Safety Simulation in the Concept Phase: Advanced Co-simulation Toolchain for Conventional, Hybrid and Fully Electric Vehicles

Stephen Jones, Eric Armengaud, Hannes Böhm, Caizhen Cheng, Gerhard Griessnig, Arno Huss, Emre Kural and Mihai Nica

Abstract. Modern vehicle powertrains include electronically controlled mechanical, electrical and hydraulic systems, such as double clutch transmissions (DCT), powerful regenerative braking systems and distributed e-Machines (EM), which leads to new safety challenges. Functional failure analysis of events such as the sudden failure of a DCT or EM, and the development and the validation of suitable controllers and networks, can now be evaluated using co-simulation techniques, from the early stages of product development. A co-simulation toolchain with a 3D vehicle and road model, coupled with a 1D powertrain model, is used to enable the definition of hardware and software functions, and also to support the rating of the Automotive Safety Integrity Level (ASIL) during hazard analysis and risk assessment in the context of ISO 26262. This innovative approach may be applied to a wide range of powertrain topologies, including conventional, hybrid electric and fully electric, for cars, motorcycles, light or heavy duty truck or bus applications.

Keywords: functional safety, safety, hazard, ISO 26262, ASIL, HRA, control, function, controllability, severity, exposure, car, bus, motorcycle, truck, trailer, hybrid, electric, powertrain, DCT, e-machine, co-simulation, vehicle dynamics, driver.

1 Introduction

In the development of vehicles with greater energy efficiency and performance targets, ever more sophisticated powertrain sub-systems and electronic controllers

S. Jones(✉) · E. Armengaud · H. Böhm · C. Cheng · G. Griessnig · A. Huss · E. Kural · M. Nica
AVL List GmbH, Hans-List-Platz 1, 8020 Graz, Austria
e-mail: {stephen.jones,eric.armengaud,hannes.boehm,caizhen.cheng, gerhard.griessnig,arno.huss,emre.kural,nica.mihai}@avl.com

J. Fischer-Wolfarth and G. Meyer (eds.), *Advanced Microsystems for Automotive Applications 2014*, Lecture Notes in Mobility,
DOI: 10.1007/978-3-319-08087-1_15,

are being implemented, in conventional, hybrid electric and fully electric vehicles. In order to control and reduce the costs and risks associated with the development of such novel technologies, vehicle manufacturers and suppliers seek to test new functionalities in the very early stage of the development, especially with respect to vehicle safety and energy efficiency.

To systematically minimize the risk of possible hazards caused by the malfunctioning behavior of electrical and/or electronic systems in passenger cars, the ISO 26262 Functional Safety Standard [1] was introduced in November 2011. A revision of the ISO 26262 is planned for the year 2016 which shall also include commercial vehicles and motorcycles. The ISO 26262 standard requires the conduction of a Hazard Analysis and Risk Assessment (HRA) in the concept phase of the development. In this HRA hazard events with corresponding Automotive Safety Integrity Levels (ASIL) are determined. As these directly impact the product development costs and time, the confidence of such determination should be supported by appropriate techniques e.g. holistic system simulation.

To determine the ASIL for a hazard event, three factors must be considered: *exposure, severity* and *controllability* of the hazardous situation. Whilst guidelines for the evaluation of exposure and severity are available [1], the controllability is difficult to evaluate as most of the controllability assumptions (C0 – Controllable in general, C1 – Simply controllable, C2 –Normally controllable, C3 – Difficult to control or uncontrollable) can in many cases only be reliably evaluated at the end of the product development cycle, on the test track in an expensive and perhaps dangerous vehicle test program. Evidently this imposes a major inconvenience and high development risk, especially if the late vehicle tests conclude that the controllability was incorrectly determined in the project and hence the ASIL must be reconsidered, i.e. part of the development must be redone.

