Introducing ASIL Inspired Dynamic Tactical Safety Decision Framework for Automated Vehicles

Siddartha Khastgir
WMG, University of Warwick
Coventry, United Kingdom
S.Khastgir@warwick.ac.uk

Hakan Sivencrona
Qamcom Research and Technology AB
Göteborg, Sweden
Hakan.Sivencrona@qamcom.se

Gunwant Dhadyalla
WMG, University of Warwick
Coventry, United Kingdom
G.Dhadyalla@warwick.ac.uk

Peter Billing
Qamcom Research and Technology AB
Göteborg, Sweden
Peter.Billing@qamcom.se

Stewart Birrell
WMG, University of Warwick
Coventry, United Kingdom
S.Birrell@warwick.ac.uk

Paul Jennings
WMG, University of Warwick
Coventry, United Kingdom
Paul.Jennings@warwick.ac.uk

***Abstract*— Existing automotive Hazard Analysis and Risk Assessment (HARA) process as discussed by the international standard ISO 26262 is static in nature. While the standard describes a systematic process to incorporate functional safety in the development process of Electrical & Electronic (E/E) systems, it fails to address the needs of Advanced Driver Assistance Systems (ADAS) and Automated Driving (AD) systems. In order to ensure the safety of ADAS and AD systems, it is important to incorporate the changing nature of interactions between the system and the environment, in the safety analysis process for ADAS and AD systems. In this paper, the authors argue the need for a dynamic approach for automotive safety analysis by adapting the tactical safety for ADAS and AD systems depending on the real-time operational capability and real-time ASIL (Automotive Safety Integrity Level) rating of a situation, and discuss a framework for this process. The novelty and therefore contribution of this paper lies in the proposed ASIL inspired dynamic tactical safety framework, which evaluates the severity, controllability and exposure ratings in real-time based on the real time values of the various vehicle and environment parameters. These ratings are used to assign a real-time ASIL value which is used to determine the tactical decisions in order to lower the ASIL value in real-time by altering the functional (operational) capability of the system. Furthermore, the framework is explained with the help of a case study based on a combined Adaptive Cruise Control (ACC) and Autonomous Emergency Braking (AEB) system.**

Keywords— ISO 26262, Tactical decisions, Hazards, HARA

I. INTRODUCTION

The increasing focus on the introduction of Advanced Driver Assistance Systems (ADASs) and Automated Driving (AD) systems is driven by their potential to increase safety of the vehicle occupants and others in the environment. This is because the cause of over 90% of the on-road accidents has been attributed to driver error [1]. Therefore, the ability of ADAS and AD systems to assist or replace the driver (respectively), has the potential to reduce the number of accidents as these systems can potentially identify and react to hazardous situations better than the human driver [2]. However, one of the major challenges for ADAS and AD systems is to ensure the safe working of these systems.

ADAS and AD systems differ from more conventional automotive Electrical/Electronic (E/E) systems in their increased dependence on the quality of environment perception and its attributes to ensure safety [3]. This dependence proves to be a challenge for testing of these systems [4] and also for their safe functioning. The large number of possible scenarios make it hard to ensure completeness of the functional scope and subsequent set of possible safety goals which ensure the safety of the systems. Additionally, the changing nature of the interaction of the ADAS and AD systems with the environment makes it challenging to ensure safety of the system with a static approach to risk analysis. With the developments in AD systems, it is expected that the systems will be able to deal with the three levels of driving task: limited strategic, tactical and operational [5]; while ADAS systems can perform only operational tasks. At a strategic level, tasks include route planning which have limited safety implications. Moreover, the strategic goals can be decomposed into tactical goals and any limited safety implications at the strategic level will be magnified to an extent that it can be addressed at the tactical level. Therefore, for the scope of this paper, the authors will address the tactical and operational driving tasks and the trade-off required between them to ensure the safety of an ADAS and AD systems.

