Towards Increased Reliability by Objectification of Hazard Analysis and Risk Assessment (HARA) of Automated Automotive Systems

Abstract

Hazard Analysis and Risk Assessment (HARA) in various domains like automotive, aviation, process industry etc. suffer from the issues of validity and reliability. While there has been an increasing appreciation of this subject, there have been limited approaches to overcome these issues. In the automotive domain, HARA is influenced by the ISO 26262 international standard which details functional safety of road vehicles. While ISO 26262 was a major step towards analysing hazards and risks, like other domains, it is also plagued by the issues of reliability. In this paper, the authors discuss the automotive HARA process. While exposing the reliability challenges of the HARA process detailed by the standard, the authors present an approach to overcome the reliability issues. The approach is obtained by creating a rule-set for automotive HARA to determine the Automotive Safety Integrity Level (ASIL) by parametrizing the individual components of an automotive HARA, i.e., severity, exposure and controllability. The initial rule-set was put to test by conducting a workshop involving international functional safety experts as participants in an experiment where rules were provided for severity and controllability ratings. Based on the qualitative results of the experiments, the rule-set was re-calibrated. The proposed HARA approach by the creation of a rule-set demonstrated reduction in variation. However, the caveat lies in the fact that the rule-set needs to be exhaustive or sufficiently explained in order to avoid any degree of subjective interpretation which is a source of variation and unreliability.

Keywords: Hazard, HARA, ISO 26262, Functional Safety, Reliability

1. Introduction

Over 90% of the on-road accidents occur due to human error (Singh, 2015). Therefore, an ability to assist or replace the human driver in the driving task has a potential to reduce the number of accidents. The introduction of Advanced Driver Assistance Systems (ADAS) and Automated Driving (AD) systems has been driven by the fact that these systems will be able to improve road traffic safety. This is due to the higher ability of an automated system to react to a possible hazardous situation as compared to the most alert manual driver (Carbaugh et al., 1998). Apart from safety benefits, AD systems and ADAS also offer the potential for increased operational efficiency by increasing road through-put by reducing the proximity between vehicles (Bishop, 2000; Kesting et al., 2008; van Arem et al., 2005).

In 1996, Sweden adopted a “Vision Zero” policy which states that *“eventually no one will be killed or seriously injured within the road transport system”* (Johansson, 2009). It brought together multiple stakeholders like vehicle manufacturers, road designers, state, city councils, municipalities and individuals, in order to achieve the mission of zero on-road fatalities. According to Vision Zero’s viewpoint, a holistic approach needs to be adopted. While changes in vehicles is a major aspect of the solution (with the introduction of passive safety, active safety and automated features), other aspects include changes in roads, streets, knowledge/awareness of individuals and legislations (Tingvall, 1998). While the principles of Vision Zero concept is valid for every country, the identification of changes and their implementation differs from country to country and the cultural aspect of the country needs to be taken into consideration in the strategic analysis plan (Johansson, 2009).

While ADAS and AD systems are an important part of achieving a Vision Zero concept, both ADAS and AD systems offer new challenges for testing and the safety analysis of the systems (Khastgir et al., 2015). Variety of ADAS and AD systems exist or are in development, each of them offer a different kind of a challenge. As we move towards higher levels of automation in the SAE's six levels of automation (level 0-5) (SAE International, 2016), testing and risk analysis becomes harder as it needs to include larger number of variables and their interactions in the analysis. The authors discuss risk analysis within the scope of this paper. Section 1.1 discusses risk analysis in a general setting, section 1.2 briefly discusses reliability through objectification of the risk analysis process and section 1.3 discusses automotive risk analysis.

1.1. Reliability and Validity of Risk Analysis

Safety analysis is a two-step process. In the first step one needs to identify the hazards for which the Hazard Analysis and Risk Assessment (HARA) is to be performed. There are various methods for identifying hazards like System Theoretic Process Analysis (STPA) / Systems Theoretic Accident Model & Processes (STAMP) (Leveson, 2004, 2011a, 2011b), JANUS (Hoffman et al., 2004), Accimaps (Salmon et al., 2012), HFACS (Baysari et al., 2009; Chen et al., 2013; D. Wiegmann and Shappell, 2001), Fault-tree analysis (Lee et al., 1985; Reay and Andrews, 2002), bow-tie analysis (Abimbola et al., 2016; Khakzad et al., 2012), FMEA (Stamatis, 2003), etc. Some of these methods were developed for simpler systems and fall short in their ability to meet the requirements for the analysis of modern systems which have multiple interactions between the system and software components and the human operator (Fleming et al., 2013). Another source of identifying hazards is from experience of previous accidents and their accident investigations. However, being retrospective in nature, they cannot be taken as the only source of possible hazards, but should influence future hazard identification process and safety management process (Stoop and Dekker, 2012). While accident investigations provide new knowledge about the possible avenues of system failures, they are never exhaustive. This is evident by the deja-vu experience of similar accidents repeating themselves in a 20-30 year cycle (Le Coze, 2013). Identifying hazards has its challenges and is a research question in its own right. While it is possible to identify hazards based on the "known knowns" and accommodate for the "known unknowns", it is extremely difficulty to foresee the unknown knowns and even more so for the "unknown unknowns" which form the *"Black Swan"* category for hazards (Aven, 2013). Previous accidents, however, provide an insight to the occurrence of "*Black Swan*" type of accidents by increasing experts' knowledge of possible factors for risk analysis (Khakzad et al., 2014). While the authors appreciate that hazard identification is an important area for research with on-going activities, it remains out of scope of this paper. Identification of hazards will be discussed by the authors in future publications.

The second step of the safety analysis process involves the analysis of the hazard and the corresponding risk assessment for the hazard. Risk in general has been suggested to be a construct and not an attribute of the system (Goerlandt and Montewka, 2015), due to the subjective nature of risk (Aven, 2010a; Tchiehe and Gauthier, 2017). However, in the automotive domain, a decomposition of risk provides a different insight. An Automotive Safety Integrity Level (ASIL) rating in automotive HARA comprises of a severity, exposure and a controllability rating. Controllability and Severity of any system are a system attribute. However, exposure for a system remains a construct and is open to subjective variation as it is influenced by the expert's knowledge which governs the probability rating (Aven, 2010b; Aven and Reniers, 2013). Automotive HARA and ASIL will be discussed in detail in section 2-6. This paper deals with the classification of hazards (once they have been identified) and their subsequent risk assessment.

While HARA governs the risk management, i.e., the mitigation steps and the rigour required in the application of the steps; it is plagued by some fundamental challenges of its validity and reliability (Aven and Zio, 2014). One of the fundamental issues with risk assessment is the biases or assumptions made by stakeholders performing the assessment due to subjective interpretation of the underlying process or lack of knowledge of the underlying uncertainties or lack of knowledge of the system safety. Lack of knowledge or improper knowledge about the system may lead to either ignoring possible risk (which may lead to false negatives) or their exaggeration (which may lead to false positives). This introduces uncertainty in the risk analysis which is not taken into consideration while making decisions (Goerlandt and Reniers, 2016). Additionally, the knowledge of the hazards and possible failures helps guide the design process of the systems by providing the ability to make informed design decisions in the design phase of the product (Björnsson, 2017; Villa et al., 2016).

Reliability refers to the *"extent to which a framework, experiment, test, or measuring instrument yields the same results over repeated trials"* (Carmines and Zeller, 1979). In a review of Quantitative Risk Analysis (QRA) method applications, (Goerlandt et al., 2016) found that significant differences existed in the results of QRA conducted by different teams/groups of experts. While mandating a specific QRA method could reduce variation (Van Xanten et al., 2013), they argued that this would not ascertain the accuracy of the results, but make results converge and more comparable.

For HARA to be scientific, it needs to be reliable (Hansson and Aven, 2014). In this paper, the authors adopt the "reliability" definition and types of reliability as defined by (Aven and Heide, 2009)*(pg. 1863)*:

- *"The degree to which the risk analysis methods produce the same results at reruns of these methods (R1).*
- *The degree to which the risk analysis produces identical results when conducted by different analysis teams, but using the same methods and data (R2)*
- *The degree to which the risk analysis produces identical results when conducted by different analysis team with the same analysis scope and objectives, but no restrictions on methods and data (R3)"*

1.2. Reliability through objectivity

According to Cambridge English Dictionary ("Cambridge English Dictionary," 2017), "objectivity" is defined as "*the state or quality of being objective and fair*", where "objective" is defined as "*based on real facts and not influenced by personal beliefs or feelings*". In order to prevent the influence of personal beliefs and mental models of experts leading to varied and unreliable HARA ratings, the authors propose the introduction of a rule-set to introduce objectivity in the process. Objectivity could potentially be a tool to help provide consistency and convergence of HARA ratings, thus providing increased reliability.