To address this problem, activities [2, 3] have been conducted by AVL based upon the implementation of an advanced 1D / 3D co-simulation toolchain able to enable the efficient frontloaded development of electrified and conventional vehicles, whether they are cars, buses, or light and heavy duty trucks. This toolchain includes the simulation software IPG CarMaker/TruckMaker, AVL CRUISE and MATLAB/Simulink. CarMaker/TruckMaker is a vehicle simulation tool with the ability to represent lateral and longitudinal vehicle dynamics, 3D driving routes, complex multi-vehicle traffic scenarios, and highly dynamic driver maneuvers and thus test cases. The integration of a CRUISE powertrain model with CarMaker/TruckMaker significantly extends powertrain modeling capability and flexibility. CarMaker/TruckMaker and CRUISE both have MATLAB /Simulink interfaces that allow for the ready inclusion of xCU control software e.g. VCU, EMS, HCU, TCU and ABS/ESP/TCS [4], enabling fully virtual functional safety testing from the concept phase and onwards in the project development cycle.

This realistic, yet computationally efficient toolchain enables model based development of control strategies and functional safety analysis based on simulation. Advantageously, once vehicles or powertrain hardware are available,

equivalent and reproducible safety analysis testing with real failure injection can be conducted on a real testbed or Hardware-in-the-Loop system, using the corresponding real-time toolchain of AVL InMotion and AVL CRUISE RT. Reusing essentially the same simulation models and critically also the same simulated test cases, as in the preceding office co-simulation phase.

2 Functional Safety – An Overview

The main target of functional safety standards such as ISO 26262 is to ensure the residual risk of a product to fail due to a malfunction of its electric / electronic control system(s) is at or below an acceptable level. Functional safety standards usually rely on appropriate quality management during the development process (to avoid systematic failures during product development), and on appropriate risk identification and risk management over the entire product lifecycle, to mitigate the effects of random failures such as component breakdown.

A cornerstone of this approach is the systematic identification and classification of the hazards for a given system. For the ISO 26262 standard, this is performed for the first time early in the concept phase by means of hazard analysis and risk assessment in order to identify the different potential hazards, and classify these according to their severity, i.e. the risk to persons, exposure, i.e. the probability of a situation to occur, and controllability, i.e. the capability for the human driver to identify and appropriately react to the given situation. This analysis is further consolidated by means of safety analysis (e.g., FMEA, FTA) to understand the effects of component failures and the resulting impact at vehicle level.

A major challenge in the concept phase is the correct analysis of the possible impacts of such hazards and the capability for the human driver to appropriately control the complex systems considered, which include multiple electronic controllers, powertrain subsystems, vehicle steering, brakes and tires, as well as the road surface and driving environment. The challenges are composed of (a) the correct understanding of the realized functions and their possible effects in event of a failure within the system, and (b) the capability to judge the controllability of the vehicle behavior by the different human drivers (e.g. beginner, normal, expert) in the different driving situations (e.g. vehicle speed, road friction, environment).

The advantages of system simulation support in the HRA lie in the reproducibility and the higher coverage of different situations which are composed from countless variations of the parameters illustrated in the preceding paragraphs.

3 Co-simulation Model Description

In order to support assessment of ASIL in very early phase of development, virtual evaluation of vehicle controllability with mechanical, hydraulic, electrical, electronic or software failures, an integrated co-simulation toolchain has been developed in AVL.

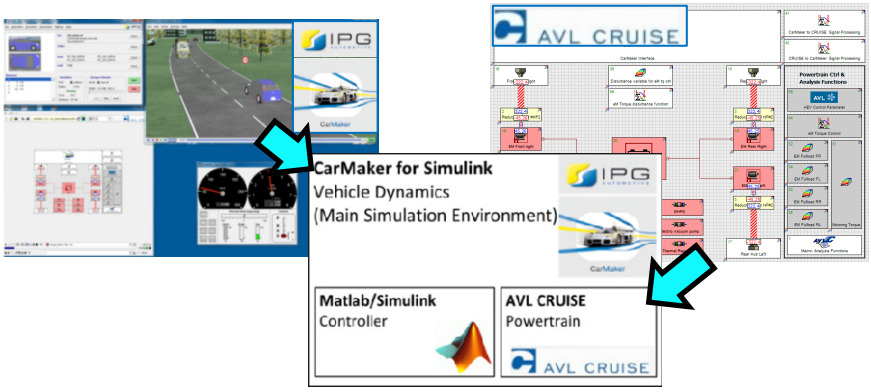

Fig. 1 Simulation environment used for simulation based determination of ASIL. The toolchain includes CarMaker® or TruckMaker®, CRUISE, and MATLAB/Simulink®.