In this paper, the authors argue for a dynamic approach to tactical decisions for ADAS and AD systems. Drawing learnings from similar challenges faced by the chemical process industry and their shift to a more dynamic approach, the authors propose a framework for the dynamic approach based on real-time ASIL value for the situation (hazardous event). A static HARA fails to capture the real-time state of the system and the environment which may have a bearing on the risk analysis probabilities. One of the main reasons for a dynamic approach is to secure the availability of the ADAS

This research is sponsored by WMG, University of Warwick, UK, WMG centre HVM Catapult and the Swedish government agency for innovation systems (VINNOVA) in the ESPLANADE project (ref 2016-04268).

and AD systems albeit with reduced operational capability in the presence of a hazardous event.

In Section II of this paper, risk analysis methods from other domains, and their shift to a more dynamic approach is discussed. Section III discusses the automotive HARA process, Section IV discusses the trade-off between operational and tactical decisions, along with the challenges offered by ADAS and AD systems. Section V introduces the dynamic tactical decision making framework. Section VI discusses a case study for a system with Adaptive Cruise Control (ACC) and Autonomous Emergency Braking (AEB) features, in which the proposed dynamic tactical decision making approach is applied. Finally, section VII concludes the paper.

II. Risk Analysis in Other Domains

Risk analysis gathered initial momentum in the nuclear sector, later shifting to chemical process industry, aviation and railways. Risk analysis in the automotive domain is a more recent activity. While risk analysis in the nuclear industry is quantitative, the chemical process industry initially followed a qualitative approach and later a hybrid approach of quantitative and qualitative risk analysis [6]. Qualitative risk analysis is criticized for its vagueness in terminology, arbitrariness and lack of transparency in selection of worst case events [7]. While Quantitative Risk Analysis (QRA) [8] is able to overcome most of these criticisms, it has the disadvantage of being computationally intensive. However, the recent improvements in on-board and off-board data acquisition systems are able to overcome this limitation. One of the applications of QRA in the chemical industry is risk based design which plays an important role in risk reduction [9]. An analytical approach adopted in a QRA helps in achieving reliable results in estimating the impact of hazards [10]. However, estimating the frequency of hazards as part of conventional QRA quickly became obsolete as it needed to take into consideration the realistic values of failure probability based on real-time conditions of systems and failures [11]. Classical QRA is a static process, giving a risk picture *"frozen in time"* [6], and fails to take into consideration the unsafe interactions [12]. As processes become complex, risk assessment made for a particular phase may not be appropriate for another phase of the system application [13]. While risk assessment has been conducted in the chemical process industry for many years, history has shown that similar accidents repeat themselves (Bhopal 1984 [14] and Texas City 2005 [15]). This has led to several efforts towards a dynamic approach to risk assessment in the chemical process industry [16]. Traditional risk assessment is based on measuring deviations from pre-defined (static) thresholds and fail to capture variation in risk during continuous operation [17]. However, in a dynamic approach, a continuous re-calculation of the probabilities is done based on the system and environment state, helping in detecting early warnings and near-miss scenarios. An incident or a near-miss scenario represents a breach of a safety mechanism and needs to be captured as it will influence failure probabilities. Such events have been mentioned in the chemical process industry literature as Accident Sequence Precursors (ASP) [18]. This is evident from the study of the BP Texas city refinery accident, where detection of near-misses, coupled with a dynamic approach to update risk assessment could have prevented the accident [10].

In order to have correct evaluation of risk, the analysis needs to be based on accurate data which represents the situation in real time [10]. One of the fundamental issues with risk analysis is due to the variation in the understanding and definition of "risk". Different risk definitions may cause variation in the risk assessment process. In this paper, the authors adopt the definition of risk from the ISO 26262 standard [19], which defines risk as the *"combination of the probability of occurrence of harm and the severity of that harm."* A dynamic approach provides an ability to cope with variations in system's operation without total loss of functionality.

