SAE International

Functional Safety for Hybrid and Electric Vehicles

2012-01-0032
Published
04/16/2012

Sébastien Christiaens, Juergen Ogrzewalla and Stefan Pischinger
FEV GmbH

doi:10.4271/2012-01-0032

ABSTRACT

Hybrid and electric vehicles present a promising trade-off between the necessary reductions in emissions and fuel consumption, the improvement in driving pleasure and performance of today's and tomorrow's vehicles. These hybrid vehicles rely primarily on electronics for the control and the coordination of the different sub-systems or components. The number and complexity of the functions distributed over many control units is increasing in these vehicles. Functional safety, defined as absence of unacceptable risk due to the hazards caused by mal-function in the electric or electronic systems is becoming a key factor in the development of modern vehicles such as electric and hybrid vehicles. This important increase in functional safety-related issues has raised the need for the automotive industry to develop its own functional safety standard, ISO 26262.

The aim of the paper is to briefly introduce the ISO 26262 standard and the specific hazards associated with hybrid and electric vehicles. The paper will highlight how the risk-based approach of ISO 26262 can influence the safety integrity level of some safety related functions specific to hybrid and electric vehicles. It will also highlight how well established safety related functions, such as torque monitoring of a conventional internal combustion engine can be influenced through vehicle hybridization. A vehicle safety concept for the torque monitoring of an electric vehicle will then be presented. The results of the implementation of this functional safety concept in an electric vehicle developed by the company FEV GmbH will be shown as example. The first measurements made in the vehicle show that the monitoring concept fulfills the reaction time requirement to ensure that unintended torque increase do not lead to uncontrollable vehicle acceleration.

INTRODUCTION

Functional safety, through the introduction of ISO 26262, as well as Battery Electric Vehicles (BEVs) and Hybrid Electric Vehicles (HEVs) are key issues for future automobile development. This paper presents some preliminary results of the application of the ISO 26262 standard to systems in hybrid and electric vehicles.

The paper will first briefly introduce hybrid and electric vehicles. Functional safety and the ISO 26262 standard will then be presented. The second part of the paper will focus on some particular aspects of the ISO 26262 hazard and risk analysis applied to systems in hybrid and electric vehicles. Finally, the last part of the paper will introduce a practical example of the concept phase of ISO 26262 applied to the torque monitoring of an electric vehicle.

HYBRID AND ELECTRIC VEHICLES

BEVs, HEVs, Plug-in Hybrid Electric Vehicles (PHEVs), Extended-Range Electric Vehicles (EREVs); are all terms that are becoming more familiar thanks to the increasing introduction of such vehicles into the automotive market. The concept of a hybrid or electric vehicle is about as old as the automotive industry itself, but in the recent years, more hybrid cars have taken the road as the development of this technology moves ahead. HEVs or BEVs are indeed seen as a promising trade-off between the necessary reductions in emissions and fuel consumption and the ever increasing demand for driving pleasure and vehicle performance. The green image associated to these vehicles is also a strong marketing argument leading to the rapid increase in the use of these terms in the automotive sector.

Basically, a hybrid vehicle is defined as a vehicle using at least two different energy sources for its propulsion. For

example, HEV's use the electrical energy stored in a battery to power an electric machine and the energy contained in fossil fuel to feed an Internal Combustion Engine (ICE). The electric machine and the ICE can be combined in different ways to propel the vehicle, as illustrated in Figure 1. If the battery of the vehicle can be externally charged from the main power grid, the vehicle is called a "plug-in". If a BEV has a second on-board energy source which is only used to keep the battery state of charge at a constant minimal level to extend its all electric range and not to propel it, it is called an Extended-Range Electric Vehicle (EREV), or "range extender"

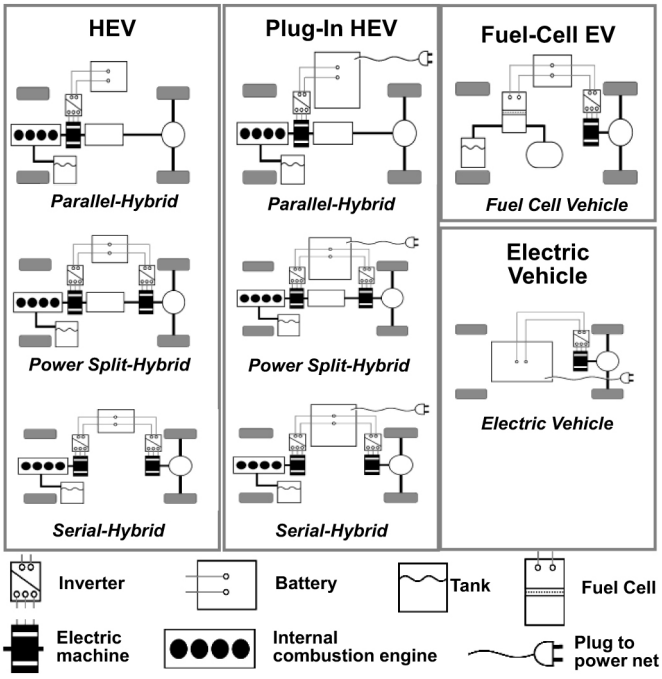

Figure 1. Typical HEV and BEV Topologies

These hybrid vehicles rely extensively on electronics for the control and coordination of the various sub-systems or components. The number and complexity of distributed functions over many control units is increasing.

