Functional safety and reliability for innovative vehicle braking system and integration with electric traction units

T. Favilli, M. Delogu, L. Pugi and L. Berzi

Università degli Studi di Firenze, Department of Industrial Engineering (DIEF), Firenze 50129, IT

E-mail: tommaso.favilli@unifi.it

Abstract. Newly electric vehicle architectures require intensive virtual and physical testing for safety assessment, due to the increasing relevance of By-Wire systems and the presence of innovative control algorithms for ordinary driving scenario, potential emergency situations or Advanced Driver-Assistance Systems implementation purpose. To reduce the development time while increasing system reliability and the a priori knowledge about its safety requirements, the evaluation of such aspects should be performed. In accordance to ISO26262 standard, authors propose a systematic approach based on Virtual FMEA, in order to assess the functional safety level of hybrid brake plant. Plant modification and securing strategy as been presented and implemented in target vehicle model, evaluating their performances in simulation environments, in order to met required Automotive Safety Integrity Level. This work is developed in the ambit of OBELICS European Project.

1. Introduction

Nowadays, the usage of embedded controller devices in the electric automotive field is further increasing, thanks to the introduction of By-Wire (BW) systems [1, 2, 3]. Also, interaction between users and Electric/Electronic (E/E) systems on board are more frequent, since are becoming more and more active, including drive prediction and Advanced Driver-Assistance Systems (ADAS). The growing complexity of such plants, due to the integration of more functionalities and the attribution of safety-related tasks (relieved from the pilot) can lead both to increased fault probability and severity. It’s also interesting to notice that in a scenario in which autonomous and assisted driving functionalities are implemented, reliability of underlying automation and actuation systems hast to be further increased, considering the limited awareness of human driver when dealing with complex nested automation layers. Those faults are quite difficult to be correctly interpreted, especially when low-mid level control layers are affected.

Reliability and Safety are crucial factors for the correct operation of a product, especially for E/E devices adopted in the automotive sector, whose developments process must follow rigorous procedures. Indeed, essential drive functionalities are implemented trough Control Unit (CU), so safety-critical active system should be developed in accordance to severe functional reliability concept. Standard ISO 26262 [4] provide useful guidelines, assisting designer through all main phases of the V-shape procedure, in order to develop a product which respects required safety performances. Occurrences of faults during operative phases of an E/E systems of Electric
Vehicle (EV)s, can lead to a deviation from the expected behaviour, with potential risk for the users, especially for those systems dealing with active safety functionalities. So, it is recommended to analyze the fault-modes of the involved devices, to avoid undesired effect in the overall system reliability, using a Virtual Failure Mode and Effect Analysis (vFMEA) approach. More in detail, relevant examples of BW commands on latest generation vehicles are: throttle, braking and steer. All of them are fundamental for vehicle safety and controllability. Literature experience describe main design criteria for such applications, including appropriate system topology, and the testing procedures needed to quantify their functional reliability, fault tolerance and applicability on road vehicles [5, 6]. In this context, ISO2626 provides a solid framework for system development which is applicable to x-by-wire analysis, possibly integrated with modeling activities [7, 8, 9, 10, 11, 12].

These aspects highlight the importance of ensuring enhanced reliability and safety performances for these systems. To avoid these situations, a systematic procedure for the design, development and validation of automotive systems could be a feasible solution to avoid a dangerous and harmful scenario. The supposed failure mechanisms, determined through Failure Mode and Effect Analysis (FMEA), are related to the vehicle Electronic Control Unit (ECU). Faults are supposed permanent (irreversible) and concern hardware and interaction failure. However, proposed solution are effective also for transient and intermittent failures. Such failures are always possible due to the aggressive and dangerous environment of automotive applications and the growing complexity of hardware components and system architecture. The investigation focuses on the proposal of a virtual simulation environment, implemented with a model-based approach, to assess the consequences of a fault on the vehicle behaviour, through Fault Injection (FI) simulations activities on a vehicle model and related sub-systems.

Proposed methodology, which is developed in the ambit of the Optimization of scalaBle rEaltime modeLs and functIonal testing for e-drive ConceptS (OBELICS) European Project (under Horizon2020), similarly to other performance assessment procedures described in literature [13, 14], concern EV functional safety concept and aims at the safety assessment of investigated brake plant. However, respect to the actual State-of-Arts (SoA), this solution is developed in accordance with ISO 26262 standard’s specifications, which strongly suggest to support the validation protocol with FI techniques. In particular, a multi-level FI approach is adopted, which consists in the simulation of investigated failure modes, useful to establish their effects on the vehicle behaviour. The proposed approach allows the validation, tolerance and recovery from a fault condition of the product’s functionalities. Depending on the development phase of the vehicle, two different approaches are selected: In an early phase, starting from the failure rate of single components, the potential combined failure are calculated using Montecarlo approach with simplified models, in order to find out main interactions within component layout; In a second phase, vehicle system topology is reproduced in a Multiphysics simulation environment and the certain faults events (e.g. those highlighted as critical by previous steps) are injected in the system. Such approach is aimed to verify the consequences of the failure itself and develop and verify the functionality of mitigation strategies. Looking at model concept, the approach suggests the modification of typical “model identity cards” adding ports suitable to represent component state-of-function, which can be expressed either as Boolean or progressive variability of performances (e.g. 0 to 100 functionality); in practice, this means that parameters usually adopted to represent component static characteristics are modified as tunable parameters or even as variables. This allows to dynamically change component functionality during simulation itself. The case study presented – a 4 Wheel Drive (4WD) concept EV – has been used to estimate stopping distance with regular and degraded components; in particular, a parameter strongly influencing the results is the time delay needed for failure recognition, which depends partly on physical construction partly on software decisions (e.g. number of failure confirmation events needed to avoid false positives): in this way, the model can be adopted not
only to verify the effectiveness of mitigation strategies, but also for pre-calculate the time-delay that vehicle designer should adopt as target, to prevent the occurrence of dangerous events, thus being also a tool to better set up vehicle specifications and, thus, reducing development time.