Dynamic Risk Analysis Approaches

While initial efforts towards a dynamic approach were made by some authors [20]–[22], the most developed methodology is termed Dynamic Risk Assessment (DRA) which dynamically estimates probabilities for accidents using Bayesian failure mechanism and consequence analysis [12], [17]. Two additional steps as compared to conventional risk analysis are key to this approach. These include updating accident analysis and failure probabilities. Firstly, for updating accident analysis, event/fault tree (bow tie approach [23]) is used in addition to real-time process data. Secondly, to update probabilities, Bayesian functions are used. Alternatively, a non-Bayesian approach to probability updating can be applied which requires real-time parameter values and status health of the system [17], [23]. The versatility of the DRA method for chemical process systems has been demonstrated by applications in real life cases like BP Texas Refinery accident [15], off shore drilling [24] and BP Deepwater Horizon accident [25]. However, the DRA approach too falls short in certain aspects. None of the DRA approaches (bow-tie, Bayesian etc.) is able to update both failure probabilities and consequences in real-time [26].

In order to overcome some of the challenges of DRA, the DRA and Dynamic Procedure for Atypical Scenarios Identification (DyPASI) methods have been combined in some studies [27]. DyPASI is a hazard identification process and improves the completeness of the hazards by identifying worst case scenarios [16], [18]. Other DRA approaches used in chemical process industry include using a risk barometer [16]. These dynamic approaches help in reducing risk by monitoring the state of safety critical barriers using real time data associated with the systems.

III. Automotive HARA Process

Automotive HARA is followed as per the ISO 26262 standard which is considered as the state-of-the-art for ensuring safety of E/E systems in the automotive domain. The standard introduces the concept of the Automotive Safety Integrity Level or ASIL rating. An ASIL rating is obtained from an ASIL determination table which has three parameters: Severity, Controllability and Exposure. ISO 26262 identifies various ASIL levels which are QM, ASIL A, ASIL B, ASIL C

and ASIL D, with ASIL D being the highest integrity level necessitating the most rigorous requirements on the product development cycle and QM being the lowest integrity level. However, the determination of ASIL ratings is subjective and is based on expert opinion which causes variation in the ratings assigned to a hazardous event [28]. There is also questionability on the scientific approach to explain how the ratings affect safety [29].

An automotive safety analysis process, like other domains is essentially a two stage process. *The first step involves identification of hazards and their corresponding hazardous events*, which should (ideally) have a corresponding Safety Goal (SG). A hazardous event is defined as the *"combination of a hazard and an operational situation"* [19]. One of the challenges offered by ADAS and AD systems is the ability to identify various hazardous events during analysis and the lack of a systematic approach to address this issue. One approach to tackle this challenge is to define a generic hazard and subsequently hazardous events. While this would benefit from a shorter and easier HARA, it might suffer from high ASIL levels due to wider safety implications and the temptation to select worst case events. A high ASIL may lead to higher development cost due to the additional design and verification efforts recommended in ISO 26262, making the approach infeasible for the automotive industry. Alternately, a more exhaustive set of hazards and hazardous events might lead to lower ASIL levels of some sub-systems. It might be prudent to adopt the later approach to ensure completeness within the resource constraints.

The second step involves the HARA process, in which the identified hazardous event is assigned an ASIL rating which is evaluated based on the severity, exposure and controllability ratings for the hazardous event. The authors adopt an objective approach to ASIL classification as defined in [28].

IV. Tactical and Operational Decisions and Safety

Safety during a driving task can be considered individually for each of the three driving tasks: strategic, tactical and operational. Strategic safety may be achieved by, for example route planning of a route with less traffic or where the exposure of vulnerable road users is less as compared to other available route options. Strategic safety is achieved at a higher abstraction level. Tactical safety may be achieved by making decisions about vehicle parameters like speed, distance between the lead car and own vehicle, carrying out an overtaking manoeuvre etc., in a way that reduces the overall risk of the system and scenario. Operational safety involves the ability of the sensing system to perceive the environment and the use of actuators (brakes, accelerator, steering wheel etc.) safely and understanding their capabilities and limitations. This paper will discuss the trade-off between the tactical and the operational decision making and its impact on ensuring safety of the system. A manual driver is able to make this trade-off as the driver has the full responsibility of the tactical task and the operational task. The clear assignment of responsibility makes it easier to operate safely in the absence of automation.