FUNCTIONAL SAFETY

This trend of increasing complexity and distributed functionality makes safety one of the key issues of future automotive development. Functional safety, defined as the absence of unacceptable risk due to hazards caused by mal-functioning of electric or electronic systems is then becoming a key factor in the development of modern vehicles, such as HEVs and BEVs. Therefore, functional safety is a vehicle property, rather than an application domain and it applies to every function implemented via any electric or electronic component, independently from the application domain. Functional safety applies to all automotive areas, not only to HEVs and BEVs but also goes far beyond the scope of automotive safety related functions, such as ABS, ESP and the Airbag. It also covers functionalities such as driver assistance, vehicle dynamics, lightning, throttle control, active damping and gearbox actuation.

ISO 26262

This important increase in functional safety related issues has raised the need for the automotive industry to develop its own functional safety standard (ISO26262). ISO 26262 standard is based upon IEC 61508, the stand-alone functional safety norm, which is the mother of many sector-specific norms. ISO 26262 addresses the specific needs of the automotive domain, while IEC 61508 originated from the process and automation industry. Functional safety takes into account all hazards caused by mal-functioning behavior of electric or electronic systems, regarding specification, implementation or realization errors - failure during operation period - reasonably and foreseeable operational errors, as well as - reasonable and foreseeable misuse. Therefore, ISO 26262 defines a safety lifecycle [1] covering the typical automotive project development lifecycle, as illustrated in Figure 2.

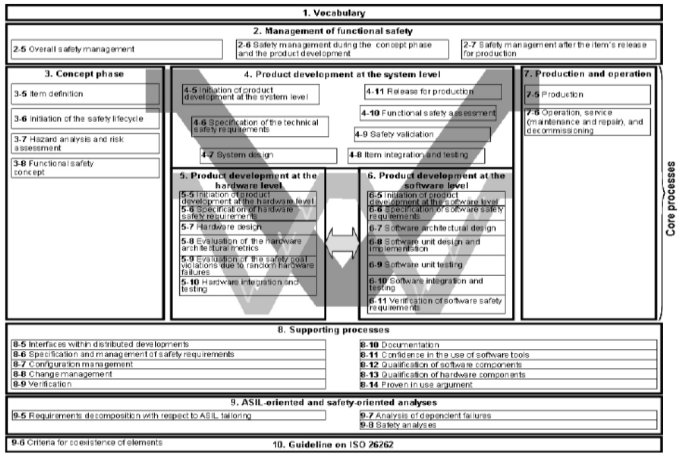

Figure 2. ISO 26262 Safety Lifecycle [1]

The safety lifecycle, defined by ISO 26262, is based upon a "V-Model" that covers the different phases of product development such as concept, system design, hardware and software design phases, production and operation until disposal and decommissioning. As both random and systematic failures are addressed in ISO 26262, it also defines a number of safety measures at the management of functional safety level and some supporting processes, such as change management, versioning and documentation.

A risk based approach

For liability issues, ISO 26262 has kept the same risk-based approach as IEC 61508. In order to assess the risks associated with the item (i.e. *system or array of systems or a function to which ISO 26262 is applied* [1]) and then to define the necessary requirements for the item, such that unreasonable

risk is avoided, the operational situations and operating modes in which the item's malfunctioning behavior is able to trigger the related hazards shall be identified and analyzed.

The combination of a hazard and an operational situation is defined as a hazardous event [1]. These hazardous events, together with the severity of their potential consequences are the necessary inputs for the risk assessment defined in ISO 26262.

The standard defines four classes for the probability of exposure of each operational situation. These four classes are illustrated in Table 1.

Table 1. Classes of Probability of Exposure Regarding Operational Situations [2]

Classes	Description
E0	Incredible
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

The difference in probability from one class to the next is an order of magnitude. Additional informative examples about typical driving situations for each of the above mentioned classes are provided in the standard [2].

It is important to notice that the exposure determination is based on a representative sample of customers for the target market, and the number of vehicles equipped with the item shall not be considered when estimating this probability of exposure [2]. This means that the probability of exposure of one driving situation is the same for both conventional and HEVs or BEVs, even if the number of HEVs or BEVs driving on the public roads is many orders of magnitude lower than that of conventional vehicles.

The second factor to be assessed during the risk analysis is the controllability. Controllability is defined as the possibility of avoidance of the specified harm or damage through the timely reactions of the persons involved [1]. It may be the driver or any other endangered person such as a pedestrian, a cyclist or the driver of any other endangered vehicle that could provide the control. The controllability is represented by the parameter C, as shown in Table 2.

Table 2. Classes of Controllability [2]

Classes	Description
C0	Controllable in general
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

Once again, please refer to the standard [2] for more information about typical examples for each of the classes mentioned above.

The last factor to take into account in order to assess the risks associated to the item is the severity of the potential harm of each hazardous event. It focuses on the harm of the endangered person, may it be the driver or any other endangered road participant. The severity is represented by the factor S, as shown in Table 3.

Table 3. Classes of Severity [2]

Classes	Description
S0	No injuries
S1	Light and moderate injuries
S2	Severe and life-threatening injuries (survival probable)
S3	Life-threatening injuries (survival uncertain), fatal injuries

Informative examples of different types of severity and accidents, as well as a relationship to the Abbreviated Injury Scale (AIS) can also be found in the standard [2].