The current activities propose the definition of a systematic methodology based on vFMEA approach and ISO 26262 standard specifications to evaluate and assess the actual and target Automotive Safety Integrity Level (ASIL) for the investigated brake functionalities related to complex vehicle architecture, due to the growing relevance of active stability ECUs and BW systems. This study aim at identify the major weakness of the brake plant and establish proper architecture modification or control strategy to fit the previously determined safety requirement. Results will reduce man-hour and cost of the Brake By-Wire (BBW) reliability analysis.

2. Proposed Methodology

The purpose of this activity concerns different aspects: ensuring braking performances of the EV and the BBW system reliability, as well as the availability of safety-related functionalities in which brake is involved, despite the operation of the various subsystems dealing with brake effort management (Electronic Braking Distributor (EBD), Anti-lock Braking System (ABS), Electronic Stability Program (ESP) or Automatic Emergency Braking (AEB)) and application (Brake Blending (BB)). At this purpose, while reducing time and cost effort, authors define a systematic model-based methodology, to implement vFMEA and FI analysis.

Developed reliability analysis solution consists of different phases:

(i) **SoA investigation**: an in-depth literature review is conducted, to identify the failure rate and distribution of the brake component.

(ii) **FMEA**: Failure Modes and Effects Analysis is executed on the target BBW components. This step aims to identify failure mode, causes and consequences of involved components. FMEA constitutes an essential methodology in the development process of a product, allowing reliable forecast and letting designer focus on most critical plant parts, assisting them in the application of the securing mechanism that should be implemented to fulfil minimum safety requirements.

(iii) **ISO 26262 guidelines application**: guidelines of the standards have been applied to the reference brake system, in order to evaluate target and actual ASIL, respect to the investigated plant functionalities.

(iv) **Simulation-based FI**: performed in a virtual simulation environment. This consist in the execution of controlled tests, where the behaviour of the EV is observed when one or more faults are triggered [15, 16]. In particular, FI is used to evaluate if the response of the system fulfils the specification when faults occur. ISO 26262 strongly recommends this procedure as a supporting tool to develop fault removal and prevention tasks. Also, the standard encourages the application of multi-level FI, redefining specific solution to increase system reliability and functional safety, to be applied during the whole development process. In this work, a double-level FI approach is used. Firstly, it is applied in the early stages of design, on a high-level abstracted model, to establish the most significant faults. Then, simulations are repeated on a more sophisticated model (developed in MATLAB Simulink), to evaluate the appropriateness of the supposed boundary condition, coherence with previous results and effectiveness of proposed securing solutions.

(v) **Securing Solutions**: finally, plant modification and securing strategy are proposed and implemented in the Simulink environment, to better understand the impact of them in brake system reliability and performance.
For a better understanding of the approach adopted in this activity, a flowchart of the proposed methodology is visible in Figure 1. Once the benchmark vehicle is chosen, physical and functional scheme of the corresponding BBW system is identified. Failure rates and probability distributions of the brake plant components are identified during the SoA review. Then, proceed with the analysis of the causes, modes and effects of the investigated faults.

This phase is fundamental in order to select most critical malfuncionalities and propose securing solutions. At this point, guidelines of ISO 26262 standard are applied to establish target ASIL and the FI simulation activities performed, to assess the plant reliability aspect, respect to specific functionalities. If the target ASIL is reached, the process ends: it can be state that the system fulfills standard specifications; otherwise, appropriate securing mechanisms are implemented in the vehicle models and simulations repeated, to confirm their effectiveness.

FMEA and FI techniques show strong similarities and share several common goals. Most relevant concerns the identification of the critical system faults. This purpose can be achieved by analyzing causes and effects trough FMEA process and observing their impact using FI. Also, both aim at the definition of those subsystems which require a securing mechanism, specifically addressed for diagnostic and mitigation of failures.

### Figure 1. Flowchart of the proposed methodology

#### 3. Benchmark Electric Vehicle

The procedure described in the previous section is applied to a reference Use Case (UC), represented in Figure 2. Investigated EV is a fully electric concept car developed by Valeo, equipped with 4 independent In-Wheel Motor (IWM)s. Main parameters of the benchmark vehicle are summarized in Table 1.

The investigated system involves several mechanical, electrical and electronic sub-components, belonging to different physical domains. Considering the following layout of Figure 3, based on a functional analysis of the scheme proposed in [17, 18, 19, 20], is possible to identify the following elements:

- **Brake Pedal Interface**: pedal position command is translated in a brake demand that is transferred to an Electronic Brake Control;
- **Electronic Brake Control**: It’s an underlying automation layer which produces an actuation reference according to brake demand, vehicle dynamics and other connected autonomous systems, implementing also active safety functionalities (EBD, ABS, ESP);
• Wheel Brake Control Unit: brake reference is actuated on the wheel, regardless of whatever the torque is applied by disc or electric motor. It includes Motor Control Unit (MCU) and BB controller.
• Electric Vehicle equipment: consisting of all the sub-systems of the vehicle, e.g. battery, Battery Management System (BMS), inverter, Electric Motor (EM), hydraulic brake plant.

This consideration allows a concept abstraction respect to the considered vehicle layout, to propose a flexible methodology which can effectively be applied to different powertrain architectures and UCs, allowing man-hour and cost reduction, thanks to the possibility to automatically adapt the proposed approach to several EV’s e-powertrain and brake system configurations.

