A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment

Microelectronics Reliability 109 (2020) 113661

Contents lists available at ScienceDirect

Microelectronics Reliability

journal homepage: www.elsevier.com/locate/microrel

A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment

Jacopo Sini*, Massimo Violante

Department of Control and Computer Engineering, Politecnico di Torino, Torino, Italy

ARTICLE INFO

Keywords:
Automotive
ADAS
Functional safety
Hazard analysis
Reliability
Risk assessment

ABSTRACT

The increasing complexity of the Advanced Driver Assistance Systems (ADAS) is making more difficult to perform the Hazard Analysis and Risk Assessment (HARA). These items require high-performance Electronic Control Units (ECU) with extensive software functionalities. To correctly operate they interact with the driver, environment and other vehicle functions through high-speed in-vehicle networks, as well as a wide range of sensors and actuators. As a result, they implement complex behaviors whose outcome in presence of faults is not trivial to identify and classify as requested by the concept phase included in the most recent functional safety standards. In this paper we present a simulation-based methodology to perform the HARA of a vehicle function by mixing the usual industrial approach, based on the designers' knowledge, with one that makes use of a vehicle-level simulator. The simulation-based approach provides an automatic and systematic method to assess the complex interaction of the item under analysis with other vehicle functions in possibly complex operational situations, thus making the prediction of hazards easier. We choose to demonstrate the approach by applying it to a well-known automotive industry case study: an Advanced Emergency Braking System (AEBS). In this way, it is possible to analyze the effects of the function provided by the item, keeping into account the simulations results and comparing them to similar situations analysis available in literature. Thanks to the obtained simulation-based results, safety engineers can formulate a more objective hypothesis, in particular during the hazard classification subphase.

1. Introduction

Electric and electronic (E/E) devices play a central role in road vehicles. They are now in charge of almost all the vehicle-level functions. This trend started in the '90s, when electronic fuel injection, electric power steering system, and anti-lock braking system become standard equipment. These functions are safety-related, hence they need to guarantee their performances also in case of failures (*fail-operational*) or, at least, to move the system into a safe state in a guaranteed way (*fail-safe*).

The ISO 26262 standard is the adaptation of the IEC 61508 to address the specific needs of E/E systems installed in road vehicles. Its first edition, published in 2011, was limited to lightweight passenger vehicles, while the second one [1], published in December 2018, considers all series production road vehicles, excluding mopeds. Autonomous and semiautonomous vehicles can be considered as a subset of the autonomous and intelligent systems (A/IS), so their testing is more challenging with respect to the usual car. On one hand, we have to test if the sensors system is able to perceive, with sufficient precision and *situational awareness*, the external world. On the other, the computation can adopt approaches that are not completely deterministic, like the neural networks adopted for computer vision applications. There is no single correct outcome from a test, but a set of slightly different results. The test is passed if the chosen behavior keeps the car into a *safe* situation. To help designers to deal with these situations, another standard, the ISO/PAS 21448 "*Safety of the intended functionality*" (SOTIF) [2], has been developed. Unlike ISO 26262, SOTIF does not cover how to avoid random or systematic incorrect behaviors, due to hardware failures, design errors, and software bugs, but those caused by non-deterministic outcomes of the system, due to sensor aging, processing stages based on artificial intelligence, when the vehicle found itself in a situation not foreseen in drafting of requirements, incorrect HMI or a user misuse that has not been forecasted.

Nowadays cars embed a various E/E items (defined in [1] as "System or combination of systems, to which ISO 26262 is applied, that implements a function or part of a function at the vehicle level") able to provide complex safety-related functionalities, like Electronic Stability Control (ESC) and lane departure warning systems that, in the last

* Corresponding author: Department of Control and Computer Engineering, C.So Duca Degli Abruzzi, 24, 10129 Torino, Italy.
E-mail addresses: jacopo.sini@polito.it (J. Sini), massimo.violante@polito.it (M. Violante).

https://doi.org/10.1016/j.microrel.2020.113661
Received 30 July 2019; Received in revised form 28 February 2020; Accepted 7 April 2020

decade, become integrated into Advanced Driver-Assistance Systems (ADAS). In the future, following the current technology improvement trends, this kind of devices will become more and more important to guarantee road safety: a more structured integration of these systems will allow car makers to sell fully autonomous cars.

Guaranteeing the safety of autonomous and semi-autonomous (ADAS equipped) vehicles is a very multidisciplinary activity, that involves safety engineering, hardware reliability, software validation, human-computer interaction, social acceptance, and a viable legal framework [3].

The key point of ISO 26262 [1] is the "safety lifecycle" concept. It "encompasses principal safety activities during the concept phase, product development and after start of production".