The introduction of ADAS blurs the boundaries of responsibility making it difficult to allocate responsibility for safety related decisions. Both ADAS and AD systems need to make operational choices as part of the driving task. However, the difference in the nature of these interactions for the two systems lead to a different safety assessment for them. ADAS is an assisting system and always has the driver as a fall back measure, which means that the operational choices for driving task is shared between the driver and ADAS, without clear role assignment. However, for an AD system, both tactical and operational tasks rest with the system [3]. Since the AD system has control over both tactical and operational tasks, an efficient strategy could be devised for a trade-off between the two tasks. In other words, the tactical decision making system should request only those functions which the operational system can perform [30].

While some authors have argued that implementing ADAS is easier than an AD system from a technological point of view [31], the reverse is true from a functional safety perspective [30]. While dynamic approaches in other domains have considered continuously updating the frequency and consequence factors, an additional factor of controllability needs to be updated in the automotive risk assessment process (when ADAS is being considered). As automated automotive systems evolve, one possible solution to achieve a trade-off between the operational and tactical task depending on the real-time situation of an ADAS or an AD system would be to adopt a dynamic approach to tactical decisions.

V. Dynamic Tactical Decision Making Framework

In order to adapt the tactical decisions to incorporate the changing operational capability and interactions between the system and the environment, the authors propose an ASIL inspired dynamic framework (Fig. 1). The proposed framework has the following aspects:

1. Item definition
2. Hazardous event detection system
3. Objectification of Automotive HARA
4. Real-time ASIL determination
5. Decision and Control for countermeasure (updating item definition to lower the ASIL)

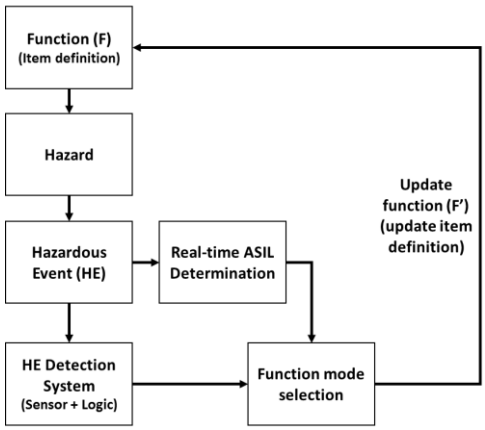

Fig. 1. Dynamic tactical decision making framework

The first step in the proposed process involves defining the function or the item. This definition is essential for establishing the capability of the function and the different possible modes of the function in which the function availability can be increased by reducing the capability of the functionality, i.e., altering the item definition. One of the key aspects of the framework is the ability of the system to identify a hazardous event which is achieved by the hazardous event detection system in Fig. 1. An item is defined as the *"system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied"* [19]. The benefit of proposed process over dynamic risk analysis framework (discussed in section II) is the ability to evaluate all three aspects (severity, controllability and exposure) in real time as compared to only probabilities. In the automotive context, all three parameters are context dependent.

A. *Objectification of Automotive HARA*

Automotive HARA like other domains suffers from reliability issues causing variation in ratings [28]. Two types of variation exist: 1) inter-rateability variation and 2) intra-rateability variation. Objectification of the HARA process aims to remove these two types of variation which are caused by different mental models between experts and their varying mental models over time. Objectification of the automotive HARA involves parametrization of the Severity, Exposure and the Controllability ratings to create a rule set for assigning an ASIL rating based on the values of the parameters [28]. Objectification of the HARA process is an essential prerequisite for establishing a real-time ASIL value for a given hazardous event. A sample rule-set for severity rating is shown in Table 1.

