SAHARA: SIMULATION AIDED HAZARD ANALYSIS AND RISK ASSESSMENT METHODOLOGY

RAFAEL A. BARRETO J. & ZAKARIA BACHIR
CodesignS – Flanders Make, Belgium

ABSTRACT

Hazard Analysis and Risk Assessment (HARA) in the automotive industry, is a structured process described in the ISO 26262 standard in force for the development of safety-related systems comprised of electrical, electronic and software components. Risks that are identified for malfunctioning behaviour of an item should be classified in terms of *Automotive Safety Integrity Level (ASIL)* in function of discrete qualifications of *Controllability (C)*, *Severity (S)* and *Exposure (E)*. Even though the standard gives definitions and examples on how to select the correct qualification, in practice, this exercise strongly depends on expert judgement, and therefore is (i) time-consuming and (ii) a qualification may differ for the same risk if it is analysed by different teams. This paper shows how simulations can be used to reduce the dependence on expert judgement and can automate part of the HARA process in order to assess a large number of scenarios, making the process less error prone and reducing the required design time. The paper describes the *Simulation Aided Hazard Analysis and Risk Assessment (SAHARA)* method that models hazardous situations from textual descriptions, integrates an item model into a vehicle model, simulates its behaviour and interaction with the environment and evaluates the generated traces through contract-based analysis to estimate C, S, E and ASIL.

Keywords: functional safety, ISO 26262, HARA, Simulation Aided Hazard Analysis and Risk Assessment, vehicle model, ASIL.

1 INTRODUCTION

Development in the automotive industry is becoming increasingly more complex. Nowadays, a vehicle easily integrates dozens of microcontrollers, including those required to perform safety-related functionalities. Electric/Electronic/Programmable Electronic (E/E/PE) components are the common practice to implement safety mechanisms that maintain the system free of unreasonable risk. The design of such systems has to be compliant with the ISO 26262 standard [1] and the lifecycle described therein, where a Hazard Analysis and Risk Assessment (HARA) shall be performed for new items or modifications. In this activity, *Hazardous Events* (HE) should be defined and evaluated in terms of *Exposure* (*E*), *Controllability* (*C*) and *Severity* (*S*), that combined define an *Automotive Safety Integrity Level* (*ASIL*).

Although the standard defines how to evaluate HE and gives some examples, performing hazard analysis and risk assessment is a challenging task [2]. Major transformations in product development are ongoing at big manufacturers, where one of the main goals is to significantly reduce the time of a vehicle design [3] and increase its safety. In this sense, precise, complete and correct risk assessment and requirements coming from HARA are keys for success [4].

The use of structured approach and methods to better estimate ASIL has been presented in [5] and [6], and the use of simulation during HARA in [7]. This work presents a methodology to perform a *Simulation Aided HARA* (*SAHARA*) that uses simulations of vehicle models including a specific item model, fault injection algorithms, textual descriptions of scenarios and contract-based analysis for HE classifications to create a semi-automated safety case, guiding the functional safety engineer to make the objective, more complete and less error-prone assessment in an easier way, reducing the time spent to complete the task.

This paper is organised as follows. In Section 2 the SAHARA methodology is described. In Section 3, a case study is presented where the implementation strategies and algorithms for

WIT Transactions on Engineering Sciences, Vol 129, © 2020 WIT Press
www.witpress.com, ISSN 1743-3533 (on-line)
doi:10.2495/RISK200041

each phase of the methodology are described. In Section 4, general results are discussed and finally in Section 5 conclusions are drawn and further work are highlighted.

2 SAHARA TOOL/METHODOLOGY

The classic HARA approach is dependent on expert's judgement, past experiences of the group of analysis and can be time consuming and error prone. The most common information to be included in an HARA report is functional behaviours, shortfall guiding words, road conditions, operational situations, operating modes, E, C, S and ASIL. This information is obtained from different sources such as previous safety analyses, official databases and simulations. An architecture for the technical realisation of SAHARA is shown in Fig. 1. This new methodology captures needed information to construct scenarios from textual descriptions that, where applicable, can be selected by the user. These *influence factors* (i.f.) cover dynamic and static characteristics of the vehicle, trajectories, environmental and road use conditions, as well as driver and pedestrian interactions that can describe a particular scenario with a sufficient granularity level (ISO 26262-3-6.4.2.7). They are classified in a structured way as shown in [5], then scenarios are modelled by the combination of i.f. in tools such as *PreScan* [8] or *CarMaker* [9].

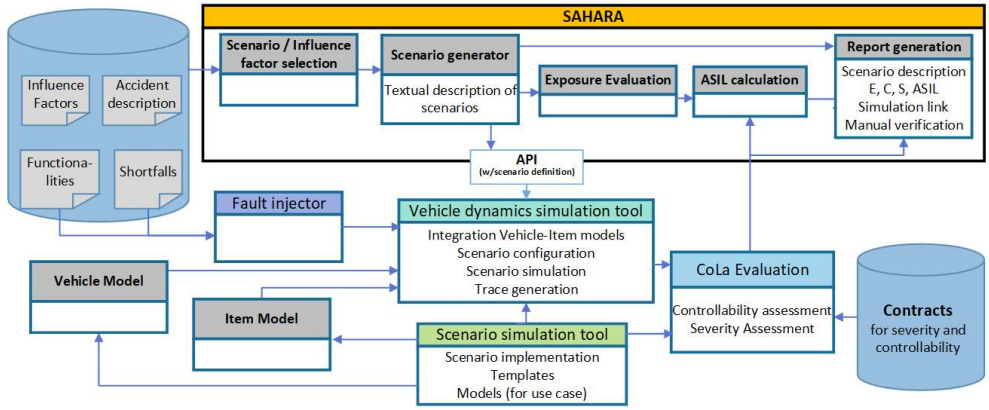

Figure 1: SAHARA architecture for technical realisation.

