CHEMICAL ENGINEERING TRANSACTIONS

VOL. 33, 2013

A publication of AIDIC
The Italian Association
of Chemical Engineering
www.aidic.it/cet

Guest Editors: Enrico Zio, Piero Baraldi
Copyright © 2013, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-24-2; **ISSN** 1974-9791

DOI: 10.3303/CET1333131

HEMIS: Electrical Powertrain Health Monitoring for Increased Safety of FEVs

Beatriz Sedano[a], Alastair R. Ruddle[b], Inigo Unanue[c], Lester Low[b], Daniel Astigarraga [a], Ireri Ibarra[b], Ibon Cerro[c], Ainhoa Galarza [a]

[a]CEIT, Manuel de Lardizabal 15, 20018 San Sebastián, Spain
[b]MIRA Limited, Watling Street, Nuneaton, CV10 0TU, UK
[c]Jema Energy, Pº del Circuito 10 - 20160 Lasarte-Oria, Spain
bsedano@ceit.es

To achieve the aims of reducing energy consumption and CO_2 emissions, Fully Electric Vehicles (FEVs) need to reach a significant market share. However, the advent of FEVs in mass production presents new challenges to automotive manufacturers due to the relative immaturity of the new building blocks, which may impact on the FEV's safety and reliability. Among the most important of these is the electric powertrain: i.e. electric traction motors and their power electronics controllers.

This paper presents the FP7 project HEMIS. One of the main aims of this project is to design an in-vehicle Prognostic Health Monitoring System (PHMS) for the powertrain in order to enhance safety and maintainability. The article presents the architecture proposed for a generic FEV and its electric powertrain. The results of a RAMS analysis undertaken to assess the use of the PHMS are also summarised.

1. Introduction

Nowadays, road transport relies almost exclusively on fossil fuels, accounting for 60% of all the oil consumed in the EU. In fact, road transport is responsible for one-fifth of the EU's total emissions of carbon dioxide, the main greenhouse gas. Moreover, emissions from transport have increased by 26% since 1990. Therefore, in order to reach the 2020 target of reducing the 1990 greenhouse emission figure by 20%, the European Commission considers the fully electric vehicle (FEV) an absolute must.

Progress towards mass production of FEVs presents vehicle manufacturers with new challenges due to the relative immaturity of the new technologies that are involved. The most notable of these is the electric powertrain, comprising the electric traction machine and its associated power electronics. One of the main aims of the FP7 project HEMIS is therefore to design a PHMS for the powertrain in order to enhance the safety and maintainability of FEVs.

In order to do so, a generic architecture has been defined describing common features of near-future FEVs, as the HEMIS project is not focused on any specific vehicle. Based on the generic architecture, a Preliminary Hazard Analysis (PHA) has been carried out in order to identify and classify the potential hazards. The contributors to these hazards were further investigated using Fault Tree Analysis (FTA) and Failure Mode and Effects (FMEA) techniques in order to identify corrective actions to mitigate the hazards. The results of the safety and failure analyses confirm that adding a PHMS to monitor the electrical powertrain would reduce the risks associated with failures of the electrical powertrain while a prognostic capability would enhance maintainability.

2. FEV Architecture

A generic vehicle architecture has been defined describing common features of the FEVs, as the HEMIS project is not focused on any specific vehicle. This architecture description focuses on the electrical powertrain and other systems that have an impact on the operation of the electrical powertrain.

Please cite this article as: Sedano B., Ruddle A.R., Unanue I., Low L., Astigarraga D., Ibarra I., Cerro I., Galarza A., 2013, Hemis: electrical powertrain health monitoring for increased safety of fevs, Chemical Engineering Transactions, 33, 781-786
DOI: 10.3303/CET1333131

2.1 Architecture of a generic FEV

The proposed architecture (Figure 1) shows the main functional domains that comprise the FEV's electrical system, emphasizing in particular the Powertrain Domain. It also shows the various communication networks inside the car that allow information exchange between functional domains (VEESA project Consortium, 2004; Hiller *et al*., 2004; and Kelling et al., 2009). Finally, this architecture also shows the external interfaces of the FEV, such as the Driver, Vehicle Charging Station, External Networks or Environment.