This toolchain connects CarMaker or, if a commercial heavy duty vehicle or bus shall be simulated TruckMaker, with CRUISE, and MATLAB/Simulink (Figure 1). The 3D vehicle dynamics model including wheel suspension and tire model, a realistic human driver and road models are simulated in CarMaker or TruckMaker, whilst the complex 1D powertrain model is developed in CRUISE, and control software is developed and / or integrated via MATLAB/Simulink. This allows the utilization of the capabilities of specialized simulation and authoring tools for maximum overall ease, speed and accuracy.

4 Applications of Concept Safety Simulation for Various Vehicle Configurations

With the described co-simulation toolchain, vehicle dynamics, including controllability, can be readily simulated for many test cases, i.e. a range of different driving maneuvers, with various failure modes injected (e.g. an e-machine failure in an electric vehicle with multiple EMs). Based on the simulation results, the vehicle controllability is evaluated for various selected hazardous situations.

In this paper several simulation scenarios are presented to demonstrate the virtual assessment of ASIL. The first example is a conventional car with a DCT, the second is a heavy duty truck. Thirdly a 4WD HEV in P1 configuration, with a second EM driving the rear wheels is presented. Finally, an EV with the 4 wheels individually driven by 4 separate EMs is shown.

4.1 Vehicles with Conventional Powertrains

4.1.1 Passenger Car with DCT

The first simulation scenario shown involves a conventional front wheel drive passenger car with a DCT. The simulated system malfunction consists of the

simultaneous engagement of both the odd and even gear clutches, for a brief period of time (70 ms), which will introduce a sudden brake torque on the driven wheels, and might result in a loss of vehicle control, particularly if failure occurs in a corner on a wet or icy road surface. In this test scenario, the vehicle drives in a circle with radius of 110 m, with a tire-road friction coefficient (μ) of 0.4, at a constant speed of 70 km/h. Figure 2 shows the DCT clutch actuators, clutch torques, and the driver and vehicle responses (the latter two over a much longer time scale). It can be seen that the vehicle laterally diverts more than 2 m, and therefore could run into the path of an oncoming vehicle, or a road side obstacle.

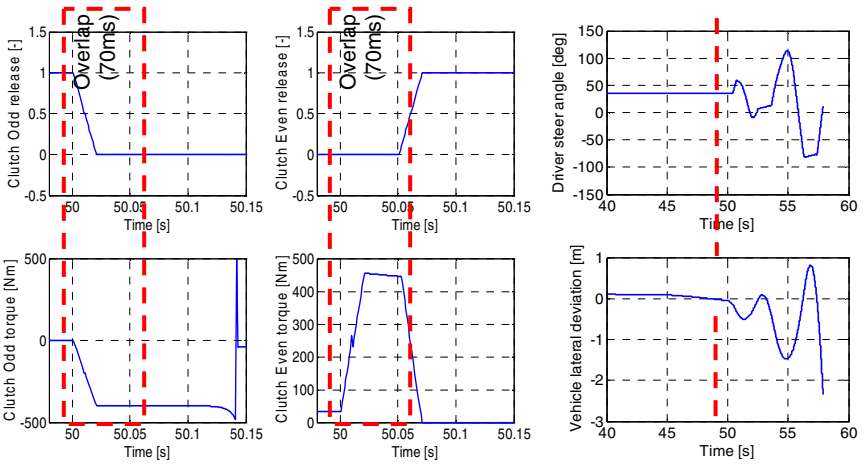

Fig. 2 Simulated signals of DCT clutch actuators and torques, with driver and vehicle response shown over much longer time scales, during a 70 ms double clutch engagement overlap