On the other hand, *vehicle models* containing the *item model* as defined in ISO 26262, which is object of analysis, can simulate dynamic behaviours. A VI-model is the combination of the vehicle model with the item model. They should have interfaces capable of exchanging the necessary information. Tools such as *Simulink* [10] or *CarSim* [11] are often used for this purpose. If both vehicle and item models have interfaces that can communicate with each other and provide the necessary and sufficient information, then items are integrated automatically into different vehicle models to build a complete Vehicle-Item model (*VI-model*). Afterwards, this is integrated into a scenario.

Once the set of scenarios and the VI-model are set, they are combined and the simulations are automatically generated and executed [12] to produce traces containing, e.g., longitudinal and vertical accelerations, yaw angle and planned-actual trajectories deviation. An algorithm of fault injection including functionalities and shortfalls is then put into place and, by analysing those variables and using *contract expressions*, C and S are estimated while E is estimated by a developed technique based on [5], [6] and [13].

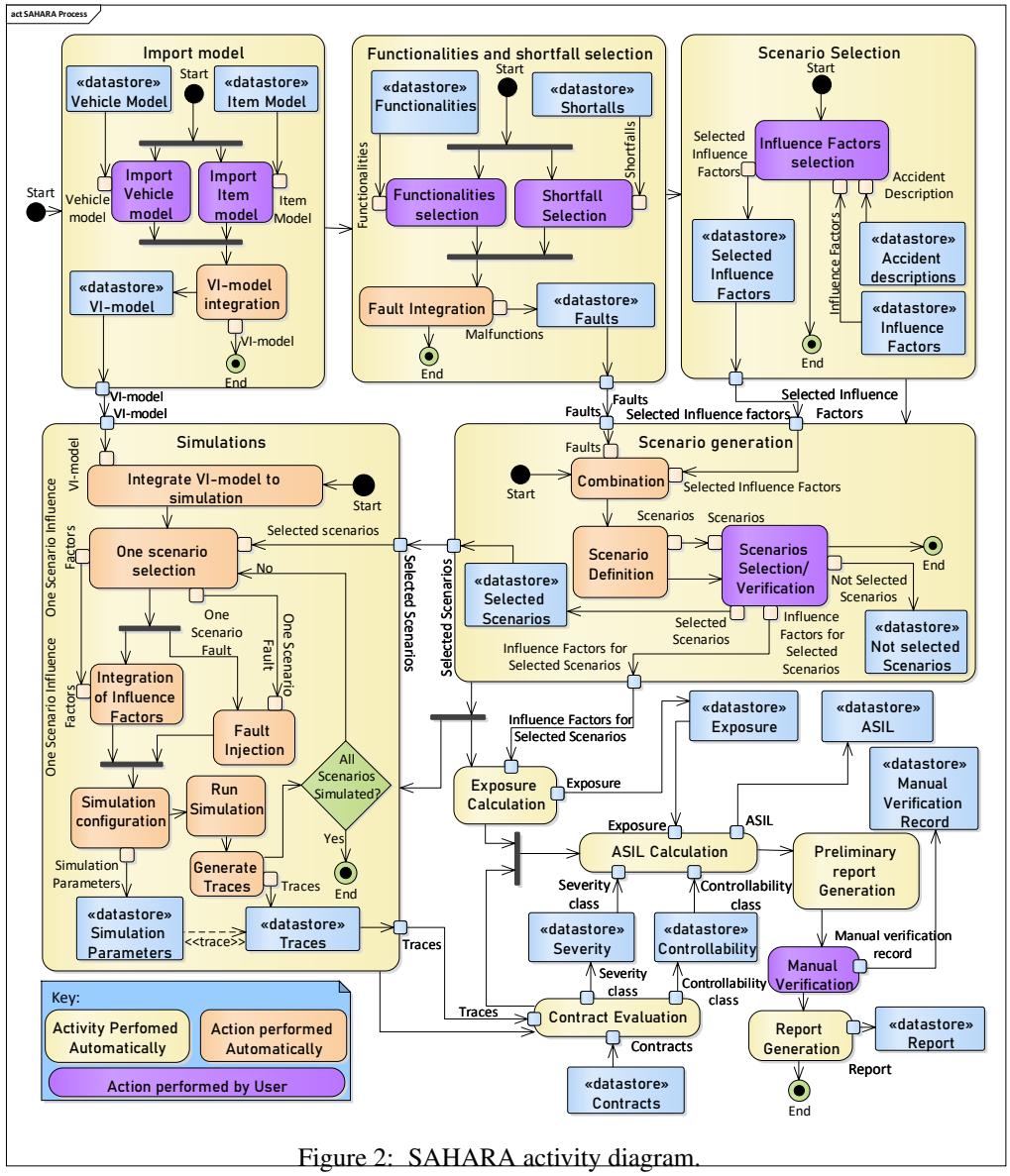

Figure 2: SAHARA activity diagram.