The risk (a combination of the probability of occurrence of the harm and severity of that harm) is assessed by determining, for each hazardous event, the three factors mentioned above: Exposure, Controllability and Severity. These factors are then combined with each other according to the table given in Figure 3.

The ASIL (Automotive Safety Integrity Level) obtained at the end of this analysis falls into one of four classes to specify the item's necessary safety requirements for achieving an acceptable residual risk with D representing the highest and A the lowest class. All of the normative sections of ISO 26262 have an ASIL dependency. The aim of implementing the ASIL is to introduce measures for sufficient avoidance of systematic failures and implement sufficient measures to mitigate risks from random hardware failures to acceptable levels.

As a subjective methodology, this risk assessment step requires some expertise in order not to end-up with over dimensioned safety specifications and to keep a level of standardization in functionalities common to many different vehicles (and very often provided by the same supplier).

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 3. Risk Graph of ISO 26262

FUNCTIONAL SAFETY FOR HYBRID AND ELECTRIC VEHICLES

This Section introduces some specific hazards of hybrid and electric vehicles, as well as discusses how the risk based approach of ISO 26262 can influence the safety integrity level of some safety related functions specific to hybrid and electric vehicles. It will also highlight how well established safety related functions, such as torque monitoring of a conventional internal combustion engine can be influenced by vehicle hybridization.

HAZARD IDENTIFICATION

One of the very first steps in the concept phase for the development of safety related functionality, according to ISO 26262, is hazard identification. Once the item has been defined with regard to its functionality, interfaces, environmental conditions and legal requirements, the hazards associated with the item can be identified and then classified.

The potential sources of harm, i.e. the hazards, for a HEV or a BEV can be classified according to their type (electrical, chemical, functional, etc.) as shown in Table 4. The hazards listed on the right column of Table 4 are described both by their origin and their potential consequences, shown in parentheses.

Table 4. Examples of Hazards for HEVs and BEVs

Type of hazards	Hazards
Electrical	Direct contact with live parts (electrical shock)
	Indirect contact with live parts, i.e. due to electrical equipment parts which become live under fault conditions (electrical shock)
	Arcing (burn, fire, projection of molten particles)
	Electromagnetic phenomena (effects on medical implants)
	Overload (fire)
	Short-circuit (fire, burn, projection of molten particles)
Thermal	Thermal runaway of battery (explosion, burn, fire)
	Radiation from heat sources (burn)
Chemical	Release of gaseous toxic substances (breathing difficulties, suffocation, poisoning)
	Release of liquid toxic substances (burn, damage to eyes and skin)
	Release of flammable substances (fire, explosion due to external ignition source)
Functional	Unintended vehicle acceleration (run-over pedestrian, crash with infrastructure or other vehicle)
	Unintended vehicle deceleration (crash with infrastructure or other vehicle)
	Unintended acceleration from standstill or low vehicle speed in wrong direction (run-over pedestrian, crash with infrastructure or other vehicle)
	Unexpected rotation of accessible elements (crushing, entanglement due to unexpected restart of ICE during service)

The hazards which are caused by malfunctioning behavior of Electric/Electronic (E/E) safety-related systems are the basis for the risk assessment and for the ASIL and safety goal determination step of ISO 26262.

RISK ANALYSIS

Once the item has been defined and the associated hazards identified, the risk analysis introduced in the chapter about ISO 26262 can then be conducted. We assume here that the item is a BEV powertrain, equipped with a 30kW electric machine (Figure 4).

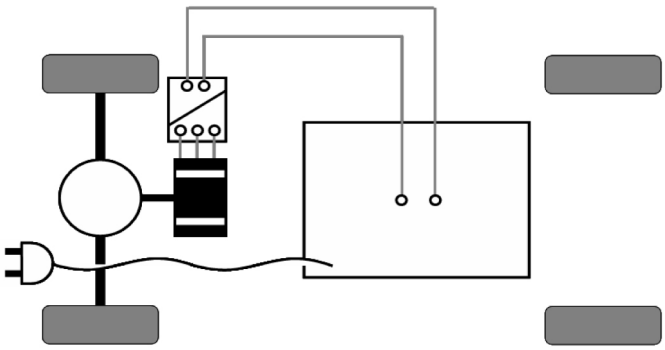

Figure 4. Example of BEV powertrain

The electric machine can produce torque in both directions, i.e. it can accelerate and decelerate the vehicle. Therefore, a potential hazard exists for unintended vehicle deceleration, due to a malfunction of the e-machine control. This may lead to sudden vehicle braking and then to a crash with the surrounding infrastructure or another vehicle. We will further assume the vehicle is driving around 100km/h on a secondary road with dense traffic. The drivers involved are supposed to possess a driver's license, be sufficiently aware of their surrounding and fit to be able to drive a vehicle on public roads. However, like the average driver, they are not trained to handle critical situations. The risk analysis for such a case may give the following results:

1. Frequency of exposure: E4. This driving situation can potentially happen each time the vehicle is driven

2. Controllability: C2. The vehicle will decelerate, but may remain stable as only the front wheels are braking the vehicle. In addition, the drivers behind may react in time and brake when they see the distance to the vehicle in front of them is decreasing, even if the brake lights are not on.

3. Severity: S2. Such an accident may end up with severe and life-threatening injuries (survival probable) as the speed difference between the two vehicles may be kept low thanks to the reaction of the driver behind.

The ASIL of this function is then ASIL B and a possible safety goal may be to: “Prevent unintended vehicle deceleration or keep it to a controllable level, ASIL B.”