1.3. Automotive Functional Safety

In the automotive domain, the ISO 26262-2011 standard (automotive functional safety international standard) lacks a quantified and a robust process for automotive certification (Yu et al., 2016). The standard refers to ASIL as a metric for hazard analysis which is influence by Severity (S), Exposure (E) and Controllability (C) rating. However, the methodology for determining these parameters and their quantification is not mentioned. Instead a set of sample tables have been provided (Ellims and Monkhouse, 2012). SAE J2980 provides some guidance to certain degree of objectivity to automotive HARA. But it too falls short in defining various aspects influencing severity, exposure and controllability rating (SAE International, 2015). SAE J2980 provides one table to parametrise severity using speed and collision type as parameters. It doesn't provide any guidance for controllability and exposure ratings. Even for severity, the parameters used are not exhaustive enough.

Thus, there is a need for creating a method for extracting patterns and creating templates for safety case development which would influence the HARA (Kelly, 2004). While ISO 26262 (2011) - Part 3 (ISO, 2011a) comprehensively describes the hazard analysis and identification of hazards using various methods like HAZOP (Cagno et al., 1960), FMEA etc.; it falls short of identifying an objective rating methodology for the hazardous events identified. This leaves the rating to the skills and the mental model of the domain technical experts performing the rating task. An expert's mental model is created and influenced by their own knowledge, experience and environment, leading them to base their risk analysis on some underlying assumptions (Rosqvist, 2010). Any risk rating given by an expert is dependent on the expert's interpretation of the background knowledge (based on their mental model) related to the hazard. This background knowledge may be incomplete in three specific areas: structure of the hazard, parameters responsible for the hazard and probabilities for the parameters (Aven and Heide, 2009). Thus the mental model formed by the expert is a limited representation of the real world. In addition, the dominance of various factors influencing expert's mental model differ at different points in time for the same expert, leading to a varying decision making analysis. Thus, the following two types of variations exist in industry when hazard analysis and risk assessment is performed:

- Inter-rateability variation: due to different mental models between different experts or different groups of experts
- Intra-rateability variation: due variation in mental models of the same expert or same group of experts at different points in time

In a study to evaluate the reliability of the Human Factors Analysis and Classification System (HFACS) (Shappell et al., 2007; D. A. Wiegmann and Shappell, 2001), which is a retrospective accident analysis framework, it was found that while training of experts improved reliability of the analysis, the results demonstrated significant inter- and intra-rater variation (Ergai et al., 2016). Even classification of a hazardous event as a "black swan" is of subjective nature and is prone to inter-rater variations. It is also influence by knowledge or beliefs of the experts which is based on their individual mental models (Aven, 2015; Flage and Aven, 2015).

1.4. Research Question

In order to overcome this challenge, an approach would be to increase focus on the knowledge aspect of HARA by having two teams independently performing the HARA. The role of the second team being to check the bias and the assumptions made by the first team (Veland and Aven, 2015). While such an approach has its merits, it is not practical to adopt this approach in the automotive industry due to the time and human resource required for the approach. The automotive industry is overwhelmed by time and cost constraints to meet production deadlines, therefore a novel approach is required for addressing the reliability issues of the automotive HARA process, while meeting constraints of the automotive industry.

While existing literature acknowledges the reliability issues, a solution to tackle the inter- and intra-rater variation still evades the research community. The work presented in this paper focusses on increasing reliability of the automotive HARA process by objectivising the severity and controllability ratings by introducing a rule-set for both the ratings. No rule-set was provided for exposure ratings, as according to the analysis of the authors and independent functional safety experts, the exposure ratings would have remained constant for the system and scenario under consideration. This work is one of the first steps towards achieving reliable ratings through an objective decision making process for HARA. The three research questions focussed in this paper are: How to improve the inter-rater-reliability of the automotive HARA process ((R2 and R3 aspects of reliability)? Can introduction of a rule-set for HARA improve the reliability of an automotive HARA? If yes, what does the rule-set comprise of?

In section two, the automotive HARA process is briefly discussed. Section three discusses the methodology of the study. In section four, the initial rule-set is introduced and section five discusses the validation of the rule-set. Section six provides a discussion on the approach, section seven discusses some of the future work and section eight concludes the paper.

2. Automotive HARA

2.1. ASIL

The ISO 26262 – 2011defines Automotive Safety Integrity Level or ASIL as *“one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level”*. Various ASIL levels identified by ISO 26262-2011 are QM, ASIL A, ASIL B, ASIL C, and ASIL D, where QM (quality management) denotes that lowest integrity level with no requirements to comply with ISO 26262 and ASIL D applies the most stringent requirements on product development cycle to comply with ISO 26262. The difference in requirements is also evident in Table 2. Based on the severity, exposure and the controllability rating, an ASIL rating is determined using the ASIL determination table specified in the ISO 26262 – 2011 Part 3 (ISO, 2011a) (Table 1), which shows the relation between them. The ISO 26262 standard provides ASIL dependent requirements for the development process of safety functions involving hardware and software components. The level of rigour required for higher ASIL values is considerably high as compared to a lower ASIL value. Therefore, the automotive industry is always driven towards lower ASIL values in order to keep their development costs down. This inherent bias can also sometimes lead to an inconsistency in the ASIL ratings.

Table 1: ASIL determination table (adapted from ISO 26262 – 2011: Part 3 (ISO, 2011a))

Severity Class	**Exposure class**	**Controllability class**		
		C1	**C2**	**C3**
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

The difference in the requirements for development processes to be followed for various ASIL levels is mentioned in the standard via many tables. Table 2 illustrates the increased rigour required in the methods for software unit testing as the ASIL level increases. For an ASIL C and ASIL D system, back-to-back comparison test between model and code is highly recommended as per the standard which adds considerable cost to the product development cycle.

Table 2: Methods for the verification of the requirements (adapted from ISO 26262 – 2011: Part 6 (ISO, 2011b)*)*

	Method	**ASIL A**	**ASIL B**	**ASIL C**	**ASIL D**
1a	Requirements-based test	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test	+	+	+	++
1d	Resource usage test	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable	+	+	++	++
++ : highly recommended; + : recommended; o : no recommendation for or against					

2.2. Severity

The ISO 26262 – 2011defines "severity" as *"estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation"*, for the driver or the passengers of the vehicle or other vulnerable road users like cyclists, pedestrians in the vicinity of the vehicle. The standard refers to the Abbreviated Injury Scale (AIS) (Baker et al., 1974) as one of the methods for calculating the severity rating. The standard defines four classes for severity: 1) S0 (no injuries) 2) S1 (Light and moderate injuries) 3) S2 (Sever and life threatening injuries) 4) S3 (life-threatening injuries, fatal injuries).

2.3. Exposure

The ISO 26262 – 2011defines "exposure" as *"state of being in an operational situation that can be hazardous if coincident with the failure"*. The standard defines five classes for exposure: 1) E0 incredible 2) E1 (very low probability: Occurs less often than once a year for the great majority of drivers) 3) E2 (low probability: Occurs a few times a year for the great majority of drivers) 4) E3 (medium probability: Occurs once a month or more often for an average driver) 5) E4 (high probability: occurs during almost every drive on average).

2.4. Controllability

The ISO 26262-2011 (ISO, 2011c) standard states that *"the evaluation of the controllability is an estimate of the probability that the driver or other persons potentially at risk are able to gain sufficient control of the hazardous event, such that they are able to avoid the specific harm"*.

While the standard classifies controllability into four classes: 1) C0 (Controllable in general) 2) C1 (simply controllable: 99 % or more of all drivers or other traffic participants are usually able to avoid harm) 3) C2 (normally controllable: 90 % or more of all drivers or other traffic participants are usually able to avoid harm) 4) C3 (difficult to control or uncontrollable: less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm), it fails to elaborate on the criteria for the classification and defining the levels in a more objective manner. This introduces a degree of vagueness and subjectivity to the classification. To give a rating for controllability, the experts needs to understand how a driver/operator would react to a hazard caused by a failure for any given situation to have a valid rating. As discussed in section 1, such an analysis will be based on the expert's mental model and background knowledge leading to inter-rater variation, as the assumptions and mental models may differ significantly between experts. The two distinct short-comings of the current ISO 26262-2011 standard are guided by the subjective nature of the experts' mental models leading to unreliable ratings and the ability to identify a hazard (including the black swan events). Additionally, controllability argument changes when an autonomous system is considered as the driver is no longer a fall-back option.

