1 General Information

Laboratory	FEMTO_ST
University	University of Technology of Belfort-Montbéliard (UTBM), Univ. Bourgogne Franche-Comte (UBFC)
Contact	**Thesis advisor :** Dr. Abdesslem Djerdir (abdesslem.djerdir@utbm.fr)

2 Thesis Title and Keywords

Functional Safety Management for Fuel Cell Vehicles According to Modern Automotive Standards

Keywords: Fuel Cell electric vehicles (FCEV), PEM Fuel Cell, embedded hydrogen tanks, Lithium battery, supercapacitors, Causal and Fault Tree analysis, Degradation, Availability, Security Integrity Level, standards: ISO 26262, IEC 61508, IEC 61511, regulations: CE406/2010, CE 79/2009.

3 Thesis Subject

Standard, ISO 26262 "Road vehicles – Functional safety", has been created as the automotive functional safety standard. It is applicable to electronic programmable systems used in passenger cars with a maximum gross weight of 3500 kg. Fuel cell (FC) base transport systems are more and considered, by public and private research organizations, as one of the most suitable solution for clean transportation. At French level, one of the most important experiences in terms of Fuel cell vehicles is those manufactured thanks to the MobyPost project (http://mobypost-project.eu/). The expected wide public using of these vehicles requires a maximum availability and safety constraints of theirs main functions (hybrid fuel cell source, drivetrain, harness, etc.). In order to move towards a competitive vehicle in terms of safety and reliability, it is necessary to continue the development of such new technology in line with modern automotive standards.

ISO 26262 requires that a hazard analysis and risk assessment should be done at the system level. Each possible system malfunction should be analyzed and its risk determined. If the risk is deemed too high, safety goals should be defined and risk reduction techniques should be applied to enhance functional safety in the face of the complexity and functional risks of electrical/electronic/ programmable electronic (E / E / PE) on-board equipment. Since 2011, the automotive industry has adopted an ISO 2626-2 methodological and technical standard on the basis of IEC 61508 IEC 61511 standards. On the other hand, the CE406 / 2010 and CE 79/2009 regulations require an approach of specific approval for hydrogen vehicles.

The aim of this thesis is firstly to identify the events feared during the preliminary risk analysis of different architectures of the hybrid fuel cell embedded source in automotive applications. These dreaded events will be declined in the form of security requirements. As shown in Table 1 each dangerous situation should be rated according to a level of security requirement from Automotive Security Integrity Level (ASIL-A to ASIL-D). ASIL-A defines the minimum and ASIL-D the maximum achievable safety targets, otherwise Quality Managment (QM) when it there are no special requirements for this, apart from those already fore seen by the quality management system dictated by the manufacturer of the system. These points are treated in accordance with a quality management standard ISO/TS 16949. Instrumented security functions are developed to reduce the level of risk and act on the architecture choices to ensure the level of integrity of the security system (SIL: Security Integrity Level):

SIL 1: risk reduction by a factor> 10
SIL 2: risk reduction by a factor> 100
SIL 3: risk reduction by a factor> 1,000
SIL 4: risk reduction by a factor> 10,000

Secondly, the thesis work will evaluate the level of security of products throughout their development using the tools: Fault Tree Analysis (FTA), Failure Mode and Effect of Diagnosis Analysis (FME). ISO 26262 risk is evaluated through three criteria: Severity (S), Exposure (E) and Controllability (C).

Severity	Probability of exposure	Controlability	
		C1	C2
S0 No injuries	E0 : very week	QM	QM
	E1 : week	QM	QM
	E2 :medium	QM	QM
	E3 :high	QM	ASIL A
S1 Light injuries	E0	QM	QM
	E1	QM	QM
	E2	QM	ASIL A
	E3	ASIL A	ASIL B
S2 Severe injuries	E0	QM	QM
	E1	QM	ASIL A
	E2	ASIL A	ASIL B
	E3	ASIL B	ASIL C

Table 1 : Automotive Security Integrated Level for ISO26262 standard

Finally, in order to reduce the risk to a level as required by the functional safety standard technical solutions will be developed.

E0 = 0.001: rare event (once a year)
E1 = 0.01: 1% of the time of use of the vehicle
E2 = 0.1: from 1% to 10% of the time of use of the vehicle
E3 = 1: from 10% to 100% of the time of use of the car
C1 = 0.01: less than one in a hundred driver are able to control the situation
C2 = 0.1: less than one in ten driver are able to control the situation
C3 = 1: uncontrollable situation

4 Expected Collaborations

This work will continue the existing collaboration between UTBM (https://www.utbm.fr/) and Spacetrain (https://space-train.fr/) and it will create new collocations with new national and international partners with both academics and private institutions. One goal is to apply for French and European projects calls within the BPI, H2020 and FCH-JU programs.

5 Background

The candidate must have strong theoretical and experimental skills in power electronics and drives, in simulation and rapid prototyping in order to propose an optimal solution and to build its prototype.

6 References

[1]. Raja Yahmadi, Kais Brik, Faouzi Ben Ammar, « Research of critical causes and improvement of energy storage system reliability in power electronic applications » International Journal of Hydrogen Energy Vol 42 (13), pp 8765-8776, Mars 2017

[2]. Kais Brik, Faouzi Ben Ammar, "Improved performance and energy management strategy of proton exchange membrane cell/backup battery in power electronic systems International Journal of Hydrogen Energy", 42 (13), 8845-8856, 2017

[3]. K Brik, Faouzi Ben Ammar, A Djerdir, A Miraoui, "Causal and fault trees analysis of proton exchange membrane fuel cell degradation", Journal of Fuel Cell Science and Technology 12 (5), 051002