TABLE I. SEVERITY PARAMETERS AND SEVERITY RULE-SET

Type of Obstacle [a]	Vehicle Velocity	Oncoming Obj. Velocity	Severity Rating
Pedestrian	< 11 kmph	< 2 kmph	S0
		< 6 kmph	S1
		< 12 kmph	S1
	11 - 16 kmph	< 2 kmph	S1
		< 6 kmph	S2
		< 12 kmph	S2
	> 16 kmph	< 2 kmph	S2
		< 6 kmph	S3
		< 12 kmph	S3

[a.] Table from section 3.1 in [28]

B. *Real time parameter monitoring and ASIL determination*

In order to evaluate the ASIL rating for a hazardous event dynamically, the parameters identified for objectification of the HARA process need to be measured in real-time and fed to the ASIL determination engine. This enables an accurate ASIL determination based on the current vehicle and environment states (Fig. 2).

C. *Decision and Control for countermeasure*

The Decision and Control (DC) sub-system receives the real-time ASIL rating and the sensors values for environment perception to make a tactical choice for the vehicle which is within the operational boundary of the vehicle. In other words,

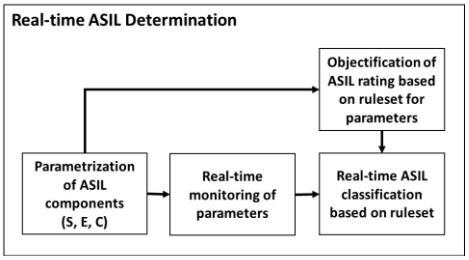

Fig. 2. Real-time ASIL Determination framework

the DC subsystem performs the task of the mode selection (i.e., a safety measure) to modify the ASIL value for the current hazardous event situation in order to secure the availability of the system, albeit with reduced capability. The operational boundary of the vehicle is inspired by the real-time ASIL rating for the situation and sensor values (environment perception). Once an ASIL rating and the operational boundary of the system are established for a given hazardous event, the counter-measure is determined (which is a trade-off between the tactical and the operational task).

A countermeasure could have any one of the following four attributes [18]:

1. *To avoid:* an attribute acting upstream in the accident model
2. *To prevent:* an attribute acting upstream in the accident model
3. *To control:* an attribute acting downstream in the accident model
4. *To limit:* an attribute acting downstream in the accident model

However, the decision to choose between one of the four countermeasures is also dependent on the system's operational capability to achieve the countermeasure action. Therefore, the real-time operational capability needs to be monitored to define the tactical behaviour (which involves the countermeasure action) of the ADAS or AD system. The tactical decision becomes the safety measure for the identified hazardous event which alters the parameters determining the ASIL rating to lower the ASIL rating assigned to the situation (Fig. 3) and thus increasing the availability of the system with lower functionality.

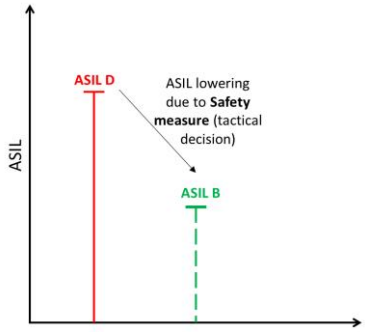

Fig. 3. Lowering of ASIL with a tactical decision

VI. Case Study

An example case study is presented in this paper, explaining the application of the dynamic tactical decision making framework. The case study uses an ADAS with ACC and AEB capability as an example.

A. *Function Definition: Adaptive Cruise Control (ACC) + Autonomous Emergency Braking (AEB) system*

A system with Adaptive Cruise Control (ACC) system and Autonomous Emergency Braking (AEB) capability performing the longitudinal control for the vehicle is chosen as an example. An ACC system maintains a set headway between the host vehicle and the target vehicle. An ACC system has the capability to adapt the speed of the vehicle and apply brakes (within certain design limitations). An AEB system performs emergency (severe) braking by applying necessary braking force in order to avoid an obstacle. In the system under discussion, an ACC + AEB system has tasks of applying the brakes and throttle based on the set speed and road traffic (tactical choice being the selection of the priority of the operational decisions). An ACC system is known to have decreased capability during fog and rain. Within the dynamic framework, this information will be provided by the sensors (in real time) to the ASIL level determination engine, which will use the objectification engine to derive a real-time ASIL for the ACC + AEB system in the given situation. However, in order to classify an ASIL value, the hazardous event detection system needs to identify the hazardous event. For the ACC + AEB system, this is achieved by a water spray detection system which detects the presence of water spray (Fig. 4).