4.1.2 Heavy Duty Vehicles

The described methodology has also been applied on heavy duty vehicles, including buses and trucks, with semi-trailers and full trailers. A matrix of test cases has been established and simulated involving a tractor or cab with a mass of 7 tons, and a semi-trailer (11 tons when empty or 19 tons when fully loaded) driving round a corner of a radius of 100 m, at a velocity of 65 km/h. Several types of failures were virtually injected, including positive and negative (i.e. braking) torque on inner and outer rear driven wheels, as well as an unintended steering wheel angle reduction (gradually applied over 1.5 s). The human driver reaction time was assumed to be 1.5 s. Simulations were performed with wet (μ=0.7) and dry (μ=1.0) roads. Here selected simulation results are presented of the case involving unintended brake torque (5000 Nm) on the driven rear axle, while driving on a wet road. Figure 3 summarizes the simulated signals. After failure activation (t=200 s), the human driver model seeks to control the vehicle, i.e. minimize the vehicles lateral deviation from nominal track position; here the maximum deviation resulting is ~0.7 m, suggesting the vehicle is likely to just stay in its lane. Aside of perilous lateral vehicular excursions required to control the vehicle after

such a possible powertrain failure, the relatively high center of gravity of commercial vehicles, increases the risk of the vehicle tipping over during driver reactions intended to re-gain vehicle control.

Figure 4 shows a modified version of the previously described case in which the vehicle velocity was increased to 71 km/h, and a positive drive torque is introduced and a dry road assumed. The vehicle accelerates for 1.5 s until driver reactions become visible: while the steering wheel angle is increased, the vehicle rolling slightly along its longitudinal axis, the driven inner rear wheel lifting from the ground.

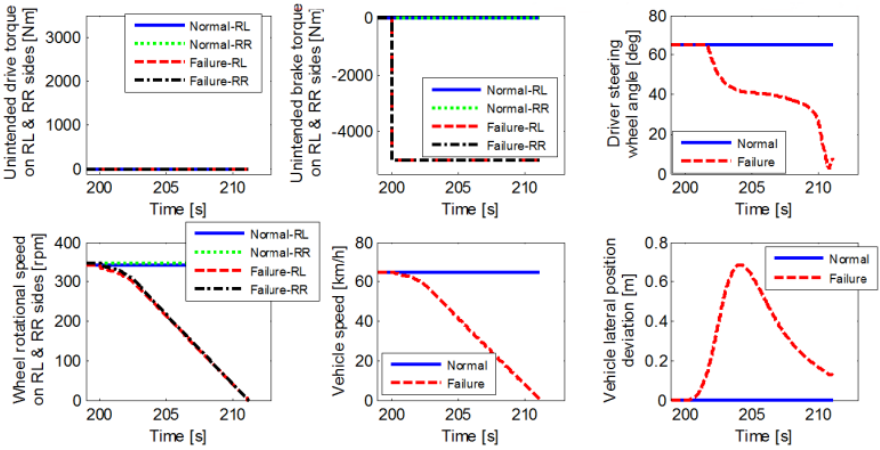

Fig. 3 Simulated signals of tractor with fully loaded semi-trailer at constant vehicle speed of 65 km/h, wet road and unintended brake torque on driven axle. Max. lateral excursion of 0.7 m.