3. Methodology

In order to answer the research question detailed in section 1.4, the authors created a rule-set for severity and controllability ratings. To test the hypothesis that a rule-set could increase the objectivity of the HARA process and potentially lead to convergence, a workshop study involving international functional safety experts was conducted. The workshop was modelled on the World Café method (Fouche and Light, 2011).

3.1. Ethical Approval

Ethical approval for the workshop was secured from the University of Warwick's Biomedical & Scientific Research Ethics Committee (BSREC). All data gathered from the workshop was treated in a confidential manner, in accordance with the University of Warwick's Data Protection Policy[1]. Informed consent was obtained from all participants.

3.2. Participants

Twelve participants were involved in the workshop, who had experience in automotive functional safety assessments. Eight out of the 12 participants identified themselves as automotive functional safety specialists and had taken part in international ISO 26262 functional safety technical committee discussions. The remaining four participants identified themselves as development/systems engineer applying automotive functional safety principles in their function development process. Participants represented different levels of supply chain across the automotive supply chain. Two participants were from OEM (original equipment manufacturer), seven were from Tier One suppliers, two were from Tier Two suppliers and remaining one participant was from academia/research organization background. All participants were from North America and Europe.

3.3. Workshop structure

Participants were grouped into three groups of four participants each. The workshop consisted of an introduction which was followed by four rounds of 25 minutes each. Each group was provided with two different hazardous events and were asked to rate the two given hazardous events. The same hazardous events were given in each of the four rounds. Figure 1 shows the workshop structure.

In the introduction stage, participants were briefed about the system for which they were being asked to perform the HARA.

Before starting the rounds of discussion for HARA, each group (assigned a table) was asked to nominate one participant as the moderator for the group. In round one, each group was supposed to discuss and come to a consensus for each of the two hazardous events, on a rating for Severity (S), Exposure (E) and Controllability (C) and subsequently for ASIL. After round one, the members of the groups were shuffled, but the moderator for each group remained same. The shuffling was done in a way that the table had at least two new participants as compared to the previous round. In round two, the new groups were asked to discuss and give a ratings for S, E and C. After round two, participants were provided with a rule-set by the authors for conducting HARA. The participants were instructed how to use the rule-set. Participants were instructed not to question the rules for their validity. However, they were given the freedom to interpret the rules as per their understanding. In round three, participants used the provided rule-set for HARA to complete the task of S, E and C ratings for the two hazardous events. The groups were same in round two and round three. After round three, the groups were again shuffled, but the moderator for the groups remained the same. In round four, the new groups were again tasked to use the rule-set for HARA (provided to them) to rate the two hazards for S, E and C. The mixing of groups after round 1 and round 3 helps address the research question of inter-rater variability (with and without the rule-set). Moderators were asked to provide a brief explanation of the discussion in each round and the reasoning behind the rating for each of the parameters (S, E and C).

This provided a possibility to perform both quantitative and qualitative analysis on the gathered data which includes the ratings in each round (quantitative) and the moderators' explanation in each round (qualitative).

At the end of four rounds, each group was asked to provide feedback on the workshop by answering two questions:

- (During the workshop) Have you experienced variation in hazard analysis discussions based on the group of people involved in the discussion?

[1] Available at: http://www2.warwick.ac.uk/services/vco/exec/registrar/legalservices/dataprotection/ accessed on 14 March 2017

- Do you think by having rules by parametrizing hazard analysis, we can have a more objective approach?

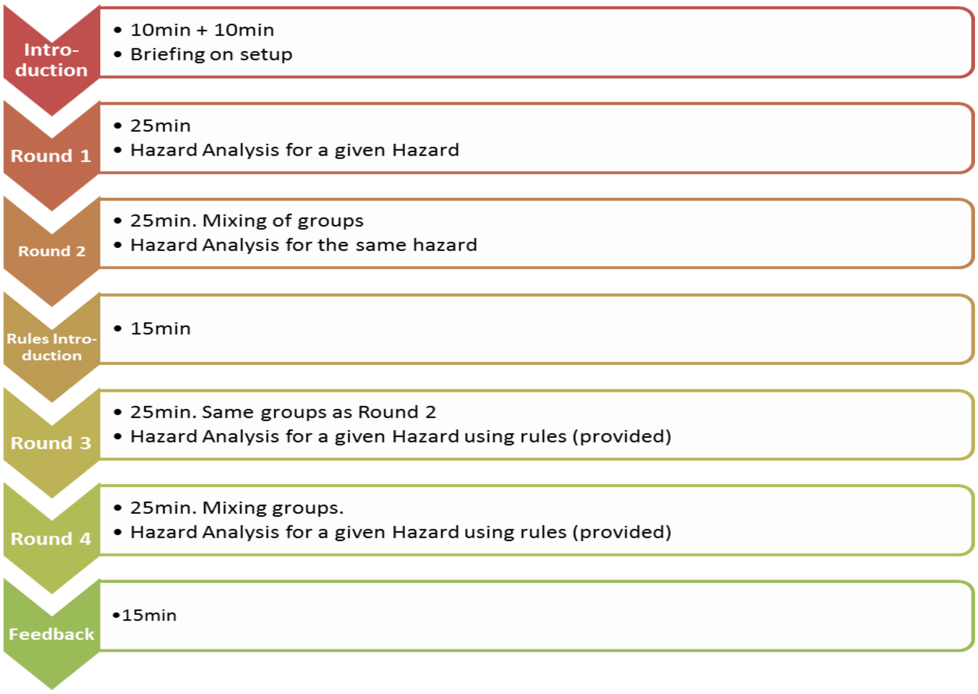

Figure 1: Workshop structure

3.3.1. System definition

Participants were asked to perform a HARA for the provided hazard and hazardous events for a Low Speed Autonomous Vehicle (LSAV). i.e. a pod. The system features presented to the participants were:

- Fully Autonomous (SAE Level 5 autonomous vehicle)
- Connected vehicle with Vehicle-to-Infrastructure (V2I) capability
- Emergency stop button. No trained safety driver
- No steering wheel or pedals
- Top speed of 25 km per hour

Participants were asked to make the assumption that the current ISO 26262-2011 Part 3, which is an automotive functional safety standard for passenger vehicles is applicable for LSAV/pod. Participants were advised to use the ASIL determination table which was provided to them during the workshop from the mentioned standard.

3.3.2. Hazard definition

The hazard provided to the participant was *"Collision (of pod) with static or dynamic obstacle due to stopping or accelerating to a vulnerable position"*. Based on the hazard, participants were provided two hazardous events and were asked to discuss the HARA for the two given events to give S, E and C ratings. The two hazardous events provided were:

- Pod travels into pedestrian / cyclist
- Pod does unintended braking

The hazard provided was identified after conducting in-depth hazard analysis for a low-speed autonomous vehicle and a qualitative analysis was carried out on the explanation for the analysis. The in-depth hazard analysis was conducted by independent functional safety experts involved in the UK Autodrive[2] project. The hazard and the hazardous events definition for the pod was a result of this HARA. Various functions like Torque management, braking and route planning could cause the given hazard. However, all functions causing the hazard were related to vehicle's movement.

4. Initial rule-set

The initial rule-set is comprised of rules for severity and controllability ratings, while no rules were generated for exposure. The authors in their analysis of the hazards with a different set of experts had come to a conclusion that the exposure rating for the given hazardous events and the given system (discussed in section 3.3.1 and section 3.3.2) will most certainly be E4 (highly probable). In order to objectify the HARA process, severity and controllability ratings' rule-set were parametrized in terms of factors identified by the authors. While various hazards and hazardous events were identified, various parameters were used to classify a hazardous event. These included acceleration value, velocity etc. The first set of parameters were identified from this set. In addition, existing literature was reviewed for factors influencing severity and controllability (Baker et al., 1974; Ellims and Monkhouse, 2012; Green, 2000; Lortie and Rizzo, 1998; Monkhouse et al., 2015; Summala, 2000; Verma and Goertz, 2010). The parametrization of the HARA components should help meet the R1, R2 and R3 reliability criteria defined by (Aven and Heide, 2009) by objectivising the decision making process involved in HARA ratings. Figure 2 depicts the process of development of the initial rule-set, along with stakeholder roles at each step. Due to logistical reasons, a condensed version of the rule-set was used in the workshop study. Feedback on the condensed version of the rule-set was received from independent functional safety experts.

