A Novel Simulation-Based Approach for ISO 26262 Hazard Analysis and Risk Assessment

J. Sini, M. Violante
Politecnico di Torino
Torino, Italy
{jacopo.sini, massimo.violante}@polito.it

V. Dodde, R. Gnaniah, L. Pecorella
MCA Engineering
Torino, Italy
{lpecorella, vincenzo.dodde, rubin.gnaniah}
@mca-engineering.it

Abstract—**Development and verification of Advanced Driver Assistance Systems (ADAS) are challenging activities. Since ADAS have to deal with a huge number of possible operational situations happening in the real world and misbehavior can lead to high-severity hazards, it is imperative to test their behavior thoroughly. However, it is not cost-effective to reproduce all the possible operational situations in controlled environments (e.g., icy road, fog, very snowy steep road, ecc.) for testing ADAS through field test, i.e., through test vehicles, and it is unacceptable to demand the test to end-users. Moreover, discovering safety violations during field tests would lead to huge cost in terms of redesign and increased time-to-market, and it is therefore mandatory to anticipate this phase as early as possible. This can be achieved by means of an effective Hazard Analysis and Risk Assessment (HARA) as prescribed by the ISO26262, when the concept of the item, in our case the ADAS, is developed. Commonly recognized problems of this phase are repeatably and objectivity in terms of independence of its results from the involved engineers. This paper proposes an approach to perform HARA through clever use of vehicle-level simulators to test an initial specification of the ADAS behavior against simulated operational situations, considering also corner cases very difficult or too dangerous to be reproduced during field testing. As a proof-of-concept, the approach is applied to an Advanced Emergency Braking System (AEBS).**

Keywords—***Automotive; ADAS; CAD; Functional Safety; Safety; Safety critical; Hazard Analysis; Risk Assessment;***

I. INTRODUCTION

Nowadays, the importance of the functionalities provided by the electric and electronic (E/E) systems embedded in cars is growing day by day. Starting from the '90s, these items have been increasingly involved in safety-relevant operations.
Thus, guaranteeing the safety of future autonomous and current Advanced Driver Assistance Systems (ADAS) equipped vehicles is a very challenging activity [2].

To design ADAS devices, due to their intrinsic complexity, we have to know all the possible conditions in which they have to operate. Road tests are very useful for this purpose, but it is almost impossible to perform them in all the possible condition a device designed to be installed in millions of cars will find in its operating life. From this perspective, vehicle-level simulators become the only way to overcome this limitation. Moreover, simulation allows designers to verify the safety-relevant effects of the item from its specifications, without needing any hardware.

Since 2011 ISO 26262 [1] regulates how E/E automotive components that equip passenger lightweight vehicles have to be designed, validated, and produced.

This paper proposes a methodology, involving vehicle-level simulators, to aid the first phase of the ISO 26262 safety lifecycle, called Hazard Analysis and Risk Assessment (HARA). We propose to improve HARA through the aid of vehicle-level simulators. As a matter of fact, today HARA is mainly a human-made activity based on brain storming, possibly supported by processes such a functional failure mode analysis. However, these approaches greatly rely on the experience of the involved engineers and they fall short as far as repeatability and objectivity are concerned. By using vehicle-level simulators, we address to following goals. The first is to improve the reliability of the risk assessment process, thanks to the combined usage of assessment tables (current state of the art to increase HARA objectivity) and simulation results while the second is to improve the repeatability of the overall HARA process, make it less dependent by the safety engineers knowledge thanks to the vehicle-level simulator and so more objective.

II. STATE OF ART

HARA is one of the key activities required by the ISO 26262 safety lifecycle. Its main purpose is to determine an Automotive Safety Integrated Level (ASIL), representing the criticality from the safety point of view, for each of the safety goals of a given automotive item.
Main issues about the HARA regard its validity (repeatability) and reliability (objectivity) [3]. In the same article, it has been shown that different group of engineers have provided different classifications for the same safety goal and sometimes changed their minds about a previously done classification.
Other similar structured methodologies to improve the quality of HARA analysis have been proposed in [4][5].

During the HARA process, designers have to obtain:

- A list of operational situations;
- A detailed description of the item failure modes and related hazards.

978-1-7281-2490-2/19/$31.00 ©2019 IEEE

It had been shown that a good way to obtain a suitable hazard list for an item, since only the actuators can act on the environment, is to analyze the actuators possible misbehaviors [6].

The ISO26262 ASIL determination is based on the assessment of three different parameters: severity, controllability, and exposure. For what regards the severity assessment, a good set of rules is described in [3]. The same article also describes a complete HARA process of a low-speed autonomous vehicle. Tables that could be used to formally determine the severity level can be found in [7], in where it is described how to parametrize the severity by using as parameters the speed and the collision direction at the moment of the crash. Other parameters come from the Abbreviated Injury Scale [8]. For what regards the controllability, a suitable criterion can be the Time To Collision (TTC) [5]. This parameter is usually assessed by simulation of possible malfunctions on real vehicles in test circuits. For the exposure, we used the definitions provided by [1].
The simulations outcomes, in terms of vehicles relative speed and TTC, can provide objective measures of the hazards and their effects due to safety goals violations.