B. *Scenario and Hazard Definition*

In this case study the authors present a scenario in which the host vehicle (HV) equipped with radar based ACC + AEB system is following a target vehicle (TV) or lead vehicle. The HV has a rear vehicle (RV) traveling behind it (Fig. 5). For the given scenario, the hazard under consideration is the "unintended braking" of the host vehicle which could potentially cause a collision from behind between the RV and the HV. The hazardous event being considered for the given hazard is, "water spray causing unintended braking leading to collision" as the water spray is being falsely interpreted as a lead vehicle by the radar system.

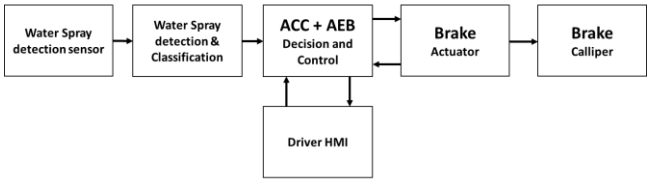

Fig. 4. ACC + AEB system architecture

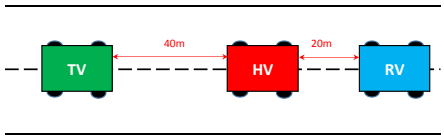

Fig. 5. ACC + AEB Scenario under consideration

C. *Parameterization*

The following parameters were identified for the system and scenario under consideration: vehicle type, relative distance, relative speed and acceleration/deceleration. The parameters are used to assign a real-time ASIL value for the hazardous event. As the relative speed increased between HV and RV, the ASIL value decreased for the hazardous event.

D. *Dynamic Tactical Safety Decisions*

Let us assume that TV and HV are traveling with a speed of 72 kmph, with a relative distance of 40m and both vehicles (types) are passenger vehicles. In addition, let us assume the same characteristics for HV and RV combination, except that the relative distance is 20m. The unintended deceleration of HV is 0.8g. For the given set of parameter values and hazardous event, the real-time ASIL determination system (via the objectification of ASIL ratings' rule-set) assigns an ASIL D value (Severity: S3, Exposure: E4 and Controllability: C3) for the hazardous event. In order to bring the ASIL to a lower value, a safety measure needs to be introduced. A tactical decision altering the values of the parameters (speed, acceleration/deceleration and relative distance used for ASIL determination) could be a possible safety measure.

Assuming TV and RV have constant speed, a tactical decision can be implemented to reduce the HV speed, increasing the relative speed between HV and TV and thus lowering the ASIL rating. Alternatively, a tactical decision could be to increase the speed of HV, increasing the relative speed between HV and RV and thus lowering the ASIL rating by lowering the Severity rating from S3 to S2 and controllability rating from C3 to C2, while exposure remains same at the highest value of E4. This reduces the ASIL rating from ASIL D to ASIL B (Fig. 6). Since the hazardous event under consideration is collision from behind, the later approach is valid until a frontal collision becomes a new hazardous event. This presents a situation where the possible tactical decision options are conflicting in nature and an optimization is needed between the two tactical decisions.

It is important to note that the success of the proposed process is dependent upon a well-developed hazard detection system which in itself will be an ASIL D sub-system. However, the proposed process is highly scalable as the ASIL determination is based on priori parameters identified. Future manuscripts will discuss the real world implementation of the

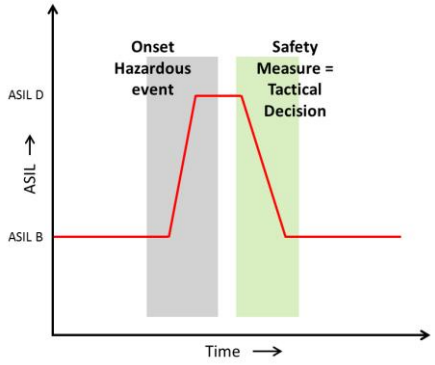

Fig. 6. Dynamic tactical decision lowering ASIL value

proposed concept and demonstrate the scalability in combinatorial real-world decision making situations.