If we now assume that the e-machine is not connected to the front wheels of the vehicle, but rather to the rear wheels, the risk analysis may be modified as follows:

1. Frequency of exposure: E4. This driving situation can potentially happen each time the vehicle is driven

2. Controllability: C3. The vehicle will decelerate, but may not remain stable, as only the rear wheels are braking the vehicle. The drivers behind may still react in time when they see the distance to the vehicle in front of them is decreasing, even if the brake lights are not on. However, they may not be able to react correctly if the vehicle in front of them starts spinning around.

3. Severity: S2. Such an accident may end up with severe and life-threatening injuries (survival probable) as the speed difference between the two vehicles may be kept low thanks to the reaction of the driver behind.

The ASIL of the same function for a similar vehicle with a different powertrain layout is then, in this case, an ASIL C.

If we now assume that the e-machine power is not 30kW, but 100kW. This electric machine obviously has the ability to produce an even higher braking torque than the 30kW e-machine and this may lead to even higher vehicle deceleration. The time left for the driver of the following vehicle to react is then even shorter and the speed difference between the two vehicles may be even higher in case of a crash. This leads to a possible increase in the severity of the hazardous event and the risk analysis may then identify an ASIL C or D for the same function according to the powertrain layout.

Unintended acceleration is a potential hazard, which is well known in the automotive industry. This hazard appeared due to the introduction of the electronic accelerator pedal, which replaced the mechanical link between the pedal and the engine by an electrical signal flowing from the accelerator pedal to the engine throttle and is controlled by the Engine Management System (EMS). This “drive-by-wire” system is now the state of the art in the automotive industry thanks to the development of recommended practices or OEM standards, such as the EGAS safety concept [3]. On the other hand, the hazard “Unintended and uncontrollable vehicle deceleration” is possible with BEVs and HEVs, because the electric machine can produce torque in both directions.

Another important hazard for HEVs and BEVs is related to the explosion of the high voltage battery. This crucial component is monitored by a dedicated control unit, the Battery Management System (BMS). The primary aim of the BMS is to prevent the battery from operating in an unsafe area. The risk analysis for the hazard “Thermal runaway of the battery” could provide the following results.

1. Frequency of exposure: E4. The driver is potentially exposed to this hazard in any vehicle operating situation.

2. Controllability: C3. It will be very difficult and, perhaps, nearly impossible for the driver to react in time to avoid the harm due to a battery explosion, because they will not even

notice that the battery is operating in an operating region before it explodes.

3. Severity: S2. Such a hazardous event may end up with severe and life-threatening injuries (survival probable) depending on the battery type and installation in the vehicle.

The ASIL of this function is then ASIL C and a possible safety goal may be: "An overvoltage / over temperature of the Electrical Energy Storage System (EESS) shall be prevented, ASIL C."

This example can be used to illustrate another particularity of HEVs and BEVs regarding functional safety. In conventional vehicles, it is often possible to decrease the risks associated with a hazardous event thanks to the controllability factor. Indeed, many of the safety related functions of conventional vehicles have a (in)direct influence on vehicle behavior (drive-by-wire, active steering, active suspension, etc.) or have a noticeable consequence at the vehicle level (lights are suddenly turned off during night driving, seat adjustment is suddenly moving, etc.) and the driver can then take timely reactions to decrease the possible harm. In HEVs and BEVs, many of the hazards associated to the EESS are uncontrollable as they are caused by internal failures that are undetectable for the driver, such as over temperature, over voltage or an internal short-circuit. This leads to a controllability factor of C3 (Difficult to control or uncontrollable) and to a relatively high ASIL for these functions. This remark is even more obvious when the hazard happens during vehicle charging. In this case, the vehicles are left active and charging, most of the time, without anybody to control the charging process. The hazards occurring during charging are then also very often uncontrollable and the related safety goals typically inherits a relatively high ASIL.

The fact that the BEVs and the PHEVs can be connected to the grid to recharge their batteries also implies that, at least the BMS, has a higher operating time than a controller used in conventional vehicle or which would be only used during driving. Indeed, the time during which the battery of a PHEV is being charged over the grid to recharge the battery can be up to 3 to 4 times longer than the time the vehicle is being driven. A typical operating time for an automotive control unit is about 5000 to 10000 hours. This time will easily reach 20000 hours or more for the controllers of PHEVs, which are active both during driving and charging, as a part of the BMS. ISO 26262 aims at preventing a violation of safety goals, due to both systematic failures and random hardware failures. In order to give guidance about how to cope with random hardware failures, ISO 26262 defines informative random hardware failure target values, depending on the ASIL of the safety goal [4]. The safety engineer should then bear in mind this difference in operating time of some BEVs and PHEVs controllers and shall then adjust these target values accordingly.

SAFETY CONCEPT

In order to comply with the safety goals, the basic safety requirements shall be identified and allocated to the elements of the vehicle. This is the aim of the safety concept phase defined in ISO 26262. A PHEV powertrain example is illustrated in Figure 5.