The methodology is described by the activity diagram shown in Fig. 2 and is interpreted as follows: (i) The user imports an item and a vehicle model from a database. The tool integrates both into a single VI-model. (ii) The user selects the functionalities and shortfalls of interest. The tool constructs the faults and identify where to inject them. (iii) The user selects the i.f. to be included in the simulations. (iv) The tool combines the selected i.f. and the faults to generate a set of scenarios. The user can, at this point, select the scenarios that are relevant for the study. (v) With i.f. defined, E is calculated. (vi) The tool builds and executes all the scenarios, one by one, and stores the traces in the database. (vii) The tool evaluates the traces with the predefined contracts for C. (viii) The tool evaluates the traces with contracts for S. (ix) ASIL is calculated with E, C, and S. (x) The tool generates a report with the results where

manual verification is available beforehand. Additionally, SAHARA is capable to manage traceability for all the information that is generated.

3 CASE STUDY

3.1 Case study description

SAHARA methodology is illustrated on an item defined as a path follower from a lateral guiding system that is included in a generic vehicle design as shown in Fig. 3. Simulink and PreScan are chosen to be the tools to run the simulations of dynamic behaviour and the interaction with the environment. The item receives, as inputs, information about the actual position, velocity, and trajectory plan, and the generated outputs are steering wheel angle and acceleration requests. The goal is to produce a HARA report with different identified and classified hazardous events.

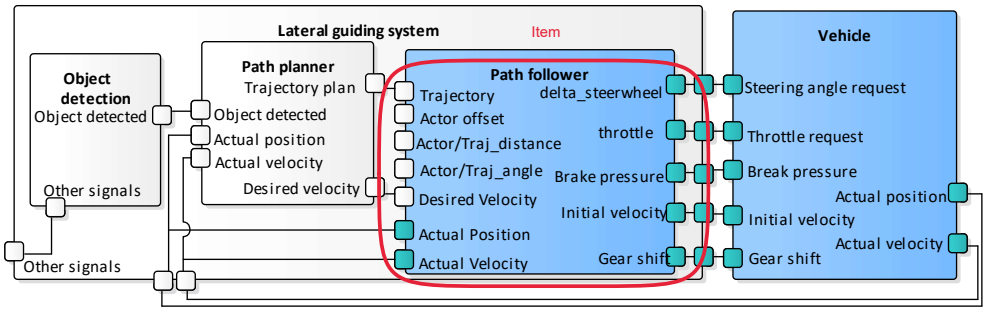

Figure 3: Block representation of a path follower.

3.2 Import VI-model

Several generic Simulink-based vehicle models are proposed by PreScan. They are capable to calculate 2D and 3D dynamics within a defined environment and include modelling of components such as engine, transmission, final drive ratio, chassis and shift logic. Additional sensors are added in order to detect relative position, velocity, obstacles and collision detection.

For the case study, a path follower model proposed from the same tool is selected. It uses as variables, the *actual position, actual velocity, delta steering angle, throttle, break pressure, initial velocity* and *auto gear shift* in order to follow a path that has been set by the path planner (another item out of the scope of this analysis). These variables can be defined as the *interface* Vehicle-Item. In the database, different vehicle models that have the same interface are stored, and item models can be developed and further integrated. Another particular vehicle model that has the correct interface can be used if needed and available. Once both vehicle and item models are prepared and stored, SAHARA tool connects the interfaces by means of scripts using Simulink's application program interface (API). A vehicle model of an Audi A8 Sedan proposed by PreScan and controlled by a path follower model were selected. The result of this operation is the VI-model shown in Fig. 4.

3.3 Functionalities and shortfall selection

In practice, a *malfunctioning behaviour* [1] can be described as a behaviour of a physical variable (e.g., acceleration or steering requests) outside the expected limits or a combination of

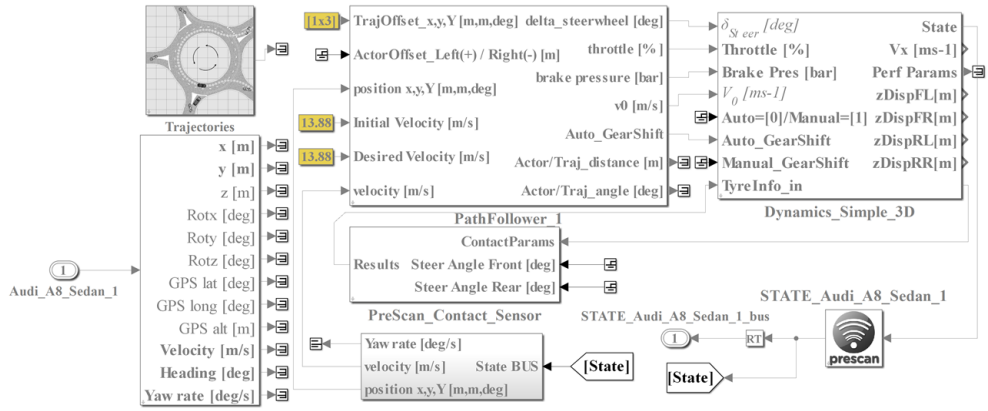

Figure 4: VI-model implementation in MATLAB-Simulink.

a functionality and a shortfall. In the highlighted case study steering functionality was selected. The aim is to have a table with a textual description of functionalities mapped to variables in the VI-model.