ADASs are composed of complex sensors and mechatronic actuators, that need to be operated by Electronic Control Units (ECUs) running large software. Validation (vehicle-level road tests [1]) of these devices is fundamental, but since such devices have to be installed in millions of vehicles, they can find a huge set of operational conditions that can be impossible to reproduce in controlled road tests, hence a vehicle-level simulators to simulate such conditions is needed. The ISO/PAS 21448 (SOTIF) [3] subdivides the operational situation the vehicle can potentially face considering if they are known/unknown or safe/unsafe. It aims to aid designers to lower as much as possible the number of situations that are unknown and unsafe, at least moving them into the known and unsafe subset. This is fundamental since after that the unsafe situations are known, it is possible to find ways to mitigate their severity or their exposure, lowering the associated risk.

This paper, that extends [4], proposes a methodology where vehicle-level simulators are used starting from the concept phase (described in part 3 of [1]), when the safety goals of the item have to be defined. This phase is crucial, since it identifies the hazards that the item may face during its operations, and it provides an assessment of the level of criticality of each hazard. More in detail, [1] states "*the hazard classification scheme comprises the determination of the Severity (S), the Exposure (E) and the Controllability (C) associated with the considered hazard of the item. For a given hazard, this* [Automotive Safety Integrated Level, (ASIL)] *classification will result in one or more combinations of S, E and C classes*". The overall development process is affected by this classification, in terms of both complexity and development time.

HARA is one of the key activities required by the ISO 26262 safety lifecycle. In our work, we propose to improve HARA through the aid of a vehicle-level simulator. As a matter of fact, HARA is today mainly a human-made activity, based on brainstorming, possibly supported by processes such as System Failure Mode and Effect Analysis (System FMEA). However, these approaches greatly rely on the experience of the involved engineers and they fall short as far as repeatability and objectivity are concerned.

In this paper we address the following goals:

- 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 simulations results;
- Increase the repeatability of the overall HARA process, since the vehicle-level simulator allow to make it less dependent by the safety engineers knowledge and so more repeatable;
- Demonstrate the approach on a well-known industrial case study, by performing the simulations with the same tests that are used for the item validation in road tests.

A benchmark case, an Advanced Emergency Braking System (AEBS), will be presented to describe the proposed methodology. We choose to apply it to a well-known case, in order to compare the results obtained with our approach with the one obtained by other groups and available in the literature.

The paper is organized as follows. Section 2 reports background materials. Section 3 describes the proposed approach. Section 4 describes the experimental setup and the results obtained considering the AEBS benchmark application. Finally, Section 5 draws some conclusions.

2. State of art

The ISO 26262 standard states that "Its [HARA] objective is to identify and categorize the potential hazards of the item and formulate safety goals related to the prevention or mitigation of these hazards in order to achieve an acceptable residual risk. For this, the item is evaluated with regard to its safety implication.

The HARA shall be conducted in three stages:

- Situation analysis and hazard identification (SA/HI)
- Hazard classification (HC);
- ASIL determination." [1]

As said before, main issues about the HARA regard its validity (repeatability) and reliability (objectivity) [5]. Structured methodologies to improve the quality of HARA analysis have been proposed in [6,7]. Even if these works propose different methodologies, they share the common goals to make this phase more repeatable and objective, by making it less dependent as possible from the knowledge background of the safety engineers involved in the process.

From the SA/HI point of view, 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 actuator-level possible misbehaviors [8], regardless of the stages that caused it. A similar way, but in this case based on the high-level item description, can be found in [9]. This theoretical result makes it possible to perform simulations when the item is defined only at the functional level.

On the other hand, from the HC point of view, all the works presented in the State of Art section make use of classification tables that, starting from the severity, controllability, and exposure levels described at a high level of abstraction in the Standard, make them fit the specific application. From this point of view, in this work we proceeded in the same way: the preparation of the classification criteria tables will be discussed in the experimental setup section.

Before starting with the description of the literature about the HARA process, it can be useful to provide a brief description of ADAS devices.

These systems are composed of:

- Sensors;
- "Data fusion" (DF) algorithm, that merges the information coming from all the sensors in a unique and coherent virtual representation of the surrounding environment;
- The "logic" algorithm that takes the opportune responses based on the virtual representation;
- Actuators, that physically actuate the responses on the physical environment.

The typical structure of an ADAS item is shown in Fig. 1.

Typical sensors are RADAR, LIDAR, IMU, Camera, and GPS. Typical actuators are the engine (positive and negative torque requests), the

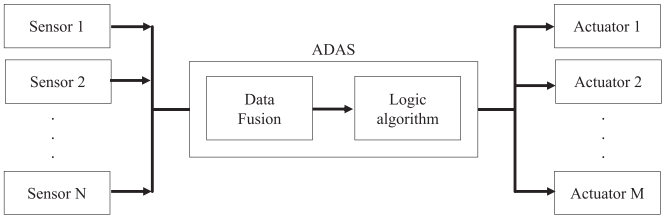

Fig. 1. Structure of an ADAS item.

power steering (angular position of the directional wheels) unit, and the brakes (braking torque). The sensors and the data fusion algorithm are in charge to guarantee the *situational awareness* for our semi-autonomous function.