2.2 Electrical powertrain architecture

In order to better understand the architecture at a level suitable for the analysis some assumptions have been made concerning the nature of the electric powertrain:

- Traction power will be provided only via electrical machines, and not mechanically from any on-board energy source, such as an internal combustion engine (ICE).
- The electrical machine could be operated as a traction motor, or as a generator under braking conditions.
- The vehicle contains at least one such machine, but possibly more (e.g. one in each wheel, or one for each axle).
- Electrical energy storage is provided by a high voltage traction battery, as this is the most commonly used solution;
- Energy may be obtained from the electricity grid and during regenerative braking, and possibly also from an on-board energy source such as a fuel cell or other generator.

The electrical powertrain corresponds to the "Electrical Transmission" system of Figure 1, which comprises the "Electrical Machine" (i.e. the traction machine and associated sensors) and the "Control" (i.e. the inverter, its controller, and associated sensors). For the purposes of HEMIS, the traction machine is assumed to be a permanent magnet synchronous machine, squirrel cage induction machine, or switched reluctance machine.

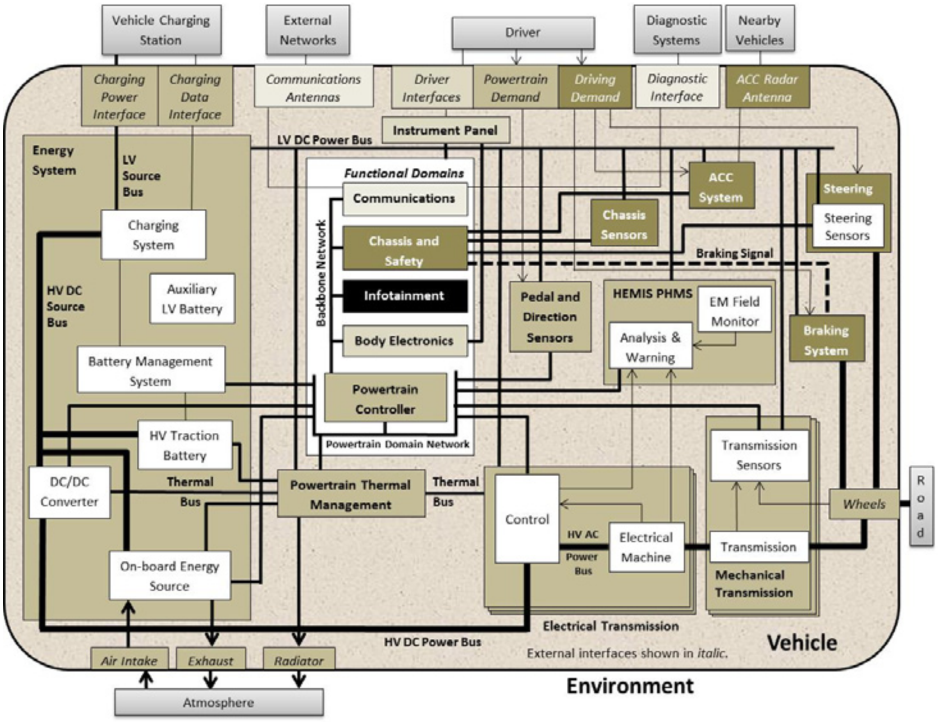

Figure 1: HEMIS generic FEV architecture

The architecture assumes that these Electrical Transmission components will be monitored by the PHMS, hence sensor outputs are indicated from the Control and Electrical Machine. It should be noted, however, that the PHMS is assumed to have no direct control functions, but only monitors the Electrical

Transmission and warns the driver of actual or impending failures of the Traction Machine and its control electronics.

3. RAMS Analysis

In order to define the need for hazard mitigation techniques, a RAMS analysis has been carried out. Firstly, the most significant hazards have been identified through a preliminary hazard analysis (PHA); secondly, a tolerable hazard rate has been established; and finally, a RAMS apportionment has been carried out in order to identify corrective actions to mitigate the hazard which will be a key aspect to define the PHMS.