The layout of Figure 3 is applicable. However, it should be considered the integration of a multiple braking actuation, in which the mechanical brake system is integrated with the electric one. This makes of the Battery Electric Vehicle (BEV) an over-actuated system from the braking functionalities aspects, offering opportunities to achieve increased ASIL, due to the redundancy of the brake plant. Indeed, enhanced brake plant reliability could be reached by the application of innovative BB strategies and the proposal of specific procedures for the vehicle securing, implemented thought control algorithms.

It is considered the integration in the system of a BB strategy, using the EV architecture represented in Figure 4: since each wheel has its independent braking and traction control unit, the brake blending system is integrated at the level of a single wheel. This is an example of lower-level integration which assures a higher level of redundancy, since the BB ECU failure affects only one wheel. On the other hand, specific securing procedures have to be implemented, to avoid undesired vehicle dynamics behaviour, such possible yaw moment generated by the differential braking between right and left tires.
Table 1. Main benchmark EV parameters

| Parameter                  | Symbol | Value [Unit] |
|----------------------------|--------|--------------|
| Mass                       | \(M_v\) | 1094.4 [kg] |
| Drive Range                | \(D_r\) | 280.8 [km]  |
| Acceleration (0-100 km/h)  | \(a_{0-100}\) | 11.96 [s]  |
| Speed (max)                | \(V_{max}\) | 140 [km/h] |
| E-Motor Power              | \(P\)  | 15x4 [kW]   |
| E-Motor Torque (max)       | \(T_{d_{max}}\) | 55 [Nm]    |
| E-Motor Voltage            | \(V_{nom}\) | 48 [V]     |
| Battery Capacity           | \(C_{nom}\) | 64 [Ah]    |
| Wheel Radius               | \(R_w\) | 0.292 [m]   |
| Front Track                | \(t_f\) | 1500 [mm]   |
| Rear Track                 | \(t_r\) | 1500 [mm]   |
| Front Wheelbase            | \(a\)  | 1056 [mm]   |
| Rear Wheelbase             | \(b\)  | 1056 [mm]   |
| CoG vertical distance      | \(h\)  | 375 [mm]    |
| Gear Ratio                 | \(G_r\) | 8 [/]       |

*CoG: Centre of Gravity

Our investigation focuses on this architecture, which is used only with the aim of the higher possible generality to 4WD architectures, allowing to implement the most innovative solution to increase vehicle reliability. Also, improved handling and stability performances respect to chassis dynamic behaviour could be reached, thanks to the possibility to execute advanced torque vectoring techniques, by independently controlling the torques provided to each wheel.

Figure 3. Reference BBW system layout
3.1. State-of-Art review

For this kind of generic BBW system, there are some sources in literature to be considered: works of Sinha et al. [22] simply introduce an analysis of the level of redundancy and reliability of ECUs and communication bus, to ensure the overall reliability requirements of the braking system. Respect to the investigated BBW plant layout of Figure 4, a preliminary SoA review is performed to find the appropriate fault distribution and Mean Time Between Failure (MTBF) for each of the brake system component.

Despite some tech data-sheet from Original Equipment Manufacturer (OEM)s suggest a bathtub rate distribution (e.g. Texas Instrument), authors suppose to consider only components in the fit region. So, the adoption a uniform distribution for the CUs is assumed, using the maximum value of failure rate of the fit region, which are summarized in Table 2.

3.2. Failure Mode and Effect Analysis

FMEA is a bottom-up failure identification systematic process, applied to the EV layout of Figure 4. It consist of several stages: plant decomposition in independent unit, identification of functionalities and interconnections between sub-systems and definition of modes and effects of the faults for each unit. This risk analysis is essential in order to identify major weakness of the BBW plant, letting designer to focus mainly on most critical elements and define appropriate securing strategy. FMEA methodology appear versatile and flexible, concerning single element or whole system faults. Output of this phase is the EV layout block diagram of Figure 5. It is assumed the presence of an additional CU, the Supervisor Controller, which superintends at the the securing strategy functionalities.

**Table 2.** Failure rate of different components used in our analysis

| Component       | Failure Rate $\lambda [1/h]$ |
|-----------------|------------------------------|
| Pedal sensor    | $1 \cdot 10^{-7}$            |
| Wheel speed sensor | $1 \cdot 10^{-7}$            |
| Pressure sensor | $5.69 \cdot 10^{-7}$          |
| ECU             | $5.88 \cdot 10^{-7}$          |
| Wires           | $1 \cdot 10^{-9}$             |
| CAN bus         | $2.58 \cdot 10^{-9}$          |
| Battery         | $2 \cdot 10^{-6}$             |
| Inverter        | $3.77 \cdot 10^{-7}$          |
FMEA of the whole EV BBW model components is summarized in Table 3, where a column is dedicated to the proposal of safety solutions that can be implemented. Also, specific fault mode and effect analysis have been applied to ABS functionalities. Reliability of this device depends not only by the proper operation of the single component but also by their integration: FMEA indeed considers all the existing interaction between the single plant’s elements (Table 4). For this analysis are considered only malfunctionalities related to E/E systems.

In particular, proposed solutions concern:

- **Fault prevention**: failure forecasting is done evaluating systems behaviour, respect to injection.
  - Qualitative evaluation: identification and classification of fault mode and/or combinations.
  - Quantitative/probabilistic evaluation: reliability measurements, such as Mean Time Between Fault (MTBF) or failure rate.
- **Fault tolerance**: integrating technique of management, detection, correction of fault and redundancy, in order to define fault-tolerant system architecture.
- **Fault removal**: aiming at reducing fault occurrences during the development stage. Consisting of a verification process which leads to the system’s weakness diagnosis, useful to investigate possible securing intervention.