During the Situation Analysis and Hazard Identification (SA/HI) stage, "*it is necessary to identify the potential unintended behavior that could lead to a hazardous event*" [1]. It is necessary to analyze all the operational situations and operating modes in which the item can trigger hazards. This analysis has to be performed for all the cases where the item is correctly used, incorrectly used in a foreseeable way by the driver, or in cases of a failure of submodules of the item. During this process, designers have to obtain:

- A list of operational situations and the related failure modes to be evaluated; the completeness of this list is fundamental to reduce the number of *unsafe* and *unknown* cases as defined by the ISO/PAS 21448 (SOTIF).
- A detailed description of the item failure modes and related hazards. Of course, since we are in the concept phase, these descriptions have to be provided at the functional level, since no implementation strategy has been developed at this stage.

Since to perform these operations it is necessary a good knowledge of the item, it is very difficult to automate this phase.

At the end of the second stage, called "Hazard Classification", all the hazard identified have to be classified by using three parameters: Severity (S), Exposure (E), and Controllability (C). In the paper [10] interested readers can find a proposal aimed to aid the development and the validation of suitable controllers, even from the early stages of product development by using co-simulation techniques.

Considering the AEBS case, for what regards the severity assessment, a good set of rules is described in [5]. This paper also describes a complete HARA process of a low-speed autonomous vehicle. The tables used to formally determine the severity level are based on the one proposed in [11], that describes how to parametrize severity by using the speed at the moment of the crash and the collision direction. Other parameters come from the Abbreviated Injury Scale [12]. A subset of these rules, adapted for our case, is reported in the experimental result section.

For what regards the controllability, a suitable criterion can be the Time To Collision (TTC) [7]. This parameter is usually assessed by simulation of possible malfunctions on real vehicles in test circuits (validation phase).

For the exposure, we used the definitions provided by [1], as described in the *experimental result* section.

Use of vehicle-level simulator is adopted in the automotive industry for software verification purposes [13]. There are various off-the-shelf tools capable to aid designers during the concept phase of the development, like IPG™ CarMaker™ (the one chosen for this paper) [14], AVL™ Vehicle Simulation (VSM™) [15], and FEV™ VirtualDynamics™ [16].

This approach can also be extended to aid also Failure Mode and Effect Analysis (FMEA) and the Failure Mode, Effect, and Diagnostic Analysis (FMEDA). From the FMEA point of view, considering the 6th phase (Optimization) of the 7 steps process described by the last manual jointly published by the AIAG&VDA in June 2019 [17], the scenarios prepared for the HARA can be used to determine, thanks to high level of abstraction models of the detection and mitigation strategies, how they are capable to provide mitigation. In a similar way, by running a spice-level simulation of the item alongside with its embedded software, it is possible to use again these scenarios to compute the random hardware failure metrics required by the part 5 of the ISO26262 standard (like as what did in [18] and, also assessing embedded software mitigation capabilities, in [19]).

We claim that thanks to the simulation results, and by adopting the methodology described in the following of this paper, it is possible to aid safety engineers to reduce the repeatability issues of the HARA demonstrated in [5], allowing to improve its objectivity.

3. Proposed approach

To describe the proposed methodology, it is useful to match it with the three stages [1] of the HARA process.

For what regards the first stage, SA/HI, the SA sub-phase can be performed by representing the various scenarios in the simulation environment. These scenarios have been prepared to describe standard tests for the class of device we have to classify. The behavior of the vehicle, considered in nominal (non-faulty) conditions in the simulated environment, helps the situation analysis.

The HI sub-phase is aided by the combined usage of vehicle-level simulator and a functional model of the item: in general, it is possible to simulate misbehaviors by changing the nominal performance of the item or disabling the safety-related function. Since we are in the concept phase, it is not possible to know the exact way the item can fail, hence the actual behavior in case of a failure (especially for what regards hardware random failures).

Thanks to the functional model of the item and the vehicle-level simulator, it is possible to assess the worst-case consequences of the failure, leading to an evaluation of its severity. At the same time, by analyzing the effect of the failure on the vehicle speed or trajectory, it is possible to assess the capability of an average human driver to mitigate the failure effects, to make achievable to determine the controllability. A similar approach has been proposed in [20], where it is described how to assess the controllability on a benchmark case of an electric steering device. The simulations results, compared with tables that provide metrics about controllability and severity in case of a crash (classification rules), are used to classify the hazard in the HC phase [1].

The ASIL classification is obtained from the combination of the three parameters S, C, and E, through the so-called *ASIL determination table*. This classification can range on five different levels, starting from QM, referred to vehicle functions that cannot impact safety, to A, B, C, and D, representing functions whose malfunction gradually causes greater damage.