3.1 Hazard analysis

The PHA is carried out by reviewing the mission of a system (i.e. its high level functionality), together with its operating environment. In this way it is possible to identify system hazards when the mission is not fulfilled. As the PHA is intended to be systematic and repeatable the use of guidewords is encouraged. The PHA distinguishes between system hazards and failures, and the system under analysis is to be considered without any safeguards or mitigations. Furthermore, implementation details are not relevant for this type of study.

The generic architecture outlined in section 1 formed the basis of the HEMIS PHA. The focus of this analysis was to identify acceleration and deceleration hazards, as well as those affecting vehicle handling and stopping distance. The functional domains that were analysed included the powertrain domain and the chassis and safety domain, with the electrical transmission and energy systems being the primary interests. The high level functions of the systems were specified, based on the architectural description, in order to identify functional failures that could result in hazards. The hazard identification was carried out in two parts: the first part identified hazards related to functional failures of the system; the second part identified non-functional hazards that are inherent in the novel technologies assumed to be used in the vehicle.

The objective of the PHA is to translate system hazards into design constraints, or functional safety requirements. Once the hazards were identified, each was assessed in terms of their potential consequences (“severity”), likelihood of occurrence (“exposure”) and opportunities for the driver to influence the outcome (“controllability”). A risk graph is then used in order to establish and classify the associated risks in terms of the Automotive Integrity Levels (ASILs).

3.2 Tolerable Hazard Rate

The approach for probabilistic Safety Integrity Levels (SILs) can be found in a number of standards, depending on the environment, such as EIC 61508 (generic), IEC 61513 (nuclear power), IEC 62061 (machinery), and EN 50129 (railway). These domains rely on the concept of safety functions as a mechanism of risk reduction. For the automotive industry, however, safety functions are not easily distinguished from non-safety functions. Hence in ISO 26262, which is the automotive interpretation of IEC 61508, no quantitative targets are associated with the ASILs.

The *tolerable hazard rate* (THR) is a rate of occurrence of dangerous events that is deemed to be acceptable from a piece of equipment in order to achieve overall safety targets. Although this concept is used in EN 50129, THR in the form of quantified safety targets for each particular railway application are the responsibility of the relevant railway authority, and are not defined by the standard. However, THR is not used in ISO26262, so a proposed mapping between ASIL, SIL and THR (shown In
Table 1) was derived from a risk model including both systematic and random faults, taking account of controllability and severity aspects, based on safety targets described by Evans and Moffett (2000).

Table 1: Mapping between ASIL of ISO 26262, SIL of IEC 61508, and THR

ISO 26262	IEC 61508	THR
ASIL A	SIL 1	$10^{-5} \le \text{THR} < 10^{-4}$
ASIL B	SIL 2	$10^{-6} \le \text{THR} < 10^{-5}$
ASIL C	SIL 3	$10^{-7} \le \text{THR} < 10^{-6}$
ASIL D	SIL 3	$10^{-8} \le \text{THR} < 10^{-7}$

The approach for probabilistic Safety Integrity Levels (SILs) can be found in the aforementioned standards. These domains rely on the concept of safety functions as a mechanism of risk reduction. However for the automotive industry a safety function is not easily distinguished from a non-safety function. Hence for the

ISO 26262 standard, which is the automotive tailoring of IEC 61508, no numerical targets are associated with Automotive Integrity Levels (ASILs).

In HEMIS project, the identified hazards were classified using the ISO 26262 risk criteria. However, the equivalences of the integrity level with the tolerable hazard rate were previously established in order to relate the hazards associated with the failure of electronic control systems to THR. The classification took into consideration example situations, illustrated in Table 2, and the most severe outcome was recorded.