![EV block diagram for the FMEA process](image)

**Figure 5.** EV block diagram for the FMEA process

### 3.3. ISO 26262

The management of safety-critical decision by the E/E system in automotive sector inevitably increase the complexity of the vehicle architectures. Indeed, risk of systematic and random hardware failure is greater. To assist designers at ensuring the highest safety standards and lead the development of safe automotive systems, specific regulations should be considered. The *ISO 26262 Road Vehicle - Functional Safety* series of standards [4] is the adaptation of IEC 61508 [21] to address the sector-specific needs of E/E systems within road vehicles.
| Component       | Failure mode | Effects                  | Causes                  | Securing solutions |
|-----------------|--------------|--------------------------|-------------------------|--------------------|
| Pedal unit      | Pedal failure| No pedal stroke          | Power supply failure    | Redundancy         |
|                 |              | No signal to EBD        | Sensor failure          |                    |
| EBD             | ECU failure  | No f/r allocation       | Power supply failure    | Redundancy         |
|                 |              | No signal to ESP        | Sensor failure          | Bypass EBD         |
| ESP             | ECU failure  | No lateral stability    | Power supply failure    | Redundancy         |
|                 |              | No signal to ABS        | Sensor failure          | Bypass ESP         |
| ABS             | ECU failure  | Wheels locking          | Power supply failure    | Redundancy         |
|                 |              | No signal to BB         | Sensor failure          | Bypass ABS         |
| BB              | ECU failure  | No regeneration         | Power supply failure    | Redundancy         |
|                 |              |                          | Sensor failure          | Bypass BB          |
| BMS             | ECU failure  | Overcharging            | Power supply failure    | Redundancy         |
|                 |              | Underdischarging        | Sensor failure          | Hydraulic braking  |
| MCU             | ECU failure  | No electric torque      | Power supply failure    | Redundancy         |
|                 |              |                          | Sensor failure          | Hydraulic braking  |
| HCU             | ECU failure  | No hydraulic torque     | Power supply failure    | Redundancy         |
|                 |              |                          | Sensor failure          |                    |

Table 4. FMEA of the ABS control unit

| Component | Failure mode       | Effects     | Causes                   | RPN  | Securing solutions |
|-----------|--------------------|-------------|--------------------------|------|--------------------|
| Sensors   | No signal          | ABS off     | Operative fault          | 18   | Redundancy         |
|           | Wrong signal       |             | Operative fault          | 96   | Warning light      |
| Wires     | No signal          | ABS off     | Short circuit             | 18   | Redundancy         |
|           | Wrong signal       |             | Disconnection             |      | Warning light      |
| ECU       | No signal          | ABS off     | Operative fault          | 108  | Redundancy         |
|           | Wrong diagnostic   |             | Software fault            |      | Warning light      |
|           | Wrong signal       |             | Software fault            |      |                    |

RPN: Risk Priority Number

This adaptation applies to all activities during the safety life-cycle of safety-related systems, comprised of electrical, electronic and software components. It provides methods and techniques which should be integrated into the development process to ensure the required functional safety level of E/E devices in road vehicles. In particular, it states the necessity to assist traditional reliability assessment solutions, e.g. FMEA, Failure Mode, Effect and Criticality Analysis (FMECA), Fault Tree Analysis (FTA) or Block Reliability Diagram (BRD) with FI strategy. ASIL of a specific fault modality can be determined through 3 parameters and its values ranging from QM (minimum) to D (maximum). ISO 26262 assist developers in the definition of Severity, Exposure and Controllability.

Severity is related to the level of risk for the users resulting from the fault occurrence. This value is established using the Abbreviated Injury Scale (AIS), developed by the Association for the Advancement of Automotive Medicine. Respect to these values, the standard provides a direct correspondence with a new scale ranging from S0 (min) to S3 (max).

Exposure is strictly dependent from the probability to be in a specific driving scenario, in which the fault could occur. All the operative condition should be considered, e.g. road condition.
and typology, weather condition or performed manoeuvres. In this work, both the table proposed by IEC 61508 and ISO 26262 are considered. Exposure value range from E0 (incredible) to E4 (high probability).

Controllability replicate the concepts of fault detection and reaction, indicating which amount of common driver (expressed in percentage) can manage and handle the considered fault event, in order to avert or minimize the extent of risk. Even in this case, the standard proposes a corresponding table, with values ranging from C0 (controllable in general) to C3 (less than 90% of drivers can handle the harm situation). This parameters could be mitigated by appropriate reports to the driver and diagnostic procedures (e.g. warning light on the dashboard).

Estimated ASIL target values for the E/E devices of the benchmark EV of Figure 5, in accordance with specifications provided by ISO 26262, are visible in Table 5 and Table 6, regarding respectively vehicle with human driver or ADAS. In the second case, values of Severity could be increased, since in those failure scenarios, where it is coherent to assume distracted passengers, the consequences could be more dangerous. Only for some failure modes is assumed a major Controllability, related to more sophisticated diagnostic procedures. Generally speaking, ADAS require higher ASIL, since the level of demanded automation is greater. For each scenario which result in ASIL>QM, one or more safety goal are formulated, which represent a safety requirement that should be achieved to avert the risk in dangerous situations. If quite similar safety goals are formulated for several events related to the same sub-component, they must be combined into a single security goal with the highest ASIL among those considered. In this activity, the evaluation of the coherence of the BBW system with the ISO 26262 specifications is performed, respect to the metric of the Random Hardware Failure Rate, whose requirements are those of Table 7.