How to determine the exposure as required by [1] will be discussed in the experimental verification section.

The key points of the proposed approach are:

- It bases its hazard analysis on simulation scenarios, thanks to a vehicle-level simulator;
- It allows decoupling between the knowledge of the safety engineers and the final assessment, improving the objectivity of the result;
- Since the risk assessment phase is based on the simulation results, in particular speed difference between the vehicles involved in the crash and the TTC from the start of the dangerous condition (considered in the following standard scenario as a distance between the vehicle less than the recommended safety distance), it improves the repeatability of the evaluation.

From the implementation point of view, to set-up an environment suitable for this methodology, these software components are necessary (see Fig. 2):

- The functional model of the ADAS item under assessment;
- A vehicle-level simulator;
- A software layer able to put in communication the ADAS model and the vehicle-level simulator;
- Scenarios, that are formal descriptions of the operational situations. Usually, the vehicle-level simulator embeds a tool to design the scenarios.
- A semi-formal functional description of the possible failures of the item under assessment;

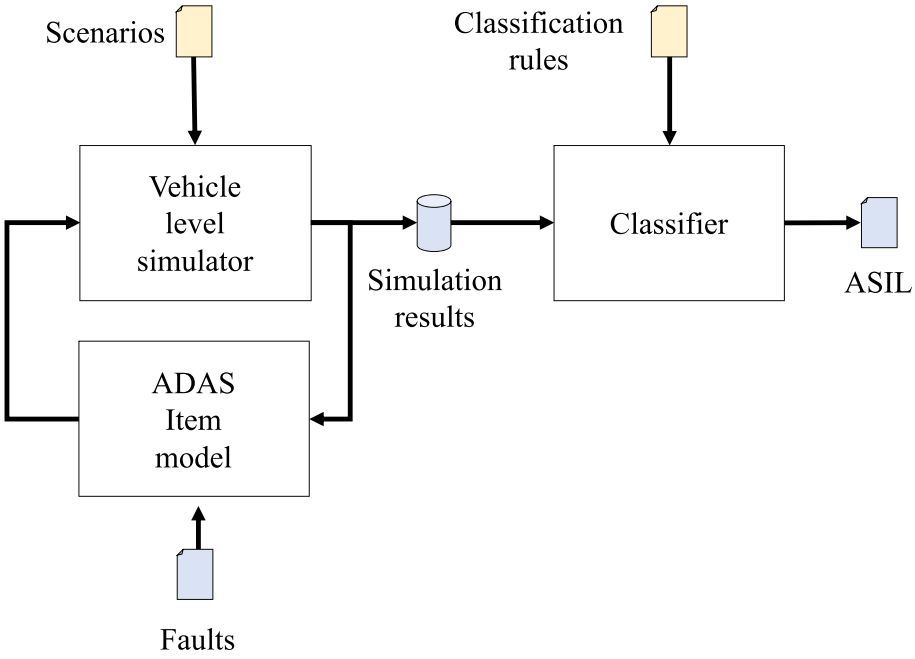

Fig. 2. The architecture of the proposed methodology.

- Classification rules in terms of severity and controllability for the item functionality.

In the considered case, the vehicle-level simulator generates the nearest object distance measurement and receive the braking force required by the ADAS item model. The driver behavior is part of the scenario file. All the physics simulation of the vehicle is in charge of the vehicle level simulator.

The actual implementation of the benchmark system is described in the experimental verification section.

4. Experimental results

4.1. Simulation environment

To demonstrate the approach, we performed the HARA of an AEBS.

AEBS bases its functionality on sensors able to measure the gap between the vehicle and the nearest object in front of it, hence detecting the risk of a collision. The simulated driver does not brake in any condition, so only the AEBS can avoid the crash. His/her behavior, in terms of speed and trajectory, is defined in the test cases.

There are different types of cruise functions: the regular cruise control a.k.a. cruise control system (CCS) can maintain a constant speed selected by the driver without requesting intervention on the gas pedal. When the driver presses the brake or the clutch pedal, the CCS is suspended, and the system does not provide torque requests. Another cruise function is an adaptive version of cruise control a.k.a. Adaptive Cruise Control System (ACCS). It is like a CCS but it is moreover able to maintain the safety distance with respect to the followed vehicle, by adapting automatically the speed set. The braking capability of the ACCS is defined in the ISO 15622 [21] and thus it does not guarantee a safety condition. CCS and ACCS are comfort functions. On the other hand, when the AEBS works in stand-alone mode, it provides the driver visual and sound warning and, if the driver does not react, it performs an emergency brake.

In this case, the misbehavior of the item has been simulated by disabling it without providing any warning to the driver. During the concept phase, this can be a good semi-formal description of the failure. Of course, during the next development phases, since we are propagating the misbehavior effect from the item level to the vehicle level, the more the misbehavior model of the item is detailed, the more the simulation results are coherent with road validation observations. This guarantee good scalability for the approach, that can aid all the item development phases.

