POLITECNICO DI TORINO

Master degree in Mechatronic Engineering

Master Thesis

Analysis of the safety functions according to ISO26262 of the Epic0 vehicle and critical overhaul of the control unit

Relatore

Prof. Massimo Violante

Candidato

Giacomo De Leo

A.A. 2021/22

Abstract

Safety has always been an important part, independently on the field of work that it accounts for. Nowadays, road vehicles, including trucks, are characterized by an increased complexity due to a greater variety of software, and a greater number of sensors and actuators. As a consequence, there is an increased risk of failures, both HW and SW, that could lead to unacceptable hazards. The presence of these risks led to the definition of functional safety, a crucial property that must be ensured to avoid or mitigate these potential unacceptable hazards.

Functional safety standard that is currently used in the automotive domain is the ISO 26262, an adaptation of the IEC 61508 safety standard. The version of ISO 26262 that is used in this thesis is the final draft released in December, 2016. Various parts of the ISO 26262 functional safety standard had been considered and applied, during stage and thesis work, in order to understand the differences and interdependencies between them, as follow:

- Part 1: Vocabulary,
- Part 3: Concept phase,
- Part 4: Product development at the system level,
- Part 5: Product development at the hardware level,
- Part 6: Product development at the software level,
- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

By now, L7e vehicles do not have to be compliant with the standard. However, it is likely that by 2022 they will have to. To be ready by 2022, Mecaprom Technologies Italia and Regis Motor are interested in investigating ISO26262 as well as safety case provision.
Thus this thesis focuses on the adaptation of the torque management system to the ISO 26262 standard, focusing on the evolution of the LMU board from the old version (2017) to the latest version (2022).

Acknowledgements

First of all, I would like to thank my supervisor at Mecaprom Technologies Corporation Italia Srl: Ing. Enrico Bianconi. He has supported me throughout the whole project, answering every question I had and discussing all the details until I fully understood the architecture of the vehicle and the work scenario.
He showed me how decisions are made in a structured company and how negotiations with partners are managed. In this short timespan he familiarized me to the automotive industry and helped me develop a vision for my career.
My professor Massimo Violante from Politecnico di Torino, has given me a lot of guidance and suggestions both during stage months and thesis compilation phase. From the first day until the final days of this thesis, he made sure I kept my focus on feasible goals, teaching me a 'pragmatic way' to proceed. Without his experience and guidance this project would still be in the conceptual phase.
As well I would like to thank the Human Resources Manager at Mecaprom: Alessandra Botta.
She allowed me to get in touch with Mecaprom and be able to proceed with the internship without having to worry about all the bureaucratic part requested by the University.
My colleagues in Maserati for the support and the availability to give me time and space in order to let me write and complete my thesis work in the last month.
I also would like to thank all the gastroenterology team of Mauriziano Hospital and Santa Maria delle Croci Hospital, in particular Dr. Marco Daperno and Dr. Stefano Gasperoni to allow me to cure me and continue to fight month after month against the disease.
Finally, I would like to thank my family. They always pushed me to reach my best during the whole period of my university studies. I appreciate all the emotional support.
Especially my mother, father and Caterina for always reminding me that I can do it.
Least but not last I would like to thank all my friends and all the colleagues that I have met in this years, especially Edo, Ste, Jack, Lalla and Babbe with which I shared the heaviest efforts, but also the most beautiful and iconic moments of my life as a student.
So here it is, I've done it!

Summary

List of figures

List of tables

Abbreviations

ISO	International Organization for Standardization.
QM	Quality Management.
TSR	Technical Safety Requirement.
HARA	Hazard Analysis and Risk Assessment.
FSR	Functional Safety Requirements.
FMEA	Failures Modes and Effect Analysis.
LMU	Vehicle Monitoring Unit.
BMS	Battery Monitoring System.
FMEDA	Failure Mode, Effects and Diagnostic Analysis.
E/E	Electric and Electronic.
ASIL	Automotive Safety and Integrity Level.
WHO	World Health Organization.
IEC	International Electrotechnical Commission.
SW	Software.
HW	Hardware.
CAN	Controller Area Network.
CRC	Cyclic Redundancy Check.
PCB	Printed Circuit Board.
ECU	Electronic Control Unit.
A	Analog
BMS	Battery Management System
BTPK	Battery Pack
BZZ	Buzzer
CAN	Controller Area Network
C	Communication
D	Digital
DC	Direct Current
DNC	Do Not Care
GND	Ground
HV	High Voltage

