier, "A survey on motion prediction and risk assessment for intelligent vehicles," *ROBOMECH J.*, vol. 1, no. 1, pp. 1–14, 2014, doi: 10.1186/s40648-014-0001-z.

Wei Ming Dan Chia (Member, IEEE) is currently pursuing the Ph.D. degree from the University of Glasgow. He had 17 years of industry experience spanning across several automotive companies—Delphi, Siemens VDO, and Continental, from 2001 to 2017. His last role in Continental was the Director of ITS Laboratory and the Head of Advance Development in Asia for infotainment and connectivity products. He is currently a Senior Lecturer with the Singapore Institute of Technology since 2017. His main interests include applying artificial intelligence for autonomous vehicles safety operations and intelligent transport systems.

Sye Loong Keoh received the Ph.D. degree in computing science from Imperial College London in 2005. He was a Senior Scientist at Philips Research Eindhoven, The Netherlands. He is an Associate Professor with the School of Computing Science, University of Glasgow Singapore (UGS), and the Director of Research Programs. His research interests include cyber security for the Internet of Things (IoT), lightweight security systems for cyber-physical systems, and policy-based security management for pervasive and distributed systems. He leads the cyber-security research activities at UGS, where he has designed several lightweight authentication protocols and key management schemes for the IoT, building management, and industrial control systems.

Cindy Goh (Senior Member, IEEE) received the Ph.D. degree from the University of Glasgow, U.K., in 2004. She was the Director of Research Programs at the University of Glasgow Singapore (UGS) from 2013 to 2016. She is currently the Director of UGS, where she has overall responsibility for its strategy and management. Her research interests include intelligent optimization and data analytics for optimal decision-making, design to advance the state-of-the-art in complex engineering systems, energy and transport networks, and smart manufacturing. She is a fellow of HEA and a Founding Member of the International Union of Radio Science Committee, Singapore.

Christopher Johnson received the M.A. degree from the University of Cambridge and the D.Phil. and M.Sc. degrees from the University of York. His research interests include the development of complex safety and security critical systems. Over the last ten years, he had helped to author guidelines for the investigation of incidents and accidents across both the European aviation and railway industries and support United Nations work on guidelines for the cyber security of chemical, biological, radiological, and nuclear systems. He has worked with the members of the European Space Agency and with NASA on the software engineering of future space missions. He is a fellow of the Royal Society of Edinburgh, the Royal Aeronautical Society, and the British Computer Society. He is the Co-Chair of the Scientific Advisory Board for the SESAR Program on the modernization of European Air Traffic Management and a Steering Committee Member of the U.K. National Cyber Security Centre's work on Industrial Cyber Security.