As the first stage of the methodology (corresponding to the ISO 26262 HARA SA/HI phase), we used a combination of the simulator itself and a high-level semi-formal model of an Adaptive Cruise Control with Advanced Emergency Braking System capabilities (ACC/AEBS) to obtain some experimental data to be used in the HC stage.

For this class of items are available documents from European New Car Assessment Programme (EuroNCAP) [22], NHTSA [23], and European Commission [24], that provide descriptions of significative driving situations, i.e., operational situations.

We implemented, from the documents cited before, some virtual validation environment (scenarios) to represent significative driving conditions. Thanks to these scenarios, it is possible to perform the SA and, thanks to the fault injection on the high-level item model, to obtain data that will be useful for the HC. All the scenarios are referred to the safety goal “the AEBS brakes when there are obstacles in front of the vehicle”. The cases in where the AEBS lead to an unintended brake is not considered in the analysis. It is important to remark that the ASIL level has to be assigned to the safety goal and not to the whole item/vehicle-level function.

At the second stage, thanks to the vehicle behavior (note that, as prescribed by the ISO 26262 standard, in this phase is not possible to include failure detection or mitigation mechanisms in the simulation) obtained from the simulations, it is possible to perform the HC, evaluating the severity (maximum speed, direction of crash and kind of obstacles surrounding the vehicle) and controllability (effects of the failures on the vehicle behavior).

The benchmark system is composed of:

- The vehicle-level simulator (IPG™ CarMaker™ [14]);
- The ACC/AEBS semi-formal model (provided as a MathWorks™ Simulink™ model [25]);
- A classifier, able to extract from the simulation logs the relative speed between the vehicles at the moment of the crash and the TTC, and to apply the correct labels, in term of severity and

controllability, on the bases of the previously defined classification rules.

It is not necessary to develop a software layer able to put in communication MathWorks Simulink™ and IPG Automotive CarMaker™ since it provides suitable libraries out of the box.

In all the defined scenarios, in the fault-free conditions, the benchmark AEBS is able to avoid the crash. For all the tests, have been reported the relative speed of the vehicle at the moment of the crash and the time elapsed from the start of the hazardous condition, as described in the test, and the TTC. We are dealing with a semi-formal description of the functionality and not to a possible implementation. In this case, the fault-free condition is represented by a runnable model compliant with the requirements defined in [21].

4.2. EuroNCAP tests

The EuroNCAP AEBS test protocol [22] has been revised in 2017 and specifies two different test procedures:

- AEB City, considered in the assessment of the Adult Occupant Protection.
- AEB Inter-Urban, considered in the assessment of the Safety Assist.

There are three different scenarios:

- Car-to-Car Rear Stationary (CCRs)

The vehicle under test (VUT) is 120 m away from the target vehicle (TV). The TV is in a stationary condition. The simulation starts with the VUT in one case at 80 km/h and in the other at 50 km/h.

- Car-to-Car Moving (CCRm)

The VUT and the TV are at speed in the range from 50 to 80 km/h: the test starts at 50 km/h and, by increasing speed step of 5 km/h, it reaches 80 km/h.

In this work, the simulation is performed at only 50 km/h.

- Car-to-Car Braking (CCRb)

The VUT and the TV have the same speed equal to 50 km/h. The test is performed with all the combination of 2 and 6 m/s^2 decelerations of TV, with initial distances from the TV of 12 m and 40 m. The relative distance between the VUT and the TV cases with the 6 m/s^2 decelerations of the TV are represented in Figs. 3 and 4. The behavior is similar for all the cases presented in this paper (except, of course, for the initial distance and the collision time).

This test protocol explains also how to check if the Forward Collision Warning (FCW) system is working properly, but this functionality is not taken into consideration in this article.

The obtained results are shown in Table 1.

4.3. NHTSA tests

These tests [23] have been published in 1999 to test prototype ACC systems. Their main purpose is to characterize the entire prototype system, composed of sensors, data fusion and control algorithms, and vehicle platform.

These tests are related to the following operational situations:

- Test 1 (headway control mode): Closing-in on a preceding vehicle from a long range. VUT speed is 112.7 km/h while TV speed is 96.5 km/h.
- Test 2 (aborted passing maneuver): Responding to a close approach to a preceding vehicle. In this case, the speed of the VUT is initially 96.7 km/h. The speed of the TV remains 96.7 km/h for the whole test. When the gap between the VUT and the VT is 37.5 m, the driver manually accelerates to 112.7 km/h. At 2/3 of the original gap, the driver releases the gas pedal. The test continues until the steady-state following is reestablished.

The obtained results are shown in Table 2.