I	Input
INV	Inverter
LMU	Logic Management Unit
NC	Normally Close
NO	Normally Open
RGN	Regeneration
TA	Ambient Temperature
VBD	Voltage Battery
VEH	Vehicle

1. Introduction

According to the World Health Organization (WHO) "The Global status report on road safety 2018, launched by WHO in December 2018, highlights that the number of annual road traffic deaths has reached 1.35 million. Road traffic injuries are now the leading killer of people aged 5-29 years. The burden is disproportionately borne by pedestrians, cyclists and motorcyclists, in particular those living in developing countries. The report suggests that the price paid for mobility is too high, especially because proven measures exist. Drastic action is needed to put these measures in place to meet any future global target that might be set and save lives [1]".

In 2017, WHO released Save LIVES a road safety technical package which synthesizes evidence-based measures that can significantly reduce road traffic fatalities and injuries. Save LIVES: a road safety technical package focuses on Speed management, Leadership, Infrastructure design and improvement, Vehicle safety standards, Enforcement of traffic laws and post-crash Survival. The package prioritizes 6 strategies and 22 interventions addressing the risk factors highlighted above, and provides guidance to Member States on their implementation to save lives and meet the road safety target of halving the global number of deaths and injuries from road traffic crashes by 2020 [2].

By consequence, road and vehicle safety play an important role in the automotive product development cycle as well as making infrastructure safer and improving road legislation will help prevent fatalities.
In addition to all of the above, many Electric and Electronic (E/E) components have been introduced in automobiles which has led to an increase in the amount of software needed to operate them.