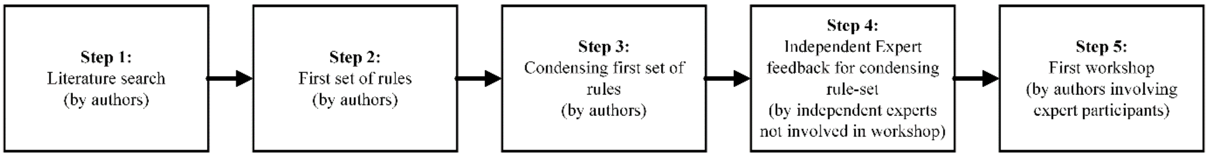

Figure 2: Process of developing initial rule-set with role description for each step

4.1. Severity rating rule-set

The severity parameters were mainly influenced by impact energy, characteristics of impact and the environment (Johansson and Nilsson, 2016a). Therefore, the parameters identified for severity rating were: 1) vehicle velocity 2) oncoming object velocity 3) type of obstacle 4) type of impact (side, head-on etc.) 5) gradient of slope 6) magnitude of delta torque (difference between required and provided torque) 7) maximum acceleration/deceleration 8) mass of vehicle. However, the severity rule-set depicted in Table 3 is a condensed version of the initial rule-set. A condensed version of the rule-set (prepared by the authors) was used due to logistical reasons of conducting the validation of the rule-set. The condensed version of the rule-set was prepared by deleting some of the secondary parameters like type of collision (head-on, side, rear), gradient of slope, country/city for which the hazard has been described for etc. These parameters were removed as their effect on severity rating hadn't been experimentally evaluated.

[2] UK Autodrive project website: http://www.ukautodrive.com/

Type of Obstacle	Vehicle Velocity	Oncoming Obj. Velocity	Severity Rating
Pedestrian	< 11 km/h	< 2 km/h	S0
		< 6 km/h	S1
		< 12km/h	S1
	11 - 16 km/h	< 2 km/h	S1
		< 6 km/h	S2
		< 12km/h	S2
	> 16 km/h	< 2 km/h	S2
		< 6 km/h	S3
		< 12km/h	S3

Type of Obstacle	Vehicle Velocity	Oncoming Obj. Velocity	Severity Rating
Infrastructure	< 11 km/h	0 km/h	S0
		0 km/h	
		0 km/h	
	11 - 16 km/h	0 km/h	S1
		0 km/h	
		0 km/h	
	> 16 km/h	0 km/h	S2
		0 km/h	
		0 km/h	

Type of Obstacle	Vehicle Velocity	Oncoming Obj. Velocity	Severity Rating
Vehicle	< 11 km/h	< 10 km/h	S0
		< 20km/h	S1
		> 20 km/h	S2
	11 - 16 km/h	< 10 km/h	S1
		< 20km/h	S1
		> 20 km/h	S2
	> 16 km/h	< 10 km/h	S1
		< 20km/h	S2
		> 20 km/h	S3

Type of Obstacle	Vehicle Velocity	Oncoming Obj. Velocity	Severity Rating
Cyclist	< 11 km/h	< 8 km/h	S0
		< 14km/h	S1
		< 20km/h	S2
	11 - 16 km/h	< 8 km/h	S1
		< 14km/h	S2
		< 20km/h	S2
	> 16 km/h	< 8 km/h	S2
		< 14km/h	S2
		< 20km/h	S3

Table 3: Severity rule-set

4.2. Controllability rating rule-set

The controllability parameters were mainly influenced by the vehicle's ability to change trajectory and the environment affecting vehicle's ability to make this change (McGehee et al., 2000; Rosén et al., 2011; Schaap et al., 2008; Young and Stanton, 2007). The parameters identified for controllability were: 1) vehicle velocity 2) time-to-collision (TTC) 3) distance to obstacle 3) maximum acceleration/deceleration 4) availability of safe area 5) road friction 6) gradient of slope. Time-to-collision (TTC) is defined as *"the time taken by the trailing vehicle to crash into the front vehicle, if the vehicles continue in the same path without adjusting their speeds"* (Chin and Quek, 1997). Similar to the severity rule-set, a condensed version of the controllability rule-set was used due to logistical reasons and is depicted in Table 4. The condensed version was prepared on the similar basis as the severity rule-set.

Emergency Deceleration Value	Distance to Obstacle	TTC	Vehicle velocity	Controllability Rating
0.4g - 0.8g	< 6 m	< 1.0 sec	< 11 km/h	C2
			11 - 16 km/h	C1
			> 16 km/h	C3
		1.0 - 2.0 sec	< 11 km/h	C1
			11 - 16 km/h	C1
			> 16 km/h	C2
		> 2.0 sec	< 11 km/h	C1
			11 - 16 km/h	C0
			> 16 km/h	C2
	> 6 m	< 1.0 sec	< 11 km/h	C2
			11 - 16 km/h	C1
			> 16 km/h	C2
		1.0 - 2.0 sec	< 11 km/h	C0
			11 - 16 km/h	C0
			> 16 km/h	C2
		> 2.0 sec	< 11 km/h	C1
			11 - 16 km/h	C0
			> 16 km/h	C1

Emergency Deceleration Value	Distance to Obstacle	TTC	Vehicle velocity	Controllability Rating
< 0.4g	< 6 m	< 1.0 sec	< 11 km/h	C3
			11 - 16 km/h	C2
			> 16 km/h	C3
		1.0 - 2.0 sec	< 11 km/h	C2
			11 - 16 km/h	C2
			> 16 km/h	C3
		> 2.0 sec	< 11 km/h	C2
			11 - 16 km/h	C1
			> 16 km/h	C3
	> 6 m	< 1.0 sec	< 11 km/h	C3
			11 - 16 km/h	C2
			> 16 km/h	C3
		1.0 - 2.0 sec	< 11 km/h	C1
			11 - 16 km/h	C1
			> 16 km/h	C3
		> 2.0 sec	< 11 km/h	C2
			11 - 16 km/h	C1
			> 16 km/h	C2

Table 4: Controllability rule-set

5. Results

5.1. Quantitative Results:

Each group was asked to provide a rating for Severity, Exposure and Controllability for the two hazardous events for each round of their discussion.

Figure 3 shows the ASIL ratings provided by the individual groups in different rounds. Different rounds have been plotted on the x-axis and the ASIL ratings have been plotted on the y-axis. Rules for HARA were provided only in round 3 and round 4. In the first round, (when no rules were provided to the participants), each group came up with a different ASIL rating with significant differences. The difference between the groups were of the order of two for group 1 and group 3 (ASIL A and ASIL C for first hazardous event) and group 2 and group 3 (QM and ASIL B for second hazardous event). The difference with the other group was of the order of one. Round two proved to have some convergence in the ratings, however there were still significant differences in the ASIL ratings. For hazardous event 1, two groups converged to an ASIL rating of ASIL C, while the third group differed significantly with an ASIL rating of QM which means the difference was of the order three. For hazardous event 2, while two of the groups converged at an ASIL A rating, the third group gave a QM rating which meant a difference of the order of 1. It is interesting to observe that the group giving QM rating to hazard 1 and hazard 2 were different.

The signification variation in the ASIL ratings provided by the groups in round 1 and round 2, illustrates the low reliability (inter-rater) of the current automotive hazard analysis method, even when done by experts in the industry. While every group was provided with the same hazardous events to rate, each of them had a different justification for the ASIL rating provided by them. The difference demonstrates the inter-rater variability in automotive HARA due to presence of subjectivity which is caused by the experts' mental models. This makes the HARA process unreliable as per the R2 and R3 criteria of reliability mentioned by (Aven and Heide, 2009). The variation in the HARA ratings will be discussed in more detail in the qualitative analysis section (section 5.2).