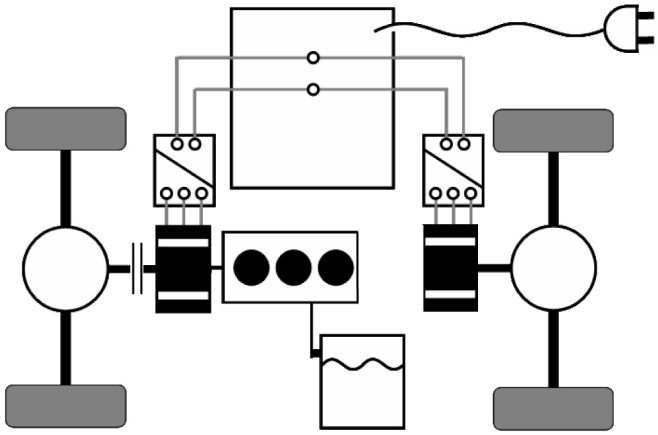

Figure 5. PHEV Powertrain Example

In this vehicle, the ICE and one e-machine are connected to the front wheels. A second e-machine is connected to the rear wheels. The ICE and the front e-machine can either be used as a range extender module, charging the battery, when the clutch is open, or as an additional propulsion source when the clutch is closed. If the vehicle is driving with the clutch closed, it is possible to request more torque to the ICE in order to both charge the battery over the front e-machine and propel the vehicle using the additional torque produced by the ICE. In order to avoid unintended vehicle acceleration or deceleration, a possible safety concept would be to define, the maximum and minimum wheel torques allowed, based on the vehicle speed and the accelerator pedal position. These maximum and minimum wheel torques can then be split and sent to the different control units that are controlling the ICE and both e-machines as target boundaries for their actual torque.

The main torque safety related functionalities, as well as the monitoring functions for the relevant control units could be summarized as illustrated in Table 5 and in Table 6.

Table 5. Example of Torque Safety Related Functions for HEV Control Units

Control unit	Safety related functions
Vehicle Control Unit (VCU)	Driver interpretation based on accelerator and brake pedal, cruise control
	Torque split between ICE and e-machines
	Sending of torque requests to EMS and MCU
	Torque coordination and driveability functionalities
	Clutch control
e-machine control unit (MCU)	Control of e-machine torque, speed, voltage
Engine Management System (EMS)	Control of ICE torque
Transmission Control Unit (TCU)	Control of gear actuation
	Sending of torque or speed requests during shift

Table 6. Example of Torque Safety Related Monitoring Functions for HEV Control Units

Control unit	Monitoring functions
Vehicle Control Unit (VCU)	Monitoring of total wheel torque against maximum and minimum limits
	Monitoring of actual clutch position (open/closed)
	Plausibility check of torque requests sent to other control units
	Coordinate vehicle reaction in case of error detected by a monitoring function
e-machine control unit (MCU)	Monitoring of e-machine torque against request from VCU
	Plausibility check of relevant data sent to other control units
Engine Management System (EMS)	Monitoring of ICE torque against request from VCU
	Plausibility check of relevant data sent to other control units
Transmission Control Unit (TCU)	Monitoring of actual gear against request from VCU
	Plausibility check of relevant data sent to other control units

The main hazard for conventional vehicles is linked to unintended and uncontrollable vehicle acceleration, as the ICE produces torque mainly in one direction, i.e. to accelerate the vehicle. The monitoring concepts, such as the EGAS, primarily ensure that the torque actually produced by the ICE is not higher than the torque requested by the driver. If the torque produced would be lower than the torque requested by the driver, due to misfire or any other malfunction, the safety monitoring system would either not detect it or would ignore it.

In the application discussed above, the monitoring of the minimum torque produced by the ICE is more important. Indeed, if the ICE cannot ensure that the actual torque meets the minimum torque limit, this could lead to an unbalanced torque distribution between the ICE, the e-machine acting as a generator and the transmission output to the wheels. In some situations, this could even lead to unintended braking of the vehicle if the torque produced by the ICE is not high enough to compensate for the torque generated by the e-machine. In addition, the safe state implemented in the EMS of the ICE for conventional vehicles in case the torque produced by the engine does not match the torque request is to turn off the injection and close the throttle. It then uses the engine drag torque to slow the vehicle down. But in the situation discussed above, this same error reaction would even increase the problem, as the torque produced by the ICE is already too low, it would not solve the problem to turn it off.

In HEVs, it is possible to compensate for the torque loss from the ICE by acting on the torque request to the e-machine(s) in order to ensure that the wheel torque stays within the allowable limits. This error reaction is coordinated at the vehicle level, between different control units, increasing its complexity, and highlighting once again the importance of functional safety aspects as addressed in ISO 26262.

PRACTICAL EXAMPLE

Recently, FEV GmbH converted a fleet of conventional 3-door hatchback Fiat 500 vehicles into electric vehicles. The electric vehicles use a 45 kW permanent magnet e-machine connected to the vehicle's front wheels through a single reduction gearbox. The battery is a 12kWh Li-Ion battery mounted under the floor. The powertrain layout is similar to the one shown in Figure 4.

The risk analysis carried-out at the beginning of the project showed that the safety goal “Prevent unintended vehicle acceleration or keep it to a controllable level” should have an ASIL B. The safety goal “Prevent unintended vehicle acceleration in te wrong direction or keep it to a controllable level” should have an ASIL A. It was decided to develop a safety concept that does not rely on the MCU, but rather on the VCU and the BMS. The software of the VCU and both the hardware and the software of the BMS were developed by FEV GmbH. In addition, the information received from the MCU and e-machine supplier showed that the MCU was not developed to reach an ASIL B. It was not possible, within the project time frame to have it modified.