On the other hand, shortfalls are modelled as failures that can be injected to the model during the simulation. For example, a shortfall such as "No or Not", can be modelled in Simulink as a zero gain block. SAHARA integrates a database of the main shortfall guiding words used in Hazard and Operability Studies (HAZOP), such as "more", "less" and "unintended". An example is found in Fig. 5.

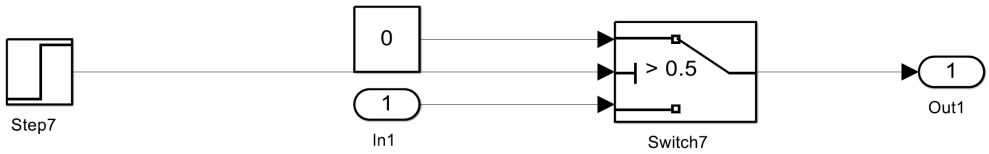

Figure 5: Implementation algorithm of "No or Not" shortfall.

The user is able to select the functionalities (e.g., for the case study: steering) and the shortfalls of interest (e.g., for the case study: "No or Not" and "Unexpected") independently.

3.4 Scenario selection

The elements used to build a scenario have been extracted from the Common Accident Data Set [14] and from [6], [15], [16] and [17]. An extract of the database for Environmental and interaction characteristics is shown in Table 1.

The database has more than three hundred i.f. that are individually tagged as follows: *Simulable*, when it can be simulated in PreScan and has a direct influence in the results of the traces, e.g., pavement. *Simulable with no effect*, when it modifies only visual aspects on an animation, e.g., twilight. *Not simulable*, when it cannot be simulated in PreScan, e.g., effect of a child as traffic participant. *Atomic*, when it corresponds to one only of the elements in PreScan, e.g., rain. *Composed*, when it corresponds to a combination of elements in PreScan, e.g., overtake, that is a combination of two way street, another vehicle as traffic participant,

Table 1: Example of influence factors for environmental and interaction characteristics.

Environmental characteristics				Interaction characteristics		
Time of the day	Precipi-tation	Road type	Pavement	Standard Manoeuvres	Passerby	Traffic participant
Twilight Daylight Nightlight	Rain Fog Mist Smoke Dry	One way Two way Highway City way Right turn	Concrete Asphalt Grass	Decelerate Accelerate Overtake Steer right Steer left	Crossing Stand-up Animal Oncoming traffic	Pedestrian Child Trailer Tree Motorcycle

steer right, accelerate and steer left. For composed i.f., a combination corresponding to the textual description is assigned in the database. This information is sufficient to generate a specific scenarios within the limits of the simulation tool.

The user is able to select what i.f. are useful for the analysis. In the case study, city way, clear weather, steer right and asphalt pavement are selected.

3.5 Scenario generation

In previous phases, the user selected functionalities, shortfalls and i.f. These elements are exhaustively combined in the SAHARA tool and a scenario identifier is added. An extract of this combination is shown in Table 2.

Table 2: Extract from the set of scenario definitions.

Scenario definitions						
ID	Functio-nality	Shortfall	Standard maneuvers	Passerby	Road type	Pavement
HE1	Steering	No	Steer right	Pedestrian	City way	Asphalt
HE2	Steering	Unexpected	Steer right	Pedestrian	City way	Asphalt
HE3	Braking	No	Steer right	Pedestrian	City way	Asphalt
HE*n*	Steering	Unexpected	Steer right	Pedestrian	City way	Concrete

The scenario generation using this methodology described has an advantage: completeness of the analysis can be achieved since all the possible scenarios are considered, hence, reducing the possibility of unintentionally skipping any of them. Conversely, challenges were identified on the implementation side, for instance, *granularity*, because the more i.f. are selected, the number of possible combinations grows exponentially; *consistency* of automatic combinations for scenario creation because the user can select two mutual exclusive i.f. to be analysed separately, e.g., traffic jam and 120 km/h; and, *filtering and grouping* since there are i.f. that necessarily imply others i.f., e.g., highway and 120 km/h (composed i.f.).

In addition, several accident descriptions can be selected in order to choose pre-assembled scenarios that are typical in HARA analysis, for example, accident with pedestrian while vehicle is braking before steering right. These scenarios are originally defined in [15].

Let us select HE3 scenario for the case study.

3.6 Exposure assessment

According to ISO 26262, *Exposure* is a state of being in an operational situation of a HE that can be expressed in terms of five discrete probability classes: $E0$ to $E4$. In this sense, the standard proposes the assignment of them with respect to the duration and to the frequency of the operational situations. SAHARA interprets this concept as the probability that a vehicle operates in a specific combination of i.f., therefore, it calculates the probability of such combination to happen. This is a conservative way to estimate E, which is recommended by the standard. Kemmann [5] has found that it is not possible in practice to automatically calculate situation exposure values and that expert judgement is always needed, for technological as well as for legal reasons. However, Van Eikema Hommes [18] shows that, based on psychological studies, humans are not good at predicting random events and then it recommends that, if no valid probabilistic values exist, the most conservative approach should be used in a risk assessment by assigning the equivalent to $E4$ value for the corresponding HE.