Before round 3, rules for HARA were introduced to the participants and they were asked to use the rules to perform the HARA. It was expected that the introduction of the rule-set would introduce objectivity in the HARA process and potentially lead to a convergence in the ASIL ratings from the

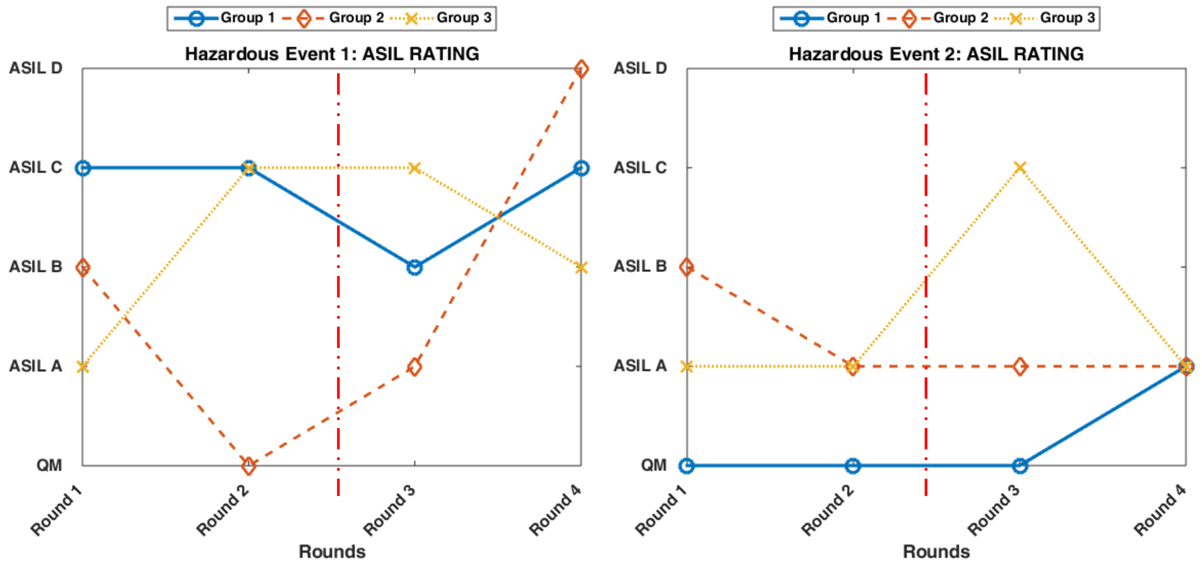

Figure 3: ASIL ratings for hazard 1 and hazard 2 given by experts in different rounds (as per Figure 1)
Round 1 and Round 2: without rule-set; Round 3 and Round 4: with rule-set

three groups of experts. However, the results (as depicted in Figure 3), illustrate the opposite. In round 3, for both hazardous event 1 and hazardous event 2, the three groups provided three different ASIL ratings with a maximum difference of order two and the minimum difference of order one. This was contrary to the expectation of the authors. However, the qualitative analysis of the round 3 results (section 5.2) provide a deeper insight on the cause of the variation. Round 4 provided an interesting set of results for hazardous event 1 and hazardous event 2, with convergence in ratings achieved for hazardous event 2.

The ASIL ratings for hazardous event 1 between rounds 1-2 and rounds 3-4, show a visual decrease in variation (Figure 3), indicating shift towards convergence, potentially due to the introduction of rule-set. In an ideal situation, for a fully reliable HARA, the variation in ratings should be zero. While ASIL ratings for hazardous event 1 provided by different groups varied significantly (with a maximum variation of order 2 and a minimum variation of order 1), ASIL ratings for hazardous event 2 converged for all groups at ASIL A. At a higher level, it might seem that the convergence of the ASIL rating for hazardous event 2 is a result of the introduction of the rule-set by the authors. But a more granular analysis of the components of ASIL provides a different view. As discussed in section 2, an ASIL rating is comprised of a severity rating (S), exposure rating (E) and a controllability rating (C). The authors will now discuss the S, E and C ratings provided by the different groups in different rounds. Figure 4-6 depict the severity, exposure and the controllability ratings respectively for hazard 1 and hazard 2.

Severity: In round 1, while two groups agreed on the severity rating, the third group provided a rating with a difference of order two for hazardous event 1 (Figure 4). In round two, all the groups converged in their severity rating at S3 for hazardous event 1. With the introduction of rules in round 3, while two of the groups converged in their severity rating at S2 (which was different from their round 2 ratings), the third group gave a rating (S3) which differed in the rating of the other two groups by the order of one. In round 4, after the groups were mixed, a similar spread was found with two groups agreeing in their severity rating at S2, while the third group gave a rating of S3. The group giving a diverging rating to the others was different in round 3 and round 4. For hazardous event 2, two groups converged completely across all the rounds. However, the third group showed significant variation across the rounds. In round 1, the severity rating of the third group was in agreement with

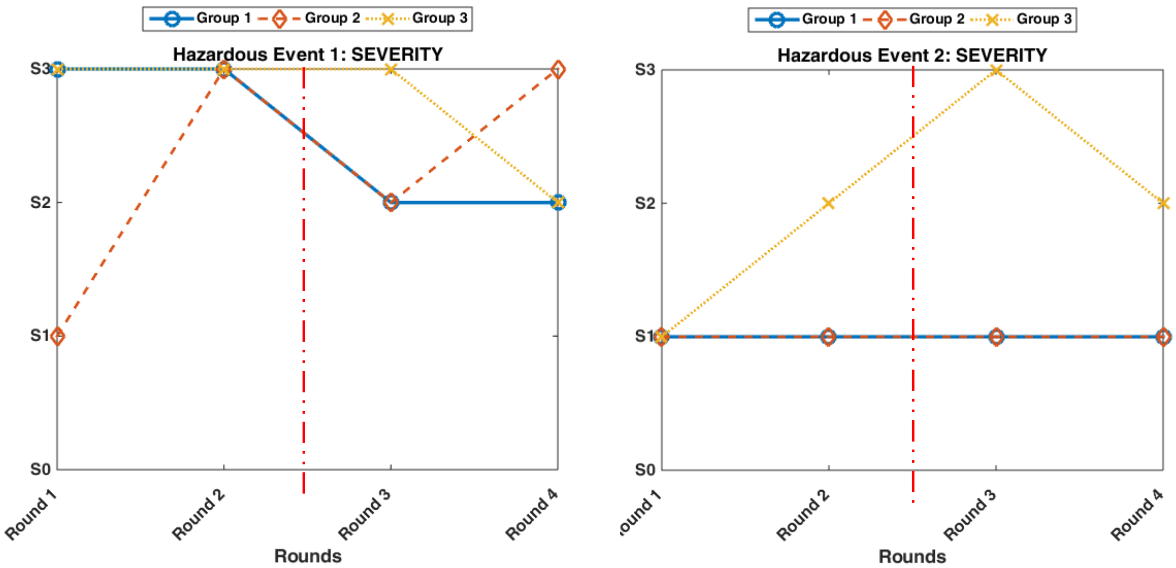

Figure 4: Severity ratings for hazard 1 and hazard 2 given by experts (in different rounds (as per Figure 1) Round 1 and Round 2: without rule-set; Round 3 and Round 4: with rule-set

the other groups at S1. However, in round 2, the group gave a rating of S2. With introduction of rules, the group gave a severity rating of S3 and S2 in round 3 and round 4 respectively.

Exposure: In the workshop experiment, the authors didn't provide rules for exposure rating. While this was due to the authors' understanding of exposure rating being almost certainly being constant, the experiment was also designed to see if there was any intra-rater variability, i.e., variation in the same group of people with experience. In case any intra-rater variance was present, this would be seen in the ratings of round 2 and round 3, as the groups in the two rounds were identical. While there was no evidence of intra-rater variability in the exposure ratings, a significant degree of inter-rater variability existed among the different groups across various rounds (Figure 5). Contrary to the authors' hypothesis, the variation of exposure ratings was high, as compared the severity and the controllability ratings for hazardous event 1. While the same was true for rounds 1-2 for hazardous event 2, rounds 3-4 for hazardous event 2 showed the least variation for exposure rating.

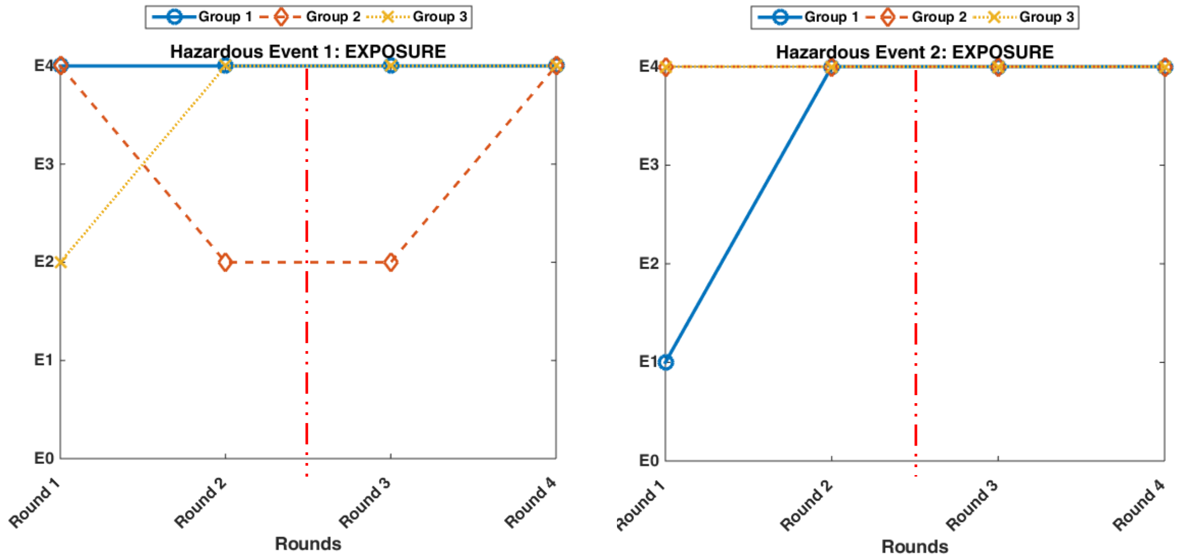

Figure 5: Exposure ratings for hazard 1 and hazard 2 given by experts in different rounds (as per Figure 1). Round 1 and Round 2: without rule-set; Round 3 and Round 4: with rule-set

Controllability: Controllability ratings for hazardous event 1 showed a similar variation as that of the severity ratings. However, the variation for controllability ratings rose for both the hazardous events, with the introduction of the rules. This could potentially be due to the interpretation of the rules provided to the participants.