3.4. Simulation Based Fault Injection

The Fault Injection (FI) [23, 24, 25], is defined as the reliability validation technique of fault-tolerant systems and consists in the execution of controlled experiments where the behavior is observed upon the introduction of one or more failures. The injection of faults aims to determine if the response of the system, in the presence of a defined set of faults, corresponds to the specifications. Lot of approaches for the analysis of the safety aspects of systems use this strategy for the validation of results obtained with static analysis of criticality, or for the study of the fault propagation. In particular, is useful to establish proper securing strategy, aiming at fault prevention and removal. Fault prevention solutions are typically based on statistical tests, which simulate distribution and rate of specific failure. Fault removal, instead, is based on functional modelling of the system. The introduction of FI in ISO 26262 [26] has renewed the interest in this methodology in the automotive sector. However, this well-established method

| Component | Severity | Exposure | Controllability | ASIL     |
|-----------|----------|----------|----------------|----------|
| Pedal CU  | S3       | E4       | C3             | D (max)  |
| EBD CU    | S2       | E4       | C2             | B        |
| ESP CU    | S3       | E3       | C3             | C        |
| ABS CU    | S3       | E3       | C3             | C        |
| BB CU     | S2       | E4       | C2             | B        |
| BMS CU    | S2       | E4       | C2             | B        |
| MCU       | S2       | E4       | C2             | B        |
| Hydraulic CU | S3   | E4       | C3             | D (max)  |
of verification is now used in different sectors. The standard motivated the adoption of newly solutions for the safety assessment of a product, redefining specific reliability concepts which should be applied during development phases, supporting conventional failure analysis methods. In particular, strongly recommend the usage of simulation-based FI techniques on model with a high level of physical abstraction, in order to identify errors in safety requirements management and propose appropriate securing strategy.

Developed simulation test campaigns consist of two different steps. In the first phase a recursive Montecarlo simulation campaign of a simplified vehicle model (high level of physical abstraction) is performed at high computational speed, considering the real value of component’s fault occurrences and probability distributions. The impact of several brake system failure modes in the vehicle stopping distance is evaluated, resulting in a quite similar reliable output. High integrity and safety levels of the brake system are involved to embed the current mechatronic system within a higher-level system, related to autonomous or assisted braking. In this stage, which components of the plant are more inclined to failure and/or had the major impact of vehicle braking performances can be established. A better understanding of those aspects allows the proposal of efficient and robust securing policies for fault prevention, which could be a useful tool for the achievement of target ASIL.

Then, once establish from the latter phase a specific number of dangerous scenarios respect to functional safety, Model-based simulation campaign of specific failure events are repeated using a more precise accurate vehicle model, from physical and functional point of view. This allows evaluating the appropriateness of the proposed approach and securing solutions, comparing result obtained at this stage and in the previous one and proposing fault removal solutions. Also, it consent to better identify causes and effects of failure, improving the knowledge of the mechanism of their occurrence and related impact on functional safety, used even to further increase the accuracy of the Montecarlo FI model. In both cases, the simulation environment involves 2 sub-models: Target system, which is the vehicle model; FI controller, consisting of a Fault Injector, which contains the vectors of possible fault and schedule their onset; the Fault Monitor, which detects malfunctions and communicates with the Supervisor controller.

### Table 6. ASIL target estimation for the EV (autonomous driving level greater than 2)

| Component  | Severity | Exposure | Controllability | ASIL |
|------------|----------|----------|-----------------|------|
| Pedal CU   | S3       | E3       | C2              | B    |
| EBD CU     | S3       | E4       | C2              | C    |
| ESP CU     | S3       | E3       | C2              | B    |
| ABS CU     | S3       | E3       | C3              | C    |
| BB CU      | S2       | E4       | C2              | B    |
| BMS CU     | S2       | E4       | C2              | B    |
| MCU        | S2       | E4       | C2              | B    |
| Hydraulic CU | S3   | E4       | C3              | D (max) |

### Table 7. ASIL target respect to Random Hardware Failure Rate

| ASIL | Failure Rate $\lambda[1/h]$ |
|------|-----------------------------|
| B    | $< 10^{-7}$                |
| C    | $< 10^{-7}$                |
| D    | $< 10^{-8}$                |
It is important to note that a delay is considered between the fault occurrences and its detection (Figure 6). This delay replicates the physiological lag of the communication channels (e.g. flooding of the CAN bus system) and time step interval (of 50 ms). Additional 300 ms time-out is supposed, in order to avoid false positive fault detection by the Supervisor controller, whose monitor the failure occurrences, turns on the warning light in the driver dashboard and triggers specific securing algorithms to start failure mitigation procedures.

Figure 6. Supposed delay between fault occurrences and confirmation

The reason behind the choice of this process is mainly referred to the necessity of reducing the simulation computational effort and time. vFMEA activities require the execution of billion recursive simulations to observe failure event, which are in the magnitude of $10^{-7} - 10^{-8}$ occurrences per hour. So, it is necessary to identify the system weakness in a shorter time and lower energy/cost consuming, in the optics of implementing fault mitigation solutions in the early phases of system and components design, evaluating also their effectiveness respect to functional safety requirements.

Concerning the specification given by the OBELICS project, developed model has the following characteristics:

- **Numerical efficient**: able to perform a large number of simulations, considering several combinations of faults and performances degradation in different operational conditions and scenarios. Real-Time (RT) implementation is required;

- **Simple and standardized**: models flexibility is ensured by proper scalability and portability properties, in order to be easily portable for different vehicle architecture and layout, as well as for different simulation environments and boundary conditions. Models are parametrized and modular, letting further modification in order to fit other UCs architecture’s specifications;

- **Robust and reliable**: respect to the physical abstraction, which in some cases can lead to complex dynamic behaviour that introduces further integration problems, especially when a fault occur.

### 3.4.1. Montecarlo Simulation

In this phase, each component of the investigated BBW system is abstracted by its primary functionality and considered as a simplified element [27], identified only by its own MTBF and fault distribution. Probability of fault occurrences is estimated from SoA, literature investigation, component and system data-sheet and proper technical considerations [16, 22, 28].