4.4. European Commission Regulation tests

These three tests come from the European Commission Regulation 347/2012 [24]. They are mandatory homologation tests for the Advanced Emergency Braking System (AEBS) in the European Union.

This regulation dates back to 2012, where standards were defined for all vehicles of category N3 and M3 (to which the level 1 of the directive have to be applied), but no international test standards had yet been established for vehicles of categories N2 and M2 equipped with hydraulic brakes and non-pneumatic rear suspensions (to which the level 2 have to be applied).

In the first test scenario, described in paragraph 2.4 of the regulation, the VUT travels against a still target, representing another car, at 80 ± 2 km/h. The test starts when the distance between the VUT and the TV is 120 m.

In the second and in the third tests, the target moves respectively at 32 ± 2 km/h (for the level 1 homologation) and 12 ± 2 km/h (for the level 2 homologation).

All the tests start when the distance between the VUT and the VT is at least 120 m.

The obtained results are shown in Table 3.

4.5. ASIL level determination

As prescribed by the ISO26262 standard, the ASIL level has to be determined by the combination of the obtained level of Severity,

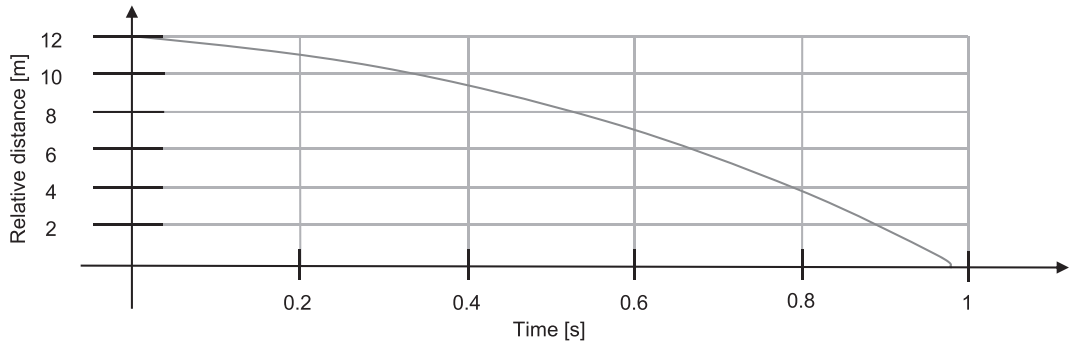

Fig. 3. Plot of the relative distance between the VUT and the TV over the time for the case CCRb (12 m, 6 m/s^2).

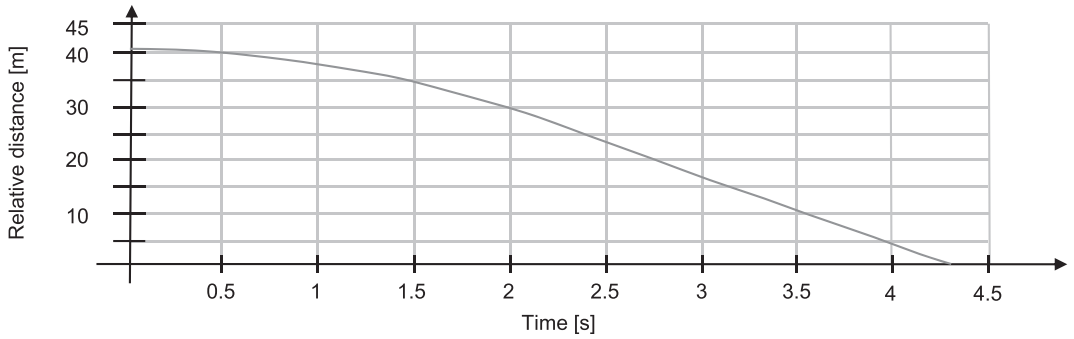

Fig. 4. Plot of the relative distance between the VUT and the TV over time the for the case CCRb (40 m, 6 m/s^2).

Table 1
Results from simulation on EuroNCAP scenarios.

Test	Relative speed [km/h]	TTC [s]
CCRs (50 km/h)	42 (S3)	8.9 (C1)
CCRs (80 km/h)	74 (S3)	5.7 (C1)
CCRb (12 m, 2 m/s^2)	22 (S1)	3.8 (C2)
CCRb (12 m, 6 m/s^2)	41 (S3)	1.0 (C3)
CCRb (40 m, 2 m/s^2)	42 (S3)	7 (C1)
CCRb (40 m, 6 m/s^2)	44 (S3)	4.3 (C1)
CCRm (50 km/h)	21 (S1)	28 (C1)

Table 2
Results from NHTSA tests.

Test	Relative speed [km/h]	TTC [s]
US Test 1	25 (S1)	33.5 (C1)
US Test 2	3.6 (S0)	10.9 (C1)

Table 3
Results from EU regulation tests.