Ideally, the introduction of the rule-set for HARA should have led to zero variation in the severity, exposure, controllability and ASIL ratings. While the reduction was observed in some of the ratings (Figure 6), it is important to analyse the results qualitatively (section 5.2) to explain the deviation.

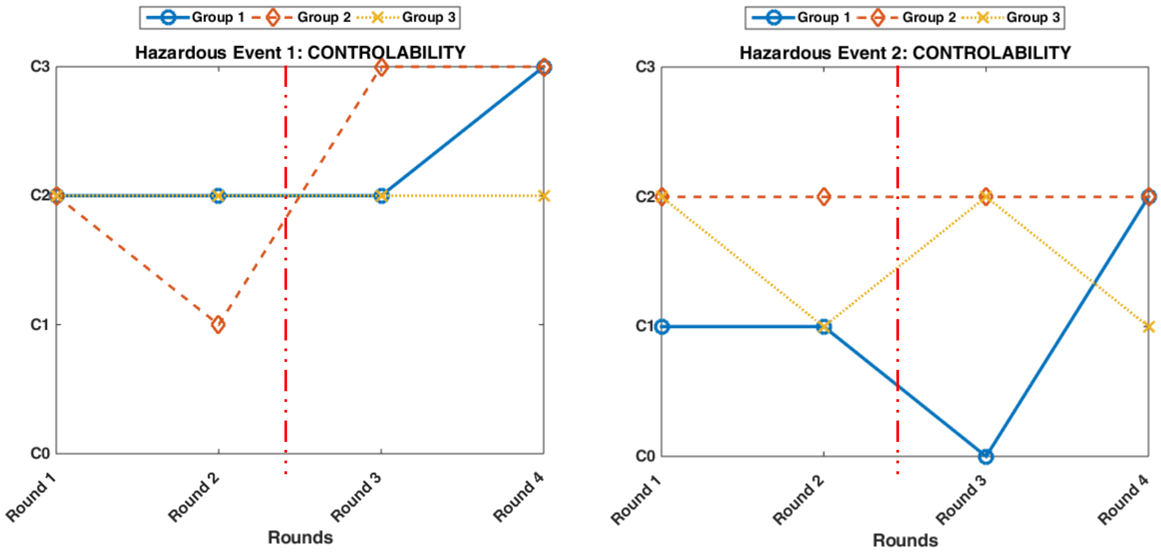

Figure 6: Controllability ratings for hazard 1 and hazard 2 given by experts in different rounds (as per Figure 1). Round 1 and Round 2: without rule-set; Round 3 and Round 4: with rule-set

5.2. Qualitative Results:

Each of the three groups were asked to provide answers to the questions mentioned in section 3.3 about their experience of HARA in the different rounds of the workshop. While answering the first question about experiencing variation in hazard analysis discussions, all three groups mentioned that they had experienced variation in HARA discussions in different rounds. All three groups concurred that the source of variation was the different perspectives presented by different individuals present in the group. However, the reasons for varying perspectives differed between the groups. One of the groups mentioned that the HARA is dependent on person's experience and their previous training/understanding of the rating procedure in HARA. This coincides with the literature discussed earlier (in section 1) about the background knowledge of the experts being one of the reasons for subjectivity (Aven and Zio, 2014). Another group mentioned that experts from different cultures, perceived "severity" and "exposure" ratings differently and there is a need to provide context regarding the environment for which the product is being made. Although, limited literature exists to support the cultural factor as a source of subjectivity in HARA, recent studies in other domains like occupational health and safety (OHS) have indicated this trend also (Aven and Zio, 2014; Tchiehe and Gauthier, 2017). Having participants from North America and different European countries was beneficial in observing this trend in the study presented in this paper.

Two out of the three groups agreed in their response to the second question on saying that the introduction of rules by parametrizing HARA made the process more objective. While the third group disagreed with the statement, but qualified their response by mentioning that the rules, the parameters and their relationship were open to subjective interpretation. The other two groups mentioned that the rules needed to be re-calibrated in certain areas (like introducing context for the rules) and more examples and instructions need to be provided before using the rules. This is further established by the fact that each of the groups in round three and four (while using the rules for HARA) made different initial assumptions about the system and the hazard due to which they came to a different severity and controllability rating. This emphasizes the importance of the initial assumptions made by the experts performing the HARA and was also highlighted by one of the groups in their feedback. Providing context to the rule-set could potentially help to remove the subjective nature of the initial assumptions and will be introduced in future workshop studies.

6. Discussion

Due to logistical reasons of conducting a workshop, a condensed rule-set (mentioned in section 4) was provided to the participants. As participants were experts, they made subjective interpretation on aspects of the rules that were not presented to them during the workshop (e.g. type of collision). This introduced an element of subjectivity. This was confirmed with the qualitative analysis of the feedback provided by the three groups. However, this scenario was not foreseen by the authors initially, and has now been taken into consideration in the formation of the re-calibrated rule-set. Another aspect highlighted in the qualitative analysis of the feedback was on the need for a few example cases and training to use the provided rule-set. This would potentially aid the experts' understanding on how to use the rule-set provided for performing HARA. In order to overcome the challenge due to unclear understanding of the process, based on the feedback from this study, the authors plan to extend the rule-set introduction time during future workshop/focus groups and also incorporate a few example cases.

An objective approach to the decision making process involved in an automotive HARA has many potential benefits. Not only does it have the potential to increase the inter-rater reliability of the process, it provides the ability to automate the HARA process which in turn can save precious time in the automotive product life-cycle. Moreover, it can potentially provide a degree of consistency across the automotive supply chain (i.e., OEMs, Tier 1 suppliers, Tier 2 suppliers etc.). While some of the results suggest positive results towards increased reliability through convergence of HARA ratings, it is not known that convergence would ever occur but this work has shown that introduction of an objective rule-set has a potential to increase the reliability of HARA ratings.

Since, contrary to the authors' hypothesis, it was found that the exposure ratings were also subject to high degree of variation, an additional rule-set for exposure ratings will also be introduced in future workshops. It is believed that an exposure rule-set along with the context definition should potentially be able to bring convergence in the exposure ratings and hence ASIL ratings too.

One of the potential future benefits of having an objective rule-set is that it paves the way for dynamic HARA. With the introduction of automated systems, a concept of dynamic HARA has been introduced recently to enable the automated system to determine its ASIL rating based on the situational health of the sensors and the automated system and the environmental conditions (Johansson and Nilsson, 2016a; Villa et al., 2016). The approach presented in this paper constitutes one of the blocks of a dynamic HARA and may aid in a reliable hazardous event rating in the dynamic HARA process (Johansson and Nilsson, 2016b). Additionally, it can potentially allow relatively unskilled practitioners with less experience, to perform HARA to a reliable degree as the need for highly specialized knowledge is reduced to a great extent. This could ease the process in terms of time and resources required for the HARA.

The hazard and the hazardous events chosen for the workshop study were a small part of a larger collection of hazards and hazardous events. The full collection was created as a result of a safety analysis of the low-speed autonomous vehicle. While the independent group of experts who performed the safety analysis had full information about the system and the hazards, the expert participants in the workshop study had limited information about given hazard. In some of the qualitative feedback, participants mentioned the need for more information. However, the authors also noticed from the discussion notes of the expert panels that they found it hard to implement the classification method. In order to mitigate such instances, the authors will provide a new set of hazard and hazardous events with more information about the situation and context in future workshops.