This abstraction concept, based on system BRD, is useful to implement an efficient and effective Montecarlo recursive study, aimed to establish the stopping distance of the vehicle when one or more component of the brake system experience fault situations. This probabilistic-based implementation, from the computational effort perspective, is designed to perform $10^3 - 10^{12}$ consecutive iteration, using a simple functional approach devoted to parallel computing (parallel pool and coded functions supported by MATLAB). This type of simulation is also suitable for numerically intensive implementation of GPU hardware, an ideal application for Hardware in the Loop (HiL) test method.
The Montecarlo simulation campaign is based on the vehicle dynamic equation, according to the simplified formula of the stopping distance calculation related to a braking manoeuvre (1):

\[ s = \frac{v_0^2}{2a} + v_0d \] (1)

Where \( s \) is the stopping distance expressed in meter, \( v_0 \) the initial vehicle speed in meter per second, \( a \) the acceleration in meter per square second and \( d \) the time delay in seconds.

The output of this test campaigns constitutes a preliminary supporting tool for the following model-based FI: the information arising from the Montecarlo simulations allows understanding the system weakness and to identify the specific plant components which mainly experience fails. At this point, it is possible to deeply study the select scenario, by their implementation in a more sophisticated simulation environment.

Considered fault event could be of 2 different types:

- **Boolean Fault**: the component can appear as completely healthy (ON) or dead (OFF). When a fault condition occur its functionalities are considered lost;
- **Derating Fault**: the component can be partially available, and its functionalities reduced in the magnitude order of a percentage.

### 3.4.2. Model-based Simulation

A more complete vehicle equipment model is implemented in the Simulink environment [17, 18, 19, 20] to assess the effect of the BBW E/E devices failure on the car vehicle behaviour. These models were previously developed in the ambit of the OBELICS activities. For this work, however, models have been modified to account fault effect by the introduction of FI controller, which allows supposing specific component failure.

The detailed FI model, developed in MATLAB Simulink environment (Figure 7), is designed for \( 10^6 - 10^9 \) iterative simulations and it is useful to evaluate the consequence of a fault or to validate expected results on a worst-case scenario, established in the previous step. This full vehicle equipment functional model consists in several sub-systems, belonging to quite different physical domains:

- **Driver**: which ensures the coherence with the reference manoeuvres through different Proportional Integrative Derivative (PID) controllers, respectively for traction, braking and steer commands.
- **Vehicle Chassis**: a 7 Degree of Freedom (DoF) model, consisting of many sub-systems, i.e. steering model (with Ackermann layout); 3 DoF body model in longitudinal, lateral and yaw directions; wheel models, which consider the tire-road interaction in accordance to Pacejka pure longitudinal slip equation [29], adding 1 DoF each.
- **Torque Regulation Controller**: comprising EBD, useful to ensure optimal front/rear torques allocation respect to longitudinal load transfer; ESP, for the lateral vehicle stability, based on hierarchical Moore-Penrose pseudo-inverse solution [20]; ABS and Anti-Slip Regulation (ASR) controllers, used to maintain wheel slips in proper bandwidth, during braking and traction phases; BB controller, which dispatches braking efforts to EM and hydraulic plant in function of the e-powertrain power availability.
- **Torque Actuation**: composed by the e-powertrain model (BMS, energy storage system, MCU and EM), replicating the ideal power-torque motor characteristics, and the hydraulic brake plant functional decomposition model [30].
- **Monitor**: to check the controllers status and to observe the vehicle dynamic behaviour when one or more faults occur.
The usage of these more accurate models is devoted mainly to confirm the coherence with the dynamic vehicle behaviour established during the Montecarlo methodology. Moreover, model-based simulations are useful also to endorse the achievement of target ASIL and evaluate the improvement permitted by plant modifications.

3.5. Securing Solutions

The proposal of securing solutions to be implemented in the vehicle model concerns the necessity to fulfill the minimum safety performances established from ISO 26262 perspective. Indeed, to reach target ASIL of Table 5, plant modifications and advanced control algorithm are required to fit functional safety level in accordance to the standard specifications. In relation to Figure 5, for the vehicle CU is assumed the presence of a redundant electronic controller, called Fail Silent Unit (FSU). Also an addition ECU, named Supervisor Controller is considered, whose task concerns the application of the securing strategy. Fault detection for ABS/ASR system is done in accordance of the logical scheme of Figure 8.

![Figure 7. EV simulation layout of the Simulink model](image)

![Figure 8. Proposed ABS fault detection and mitigation logic scheme](image)
When slip is above admitted value and the comparison between torque command, arising from upstream controllers, and output demanded signals is negligible, the fault is detected and confirmed after the time out interval, by turning on the warning light and bypassing ABS functionalities [15]. Other securing strategy, summarized in Table 4, are realized in analogy with this one.

4. Results and Discussions

In this section are summarized the result concerning the FI simulation campaign, obtained from the application of the proposed methodology to the benchmark EV, supposing different faults. Also, it assumes a specific fault of the CU related to anti-lock braking functionalities, whose simplified scheme is represented in Figure 9, in which are evident the interconnection within other BBW components. It is important to know that the proposed Supervisor Controller is able to perform diagnostic functions, turning off ABS system when errors are detected. This implemented securing strategy allows the application of braking torque to wheels, which, however, are not modulated to keep the slip in the admitted bandwidth.

![ABS functional decomposition scheme](image)

**Figure 9.** ABS functional decomposition scheme

For the purpose of this simulation campaigns, the boundary condition of the simulated tests is the one provided by ISO 21994:2007 [31]. This standard is related to the determination of the stopping distance in Straight line deceleration with ABS in open-loop test methodology, which should remain under 40 m for braking manoeuvres on good surface, starting from an initial speed of 100 km/h.