Table 2: ASIL and THR for examples of the hazards identified from the PHA

Hazard	ASIL	THR
Undemanded vehicle acceleration	D	$10^{-8} \le THR < 10^{-7}$
Undemanded vehicle deceleration	D	$10^{-8} \le THR < 10^{-7}$
No vehicle acceleration	D	$10^{-8} \le THR < 10^{-7}$
No vehicle deceleration	D	$10^{-8} \le THR < 10^{-7}$
Excessive vehicle acceleration	B	$10^{-6} \le THR < 10^{-5}$

3.3 RAMS apportionment

A RAMS analysis was performed with the goal of improving the safety of the FEV. For evaluating the safety of the FEV, its failure modes have to be investigated in detail and exhaustively. For this purpose, the Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) were used to identify the specific FEV systems or functions that may lead to potential hazards. The difference between FMEA and FTA is a matter of depth. FMEA looks at all failures and their effects, while FTA is applied only to those effects that are potentially safety related and that are of the highest criticality. FMEA and FTA are complementary methods because the focused, deductive nature of FTA may identify failures that might be missed by the broader, inductive FMEA. Conversely, the broad coverage provided by FMEA may identify relevant failures that are outside the scope of a narrowly focused fault tree analysis. So both FTA and FMEA analysis methods were used at FEV level.

FTA is a feed-back technique in that one starts with the system level hazards and attempts to work backwards by identifying all possible causes of the hazards. FTA uses Boolean logic to depict the combinations of individual failure mode that can lead to the top level hazard. Figure 2 shows a FEV level fault-tree related to the ’no acceleration’ hazard, having been constructed following the high-level functional architecture as presented in Section 2

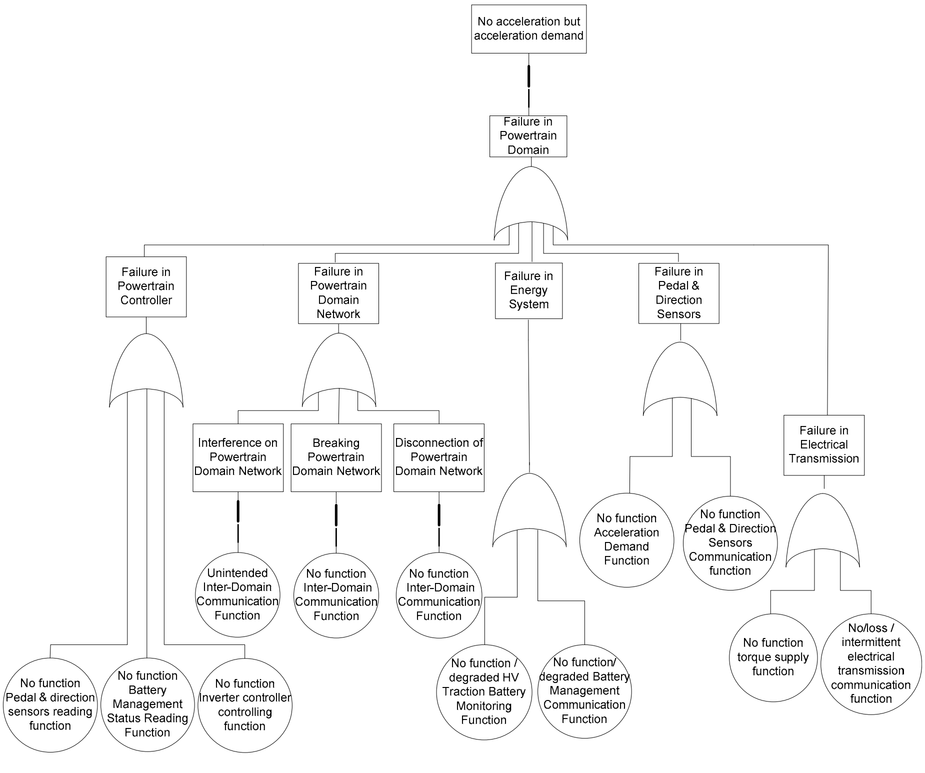
No acceleration but acceleration demand
Failure in Powertrain Domain
Failure in Powertrain Controller
Failure in Powertrain Domain Network
Failure in Energy System
Failure in Pedal & Direction Sensors
Failure in Electrical Transmission
Interference on Powertrain Domain Network
Breaking Powertrain Domain Network
Disconnection of Powertrain Domain Network
Unintended Inter-Domain Communication Function
No function Inter-Domain Communication Function
No function Inter-Domain Communication Function
No function Acceleration Demand Function
No function Pedal & Direction Sensors Communication function
No function torque supply function
No/loss / intermittent electrical transmission communication function
No function / degraded HV Traction Battery Monitoring Function
No function/ degraded Battery Management Communication Function
No function Pedal & direction sensors reading function
No function Battery Management Status Reading Function
No function Inverter controller controlling function