The objective of SAHARA is, in this sense, to support the decision process by calculating an estimation based on data collected from official sources and with a manual assessment made for a basic set of i.f. SAHARA then takes a limited set of i.f. whose probabilities of occurrence are available and furthermore, it implements the methodology proposed in [19], determining probability of state, the combinations that will allow the HE to happen and determining the correlation therein. If a new i.f. with no previous assignment of E is available, then the *Force Field Analysis* algorithm explained in [5] is used. Other algorithms are suitable to specific i.f. probability evaluation that can be used to further refine the calculations, such as the ones in [13] and [6].

For the case study, since steering while driving forward is a permanent situation, $E4$ has been assigned to the HEs. Practically, this result is stored in the database and tagged with the corresponding Hazardous Event ID.

3.7 Simulations

SAHARA uses simulation to provide evidence-based C and S classifications of each scenario generated.

Technically, SAHARA includes a set of templates containing simulable i.f. and components such as trajectories, roads and traffic participants implemented in PreScan as shown in Fig. 6. The aim of the template approach is to implement automation of the simulations as described in Section 2.

On the other hand, SAHARA builds a Simulink model file for each scenario integrating the VI-model and the template that includes the modelled corresponding generic i.f. Then it accesses the template through PreScan API and tailors it according to the specific characteristics of the selected scenario, e.g., in a scenario where traffic participants are irrelevant, SAHARA accesses the template and automatically deletes unwanted elements using PreScan. Afterwards, a fault injection algorithm is executed where the designated fault is loaded from the fault library and connected to the signal corresponding to the selected functionality. For example, for the case study, HE3 injecting “No or Not” fault on the functionality “Braking” results in a model that simulates a vehicle losing braking control in the given scenario described in Section 3.5. The same strategy is applied on other scenarios and SAHARA executes all of them one by one.

Finally, generated traces are assigned to the corresponding HEs to be used for the assessment of C and S as described in the following Sections 3.8 and 3.9. In practice the traces are aspects related to the vehicle dynamics. For example, Fig. 7 shows plots of vehicle’s yaw

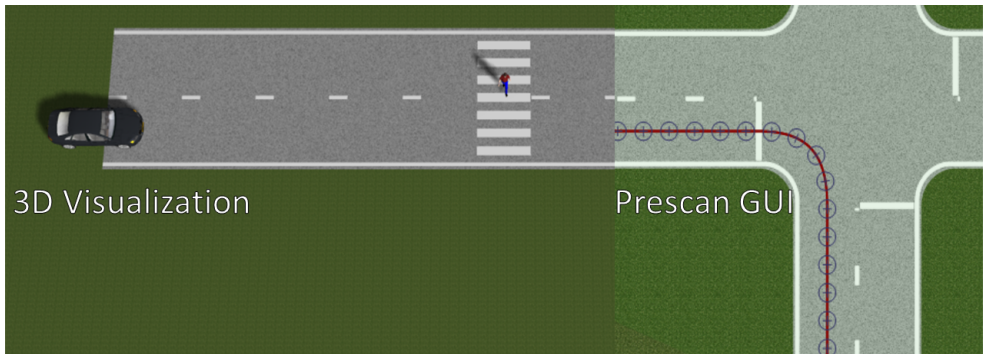

Figure 6: Part of scenarios template.

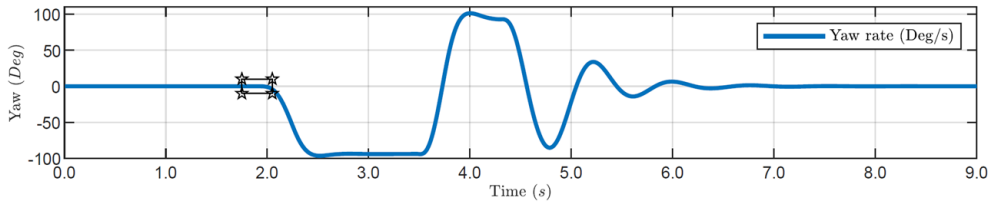

Figure 7: Generated traces from simulation of HEs.

rate, in this particular scenario the vehicle loses its braking control while driving in a right turn at 50 km/h.

The activities defined above are run automatically in the background of SAHARA without user intervention. Results from the technical implementation of this part of the SAHARA methodology are discussed in Section 4.

Results from simulations confirm the technical implementation of this phase within SAHARA methodology, in addition to that, the automation of the process described earlier may help achieving re-usability of the Simulink models and thus lowering the effort spent by the user.

3.8 Controllability assessment

According to ISO 26262, *Controllability* is the ability to avoid a specified harm by means of timely reactions of the persons involved that can be expressed in terms of four discrete probability classes, *C*0 to *C*3. SAHARA methodology assumes that the driver behaviour or ability to control the vehicle provided by the simulation tools is similar to that one of an average driver. Therefore, by analysing specific variables of the traces produced by the simulations, it is possible to determine the level of controllability for a specific HE. An approach that can implement this task is the *Contract-based* design [20].