Test	Relative speed [km/h]	TTC [s]
EU Test 1	80 (S3)	5.6 (C1)
EU Test 2	45 (S3)	9.3 (C1)
EU Test 3	68 (S3)	6.6 (C1)

Controllability and Exposure.

How to determine the ASIL level from the obtained (S, C, E) combination is specified in the *ASIL determination table* contained in part 3 of the Standard.

4.5.1. Classification rules definitions

Adapting the values from the table "*Severity Rule Set*" from [5] to our case, in which, since we are considering an AEBS, are considered only those cases involving two vehicles driving in the same direction, it is possible to obtain these association between differential speed between the two vehicles and the severity. These rules are summarized in Table 4.

From the controllability point of view, we have considered as classification parameter the Time To Collision (TTC), considering those cases in which the driver misuses the item: he/she relies on the AEBS without looking at the succeeding vehicle behavior. These rules are summarized in Table 5.

Table 4
Severity classification rules.

Severity	Relative speed [km/h]
S0	< 21
S1	≥ 21 and < 26
S2	≥ 26 and < 36
S3	≥ 36

Table 5
Controllability classification rules.

Controllability	TTC [s]
C3	< 3 (from [24])
C2	≥ 3 and < 4
C1	≥ 4

4.5.2. ASIL assignment

At this point, it is possible to summarize all the obtained results in Table 6.

At the end of this process, we can say that since in most of the cases we have obtained an ASIL B level, except for the case "EuroNCAP CCRb with 12 m of gap between VUT and TV", indicated as "CCRb (12 m, 6 m/s^2)" in Table 3, that involves a sudden slowdown of the preceding vehicle with only 12 m of safety distance. This case can be considered as a predictable misuse of the system, as the driver forces the vehicle, with a deliberate action on the gas pedal, to not respect the safety distance. A normal AEBS function will not apply any deceleration, as this item is designed only to assist the driver, it cannot overrule his/her decision. To avoid this kind of misuse, it is possible to implement some strategy by the Human Machine Interface (HMI), like a sound warning, triggered when the driver's actions are preventing the system from respecting the safety distance, in order to make he/she desist from this dangerous behavior. Due to these premises, we can assign the ASIL level B to the safety goal "the AEBS brake when there are obstacles in front of the vehicle".

The exposure assessment cannot be defined by the simulation-based approach. In general, to reduce the probability level, statistical evidence showing that the considered situation is uncommon have to be provided. For this benchmark application, since all these scenarios have

Table 6
ASIL classification of the various tests.

Test name	S	C	E	ASIL
CCRs (50 km/h)	3	1	4	B
CCRs (80 km/h)	3	1	4	B
CCRb (12 m, 2 m/s^2)	1	2	4	A
CCRb (12 m, 6 m/s^2)	3	3	4	D
CCRb (40 m, 2 m/s^2)	3	1	4	B
CCRb (40 m, 6 m/s^2)	3	1	4	B
CCRm (50 km/h)	1	1	4	QM
US Test 1	1	1	4	QM
US Test 2	0	1	4	QM
EU Test 1	3	1	4	B
EU Test 2	3	1	4	B
EU Test 3	3	1	4	B

a high probability level, we choose the maximum exposure level, so no experimental or statistical evidence is needed.

5. Conclusions

The HARA phase of the ISO 26262 safety lifecycle presents some issues about its repeatability and objectivity. A novel standard, the ISO/PAS 21448 (SOTIF), is also involved in such systems development, in order to aid designers to implement systems able to guarantee that the system has sufficient *situational awareness* in all the possible circumstances the vehicle can found itself in. In the literature, various authors tried to propose solutions to reduce these problems. A common point, shared among the proposed methodologies, is to make the process more structured and less dependent on the engineers' previous knowledge, that can affect the ASIL classification of the considered vehicle function safety goals. It had been shown [5] that different group of engineers, without these techniques, have provided different classifications for the same safety goal and sometimes changed their minds about previously done assessments. This paper proceeds in the same direction, proposing a methodology based on the use of a vehicle-level simulator. Thanks to simulations results, it is possible to obtain objective data useful to formulate hypothesis on controllability and severity in case of failures affecting the vehicle function.

To adopt this methodology are needed: scenarios in which operational situations are described; high-level functional description of the vehicle function under assessment; classification rules in terms of severity and controllability.

A case study of the methodology has been proposed, where an AEBS has been analyzed. The scenarios have been obtained from NHTSA, EuroNCAP, and European Commission documents about homologation of this kind of item. The classification rules for the severity and controllability have been adapted from the literature and are defined as thresholds on the relative speed between the vehicle under test and the target vehicle when the collision happens (for the severity), and time to collision (for the controllability). The exposure has been classified by hands. Of course, if we want to assess a novel vehicle function, these kinds of scenarios have to be defined without any external help. In any case, to demonstrate the methodology, we think that a well-known case is preferable.