Figure 2: Fault tree for hazard “No vehicle acceleration”

FMEA is widely used as a standalone tool for safety analysis in the automotive industry, where it has served as a general purpose tool for enhancing reliability. FMEA analyses potential failure modes, effects, severity and probability, from which a risk priority number (RPN) is determined. FMEA can therefore be used to determine which potential failures are critical, how they can be pinpointed, and how the effects thereof can be avoided. The RPN is the product of the Severity, Occurrence and Detection ratings:

$$RPN = Severity \cdot Occurrence \cdot Detection$$

This value may then be used to prioritize the failure modes that require a corrective action. The considered RPN threshold is 35; so if the RPN is less than 35, it has been considered that actions must be recommended to counteract or avoid these failures.

The considered scales rate all the characteristics (severity, probability of occurrence and probability of detection) to numbers between 1 and 5 in the following way: 1 denotes the most critical effect related to severity, the highest occurrence and the no detection of the failure; while 5 denotes the insignificant effect related to severity, the remote occurrence and total detection of the failure.

Each major system and its functions have been examined for failures, and a portion of the FEV level FMEA is shown in Table 3.

Table 3: Example results from FMEA at FEV level

System and Functions	Failure Mode	Subsystem Effect	System Effect	RPN
Electrical Transmission				
Torque supply function	Failure to operate when required	No torque	No acceleration	6
Torque supply function	Output higher than required	Excessive torque	Excessive acceleration	12

In the HEMIS project, the selected risk acceptance principle is the minimum endogenous mortality which is based on an individual risk (EN 50126). The FEV Endogenous Mortality is calculated considering all hazards which are caused by the failure of several systems as shown in the fault tree analysis. Every system is characterized by a failure rate of that system. The calculated Endogenous Mortality is higher than the Minimum Endogenous Mortality (2×10^{-4} fatalities/year·occupant), so the HEMIS PHMS will be added to monitor key physical characteristics (e.g. currents, voltages, etc.) that are associated with the health of the FEV powertrain in order to detect failures as early as possible. This involves two steps: first, the system must somehow sense that there has been a failure; secondly, the sensed failure must be made known to the driver. With the PHMS included, the Minimum Endogenous Mortality is reached.

4. Failure modes of the electrical powertrain

For the development of an FMEA of the powertrain at subsystems level, the architecture described in Section 2 was further refined, as shown in Figure 3. The development of FMEA and FTA for the electrical powertrain subsystems have also been undertaken, following the same criteria as for the higher level functions. There are two examples from the FMEA shown in Table 4(O'Donnell, 1983; Wolfgang, 2007).

Table 4: Example results from subsystems FMEA for Electrical Transmission

System and Functions	Failure Mode	Subsystem Effect	System Effect	RPN
Inverter				
Switch the IGBTs to chop the DC current	Short circuit	Gate driver cuts the current flow	Rotor may block	4
Stator Windings (Induction Machine)				
Provide required current path	Open circuit	Decreased current flow	Unreliable Stator Magnetic field	6

5. Conclusion and future steps

The RAMS analysis of the FEV has allowed those systems of the FEV that contribute to the FEV hazards to be identified. The results of the analysis confirm that adding a PHMS to the powertrain would reduce the risks associated with failures of the electrical powertrain reaching the Minimum Endogenous Mortality.

Furthermore, an analysis focused on the powertrain has been carried out, in order to identify the failure modes of the components of the FEV which contribute to the FEV hazards.