![Investigated reference manoeuvres](image)

**Figure 10.** Investigated reference manoeuvres

4.1. Montecarlo Simulation Campaign Results

In this kind of tests, different failures are supposed, whose specifications, respect to the BBW system layout of Figure 5, are summarized in Table 8, along with some parametric variable, useful to simulate different braking conditions (e.g. vehicle mass variation). For the E/E control units a redundant solution with FSU is suggested. This consideration is due to the high ASIL required. Results of the tests are in agreement with these assumptions, since the detection of the failure will result in acceptable stopping distance.
Consider the simulation results of Figure 11, which refers to the fault of ABS CU for a population of 100 millions of straight line deceleration event. These outcomes correspond to about 72 billion of operative hours of the brake system. This fact is due to that executed tests consider the failure rates of Table 8, which are expressed in terms of occurrences per hour, but the reference manoeuvre only lasts about 5 seconds, so between the rates there is a factor of 720, according to (2).

$$\lambda[1/h] = \lambda[1/3600s] = \lambda[1/5s] \cdot \frac{1}{720} \quad (2)$$

### Table 8. Investigated failure in the Montecarlo simulation campaign

| Sub-sytem                  | Failure   | Rate $\lambda$ [1/h] | Distribution | Parameters                      |
|---------------------------|-----------|----------------------|--------------|---------------------------------|
| Brake Pedal Interface     | ECU (D)   | $5.88 \cdot 10^{-7}$ | Uniform      | $a_{nom}; d_{nom}$              |
|                           | ECU (ND)  | $3.46 \cdot 10^{-13}$| Uniform      | $a_{min}; d_{max}$              |
|                           | CAN bus   | $5.69 \cdot 10^{-9}$ | Uniform      | $a_{min}; d_{max}$              |
|                           | ECU (D)   | $5.88 \cdot 10^{-7}$ | Uniform      | $a_{nom}; d_{nom}$              |
| Safety CU                 | ECU (ND)  | $3.46 \cdot 10^{-13}$| Uniform      | $a_{ABS}; d_{max}$              |
|                           | CAN bus   | $5.69 \cdot 10^{-9}$ | Uniform      | $a_{min}; d_{max}$              |
|                           | ECU (ND)  | $1 \cdot 10^{-7}$    | Uniform      | $3/4 \cdot a_{nom}; d_{nom}$    |
| Wheel Brake CU            | CAN bus   | $5.69 \cdot 10^{-9}$ | Uniform      | $a_{min}; d_{max}$              |
| Power Supply              | Unavailable| $3.77 \cdot 10^{-7}$ | Uniform      | $a_{min}; d_{max}$              |
| Load                      | Variation  | /                    | Normal       | $[0.8 \cdot a_{nom}; 1.2 \cdot a_{nom}]$ |
| Pad-Disc Friction         | Variation  | /                    | Normal       | $[0.8 \cdot a_{nom}; 1.2 \cdot a_{nom}]$ |
| Slope                     | Variation  | /                    | Normal       | $[0.95 \cdot a_{nom}; 1.05 \cdot a_{nom}]$ |

$a_{nom} = 9.81 m/s^2; d_{nom} = 0.005s; a_{min} = 0.1m/s^2; d_{max} = 0.035s; a_{ABS} = 8.05m/s^2$

D: detected; ND: not detected

In particular, Figure 11 shows how an additional control unit, the FSU, markedly improves braking performance, thanks to the presence of the redundant backup controller, which replaces the primary electronic regulator after the time-out (once fault is confirmed). In the case of a single CU instead, the intervention of the Supervisor Controller is needed, applying corresponding securing strategy.

### 4.2. Model-based FI Campaign Results

The braking manoeuvre [31] is repeated for the full vehicle model, supposing the fault occurrences of all the subsystems dealing with braking performances and BBW functionalities. In the model-based simulation are investigated the effect on vehicle behaviour of the securing strategy.

Output of Figure 12 shows wheel torques and slips in normal operative condition (left) and ABS control unit fault (right). In the second case the Supervisor Controller applies the securing solution of Figure 8. So, even in the extremely rare case of simultaneous failure of CU and FSU, is still possible to apply braking torques to the wheels. However, these ones are not properly modulated, so wheel locking occurs, resulting in an increased stopping distance (Table 9).

Making the vehicle replicate, for each investigated faults dealing with braking performances, the same manoeuvre allows to comparatively evaluate the effect on stopping distance related to the different fault mode and sub-systems. Stopping distances are visible in Table 9. Please note that the first two rows of the table refer to the full working vehicle stopping condition; the first one presents a stopping distance of 46.6m, which corresponds to an efficient vehicle braking on a medium-condition surface; while the second one presents a stopping distance of 39.3m,
Figure 11. Final stopping distance supposing and detected ABS CU failure without (left) and with FSU (right) during Montecarlo FI simulations.

Figure 12. Wheel torque (top) and slip (bottom) in normal operative condition (left) and fault condition (right) during Model-based FI simulations.
which corresponds to an efficient vehicle braking on a good-condition surface. All other rows are calculated assuming the same conditions expressed on the first row. For certain cases (e.g. failure of regenerative braking system), the distance increase is assumed to be almost negligible due to the simple mitigation strategy implemented (i.e. increment of mechanical braking torque request to compensate lost regenerative braking torque by the BB controller).

| Case               | Stopping Distance [m] | Maximum Deceleration [m/s²] |
|--------------------|-----------------------|----------------------------|
| Normal             | 46.6                  | 9.81                       |
| Normal (Best Case) | 39.3                  | 10.65                      |
| EBD Fault          | 50.6                  | 9.31                       |
| ABS Fault          | 57.1                  | 9.69                       |
| BB Fault           | 47.3                  | 9.88                       |
| BMS Fault          | 47.7                  | 9.84                       |
| EM Fault           | 49.6                  | 9.36                       |
| Hydraulic CU Fault | 72.6                  | 8.01                       |

5. Conclusions and Future Developments

Results of these tests, as already pointed out, concern several aspects:

(i) Definition of the actual Automotive Safety Integrity Level, respect to the investigated brake plant functionalities, summarized in Table 5 and Table 6;
(ii) Proposal of securing intervention, to let the system fulfil the ISO 26262 standard requirements, respect to brake functionalities;
(iii) Assessment of the procedure coherence and robustness with results arising from functional safety identification methodology, based on vFMEA and FI techniques.