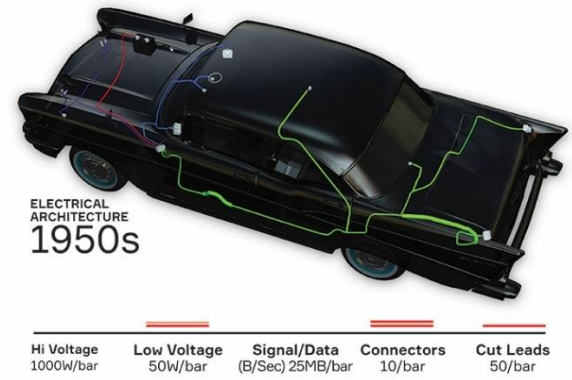


Figure 1: Electrical architecture of a 1950 vehicle

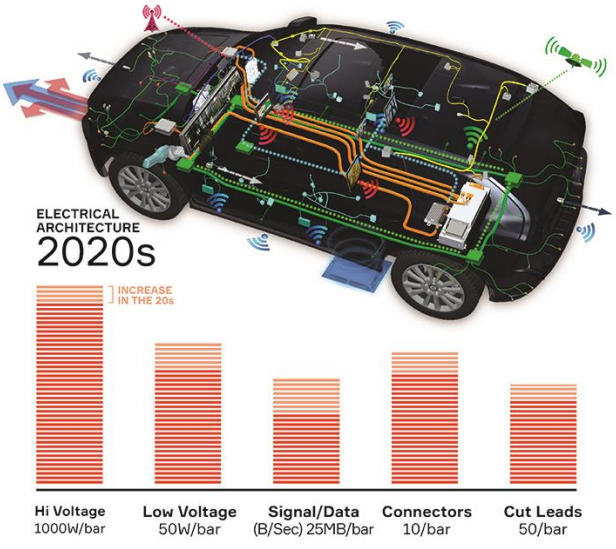


Figure 2: Electrical architecture of a 2020 vehicle

Ten years ago, only premium cars contained 100 microprocessor-based electronic control units (ECUs) networked throughout the body of a car, executing 100 million lines of code or more. Today, high-end cars with advanced technology like advanced driver-assist systems (ADAS) may contain 150 ECUs or more, while pick-up trucks top 150 million lines of code. Even low-end vehicles are quickly approaching 100 ECUs and 100 million of lines of code as more features that were once considered luxury options, such as adaptive cruise control and automatic emergency braking, are becoming standard.
How much and what types of software resides in each ECU varies greatly depending on computing capability of the ECU, functions controlled by the ECU, internal and external information and communications required to be processed and whether they are event or time triggered. Over the past decade, more ECU software has been dedicated to ensuring operational quality, reliability, safety and security [4].

These changes have the potential to improve the vehicle safety but bring other challenges as well. The functions which components of the car have to fulfill require more communication and an increasing usage of software. This higher the software complexity and, with it, the probability of failures.
Demonstration on what said before is given by the 2020 Automotive Defect and Recall Report compiled by financial advisory firm Stout Risius Ross, in which is shown that 2019 was a record-setting year with 15 million vehicles recalled for electronic component defects. Half of the recalls involved software-based defects.

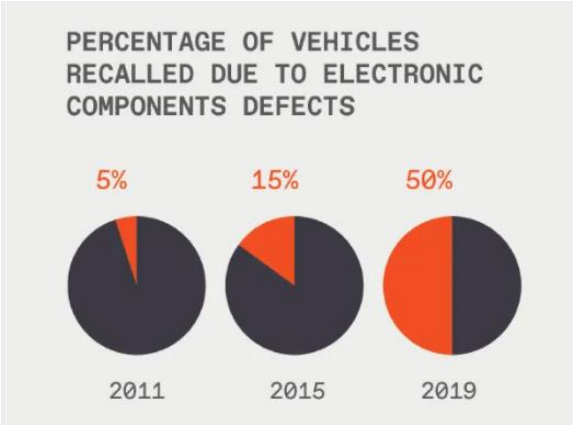


Figure 3: Percentage of vehicles recalled due to electronic component defects

Nearly 30% of the defects were related to software integration where a failure results from software interfacing with other electronic components or systems in a vehicle.
Stout Director Robert Levine notes that there has been a recent rise in component defects related to vehicle electronics “transitioning from owner convenience to safety critical components.”

Failure of even one of the various components inside an automobile is a major issue as the life of the driver, passengers or other road users might be endangered because of it.
The recent year explosion of E/E components installed in cars and SW complexity has triggered the need to adopt specific regulations relating to the E/E component of the vehicle and the definition of Functional safety.

1.1. Functional Safety in Automotive

IEC 61508 defines Safety as "the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or the environment [3]".
Safety is closely coupled to the risk of some kind of harm which might occur. In safety related systems this can be viewed from the point of view of how much harm the system causes.
The harm is evaluated with respect to the injuries it can cause to humans both the users of the system as well as other people in the environment. The lower the probability of such hazard to cause any harm the safer the system is. In automotive the overall vehicle safety can be seen from different perspectives. For example, there are active and passive safety mechanisms which reduce risk to the passengers and people near the vehicle, such as emergency braking systems. Functional safety looks at the risk which is introduced by the malfunctioning behavior of a system.
IEC 61508 defines Functional Safety as "a subset of the overall vehicle safety that depends on a system or equipment operating correctly in response to its inputs [3]".
Due to this a safety centric process that runs in parallel with the product development cycle has been introduced: functional safety analysis, concept development and integration with the software requirements has been added. The functional safety concept is developed to ensure that the component continues to work safely in the normal state of operation as well as in the state of failure.

In the automotive domain, the ISO 26262 standard captures the state of the art of functional safety. The ISO 26262 standard defines functional safety as follows: `absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems' [6].
What can be seen in the definition is that risk can never be completely removed, but should be brought down to a reasonable amount. To define malfunctioning condition it must be known with respect to what kind of expected behavior the system is supposed to have. A complete explanation of functional safety in automotive is given in [7], which explains the current techniques used in the automotive industry.