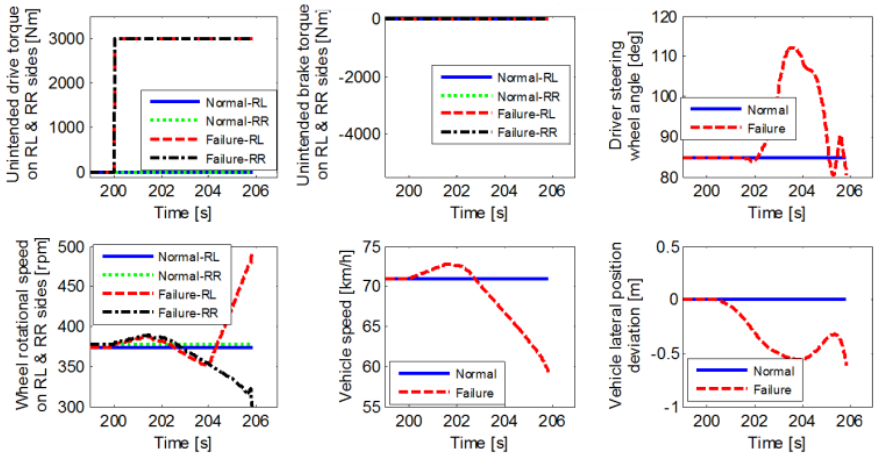

Fig. 4 Simulated signals of tractor with fully loaded semi-trailer at constant speed 71 km/h, dry road, and unintended positive drive torque. At t=204 s the sharp speed increase of the rear left wheel ("Failure-RL", left lower diagram) shows the loss of road contact of this wheel followed by the vehicle rolling over.

As the lifted wheel is still subject to a positive drive torque, its speed sharply increases (see red dashed line in the first graph in the lower row of Figure 4). As the steering wheel angle is reduced too late (around t=204 s), the tipping over of the vehicle is unavoidable (Figure 5).

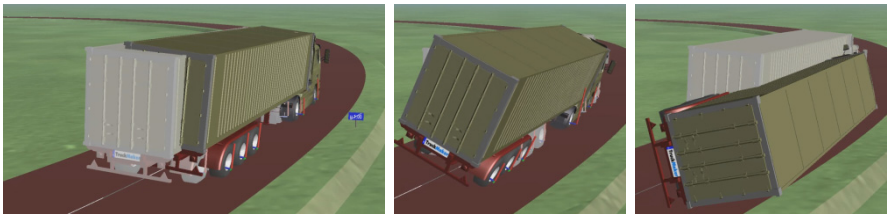

Fig. 5 Tractor with fully loaded semi-trailer at constant vehicle speed 71km/h, dry road, and unintended positive drive torque (green vehicle; the grey vehicle is the reference vehicle without powertrain failure). Vehicle tipping over cannot be avoided with the unintended positive drive torque active. Snapshots are taken at time ~ 202, 204, 206 s.

4.2 Hybrid Electric Vehicles (HEV)

To demonstrate the applicability of the concept safety simulation approach also for the example of highly complex hybrid electric vehicles, exemplary results are presented here, which were obtained from simulations of a 4WD diesel hybrid electric passenger car (1800 kg) equipped with two EMs, the first of which, is a small integrated starter generator (ISG) of 9 kW power, coupled to the 120 kW diesel driving the front wheels, while a second EM with higher power at 27 kW is directly connected to the rear axle alone.

In the following section, simulation results are shown for selected driving maneuvers including unintended full positive EM torque on rear axle while driving on dry road, and, secondly, while driving on μ-split road conditions with μ = 1.0 (dry) and 0.7 (wet), on inside and outside road strips respectively. Thirdly, a simulation case is presented with a failure consisting of sudden full negative EM torque on the rear axle, whilst driving on wet road. In all cases the hybrid vehicle is driven initially at constant speed of 100 km/h, and in a circle with constant radius of 100 m, and approaching the tire-road friction limits.

Until the virtual failures are triggered, a fixed traction power split of 50/50, between the front and the rear axles is assumed. Figure 6 summarizes the main signals along the maneuver of unintended full positive torque on dry ground. After sudden wheel torque increase the driver gently activates the brakes (not shown), and corrects the steering angle to minimize lateral deviation, which remains below 0.4 m. With μ-split road conditions, the maneuver is quite similar, except that the max. lateral deviation towards center of corner is larger, due to yaw torque introduced by different brake torques on left and right side wheels (data not shown).