III. Proposed approach

From the implementation point of view, to set-up a simulation-based environment suitable for this methodology, are necessary these software components: the functional model of the ADAS item under assessment; models of the hardware components needed by the item, including sensors and actuators; a vehicle-level simulator; a software layer able to put in communication the ADAS model, the hardware models, and the vehicle simulator.
Other components needed to set-up the environment are the scenarios, reporting where the operational situations are described; a high-level functional description of the possible failures of the item under assessment; the classification rules in terms of severity and controllability for the item functionality.

IV. Experimental results

The experimental verification has been performed by adopting the usual toolchains embraced in the automotive industry for the model-based software design [10] and a commercial vehicle-level simulator [9].

To demonstrate the approach, we performed the HARA of an Advanced Emergency Braking System (AEBS). This benchmark system is composed of: the vehicle-level simulator with a set of operational situations to be simulated; the ACC/AEBS software; a classifier, able to extract from the simulation the logs of the relative speed between the vehicles at the moment of the crash and the TTC, and to label them coherently to the assessment tables and definitions from [1]. To perform the HARA, a good set of operational situations for the item have to be specified. We provided these situations as virtual scenarios, used by the simulator to produce the results. To prepare these scenarios, we used the standard tests to be performed on real vehicles by homologation authority like [12] and [13]. Another test set come from the independent European assessor EuroNCAP [11]. In all the tests, in the fault-free conditions, the benchmark AEBS is able to avoid the crash.

The results of these simulations can be expressed, for each test case, as the speed at the moment of the crash and the TTC. The simulation results show that, in all the considered cases, except one, we have or a low speed (around 20-30 km/h, considering only car-to-car crashes with both the vehicles moving in the same direction) or a TTC greater than 3.8 s, thus obtaining as worst classification ASIL B. The exception is the EuroNCAP Car-to-Car braking test, in where, with an initial speed of 50 km/h of both vehicles, the preceding car driver decelerates at 6 m/s^2. At the start of the braking, the relative distance is only 12 m. In this simulation, we obtained a relative speed at the moment of the crash of 44 km/h and a TTC of only 2.1 s, so the accident could provoke serious harms to the involved people. Moreover, the driver has a very low time to react. Anyway, it is possible to consider it an exceptional case, since it requires that the driver not comply deliberately with the required safety distance. So, as an overall classification, we can consider the safety goals of AEBS as ASIL B.

Acknowledgments

We would like to thank E. Leo from Soluzioni Ingegneria for the fruitful discussion, A. Arcidiacono for the set-up of the simulations, and M. Russo Spena for her technical support.

References

[1] ISO 26262, "Road vehicles – Functional safety" (2011)

[2] Koopman P., Wagner M., "Autonomous Vehicle Safety: An Interdisciplinary Challenge", In: IEEE Intelligent System Transportation Systems Magazine, 90-96, Spring 2017

[3] K. Siddartha, S. Birrell, G. Dhadyalla, H. Sivencrona, P. Jennings, "Towards increased reliability by identification of Hazard Analysis and Risk Assessment (HARA) of automated automotive Systems", In: Safety Science 99 166–177, 2017

[4] Jang. H.A., Kwon H.M., Hong S., Lee, M. K., "A study on Situation Analysis for ASIL Determination", In: Journal of Industrial and Intelligent Information Vol. 3 No. 2, June 2015

[5] K Beckers, D. Holling, Coté I.M., Hatebur D., "A structured hazard analysis and risk assessment method for automotive systems – A descriptive study" In: Reliabilty Engineering and System Safety (2017) pg. 185-195

[6] Johanennessen, "Actuator Based Hazard Analysis for Safety Critical Systems", In: Computer Safety, Reliability, and Security SAFECOMP 2004 Proceedings

[7] SAE J2980 "Considerations for ISO 26262 ASIL Hazard Classification", April 2018

[8] Association for the Advancement of Automotive Medicine, "Abbreviated Injury Scale", from: https://www.aaam.org/abbreviated-injury-scale-ais/

[9] IPG CarMaker, https://ipg-automotive.com/products-services/simulation-software/carmaker/, Retrieved on 08/22/2018

[10] MathWorks Simulink, https://it.mathworks.com/products/simulink.html, Retrieved on 08/22/2018

[11] European New Car Assessment Programme (EuroNCAP), "Test Protocol – AEB systems", November 2017

[12] U.S. Department of Transportation – National Highway Traffic Safety Administration, "Intellingent Cruise Control Field Operational Test (Final Report), May 1998

[13] European Commission Regulation 347/2017 Attachment 1