1.2. ISO 26262 standard compliance

ISO 26262 is a risk-based safety that applies to electric and/or electronic systems during vehicle production. It outlines a risk classification system (Automotive Safety Integrity Levels, or ASILs) and aims to reduce possible hazards caused by the malfunctioning behavior of electrical and electronic (E/E) systems.

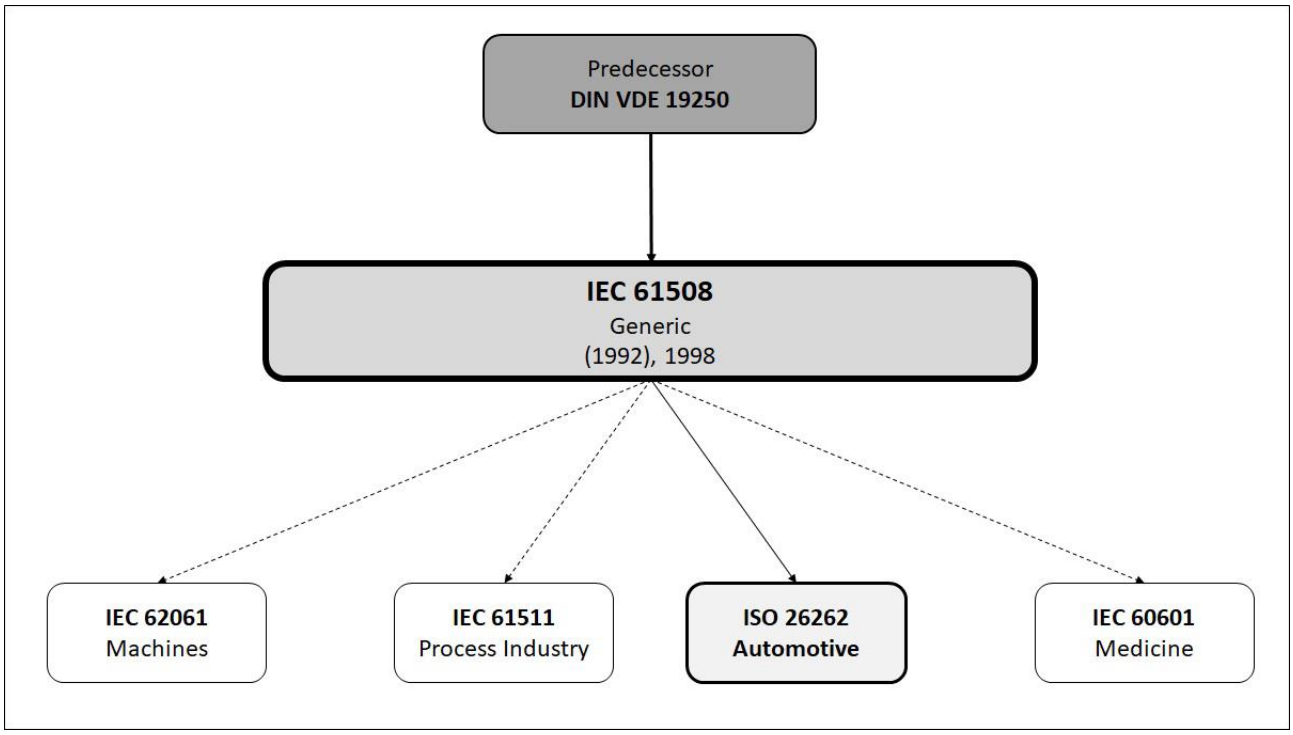


Figure 4: Evolution of safety standards in time

ISO 26262 can be shortly summarized as follow:

- Specifies a vocabulary (careful definitions of key terms like “fault” vs. “error” vs. “failure”)
- Defines standards for the safety lifecycle of individual automotive products
- Concept phase
- Product development at the system level, hardware level, and software level
- Production and operation
- Service and decommissioning

Provides an automotive-specific risk-based approach for determining risk classes (ASILs):