Finally, the results of simulation with unintended full negative torque are shown in Figure 7. Initially, the brake torque on the rear wheels causes the vehicle

to slow down, and despite driver attempts to regain vehicle stability and control, the lateral excursion reaches 2 m from the center line. Furthermore, once the vehicle velocity has dropped below 70 km/h, the rear EM reaches its max. torque of 200 Nm, which causes the vehicle to quickly yaw towards the corner center point and nearly spins it out of its lane. The maximum lateral deviation during this maneuver is 2 m. At around t = 55 s into the maneuver, the negative torque on the left rear wheel is sufficient to drive the wheel with large negative speed, i.e. in the reverse direction.

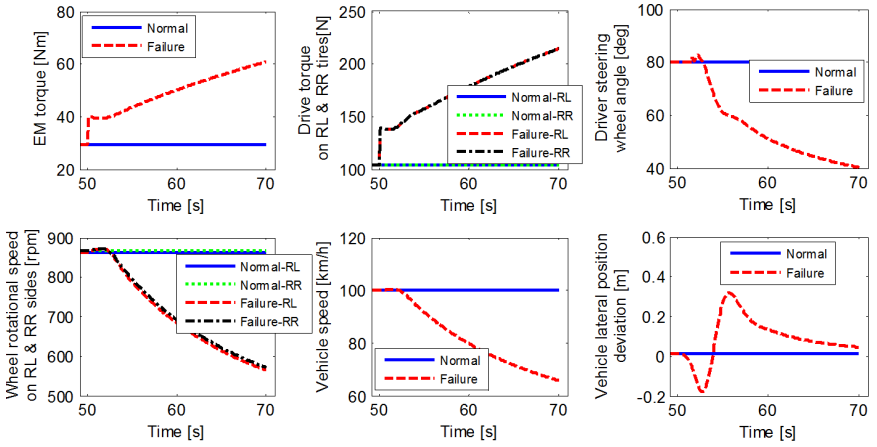

Fig. 6 Simulated signals of hybrid electric vehicle & driver exposed to unintended full positive e-motor torque on rear axle, dry road

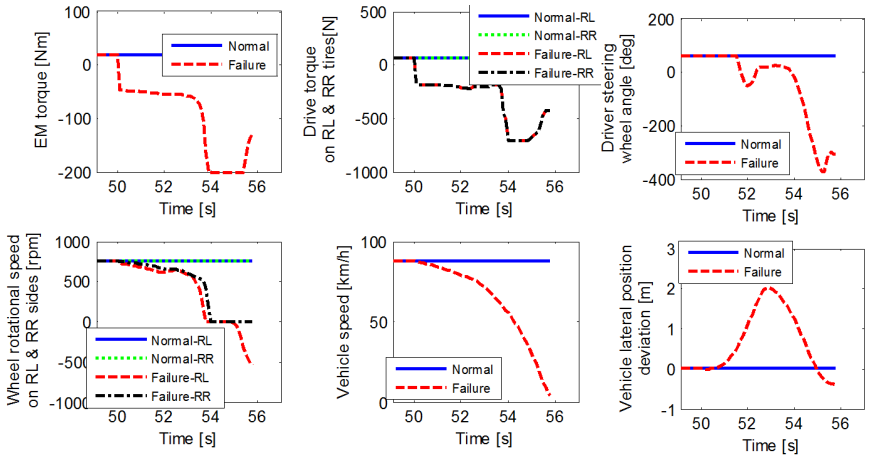

Fig. 7 Simulated signals of hybrid electric vehicle & driver exposed to unintended full negative EM torque on rear axle, wet road; at t = 54 s, the left hand side rear wheel (RL, red curve) speed assumes negative values i.e. it rotates backwards (see lower left most graph)

4.3 *Fully Electric Vehicles with Multiple E-Machines*

Various failure scenarios should be considered for electric vehicles (EV) with four EMs. For example, one of the four EMs could suddenly generate full positive, full negative or zero torque (contrary to the torque demanded by the driver), due to a sudden failure of EM hardware, related power electronics, control software, or even due to a corrupt controller application calibration.