By this benchmark, the methodology has been proven to be able to aid engineers to determine the ASIL level. Thanks to the data provided by the simulator and to the presence of objective classification rules, the HARA results are more objective and repeatable. As future works, authors would like to analyze a case in where also the exposure level can be assessed by a simulation-based approach and, if it will be possible, to apply it on a completely new vehicle function, proposed for instance by a company, to be able to compare the handmade results with the simulation-based ones. This can be useful to assess the reliability of the scenarios' generation process.

Declaration of competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] ISO 26262:2018, Road Vehicles – Functional Safety, (2018).
[2] ISO/PAS 21448, Road Vehicles–Safety of the Intended Funtionality, (2019).
[3] P. Koopman, M. Wagner, Autonomous vehicle safety: an interdisciplinary challenge, IEEE Intelligent System Transportation Systems Magazine, Spring 2017, pp. 90–96, , https://doi.org/10.1109/MITS.2016.2583491.
[4] J. Sini, M. Violante, V. Dodde, R. Gnaniah, L. Pecorella, A novel simulation-based approach for ISO26262 Hazard Analysis and Risk Assessments, 25th IEEE International Symposium on on-Line Testing and Robust System Design, 2019, https://doi.org/10.1109/IOLTS.2019.8854385.
[5] 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, Saf. Sci. 99 (2017) 166–177, https://doi.org/10.1016/j.ssci.2017.03.024.
[6] H.A. Jang, H.M. Kwon, S. Hong, M.K. Lee, A study on situation analysis for ASIL determination, Journal of Industrial and Intelligent Information 3 (2) (June 2015), https://doi.org/10.1016/j.ress.2016.09.004.
[7] 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.
[8] Johanennessen, "Actuator based hazard analysis for safety critical systems", In: Computer Safety, Reliability, and Security SAFECOMP 2004 Proceedings.
[9] H.A. Jang, H.M. Kwon, S.H. Hong, M.K. Lee, A study on situation analysis for ASIL determination, Journal of Industrial and Intelligent Information 3 (2) (June 2015), https://doi.org/10.12720/jiii.3.2.152-157.
[10] S. Jones, et al., Safety simulation in the concept phase: advanced co-simulation toolchain for conventional, hybrid and fully electric vehicles, in: J. Fischer-Wolfarth, G. Meyer (Eds.), Advanced Microsystems for Automotive Applications 2014. Lecture Notes in Mobility, Springer, Cham, 2014, , https://doi.org/10.1007/978-3-319-08087-1_15.
[11] SAE J2980, Considerations for ISO 26262 ASIL Hazard Classification, (April 2018).
[12] Association for the Advancement of Automotive Medicine, Abbreviated injury scale, from https://www.aaam.org/abbreviated-injury-scale-ais/.
[13] National Instruments™ ADAS test platform, http://www.ni.com/en-us/innovations/automotive/advanced-driver-assistance-systems.html.
[14] IPG CarMaker, https://ipg-automotive.com/products-services/simulation-software/carmaker/ Retrieved on 08/22/2018.
[15] AVL VSM 4™, https://www.avl.com/-/avl-vsm-4.
[16] FEV VirtualDynamics, https://virtualdynamics.fev.com/.
[17] AIAG & VDA FMEA Handbook, https://www.aiag.org/store/publications/details?ProductCode=FMEAAV-1, (June 2019).
[18] R. Leveugle, D. Cimonnet, A. Ammari, System level dependability analysis with RT-level fault injection accuracy, The 19th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Cannes, France, October 10–13, 2004, IEEE Computer Society Press, Los Alamitos, California, 2004, pp. 451–458, , https://doi.org/10.1109/DFTVS.2004.1347870.
[19] Sini, J, D'Auria M., Violante M. (In press), "Towards vehicle-level simulator aided failure mode, eddect, and diagnostic analysis of automotive power electronics items", In: IEEE 21st Latin America Test Symposium (LATS), March–April 2020, Maceio, Brazil.
[20] H. Kwon, R. Itabashi-Campbell, K. McLaughlin, ISO26262 application to electric steering development with a focus on hazard analysis, 2013 IEEE International Systems Conference (SysCon), Orlando, FL, 2013, pp. 655–661, , https://doi.org/10.1109/SysCon.2013.6549952.
[21] ISO 15622, Intelligent Transport Systems – Adaptive Cruise Control Systems – Performance Requirements and Test Procedures, (2018).
[22] European New Car Assessment Programme (EuroNCAP), Test Protocol–AEB Systems, (November 2017).
[23] U.S. Department of Transportation – National Highway Traffic Safety Administration, Intellingent Cruise Control Field Operational Test (Final Report), (May 1998).
[24] European Commission Regulation 347/2017 Attachment 1.
[25] MathWorks Simulink, https://it.mathworks.com/products/simulink.html, Retrieved on 08/22/2018.