- Identifies and defines safety risks

- Establishes requirements to reduce those risks to acceptable levels
- Tracks requirements to ensure that an acceptable level of safety is achieved in the delivered product

The goal of the standard is to ensure safety through the whole lifecycle of automotive equipment and systems. Specific steps are required in each phase in order to ensure safety from the earliest concept to the point when the vehicle is delivered.
The ISO 26262 standard is composed of 10 parts, and each part is composed of a set of clauses, see Figure 1.3. Parts 3 until 7 correspond to the safety life cycle, part 2 to the company processes and parts 1 and 8 to 10 provide additional information. Following the classic V-model each step produces a work product which must be verified after implementation. The parts related to the product based aspect are the parts related to the safety life cycle of the system. All these parts focus on a different stages of development: the conceptual phase, system development, hardware development, software development and vehicle production. The clauses in these parts are called with requirements to which the project must adhere to. Then, at the end of a clause, it is denoted which required information should then be collected in the work products. Each clause can also require certain work products as input.

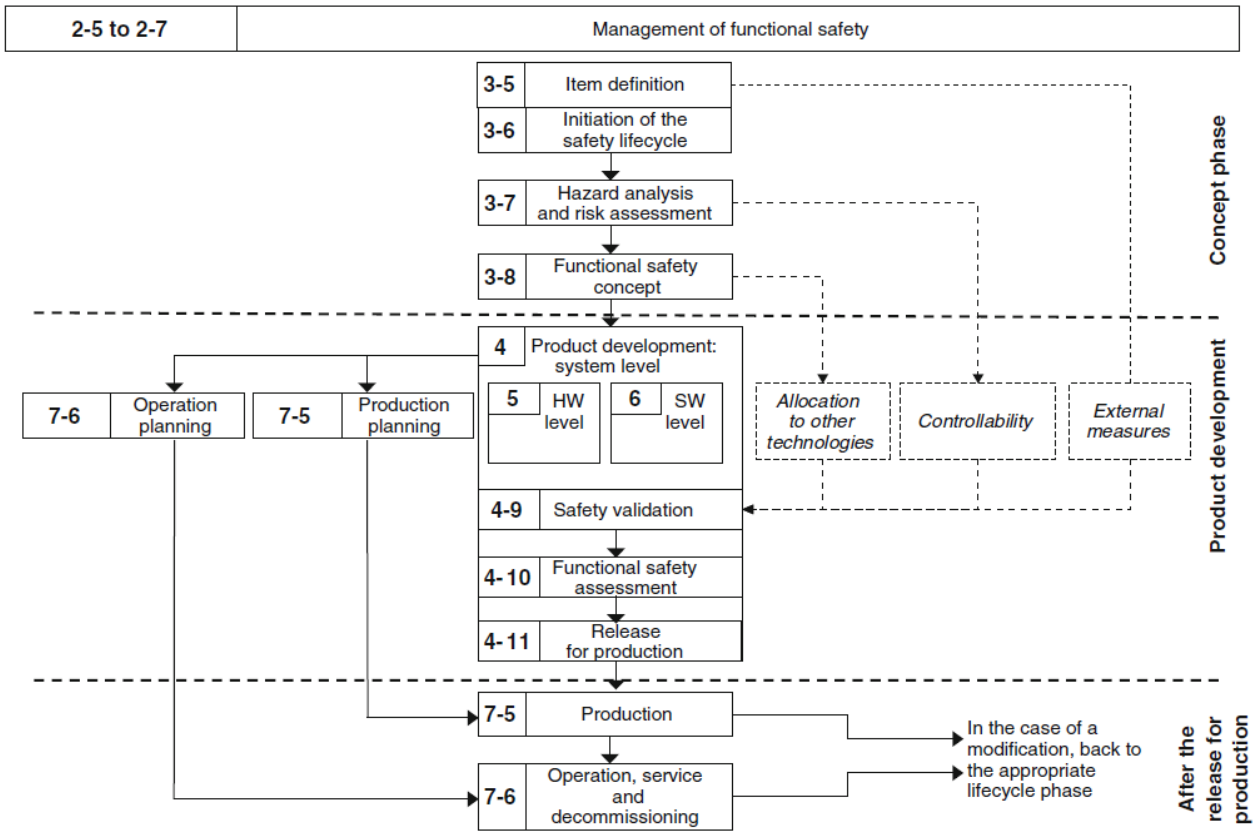


Figure 5: ISO 26262 clauses related to the safety life cycle

This work focuses on the hazard and risk analysis (HARA), clause 7 of part 3. The required work product for this section is the item definition that gives an overview of what the system do. Next to the functionalities, the dependencies and interface with the environment are defined also in the item definition. HARA consists of: situational analysis, hazard identification, hazardous event identification, determination of the Automotive Safety Integrity Level (ASIL) for the hazardous events and the creation of safety goals. The situational analysis is used to identify the operational situations and operating modes in which the vehicle can be. Then based on the functionality which the item provides it can be determined what kind of hazards can arise from a malfunction. Each hazardous event is classified using the three factors: severity (S), probability (P) of exposure (E) and controllability (C). Based on a table these factors are then converted to a discrete ASIL level (QM, A, B, C or D) for each hazardous event. The ASIL level indicates how much safety