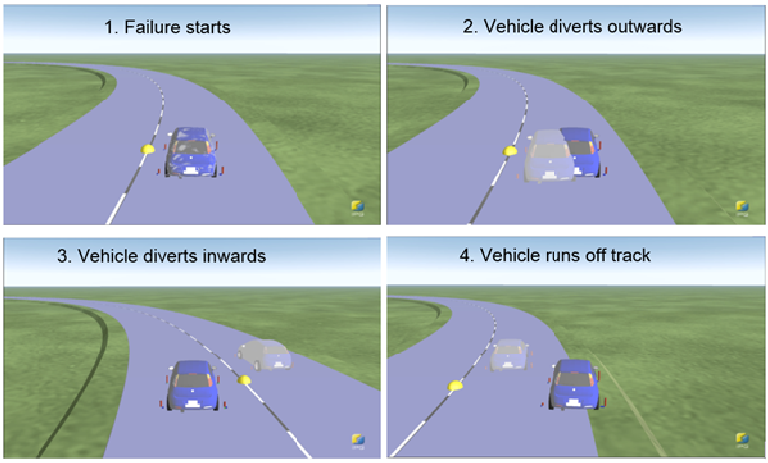

Fig. 8 Snapshots of the vehicle movement when one EM fails with full positive torque on an electric vehicle with four EMs; grey vehicle is reference without failure

Simulation results of one example maneuver are presented here in which the simulated EV runs at a constant speed of 70 km/h, in a circle with radius of 110 m, with tire-road friction coefficient (μ) of 0.4 (corresponding to a wet and slippery

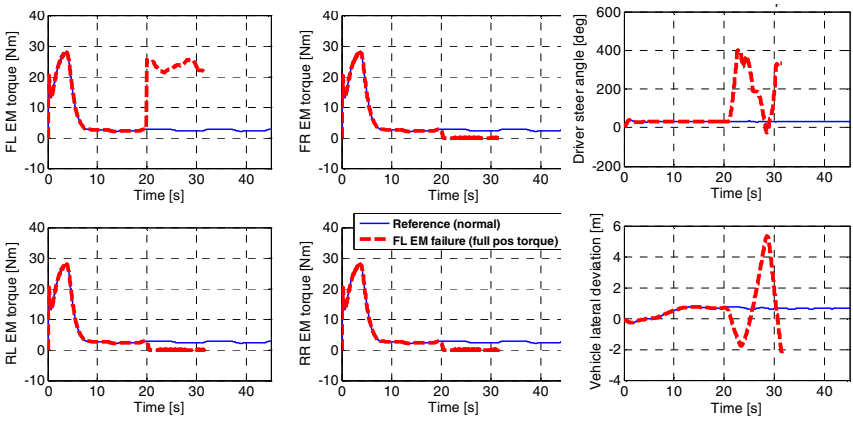

Fig. 9 EM torque signals and vehicle movement when one EM fails with full positive torque on an electric vehicle with four EMs

road). The simulated EV is equipped with four EMs, each with 13 kW mechanical power. In the first failure scenario, the front left EM suddenly provides full positive torque.

Snapshots of the simulated vehicle motion are shown in Figure 8. Two vehicles are shown of which the dark (blue) one has the failing EM, whilst the light grey one is the reference vehicle without failure.

Figure 9 shows the EM torque curves, driver steering and vehicle lateral deviation. The solid (blue) lines represent the reference vehicle, whilst the dashed (red) lines represent the vehicle with a failed EM. When the front left EM fails with full positive torque, the vehicle starts to divert from the target path; the driver tries to correct with large steering effort, but the vehicle runs off track, resulting in an unintended lane change, possibly into the path of oncoming traffic, and later the vehicle partially leave the road, possibly into a road side obstacle.

Analogously to the shown driving scenarios, other potentially critical scenarios can and need to be simulated, to cover the full range of relevant maneuvers e.g. driving on a straight road with differing road frictions, or cornering at various speed levels, for each selected failure mode, to make up a full matrix of simulated test cases (i.e. combinations of failure modes and relevant driving maneuvers).