The proposed vFMEA procedure has been applied to several components dealing with EV braking performances. Modified block able to support FI has been proposed and implemented on an existing MATLAB Simulink model, representing an electric vehicle equipped with four IWM and a conventional hydraulic braking system, integrated with BB policies. The model is useful to verify the consequences of the events considered more criytical and to verify the implications in terms of stopping distance, considering implemented securing strategy. Simulation campaing involves two environment: Montecarlo and Model-based solution.

In particular, respect to ABS functionality of benchmark vehicle, the simplified Montecarlo model provides quite reliable output (Figure 11), in accordance with the stopping distance of Table 9, identified during model-based simulation campaign.

The developed models include the possibility to vary parameters that are sensitive for final performance achievement, such as:

- Failure recognition delay (in this case, set to a total of 350 ms):
  - In real system, part of the delay is unavoidable since it depends on low level communications and physical signals measurements.
  - In both real and simulated system, an additional delay (time-out) has been implemented to represent the need to detect more than 1 single failure alarm to avoid “false positive”.
- Mitigation strategy: actions taken by the system to preserve minimum vehicle performances;
Very simple strategies, when possible, have been defined (e.g. brake blending modification in case of total or partial loss of regenerative braking torque).

The model is defined on the basis of “high level” representation, so real system topology is not reproduced. Typical examples are: redundant can-bus communication, here represented through the aggregated failure probability, based on BRD, but not through two data lines modeling; double microprocessor for operator + Supervisor Controller. Also, the inclusion of delay and “false positive” mitigation strategy are built in order to simplify implementation on embedded system taking into account the risk of communication limitations (e.g. CAN bus flooding) thus avoiding excessive data transmission rates on the communication lines.

In conclusion it can be stated that:

- A tool for the reliability assessment of a target Brake-By-Wire system has been developed, trough systematic Virtual Fault Mode and Effect Analysis methodology;
- Proposed solution, in accordance with ISO 26262 standard, adopts Fault Injection technique, applied on vehicle models with different level of detail, in order to let users scale the methodology, according to number and accuracy of desired results;
- Applied to the reference vehicle UC ABS system, allowed verifying the effectiveness of proposed securing solution (redundancy of E/E, application of fault mitigation strategy), making investigated system fulfill standard specifications respect to the random hardware failure metric (Table 7), which is in the order of $10^{-12}$ [1/h].

Possible future developments concern:

- The automation of the process, through the definition of modular library of fault and its variables;
- The extension of the study to other system and component of the automotive sector;
- The assessment of target ASIL respect to other evaluation metrics, e.g. Diagnostic Coverage, Single Point Fault, Latent Fault.

Acknowledgments
This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 769506. The information and views set out in this publication does not necessarily reflect the official opinion of the European Commission. Neither the European Union institutions and bodies nor any person acting on their behalf, may be held responsible for the use which may be made of the information contained therein.

References
[1] Martin H, Krammer M, Winkler B and Schwarzl C 2015 Model-based Engineering Workflow for Automotive Safety Concepts doi: 10.4271/2015-01-0273 pp 0273
[2] Yu L, Liu X, Xie Z and Chen Y 2016 Review of Brake-by-Wire System Used in Modern Passenger Car 18th International Conference on Advanced Vehicle Technologies; 13th International Conference on Design Education 3 (American Society of Mechanical Engineers, Charlotte North Carolina, USA)
[3] Martin H, Tschabuschnig K, Bridal O and Watzenig D 2017 Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges? Automated Driving: Safer and More Efficient Future Driving D. Watzenig, E. M. Horn and A. c. d. Cham, Eds., Springer
[4] International Electrotechnical Commission IEC 2018 ISO-26262 Road Vehicle – Functional Safety part 1-12
[5] Huang C, Naghdy F, Du H and Huang H 2019 Fault tolerant steer-by-wire systems: An overview Annual Reviews in Control 47 https://doi.org/10.1016/j.arcontrol.2019.04.001, pp 98–111
[6] Zulkifli SA, Asirvadam V S, Saad N, Aziz A R A and Mohideen A A M 2014 Implementation of electronic throttle-by-wire for a hybrid electric vehicle using National Instruments’ CompactRIO and LabVIEW Real-Time, 2014 5th International Conference on Intelligent and Advanced Systems (ICIAS), https://doi.org/10.1109/ICIAS.2014.6869555, pp 1–6
Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 217(3) pp 149–65

[28] Linzey G 1996 Development of the Electrical Wiring Interconnection System Risk Assessment Tool U.S. Department of Transportation Federal Aviation Administration

[29] Pacejka H 2005 Tire and Vehicle Dynamics Elsevier pp 657

[30] D’hondt T, Forrier B, Sarrazin M, Favilli T, Pugi L, Berzi L et al. 2020 Modeling and Identification of an Electric Vehicle Braking System: Thermal and Tribology Phenomena Assessment Available from: https://www.sae.org/content/2020-01-1094/ pp 2020-01–1094

[31] Technical Committee ISO/TC 22/SC 33 Vehicle dynamics and chassis components ISO 21994:2007 Passenger cars — Stopping distance at straight-line braking with ABS — Open-loop test method