Contract-based design is becoming increasingly popular in component-based design approaches. Contracts, developed for software components in [21], structure the properties of

a component into a set of pre- and post-conditions. For cyber-physical systems, this approach typically uses the terminology of *assumptions* and *guarantees*. The assumptions of a contract must be satisfied by the environment and, under these, the component promises to fulfil the guaranteed properties. This technique relies on the specification of properties of the different components. In this context, behavioural properties are often expressed using temporal logic formulation. Different temporal logics are available in the literature, e.g., Linear Temporal Logic, Computation Tree Logic, Metric Interval Temporal Logic and Signal Temporal Logic. Furthermore, temporal logic formalisms are often hard for engineers to specify. Pattern-based approaches exist to help engineers in specifying certain behaviour such as in [22]. To bridge the cognitive gap between the logic formalism and the design specification, domain specific languages approaches are also available in the literature, e.g., the ProMoBox approach [23]. Within SAHARA methodology, a contract language is developed to bridge this cognitive gap of the logic formalisation and the intuitive description of Controllability conditions for HE. This contract language, moreover, builds up on temporal logic formalism such as metric interval temporal logic or linear temporal logic.

In this sense, the following text-based contracts have been defined:

- If the *Error Distance* between the planned and actual trajectory of the vehicle is similar or bigger than x meters within T seconds, then Ci, $i = 0$ to 3.
- Following the results in [24]: If vehicle speed is bigger or equal to 50 km/h and smaller than 100 km/h, and yaw changes 4° in up to 1 second, then controllability is $C3$ *OR* if vehicle speed is bigger or equal to 100 km/h and smaller than 150 km/h, and yaw changes 3° in 1 second, then controllability is $C3$ *OR* if vehicle speed is bigger or equal to 150 km/h and yaw changes 2.5° in 1 second, then controllability is $C3$.

Traces in Fig. 7 are analysed with the set of contracts. Yaw angle between $t = 1.75s$ and $t = 2.05s$ varies from 0° to -4.17° (it changes more than 4° in less than one second), the velocity is set at 50 km/h, hence, a controllability contract is verified for the case study scenario and thus, $C3$ is assigned. This result is stored in the database and tagged with the corresponding Hazardous Event ID.

3.9 Severity assessment

According to ISO 26262, *Severity* is an estimate of the extent of harm to one or more individuals that occurs in a HE and that is expressed in terms of four discrete classes: $S0$ to $S3$. SAHARA methodology uses contract-based techniques detailed in Section 3.8 to assess S.

In [25], *Eiband curves* define the tolerance of a restrained individual to abrupt accelerations [26]. According to this study, the relationship between the G force (uniform acceleration), its duration on a vehicle can lead to three levels of injuries that can affect the driver or passenger: uninjured, moderate and severe. SAHARA tool interprets these levels as severity classes and thus, a classification is assigned to each level. This reasoning is shown in Fig. 8.

A contract is then formulated as follows:

- If vehicle's average Gx (horizontal acceleration) is bigger than 50 G and smaller than 100 G for up to 40 milliseconds, then severity is $S2$ *OR* if vehicle's average Gx is bigger than 160 G for more than 4 milliseconds, then severity is $S3$.

On the other hand, [7] proposes a classification of the estimated damage to a car and its severity with respect to the change of the velocity ΔV from a collision. SAHARA implements these results by formulating the following contract:

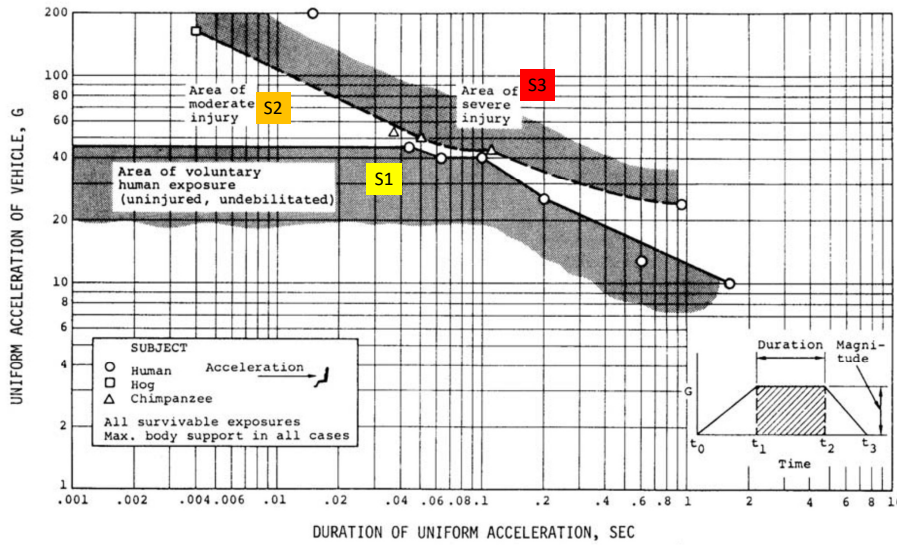

Figure 8: Severity classes assignment using *Eiband* curves from [25].

- If a collision is detected: (if $\Delta V \geq 11$ m/s then $S3$) *OR* (if 11 m/s $> \Delta V \geq 6$ m/s then $S2$) *OR* (if 6 m/s $\geq \Delta V$ then $S1$).