Table 1 EV controllability matrix for specified driving scenarios

Driving Scenario	*Road Friction*	*EM-Torque Failure*	*Controllability*
Straight 100km/h	Dry (μ=0.8)	Full pos. Trq.	Controllable
		Zero Trq.	
		Full neg. Trq.	
		2 Rear EM Full neg. Trq.	
	Wet (μ=0.4)	Full pos. Trq.	
		Zero Trq.	
		Full neg. Trq.	
		2 Rear EM Full neg. Trq.	
Circling R=110m 100km/h	Dry (μ=0.8)	Full pos. Trq.	Uncontrollable
		Zero Trq.	Controllable
		Full neg. Trq.	Uncontrollable
		2 Rear EM Full neg. Trq.	
Circling R=110m 70km/h	Wet (μ=0.4)	Full pos. Trq.	Uncontrollable
		Zero Trq.	Controllable
		Full neg. Trq.	Uncontrollable
		2 Rear EM Full neg. Trq.	
	Dry (μ=0.8)	Full pos. Trq.	Controllable
		Zero Trq.	
		Full neg. Trq.	
		2 Rear EM Full neg. Trq.	
Circling R=110m 70km/h; driver reaction time 2s	Dry (μ=0.8)	Full pos. Trq.	Uncontrollable
		Zero Trq.	Controllable
		Full neg. Trq.	Uncontrollable
		2 Rear EM Full neg. Trq.	Controllable

Controllability (here primarily evaluated on the basis of acceptable lateral vehicle deviation, assuming a driver of average driving skills) may be assessed using simulation results, and an exemplary controllability matrix, as shown in Table 1, thus generated. Exposure and severity may also be estimated from the simulation results in combination with statistical data. However, these assessments require a cross-functional team, composed of vehicle dynamics, powertrain, control systems and functional safety specialists, working together to use the system simulation results to support their deliberations, and to assist them in making expert judgments, to establish the appropriate ASIL.

5 Conclusions

The presented co-simulation toolchain permits hazard severity and vehicle controllability modelling in the presence of defined system failures, supporting improved hazard analysis and risk assessment by a cross-functional expert system engineering team. Thus the ASIL may be assessed with a higher confidence, from the early concept phase onwards. This co-simulation based methodology is available for trucks, buses, passenger cars and motorcycles, with conventional, hybrid electric and fully electric powertrains.

A refinement of the presented method relies on the definition of a broader spectrum of human driver types, with differing driving skills e.g. reaction times, steering angle rates, etc. These can be used to more precisely determine the controllability levels (C0 to C3) for each driving maneuver and powertrain failure.

Other advantages of system simulation support in the hazard analysis and risk assessment lie in the reproducibility it provides, and the higher coverage of different situations (which are composed from the countless variations of the parameters above) it permits.

The same co-simulation techniques may also be used to develop and validate fault mitigation strategies e.g. failure detection functions, improved hardware including sensors and communication networks.

Acknowledgements. The research leading to these results has received funding from the ARTEMIS Joint Undertaking under grant agreement number 295311 and from specific national programs and/or funding authorities.

References

[1] International Organization for Standardization, ISO 26262 Road vehicles - Functional safety, Geneva, Switzerland, 2011 and (2012)

[2] Jones, S., Böhm, H., Weingerl, P., Cheng, C.: Dynamic simulation of complex mechatronic systems: Torsional vibrations in powertrains, vehicle dynamics & safety. In: Systemanalyse in der Kfz-Antriebstechnik VII - Haus der Technik Fachbuch, vol. 129, p. 83. Expert Verlag, Renningen (2013)

[3] Jones, S., Ellinger, E.: Vehicle System Simulation for Electrified & Conventional Powertrains. In: SIMVEC - Berechnung, Simulation und Erprobung im Fahrzeugbau, p. 81. VDI-Bericht 2169, Baden-Baden (2012)
[4] Jones, S., Kural, E., Knoedler, K., Steinmann, J.: Optimal Energy Efficiency, Vehicle Stability and Safety on OpEneR EV with Electrified Front and Rear Axles. In: Fischer-Wolfarth, J., Meyer, G. (eds.) Advanced Microsystems for Automotive Applications 2013, Berlin, Germany (2013)