VII. Conclusions

One of the major drawbacks of conventional risk assessment methods is that it gives a picture "frozen in time". They are unable to take into consideration the changing risk nature due to environmental changes. A shift to dynamic risk assessment has been seen in other industries which faced similar challenges like the automotive domain faces currently.

The advent of ADAS and AD systems in the automotive industry have provided a challenge for ensuring safety of the systems. In this paper, the authors introduce a dynamic tactical and operational decision making framework which is inspired by real time ASIL for a situation for ADAS and AD system to better inform the system on the trade-off decision between the tactical and operational driving task choices. The authors argue that the conventional HARA process which is static in nature is not able to meet the challenges offered by the ADAS and AD systems to ensure their safety. The proposed dynamic approach is a five step approach and comprises of objectification of automotive HARA, real-time parameter monitoring, real-time ASIL rating determination and Decision and Control for countermeasure to update the functionality of the system. With the help of a preliminary case study of a system with ACC + AEB functionality, the authors demonstrate that by altering the tactical decisions to select a different mode of the functionality, the ASIL for the hazardous event is reduced.

Acknowledgment

The authors would like to thank WMG, University of Warwick, UK and the WMG centre HVM Catapult for supporting this research. WMG hosts one of the seven centres that together comprise the High Value Manufacturing Catapult in the UK. This research has also been supported by the Swedish government agency for innovation systems (VINNOVA) in the ESPLANADE project (ref 2016-04268). The authors would also like to thank Anders Sandberg for his valuable contribution to this manuscript.

References

[1] S. Singh, "Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey. (Traffic Safety Facts Crash Stats. Report No. DOT HS 812 115)," Washington, DC, 2015.

[2] J. Carbaugh, D. N. Godbole, and R. Sengupta, "Safety and capacity analysis of automated and manual highway systems," Transp. Res. Part C Emerg. Technol., vol. 6, no. 1–2, pp. 69–99, 1998.

[3] R. Johansson and J. Nilsson, "The Need for an Environment Perception Block to Address all ASIL Levels Simultaneously," in Proc. of the IEEE Intelligent Vehicles Symposium (IV), 2016.

[4] S. Khastgir, S. Birrell, G. Dhadyalla, and P. Jennings, "Identifying a Gap in Existing Validation Methodologies for Intelligent Automotive Systems : Introducing the 3xD Simulator," in Proc. of the IEEE Intelligent Vehicles Symposium (IV), 2015, pp. 648–653.

[5] J. A. Michon, "A critical view of driver behavior models: what do we know, what should we do?," in Human behavior and traffic safety, L. Evans and R. C. Schwing, Eds. Plenum Press, 1985, pp. 485–520.

[6] V. Villa, N. Paltrinieri, F. Khan, and V. Cozzani, "Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry," Saf. Sci., vol. 89, pp. 77–93, 2016.

[7] "The Buncefield Incident 11 December 2005: The final report of the Major Incident Investigation Board," 2008.

[8] H. Pasman and G. Reniers, "Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP)," J. Loss Prev. Process Ind., vol. 28, pp. 2–9, 2014.

[9] E. Fadier and C. De La Garza, "Safety design: Towards a new philosophy," Saf. Sci., vol. 44, no. 1, pp. 55–73, 2006.

[10] N. Paltrinieri, F. Khan, and V. Cozzani, "Coupling of advanced techniques for dynamic risk management," J. Risk Res., vol. 18, no. 7, pp. 910–930, 2015.

[11] G. D. Creedy, "Quantitative risk assessment: How realistic are those frequency assumptions?," J. Loss Prev. Process Ind., vol. 24, no. 3, pp. 203–207, 2011.