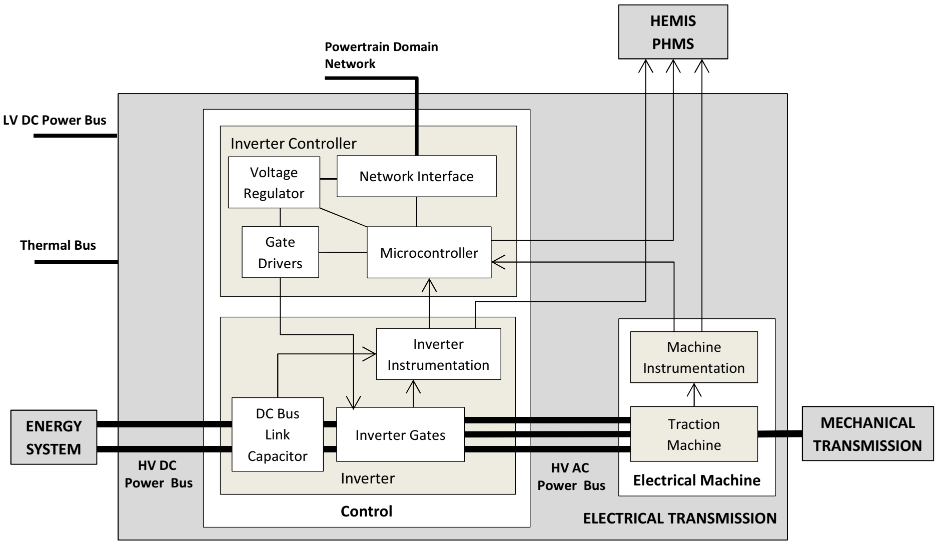

Figure 3: Electrical Transmission subsystems

In the following months the defined failure modes and the degradation process of the electrical powertrain will be analysed in order to identify which physical variables are the most suitable to monitor the failsafe state of the powertrain. The analysis will take into account not only the reliability and accuracy of the measurements, but also the associated cost and the feasibility of integration into a generic FEV. In addition to this, hybrid data and information will be integrated into a prognostic algorithm to estimate the value of the Remaining Useful Life (RUL) with uncertainty estimation.

Later, monitoring systems will be designed, implemented and tested for the motor, the associated power electronics and, if necessary, the electromagnetic field emitted by the electric powertrain. Finally, these monitoring systems will be integrated in the PHMS prototype.

Acknowledgements

The research leading to these results has received funding from the European Community's Framework Programme (FP7/2007-2013) under grant agreement nº 314609. The authors are grateful for the support and contributions frm other members of the HEMIS project consortium, from CEIT (Spain), IDIADA (Spain), Jema (Spain), MIRA (UK), Politecnico di Milano (Italy), VTT (Finland) and York EMC Services (UK). Further information can be found on the project website (www.hemis-eu.org).

References

EN 50126. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

Evans R. , Moffett J. D., 2000, Derivation of Safety Targets for the Random Failure of Programmable Vehicle Based Systems, Proceedings of the 19th International Conference on Computer Safety, Reliability and Security, 240-249, Springer-Verlag London, UK.

Hiller M., Böhm J., Chen X., Echtle K., Eymann T., Ferre A., Hedenetz B., Kelling E., Lauer V., Osella M., Voss T., van Vageningen D., 2004, General architecture framework, EASIS EU Project Deliverable D0.2.4.

ISO 26262, Road Vehicles – Functional Safety, November 2011 (parts 1-9); ISO 26262-10, Guideline, July 2012.

Kelling E., Friedewald M., Leimbach T., Menzel M., Säger P., Seudié H., Weyl B., 2009, Specification and evaluation of e-security relevant use cases, EVITA EU Project Deliverable D2.1, Version 1.2.

O'Donnell P., 1983, Report of Large Motor Reliability Survey of Industry and Commercial Installations, Part I, IEEE Transactions on Industry Applications, vol IA-21, no. 24, pp. 852-864.

VEESA project Consortium, 2004, Vehicle e-Safety Architecture, EU project IST-2001-37598, Deliverable D0: Final Report.

Wolfgang E., 2007, Examples for failures in power electronics systems, ECPE Tutorial on Reliability of Power Electronic Systems.