Three monitoring concepts were identified at the beginning of the concept phase:

1. Monitoring the Direct Current (DC) flowing to the MCU
2. Monitoring vehicle acceleration
3. Monitoring powertrain torque

Some general advantages and disadvantages of these three monitoring concepts are summarized in Table 7

Table 7. Advantages and Disadvantages of the Three Monitoring Concepts

Monitoring method 1 (MCU current)	
Advantages	- Fast reaction time possible (small vehicle movement)
Disadvantages	- Current sensor cost if additional sensor is needed. - Difficult to monitor during precharge of the HV network (torque produced during current flow for precharge) - For hybrid vehicles: relies on EMS EGAS safety (can only detect e-machine failures) - Rest-current of e-machine controller (current consumption without generating torque) must be taken into account - Not easy to take e-machine demagnetization into account (lower acceleration than expected)
Monitoring method 2 (Vehicle‘s acceleration)	
Advantages	- Sensor already used for safety applications (ESP, etc.) - Can detect wrong rotating direction - Can be applied to hybrid vehicles
Disadvantages	- Slow reaction time in case of standing vehicle - Problems during down and uphill + influence of vehicle‘s weight. - Can only be implemented if wheels speeds signals are available (and safe) - Big calibration effort (uphill + vehicle mass changes)
Monitoring method 3 (Powertrain torque)	
Advantages	- Fast reaction time (small vehicle movement) - Can detect wrong rotating direction
Disadvantages	- Sensors unusual in automotive applications - Sensor cost for reliable / precise measurement - Must be located on e-machine shaft (not always possible) - For Hybrid vehicles, many sensors may be needed or relies on EMS EGAS

These three monitoring concepts were then compared with each other considering various technical, quality, timing and cost aspects. Concerning functional safety, the technical and quality aspects are obviously the most important, as they reflect the ability of the monitoring concept to reach the necessary ASIL. Nevertheless, timing and costs aspects cannot be totally ignored for an overall successful project. That is the reason why they were also included in this analysis.

In order to be able to make a monitoring concept decision that was the best for this project, the priority of the aspects mentioned above had to be compared against each other. This comparison was defined by a number of experts, and the weight factors summarized Table 8 were obtained.

Table 8. Weights of the Selection Criteria

	Weight Factor
Technical aspects	**5.5**
Reaction time	5
Reuse (in HEV)	0
Feasibility (electrical aspects)	7
Feasibility (mechanical aspects)	8
Possibility to detect higher acceleration (or deceleration) than requested	7
Possibility to detect lower acceleration (or deceleration) than requested	6
Quality aspects	**9.5**
Maturity level (i.e. quality of the necessary components)	7
Reliability of the necessary components (i.e. random hardware failure rate)	12
Timing aspects	**3.67**
Part availability	8
Development time	2
Calibration time	1
Cost aspects	**7.5**
Cost (parts)	7
Cost (development)	8

The three monitoring concepts were then given a rating from 0 to 9 for all of the criteria listed above. A rating of 0 means that the monitoring concept is not suited for this criterion and that, the goal will not be reached. A rating of 9 means that the

safety concept is perfectly suited for this criterion and will undoubtedly reach the goal. The concept with the higher weighted total was then selected as the optimal monitoring concept for the project.

The result of this preliminary analysis showed that, for this project, the monitoring concept using the DC current flowing to the electric machine was best suited, mainly due to the high parts availability, relatively low cost and fast reaction time. The disadvantages identified in Table 7 could either be solved by other technical measures or accepted, because their weighting for this particular project was not very high.

For example, the fact that this monitoring concept could not fulfill the safety goal during the precharge phase of the HV network could be solved by implementing a precharge monitoring function on the BMS. Indeed, just after closing the main battery relays, the BMS monitors the current flowing to the HV network in the various capacitors and can react if the actual current flow and the voltage rise do not match a predefined pattern. If current would flow to propel the vehicle during this phase (or anywhere else), the BMS would detect it and would abort the precharge by immediately opening the main relays. This would ensure that the vehicle remains in a safe state.

Another identified disadvantage was that this monitoring concept could not easily be used in a HEV, because it only monitors whether the torque produced by the e-machine corresponds to the requested torque. It cannot take other power sources such as an ICE into account and still relies on monitoring functions, such as the EGAS monitoring, of the ICE implemented in EMS. Such a monitoring concept is well known and will need to be adapted to the specific needs of HEVs, that's why this disadvantage was not seen as critical.

The last main disadvantage of this monitoring concept is the fact that it is not able to reliably detect if the e-machine is demagnetized (only valid for permanent magnet e-machine, such as the one used in the project) and thus producing less torque than it actually should with the actual current flow. This disadvantage was also accepted for two reasons. First, this demagnetization of the rotor of the permanent magnet e-machines occurs at temperature level (about 190°C) which is much higher than the normal operating temperature of the e-machine (about 80°C). In order to ensure that the demagnetization temperature will not be reached, even in case of cooling circuit failure, some driving tests were conducted in the vehicle and the cooling of the e-machine was by-passed. The test results showed that the e-machine used is relatively large compared to its power output. The increase in rotor temperature, even without liquid cooling will not cause rotor demagnetization, even under aggressive driving. The fact is that the all-electric range of the vehicle is limited by the battery energy and that the time during which the vehicle can be driven aggressively is low enough that it will also help to avoid rotor demagnetization. The second reason why this disadvantage can be accepted is that the MCU monitors the rotor and stator temperatures and the available torque is decreased as the e-machine temperature increases. In addition, the VCU also monitors the coolant temperature and the requested torque is decreased when the coolant temperature becomes too high.