[12] M. Kalantarnia, F. Khan, and K. Hawboldt, "Dynamic risk assessment using failure assessment and Bayesian theory," J. Loss Prev. Process Ind., vol. 22, no. 5, pp. 600–606, 2009.

[13] A. Falck, E. Skramstad, and M. Berg, "Use of QRA for decision support in the design of an offshore oil production installation.," J. Hazard. Mater., vol. 71, no. 1–3, pp. 179–192, 2000.

[14] M. Yang, F. Khan, and P. Amyotte, "Operational risk assessment: A case of the Bhopal disaster," Process Saf. Environ. Prot., vol. 97, pp. 70–79, 2015.

[15] M. Kalantarnia, F. Khan, and K. Hawboldt, "Modelling of BP Texas City refinery accident using dynamic risk assessment approach," Process Saf. Environ. Prot., vol. 88, no. 3, pp. 191–199, 2010.

[16] N. Paltrinieri and G. Scarponi, "Addressing Dynamic Risk in the Petroleum Industry by Means of Innovative Analysis Solutions," Chem. Eng. Trans., vol. 36, pp. 451–456, 2014.

[17] N. Khakzad, F. Khan, and P. Amyotte, "Dynamic risk analysis using bow-tie approach," Reliab. Eng. Syst. Saf., vol. 104, pp. 36–44, 2012.

[18] N. Paltrinieri, A. Tugnoli, J. Buston, M. Wardman, and V. Cozzani, "Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool," J. Loss Prev. Process Ind., vol. 26, no. 4, pp. 683–695, 2013.

[19] ISO, "Road vehicles — Functional safety (ISO 26262)," 2011.

[20] P. E. Labeau, C. Smidts, and S. Swaminathan, "Dynamic reliability: Towards an integrated platform for probabilistic risk assessment," Reliab. Eng. Syst. Saf., vol. 68, no. 3, pp. 219–254, 2000.

[21] S. Swaminathan, "The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment," Reliab. Eng. Syst. Saf., vol. 63, no. 1, pp. 73–90, 1999.

[22] H. Boudali and J. B. Dugan, "A discrete-time Bayesian network reliability modeling and analysis framework," Reliab. Eng. Syst. Saf., vol. 87, no. 3, pp. 337–349, 2005.

[23] R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, "Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach," Process Saf. Environ. Prot., vol. 91, no. 1–2, pp. 1–18, 2013.

[24] M. Abimbola, F. Khan, and N. Khakzad, "Dynamic safety risk analysis of offshore drilling," J. Loss Prev. Process Ind., vol. 30, no. 1, pp. 74–85, 2014.

[25] S. Rathnayaka, F. Khan, and P. Amayotte, "Accident modeling and risk assessment framework for safety critical decision-making: application to deepwater drilling operation," J. Risk Reliab., vol. 227, no. 1, pp. 86–105, 2013.

[26] F. Khan, S. J. Hashemi, N. Paltrinieri, P. Amyotte, V. Cozzani, and G. Reniers, "Dynamic risk management: a contemporary approach to process safety management," Curr. Opin. Chem. Eng., vol. 14, pp. 9–17, 2016.

[27] N. Paltrinieri, F. Khan, P. Amyotte, and V. Cozzani, "Dynamic approach to risk management : Application to the Hoeganaes metal dust accidents," Process Saf. Environ. Prot., vol. 92, no. 6, pp. 669–679, 2013.

[28] S. Khastgir, S. Birrell, G. Dhadyalla, H. Sivencrona, and P. Jennings, "Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems," Saf. Sci., 2017.

[29] H. Yu, C.-W. Lin, and B. Kim, "Automotive Software Certification: Current Status and Challenges," SAE Int. J. Passeng. Cars - Electron. Electr. Syst., vol. 9, no. 1, pp. 2016-01–0050, 2016.

[30] R. Johansson and J. Nilsson, "Disarming the Trolley Problem – Why Self-driving Cars do not Need to Choose Whom to Kill," in Proc. of the Workshop Critical Automotive applications : Robustness & Safety, 2016.

[31] KPMG, "Self-driving cars : The next revolution."