For the case study, a conservative calculation is implemented and the algorithm for detecting ΔV assumes that the vehicle loses all the velocity at the moment it leaves the road, implying that a massive object is present (e.g., trailer as traffic participant). In this case, $\Delta V = 50$ km/h $= 13.89$ m/s. Therefore, according to the contracts, $S3$ is assigned. This result is stored in the database and tagged with the corresponding Hazardous Event ID.

3.10 ASIL calculation

According to ISO 26262, an ASIL level (A to D) specify necessary requirements and safety measures to apply for avoiding an unreasonable risk. SAHARA assigns one to each HE, using ASIL determination table in ISO 26262-3 and E, C and S classes, calculated in Sections 3.6, 3.8 and 3.9. For the case study, HE3, classes are $E4$, $S3$, $C3$ and thus, *ASIL D* is assigned.

3.11 Reporting

Using the stored data, SAHARA allows the user to manually check the results, providing the possibility to verify and/or modify them where necessary. The user has the possibility to trace back all the data produced, including models, scenarios, traces, E, C and S. The text of the contract that is verified is provided as rationale. The tool gives a link to the simulation of each HE so the details of the model, fault injection and traces can be re-checked and; if required, an animation can be produced. Once all lines are revised, the user validates each HE and generates a report in .xlsx or .pdf formats. An example of such report is found in Fig. 9.

SAHARA REPORT

Item	Lateral guidance system
Date	26-08-19

Hazard			Situation Analysis								Hazardous Event Classification				Simulation Link	Manual Verification
			Road Condition						Operational Situations							
ID	Functionality	Shortfall	Road Type	Passerby	Pavement	Precipitation	...	Traffic situation	Vehicle manoeuvre	Traffic participant	Exp.	Cont.	Sev.	ASIL		
HE1	Steering	No	Right Turn	Pedestrian	Asphalt	Dry	...	Congestion	Steer right	Other vehicle	E2	C3	S3	B	Sim_Link001	☑
HE2	Steering	Unexpected	Right Turn	Pedestrian	Asphalt	Dry	...	Congestion	Steer right	Other vehicle	E2	C2	S3	A	Sim_Link002	☑
HE3	Braking	No	Right Turn	Pedestrian	Asphalt	Dry	...	Congestion	Steer right	Other vehicle	E4	C3	S3	D	Sim_Link003	☑
HE4	Steering	No	Right Turn	Pedestrian	Concrete	Dry	...	Congestion	Steer right	Other vehicle	E3	C3	S3	C	Sim_Link004	☐
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	
HE587	Acceleration	Unexpected	Highway	None	Asphalt	Rain	...	None	Overtaking	Other vehicle	E3	C2	S3	B	Sim_Link587	☐

Figure 9: Extract of SAHARA final report.

4 RESULTS AND DISCUSSION

The results regarding the HE description, simulation and risk assessment are validated and in line with a parallel assessment done by expert judgement. The correct application of the process satisfies requirements of the standard and semi-automates the sub-processes of *Situation Analysis*, *Hazard Identification* and *Classification of HE* from ISO 26262. Furthermore, based on simulation results, the methodology helps the engineer to better assess the classification of HE by recommending classifications of E, C, S and ASIL. The tool is able to produce, automatically, a large amount of simulations using a scenario and shortfall selection. Completeness can be claimed in the sense that all the possible combinations of i.f. and faults are analysed. The user should take care to select all the elements for the scenario definition.

Although the production of a template set representing most of the i.f. combinations is time consuming, the user can feel a cut in the time to analyse large number of scenarios. Several templates are needed to cover the case study, but more templates are required to reach an acceptable generality for the tool. Nowadays, each scenario corresponds to a specific template and a specific automation script. The implementation of the tool revealed critical PreScan API limitations, e.g., it is not possible to configure additional trajectories, changing main infrastructure or adding other vehicles to the template. In this case, the scenarios are limited to the set of templates previously configured, and expanding them is not trivial. A better way to tackle the flexibility of the tool should be further investigated.

Supplementary analysis should be performed in order to clarify the impact of the fidelity of the VI-model with respect to the assessment results. Despite E, C and S classes are interpreted in a logarithmic scale, (e.g., the difference between $E1$ and $E2$ is considered as one order of magnitude) if the model and physical vehicle behaviours are significantly different, classes might be assigned incorrectly. If the results are not clear, then the more restrictive class is assigned (conservative approach) and a flag to further check by the user is set. Following this approach might lead the safety case to be significantly more conservative than necessary. Additionally, contracts can be refined, e,g., for S, by better modelling the internal acceleration during a crash and by implementing an optimal calculation of average uniform acceleration.

Despite simulation re-usability being achieved, the ability of the tool to execute only relevant scenarios, by filtering and grouping i.f. should be refined. On the other hand, with respect to fault injection, an alternative strategy can be evaluated from a different approach regarding the use of Functional Mock-up Units and Functional Mock-up Interfaces in order to achieve simulation tool independence [27] so that flexibility is increased.