Once the general monitoring concept was defined, with the preliminary architectural assumptions, the functional safety concept, as defined in ISO 26262 could be detailed. The functional safety concept addresses, aspects such as fault detection and fault mitigation, transition to a safe state and arbitration logic to select the most appropriate reaction in case of multiple requests [2]. In this concept, the safe state was to ensure that the e-machine is not able to generate any torque, i.e. that no current can flow from or to the e-machine. This was realized by opening the main relays of the HV battery. The necessary reaction time was defined according to FEV's internal rules for vehicle reaction tests. The reaction time in the case of unintended vehicle acceleration depends on the average level of the acceleration, allowing a longer reaction time if the unintended acceleration is kept to a controllable level.

In order to mitigate the possible latent faults, a hierarchical approach between the VCU and the BMS and their respective safety functions was followed to define the functional safety concept. This also allows reducing the possible systematic failures, as the development teams of these two control units were different.

The implemented torque safety concept is ensured at three levels; the first level, the function level is covered by the VCU. The main functions of this level include the following:

- Calculate the driver's torque request based on the accelerator pedal position, vehicle speed, available power from the battery, driver's gear request and actual limitations
- Decide to follow or not follow the driver direction request, based on the vehicle speed and then send the e-machine direction request to the MCU

The second level, the functional monitoring level is covered by both VCU and BMS. The main VCU functions of this level include the following:

- Plausibility check of the accelerator pedal position based on a redundant analog signal
- Plausibility check of the vehicle speed signal based on the 4-wheel speed signals, the transmission speed and the e-machine speed
- Minimum and maximum plausibility check of the VCU torque request, based on vehicle speed, accelerator pedal position, driving direction, power limitations, etc.

• Plausibility check of the actual e-machine torque based on both e-machine torque feed-back and DC current drawn by e-machine. This actual torque is compared with the requested torque.

The BMS main functions of this level are:
• Minimum and maximum plausibility check of the VCU torque request, based on vehicle speed, accelerator pedal position, driving direction, power limitations, etc. The function is easier than that of the VCU.
• Minimum and maximum plausibility check of the actual e-machine torque, based on current drawn by the inverter and e-machine speed.
• Monitor the rotating direction request from VCU and enter an error mode if it detects a change in the rotating direction request without having first detected a driver request to change the vehicle direction

The third level, the controller monitoring level is covered by the BMS:
• The BMS sends a random number over the CAN bus to the VCU. The VCU has to start a pre-defined calculation sequence with this number and sends the answer back to the BMS. BMS checks this answer against the requested number and reacts in case of repetitive error.

The safety-related data exchange between these two controllers is protected at run time against the effects of random hardware faults, interference and systematic faults within the software using end-to-end communication protection based on alive counter and additional checksums. A similar methodology is explained in greater detail in additional publications [5].

In addition, both the VCU and BMS conduct memory tests (RAM and ROM) cyclically and during initialization in order to reduce the residual faults.

The BMS, during each power up and power down process also checks to see if the main relays are stuck or not. Therefore it will ensure that the shut-off path, leading to the safe state is working before the vehicle is actually being driven.

The reaction to the various single and multiple failures that the concept is able to detect have been defined in order to ensure the highest possible reliability and availability of the vehicle. A number of error reaction steps have been defined ranging from reduced available power to opening of the battery main relays and then shutting down the e-machine supply. This opening of the battery main relays is only allowed when no other safe error reaction at the vehicle level is possible.

Figure 6 shows the behavior of the vehicle in a case of unintended vehicle acceleration that might occur during typical city driving. City driving was selected for this example, as it represents the most typical driving situation for this particular vehicle. The vehicle is driving at about 35km/h when the torque produced by the e-machine suddenly does not match the driver torque request.

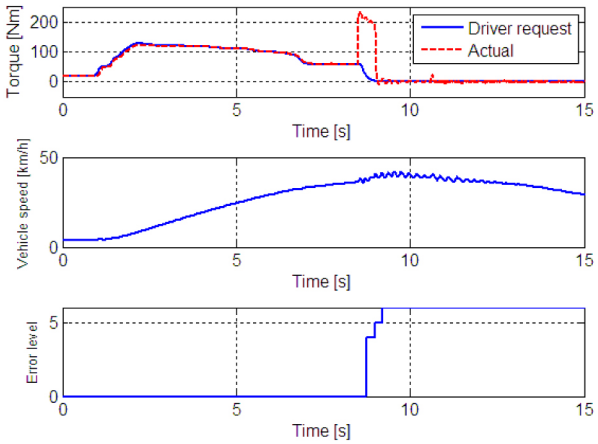

Figure 6. Unintended Vehicle Acceleration of 2.33m/s^2

This unintended torque increase leads to an unintended average vehicle acceleration of about 2.33 m/s^2. In order to reach the safety goal to prevent unintended and uncontrollable vehicle acceleration, the allowed reaction time for the monitoring function has been defined based on a target acceleration limit. This limit is defined by the intensity and the duration of the unintended acceleration. With an unintended acceleration of about 2.33 m/s^2, the defined reaction time is about 0.5s.

Figure 7 shows the behavior of the vehicle in case lower unintended vehicle acceleration is produced due to a smaller mismatch between the torque requested by the driver and what is actually produced by the e-machine.