7. Future work

Having discussed the potential benefits of the proposed method, there are a few challenges of the proposed objective HARA approach also. Hazard identification and HARA are two aspects of the safety analysis. While the former requires creativity to identify possible hazards, a more structured framework for HARA provides more guidance to experts, potentially eliminating subjective interpretation. However, it is imperative that the rules created are exhaustive and valid, to ensure the validity of the ratings. While this work didn't explicitly focus on validity of the rule-set or HARA ratings, future work includes establishing the validity of the rule-set. Some efforts were made to have a valid initial rule-set and these have been discussed in section 4. Multiple iterations of using the re-calibrated rule-set in future focus groups and workshop studies would ensure the validity of the rule-set as the experts will be asked for their feedback on the both the validity of the rules and the objective HARA process. Feedback received at the end of each iteration will be used to re-calibrate the rules till full convergence in ratings is achieved.

Results of upcoming focus-groups/workshop experiments will be published in future manuscripts. The aim of the future workshops will be to extend and re-calibrate the rule-set to get full convergence in HARA ratings between different groups of experts when the rule-set is used.

Additionally, future implementation of the dynamic HARA work completed, will also involve extending the parameters for objectification to include driver-related parameters, e.g. age of the driver, level of training, level of attention, etc. Another interesting area of research is the application of the proposed approach in other domains like process, aviation etc. to improve the reliability of the risk analysis process.

8. Conclusions

The authors have presented a novel approach by creating a rule-set for conducting automotive HARA which has a potential to mitigate any inter-rater variations caused by subjective nature of the functional safety experts' mental models and background knowledge. The proposed objective approach to HARA involves parametrization of the various automotive HARA parameters, i.e., Severity and Controllability. In this paper, rule-sets of severity and controllability ratings have been presented.

The low reliability, i.e. intra-rater variation, of the current automotive HARA process has been demonstrated through experimental evidence. A significant difference of the order of two was observed among the different groups for ASIL, severity and controllability ratings. The main focus of the presented approach was on, the inter-rater reliability. The ASIL ratings for hazardous event 2 converged to ASIL A in the last round with the rule-set. Based on the feedback from participants and the qualitative analysis of the initial rule-set, the rules were re-calibrated. One of the themes that was observed in the qualitative analysis of the feedback was the need to put in a context to the hazard in the HARA. The perception of severity, exposure and controllability varies in different context. Additionally, the experts mentioned the need for parameters like type of collision (side, front, rear) to be added to the rule-set as they had made an assumption due to the lack of the parameter in the rule-set.

While introduction of the rule-set has shown signs of improved reliability of HARA ratings, further work is needed to use the re-calibrated rule-set and this will be conducted with future workshops and focus group studies involving large number of functional safety experts in the coming months. More iterations of the rule-set may occur based on the feedback and results from the future workshop studies.

Acknowledgements

This work has been carried out under the EPSRC (Grant EP/K011618/1). The authors would like to thank WMG, University of Warwick, UK and the WMG centre HVM Catapult, for providing the necessary infrastructure for carrying out this study. WMG hosts one of the seven centres that together comprise the High Value Manufacturing Catapult in the UK. The authors would also like to thank two anonymous reviewers for their detailed comments on a previous draft of the paper, which has helped considerably to improve the paper.

References

Abimbola, M., Khan, F., Khakzad, N., 2016. Risk-based safety analysis of well integrity operations. Saf. Sci. 84, 149–160. doi:10.1016/j.ssci.2015.12.009
Aven, T., 2015. Implications of black swans to the foundations and practice of risk assessment and management. Reliab. Eng. Syst. Saf. 134, 83–91. doi:10.1016/j.ress.2014.10.004
Aven, T., 2013. On the meaning of a black swan in a risk context. Saf. Sci. 57, 44–51. doi:10.1016/j.ssci.2013.01.016
Aven, T., 2010a. On how to define, understand and describe risk. Reliab. Eng. Syst. Saf. 95, 623–631. doi:10.1016/j.ress.2010.01.011
Aven, T., 2010b. On the need for restricting the probabilistic analysis in risk assessments to variability. Risk Anal. 30, 354–360. doi:10.1111/j.1539-6924.2009.01314.x
Aven, T., Heide, B., 2009. Reliability and validity of risk analysis. Reliab. Eng. Syst. Saf. 94, 1862–1868. doi:10.1016/j.ress.2009.06.003
Aven, T., Reniers, G., 2013. How to define and interpret a probability in a risk and safety setting. Saf. Sci. 51, 223–231. doi:10.1016/j.ssci.2012.06.005
Aven, T., Zio, E., 2014. Foundational Issues in Risk Assessment and Risk Management. Risk Anal. 34, 1164–1172. doi:10.1111/risa.12132
Baker, S.P., O'Neill, B., Haddon, W., Long, W.B., 1974. The Injury Severity Score: A method for describing patients with multiple injuries and evaluating emergency care. J. Trauma 14.
Baysari, M.T., Caponecchia, C., McIntosh, A.S., Wilson, J.R., 2009. Classification of errors contributing to rail incidents and accidents: A comparison of two human error identification techniques. Saf. Sci. 47, 948–957. doi:10.1016/j.ssci.2008.09.012
Bishop, R., 2000. A Survey of Intelligent Vehicle Applications Worldwide, in: Proc. of the IEEE Intelligent Vehicles Symposium 2000. Dearborn, Michigan, USA.
Björnsson, I., 2017. Holistic approach for treatment of accidental hazards during conceptual design of bridges - A case study in Sweden. Saf. Sci. 91, 168–180. doi:10.1016/j.ssci.2016.08.009
Cagno, E., Caron, F., Mancini, M., 1960. Multilevel Hazop for Risk Analysis in Plant Commissioning 77, 309–323.
Cambridge English Dictionary [WWW Document], 2017. URL http://dictionary.cambridge.org/dictionary/english/ (accessed 3.3.17).
Carbaugh, J., Godbole, D.N., Sengupta, R., 1998. Safety and capacity analysis of automated and manual highway systems. Transp. Res. Part C Emerg. Technol. 6, 69–99. doi:10.1016/S0968-090X(98)00009-6
Carmines, E.G., Zeller, R.A., 1979. Reliability and Validity Assessment. Beverly Hills ; London : Sage Publications.
Chen, S.T., Wall, A., Davies, P., Yang, Z., Wang, J., Chou, Y.H., 2013. A Human and Organisational Factors (HOFs) analysis method for marine casualties using HFACS-Maritime Accidents (HFACS-MA). Saf. Sci. 60, 105–114. doi:10.1016/j.ssci.2013.06.009
Chin, H., Quek, S., 1997. Measurement of Traffic Conflicts. Saf. Sci. 26, 169–185.
Ellims, M., Monkhouse, H.E., 2012. AGONISING OVER ASILS : Controllability and the In-Wheel Motor, in: Proc. of the 7th IET International Conference on System Safety, Incorporating the Cyber Security Conference 2012. doi:10.1049/cp.2012.1524
Ergai, A., Cohen, T., Sharp, J., Wiegmann, D., Gramopadhye, A., Shappell, S., 2016. Assessment of the Human Factors Analysis and Classification System (HFACS): Intra-rater and inter-rater reliability. Saf. Sci. 82, 393–398. doi:10.1016/j.ssci.2015.09.028
Flage, R., Aven, T., 2015. Emerging risk – Conceptual definition and a relation to black swan type of events. Reliab. Eng. Syst. Saf. 144, 61–67. doi:10.1016/j.ress.2015.07.008
Fleming, C.H., Spencer, M., Thomas, J., Leveson, N., Wilkinson, C., 2013. Safety assurance in NextGen and complex transportation systems. Saf. Sci. 55, 173–187. doi:10.1016/j.ssci.2012.12.005
Fouche, C., Light, G., 2011. An Invitation to Dialogue: "The World Cafe" In Social Work Research. Qual. Soc. Work 10, 28–48. doi:10.1177/1473325010376016
Goerlandt, F., Khakzad, N., Reniers, G., 2016. Validity and validation of safety-related quantitative risk analysis: A review. Saf. Sci. doi:10.1016/j.ssci.2016.08.023
Goerlandt, F., Montewka, J., 2015. A framework for risk analysis of maritime transportation systems: A case study for oil spill from tankers in a ship-ship collision. Saf. Sci. 76, 42–66. doi:10.1016/j.ssci.2015.02.009
Goerlandt, F., Reniers, G., 2016. On the assessment of uncertainty in risk diagrams. Saf. Sci. 84, 67–77. doi:10.1016/j.ssci.2015.12.001
Green, M., 2000. "How Long Does It Take to Stop?" Methodological Analysis of Driver Perception-Brake Times. Transp. Hum. Factors 2, 195–216. doi:10.1207/STHF0203_1
Hansson, S.O., Aven, T., 2014. Is Risk Analysis Scientific? Risk Anal. 34, 1173–1183. doi:10.1111/risa.12230
Hoffman, R.R., Lintern, G., Eitelman, S., 2004. The Janus Principle. IEEE Intell. Syst. 19, 78–80. doi:10.1109/MIS.2004.1274915
ISO, 2011a. Road vehicles — Functional safety (ISO 26262) Part 3 : Concept phase.
ISO, 2011b. Road vehicles — Functional safety (ISO 26262): Part 6.
ISO, 2011c. Road vehicles — Functional safety (ISO 26262).
Johansson, R., 2009. Vision Zero - Implementing a Policy for Traffic Safety. Saf. Sci. 47, 826–831. doi:10.1016/j.ssci.2008.10.023
Johansson, R., Nilsson, J., 2016a. The Need for an Environment Perception Block to Address all ASIL Levels Simultaneously, in: Proc. of the IEEE Intelligent Vehicles Symposium (IV), Gothenburg, Sweden. Gothenburg, Sweden. doi:10.1109/IVS.2016.7535354
Johansson, R., Nilsson, J., 2016b. Disarming the Trolley Problem – Why Self-driving Cars do not Need to Choose Whom to Kill, in: Proc. of the Workshop CARS 2016 - Critical Automotive Applications : Robustness & Safety. G• oteborg, Sweden.
Kelly, T.P., 2004. A Systematic Approach to Safety Case Management, in: SAE Technical Paper: 2004-01-1779. pp. 257–266. doi:10.4271/2004-01-1779
Kesting, A., Treiber, M., Schönhof, M., Helbing, D., 2008. Adaptive cruise control design for active congestion avoidance. Transp. Res. Part