5 CONCLUSIONS

This work presents a methodology to guide the functional safety engineer through the process of HARA in the framework of ISO 26262. SAHARA methodology proposes a structured way to build a VI-model of a vehicle, create scenarios by the use of i.f. textual representations, run simulations and analyse the traces produced by means of contract-based techniques to assess E, C, S and thus ASIL for each HE. The methodology is represented in an activity diagram and a technical architecture for implementation is proposed. Each activity is explained with the help of a case study. The correct application of the methodology is in line with expert judgement and cuts time in the analysis of scenarios. Challenges regarding impact of the fidelity of the model with respect to the results and how to improve the contracts is tackled as well.

ACKNOWLEDGEMENTS

The authors acknowledge VLAIO (Flanders Innovation and Entrepreneurship) and Flanders Make for their support on aSET_ICON project (grant no. HBC.2017.0389). The authors thank for the support from Klaas Gadeyne, Dirk De Keukeleere and Johan Van Noten from Flanders Make; Mehrdad Moradi and Bentley Oakes from the University of Atwerpen; and, Dariusz Szymansky, currently with AID – GmBH.

REFERENCES

[1] ISO 26262 – road vehicles – functional safety. Standard, International Organization for Standardization, Geneva, CH, 2018.
[2] Beckers, K., Heisel, M., Frese, T. & Hatebur, D., A structured and model-based hazard analysis and risk assessment method for automotive systems, 2013.
[3] Olofsson, M. & Pettersson, J., Parameterization and validation of road and driver behavior models for CarMaker simulations and transmission HIL-Rig. Master's thesis, 2015.
[4] Leveson, N.G., Safeware: System safety and computers: A guide to preventing accidents and losses caused by technology, 2001.
[5] Kemmann, S., SAHARA – A structured approach for hazard analysis and risk assessments. PhD thesis, 2015.
[6] Cafiso, S., La Cava, G. & Montella, A., Safety index for evaluation of two-lane rural highways. *Transportation Research Record*, **2019**, pp. 136–145, 2007.
[7] Duracz, A., Erikssony, H., Barthaz, F., Xu, F., Zengz, Y. & Taha, W., Using rigorous simulation to support ISO 26262 hazard analysis and risk assessment. *2015 IEEE 7th International Symposium on Cyberspace Safety and Security*, pp. 1093–1096, 2015.
[8] TASS International, *PreScan*, 2018.
[9] I.P.G automotive GmbH, *Formula CarMaker*, 2016.
[10] The MathWorks Inc., *MATLAB*, 2015.
[11] Mechanical Simulation Corporation, *CarSim*, 2018.
[12] Müller, J., Gadeyne, K., Nicolai, M. & Van Der Auweraer, H., Automatic generation of simulation models for early stage evaluation of physical system topologies (wip). *Simulation Series*, **47**(8), pp. 221–26, 2015.
[13] Eggert, J., Solomon curve 2020: Relating microscopic risk models with accident statistics. *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 2293–2300, 2016.
[14] Yannis, G., Evgenikos, P., Chaziris, A. & Broughton, J., CADAS – the common accident data set, 2008.
[15] Papadimitriou, E., Yannis, G., Ziakopoulos, A. & Marinos, C., The European road safety decision support system. A clearinghouse of road safety risks and measures, deliverable 8.3 of the h2020 project safetycube, 2018.

[16] Becker, C., Nasser, A. & Attioui, F., Functional safety assessment of a generic accelerator control system with electronic throttle control in fuel cell hybrid electric vehicles, 2018.
[17] Stolte, T., Bagschik, G., Reschka, A. & Maurer, M., Hazard analysis and risk assessment for an automated unmanned protective vehicle. *2017 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1848–1855, 2017.
[18] Van Eikema Hommes, Q.D., Assessment of safety standards for automotive electronic control systems, 2016.
[19] Jang, H.A., Kwon, H.M., Hong, S. & Lee, M., A study on situation analysis for ASIL determination. *Journal of Industrial and Intelligent Information*, **3**(2), pp. 152–157, 2015.
[20] Bernaerts, M., Oakes, B., Vanherpen, K., Aelvoet, B., Vangheluwe, H. & Denil, J., Validating industrial requirements with a contract-based approach. *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, IEEE, pp. 18–27, 2019.
[21] Meyer, B., Applying "design by contract". *Computer*, **25**(10), pp. 40–51, 1992.
[22] Dwyer, M., Avrunin, G. & Corbett, J., Patterns in property specifications for finite-state verification. *Proceedings of the 21st International Conference on Software Engineering*, ACM: New York, NY, USA, ICSE '99, pp. 411–420, 1999.
[23] Meyers, B., Deshayes, R., Lucio, L., Syriani, E., Vangheluwe, H. & Wimmer, M., Promobox: A framework for generating domain-specific property languages. *Software Language Engineering*, Springer International Publishing, pp. 1–20, 2014.
[24] Neukum, A., Ufer, E., Paulig, J. & Krüger, H., Controllability of superposition steering system failures, 2008.
[25] Shanahan, D.F., Human tolerance and crash survivability. *RTO HFM Lecture Series – NATO – Science and Technology Organization*, 2004.
[26] Desjardins, S., Laananen, D. & Singley, G., Aircraft crash survival design guide, 1979.
[27] Blochwitz, T. et al., The functional mockup interface for tool independent exchange of simulation models. *Proceedings of the 8th International Modelica Conference*, pp. 105–114, 2011.