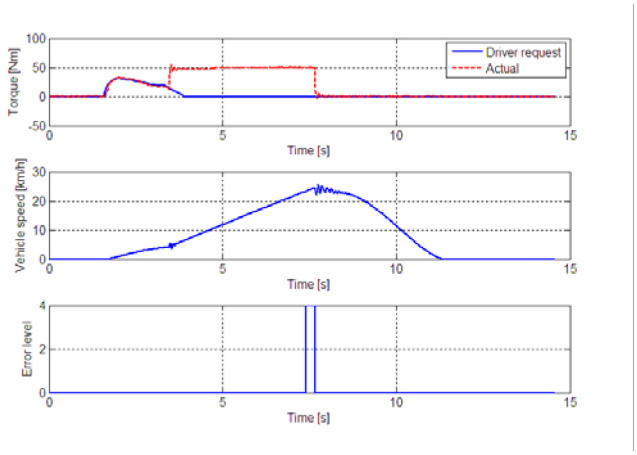

Figure 7. Unintended vehicle acceleration of 1,2 m/s^2

In this case, the average unintended vehicle acceleration is about 1.2 m/s^2. According to the target limit for controllable unintended vehicle acceleration, the reaction time is allowed to be a maximum of 4s, as shown in Figure 7.

SUMMARY/CONCLUSIONS

Hybrid vehicles rely primarily on electronics for the control and the coordination of the various sub-systems or component. The number and complexity of distributed functions among the many control units is increasing for such vehicles. Functional safety is then becoming a key factor in the development of modern electric and hybrid vehicles. Functional safety in the automotive industry is now ruled by a new international standard (ISO 26262). ISO 26262 applies only to the systems developed after its publication and, no doubt will play an important role in the development of upcoming hybrid and electric vehicles.

This paper has briefly introduced the new standard and the specific safety related functions of hybrid and electric vehicles. It has also highlighted how the risk-based approach of ISO 26262 can influence the safety integrity level of some safety related functions specific to hybrid and electric vehicles. It has also highlighted how well established safety related functions, such as torque monitoring of conventional internal combustion engines can be influenced by vehicle hybridization.

A functional safety concept aiming at reaching the safety goals “Prevent unintended vehicle acceleration or keep it to a controllable level, ASIL B” and “Prevent unintended vehicle acceleration in wrong direction or keep it to a controllable level, ASIL A” for an electric vehicle was presented. The functional safety concept relies on the monitoring of the DC current flowing to the e-machine control unit and the vehicle speed. In hybrid and electric vehicles, these signals are, either directly or indirectly, controlled by different control units in the vehicle, such as MCU, BMS and VCU. This offers a higher flexibility for the implementation of torque monitoring functions than in conventional combustion engine vehicles. The first measurements made in the vehicle show that the monitoring concept fulfills the reaction time requirement to ensure that unintended torque increase do not lead to uncontrollable vehicle acceleration.

In order to claim compliance with ISO 26262, additional activities will need to be completed. An important step is to provide evidence that the required ASIL are met. This shall be done at three levels. Firstly, it is important to show evidence that all the necessary safety activities defined in the safety lifecycle were complied with and followed. This is typically what the ISO 26262 defines as safety case [6]. Secondly, the process and the techniques/measures used for the development of the VCU and BMS software must satisfy the recommended measures of ISO 26262 [7] for the corresponding ASIL. Lastly, the fulfillment of the ASIL requirements regarding the hardware design must be shown by the calculation of the hardware architectural metrics and the evaluation of the safety goal violations due to random hardware failures.

REFERENCES

1. ISO 26262-1:2011 Road vehicles - Functional safety - Part 1: Vocabulary

2. ISO 26262-3:2011 Road vehicles - Functional safety - Part 3: Concept phase

3. Standardisiertes E-Gas-Überwachungskonzept für Motorsteuerungen von Otto- und Dieselmotoren, Version 4.0. Arbeitskreis EGAS 30.01.2007.

4. ISO 26262-5:2011 Road vehicles - Functional safety - Part 5: Product development at the hardware level

5. Specification of SW-C End-to-End Communication Protection Library V1.1.0 R4.0 Rev2, AUTOSAR, 2010

6. ISO/FDIS 26262-10 Road vehicles - Functional safety - Part 10: Guideline on ISO 26262

7. ISO 26262-6:2011 Road vehicles - Functional safety - Part 6: Product development at the software level

CONTACT INFORMATION

Dipl.-Ing.
Sébastien Christiaens
Team leader
Functional Safety and High Voltage Safety
FEV GmbH
Phone: +49 (0)241 5689 - 9504
personal Fax: +49 (0)241 5689 - 79504
christiaens@fev.com

DEFINITIONS/ABBREVIATIONS

ASIL
Automotive Safety Integrity Level

BEV
Battery Electric Vehicle

CAN
Controller Area Network

E/E
Electric/Electronic

EREV
Extended Range Electric Vehicle

HEV
Hybrid Electric Vehicle

PHEV
Plug-in Hybrid Electric Vehicle

ICE
Internal Combustion Engine

EMS
Engine Management System

VCU
Vehicle Control Unit

BMS
Battery Management System

EESS
Electrical Energy Storage System

MCU
e-machine control unit

SW
Software

HW
Hardware

DC
Direct Current

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. This process requires a minimum of three (3) reviews by industry experts.

ISSN 0148-7191

SAE Customer Service:
Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE Web Address: http://www.sae.org
Printed in USA