C Emerg. Technol. 16, 668–683. doi:10.1016/j.trc.2007.12.004
Khakzad, N., Khan, F., Amyotte, P., 2012. Dynamic risk analysis using bow-tie approach. Reliab. Eng. Syst. Saf. 104, 36–44. doi:10.1016/j.ress.2012.04.003
Khakzad, N., Khan, F., Paltrinieri, N., 2014. On the application of near accident data to risk analysis of major accidents. Reliab. Eng. Syst. Saf. 126, 116–125. doi:10.1016/j.ress.2014.01.015
Khastgir, S., Birrell, S., Dhadyalla, G., Jennings, P., 2015. Identifying a Gap in Existing Validation Methodologies for Intelligent Automotive Systems : Introducing the 3xD Simulator, in: Proc. of the 2015 IEEE Intelligent Vehicles Symposium (IV). IEEE, Seoul, South Korea, pp. 648–653. doi:10.1109/IVS.2015.7225758
Le Coze, J.-C., 2013. New models for new times. An anti-dualist move. Saf. Sci. 59, 200–218. doi:10.1016/j.ssci.2013.05.010
Lee, W.S., Grosh, D.L., Tillman, F.A., Lie, C.H., 1985. Fault Tree Analysis, Methods, and Applications - A Review. IEEE Trans. Reliab. R-34, 194–203. doi:10.1109/TR.1985.5222114
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270. doi:10.1016/S0925-7535(03)00047-X
Leveson, N.G., 2011a. Applying systems thinking to analyze and learn from events. Saf. Sci. 49, 55–64. doi:10.1016/j.ssci.2009.12.021
Leveson, N.G., 2011b. Engineering a Safer World. The MIT Press.
Lortie, M., Rizzo, P., 1998. The classification of accident data. Saf. Sci. 31, 31–57. doi:10.1016/S0925-7535(98)00053-8
McGehee, D. V., Mazzae, E.N., Baldwin, G.H.S., 2000. Driver Reaction Time in Crash Avoidance Research: Validation of a Driving Simulator Study on a Test Track, in: Proc. of the Human Factors and Ergonomics Society Annual Meeting. doi:10.1177/154193120004402026
Monkhouse, H., Habli, I., Mcdermid, J., 2015. The Notion of Controllability in an autonmous vehicle context, in: CARS 2015 - Critical Automotive Applications: Robustness & Safety. Sep 2015. Paris, France.
Reay, K. a., Andrews, J.D., 2002. A fault tree analysis strategy using binary decision diagrams. Reliab. Eng. Syst. Saf. 78, 45–56. doi:10.1016/S0951-8320(02)00107-2
Rosén, E., Stigson, H., Sander, U., 2011. Literature review of pedestrian fatality risk as a function of car impact speed. Accid. Anal. Prev. 43, 25–33. doi:10.1016/j.aap.2010.04.003
Rosqvist, T., 2010. On the validation of risk analysis - A commentary. Reliab. Eng. Syst. Saf. 95, 1261–1265. doi:10.1016/j.ress.2010.06.002
SAE International, 2016. Surface Vehicle Recommended Practice, J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles Sep.
SAE International, 2015. SAE J2980: Considerations for ISO 26262 ASIL Hazard Classification.
Salmon, P.M., Cornelissen, M., Trotter, M.J., 2012. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. Saf. Sci. 50, 1158–1170. doi:10.1016/j.ssci.2011.11.009
Schaap, T.W., Arem, B., Horst, a R. a, 2008. Drivers' behavioural reactions to unexpected events : Influence of workload, environment and driver characteristics. TRAIL Perspect. Sel. Pap. 10th Int. TRAIL Congr. 213–231.
Shappell, S.A., Detwiler, C., Holcomb, K., Hackworth, C., Boquet, A., Wiegmann, D.A., 2007. Human error and commercial aviation accidents: an analysis using the human factors analysis and classification system. Hum. Factors 49, 227–242. doi:10.1518/001872007X312469
Singh, S., 2015. 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.
Stamatis, D.H., 2003. Failure mode and effect analysis : FMEA from theory to execution, 2nd ed. Milwaukee, Wisc. : ASQ Quality Press, 2003.
Stoop, J., Dekker, S., 2012. Are safety investigations pro-active? Saf. Sci. 50, 1422–1430. doi:10.1016/j.ssci.2011.03.004
Summala, H., 2000. Brake Reaction Times and Driver Behavior Analysis. Transp. Hum. Factors 2, 217–226. doi:10.1207/STHF0203_2
Tchiehe, D.N., Gauthier, F., 2017. Classification of risk acceptability and risk tolerability factors in occupational health and safety. Saf. Sci. 92, 138–147. doi:10.1016/j.ssci.2016.10.003
Tingvall, C., 1998. The Swedish "Vision Zero" and how parliamentary approval was obtained, in: Proc. of the Road Safety Research, Policing, Education Conference, Wellington, New Zealand. llington, New Zealand.
van Arem, B., Cornelie, J.G.V.D., Visser, R., 2005. The impact of Co-operative Adaptive Cruise Control on traffic flow characteristics. IEEE Trans. Intell. Transp. Syst. 7, 429–436.
Van Xanten, N.H.W., Pietersen, C.M., Pasman, H.J., Vrijling, H.K., Kerstens, J.G.M., 2013. Rituals in risk evaluation for land-use planning. Chem. Eng. Trans. 31, 85–90. doi:10.3303/CET1331015
Veland, H., Aven, T., 2015. Improving the risk assessments of critical operations to better reflect uncertainties and the unforeseen. Saf. Sci. 79, 206–212. doi:10.1016/j.ssci.2015.06.012
Verma, M.K., Goertz, A.R., 2010. Preliminary Evaluation of Pre-Crash Safety System Effectiveness. Injury. doi:10.4271/2010-01-1042
Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. Saf. Sci. 89, 77–93. doi:10.1016/j.ssci.2016.06.002
Wiegmann, D.A., Shappell, S.A., 2001. A Human Error Analysis of Commercial Aviation Accidents Using the Human Factors Analysis and Classification System (HFACS). Virginia, USA.
Wiegmann, D., Shappell, S., 2001. Applying the human factors analysis and classification system (HFACS) to the analysis of commercial aviation accident data, in: Proc. of the 11th International Symposium on Aviation Psychology. Columbus, Ohio.
Young, M.S., Stanton, N. a, 2007. Back to the future: brake reaction times for manual and automated vehicles. Ergonomics 50, 46–58. doi:10.1080/00140130600980789
Yu, H., Lin, C.-W., Kim, B., 2016. Automotive Software Certification: Current Status and Challenges. SAE Int. J. Passeng. Cars - Electron. Electr. Syst. 9, 2016-01–0050. doi:10.4271/2016-01-0050