effort need to be applied to reduce the risks. With Quality Management (QM) being the most lenient and D being the most restrictive. Better explanation is given in later chapters.
To prevent the hazardous event safety goal is defined. In the Functional Safety Concept (FSC) this goal, together with the preliminary architectural assumptions of the item, is further refined by means of defining the functional safety requirements: If a specific safety component must fulfill a safety requirement with ASIL D then many strict measurements have to be applied in order to make sure the component will not malfunction. This mitigates the risk which makes the component safer. A direct consequence of the FSC is the definition of the Technical Safety Concept (TSC) in which a high level characteristic of HW and SW is given.
To assure that a developed project is safe, evidence needs to be collected. This evidence should not only show compliance with the ISO 26262 standard but provide a sound reasoning which provides confidence in the safety of the system. This information is given by production of a specific Failure Mode analysis.

1.3. Vehicle categories and case study

Clearly defined vehicle categories are essential for the competitiveness of the automotive industry. The categories classify vehicles for regulatory purposes, enable manufacturers to benefit from the EU Single Market, and allow them to export their products beyond the EU. Vehicle categories are a crucial part of a well-functioning type-approval system. While the EU type-approval system allows manufacturers to benefit from the opportunities offered by the internal market, worldwide technical harmonization in the context of the United Nations Economic Commission for Europe (UNECE) offers them a market extending beyond European borders.

Passenger cars receive an “M” categorization, while commercial vehicles receive an “N” categorization. Two directives of the European Parliament and of the Council serve as sources for these definitions and classifications: 2002/24/EC of 18 March 2002 and 2007/46/EC of 5 September 2007. In addition, the EU legislation on driving licenses (Directive 2006/126/EC of 20 December 2006) provides for a splitting of some categories of vehicles:

Category	Vehicle type
Category L	Mopeds, Motorcycles, Motor Tricycles and Quadricycles
Category M	Motor vehicles having al least four wheels and for the carriae of passengers
Category N	Power-driven vehicles having at least four wheels and for the carriage of goods
Category O	Trailers (including semitrailers)

Table 1: Main categories of vehicle

In particular, vehicles that belongs to L category can be decompose as:

Category	Vehicle Description
Mopeds[1]	
L1e	Two-wheel vehicles with a maximum design speed of not more than 45 km/h and characterised by an engine whose: • cylinder capacity does not exceed 50 cm^3 in the case of the internal combustion type, or • maximum continuous rated power is no more than 4 kW in the case of an electric motor
L2e	Three-wheel vehicles with a maximum design speed of not more than 45 km/h and characterised by an engine whose: • cylinder capacity does not exceed 50 cm^3 if of the spark (positive) ignition type, or • maximum net power output does not exceed 4 kW in the case of other internal combustion engines, or • maximum continuous rated power does not exceed 4 kW in the case of an electric motor
Motorcycles[2]	
L3e	Two-wheel vehicles without a sidecar fitted with an engine having a cylinder capacity of more than 50 cm^3 if of the internal combustion type and/or having a maximum design speed of more than 45 km/h
L4e	Two-wheel vehicles with a sidecar fitted with an engine having a cylinder capacity of more than 50 cm^3 if of the internal combustion type and/or having a maximum design speed of more than 45 km/h
Motor tricycles	
L5e	Vehicles with three symmetrically arranged wheels fitted with an engine having a cylinder capacity of more than 50 cm^3 if of the internal combustion type and/or a maximum design speed of more than 45 km/h
Quadricycles: motor vehicles with four wheels having the following characteristics	
L6e	Quadricycles whose unladen mass is not more than 350 kg, not including the mass of the batteries in case of electric vehicles, whose maximum design speed is not more than 45 km/h, and whose • engine cylinder capacity does not exceed 50 cm^3 for spark (positive) ignition engines, or • maximum net power output does not exceed 4 kW in the case of other internal combustion engines, or • maximum continuous rated power does not exceed 4 kW in the case of an electric motor. These vehicles shall fulfil the technical requirements applicable to three-wheel mopeds of category L2e unless specified differently.
L7e	Quadricycles other than those referred to in category L6e, whose unladen mass is not more than 400 kg (550 kg for vehicles intended for carrying goods), not including the mass of batteries in the case of electric vehicles, and whose maximum net engine power does not exceed 15 kW. These vehicles shall be considered to be motor tricycles and shall fulfil the technical requirements applicable to motor tricycles of category L5e unless specified differently.

Notes:
1. As of 19 January 2013, mopeds will be subject to driving licence category AM
2. As of 19 January 2013, motorcycles will be subject to 3 categories of driving licence: A1 (max. 125 cm^3, 11 kW & 0.1 kW/kg), A2 (max. 35 kW & 0.2 kW/kg) [indicative 125-500 cm^3], and A (other motorcycles)

Table 2: L- category vehicle classification

Focusing on case study, L7e category can be divided in:

Heavy on road quad (L7e-A)		
A1	Maximum 2 straddle seats and handlebar steering	
	Power ≤ 15kW	
A2	Maximum 2 non-straddle seats	
	Power ≤ 15kW	
Heavy quadri-mobile (L7e-C)		
CP	Maximum 4 non-straddle seats	
	Power ≤ 15kW	
	Max speed ≤ 90 km/h	
	Enclosed passenger compartment	
CU	Maximum 2 non-straddle seats and loading area criteria	
	Power ≤ 15kW	
	Max speed ≤ 90 km/h	
	Enclosed passenger compartment	
Heavy all terrain quad (L7e-B)		
B1	Maximum 2 straddle seats and handlebar steering	
	Max speed ≤ 90 km/h	
	Wheelbase to ground clearance ratio ≤ 6	
B2	Maximum 3 non-straddle seats	
	Power ≤ 15 kW	
	Wheelbase to ground clearance ratio ≤ 8	

Table 3: L7e vehicle classification

1.4. Epic0

Epic0 is the first Italian vehicle for goods transportation fully electric. Designed and engineered with automotive standards, the vehicle is homologated as a heavy quadricycle and thanks to its small dimensions and the peculiar features of the chassis it allows to carry goods in an easy and economical way. The body is made up of a metal cabin combined with a high-strength chassis, derived from the automotive world, with a loading surface of 2.5 m^2 and a 700 kg capacity in its standard configuration that ensures passenger active and passive safety. The external dimensions are 1500 mm width and 3700 mm length.

Figure 6: Different models of Regis Epic0

Nowadays, the average speed measured in urban centers is around 20 km/h. For this reason, the autonomy performances of Epic0 have been conceived to cover the entire working day without worrying for recharging. Epic0 have faced this difficulty by equipping the battery pack with the latest-generation high efficiency cylindrical cells together with a composite architecture made of a BMS, an inverter and a LMU control unit designed by Regis Motor, that allow to achieve the best performances.

The vehicle can be equipped with different configuration as follows:

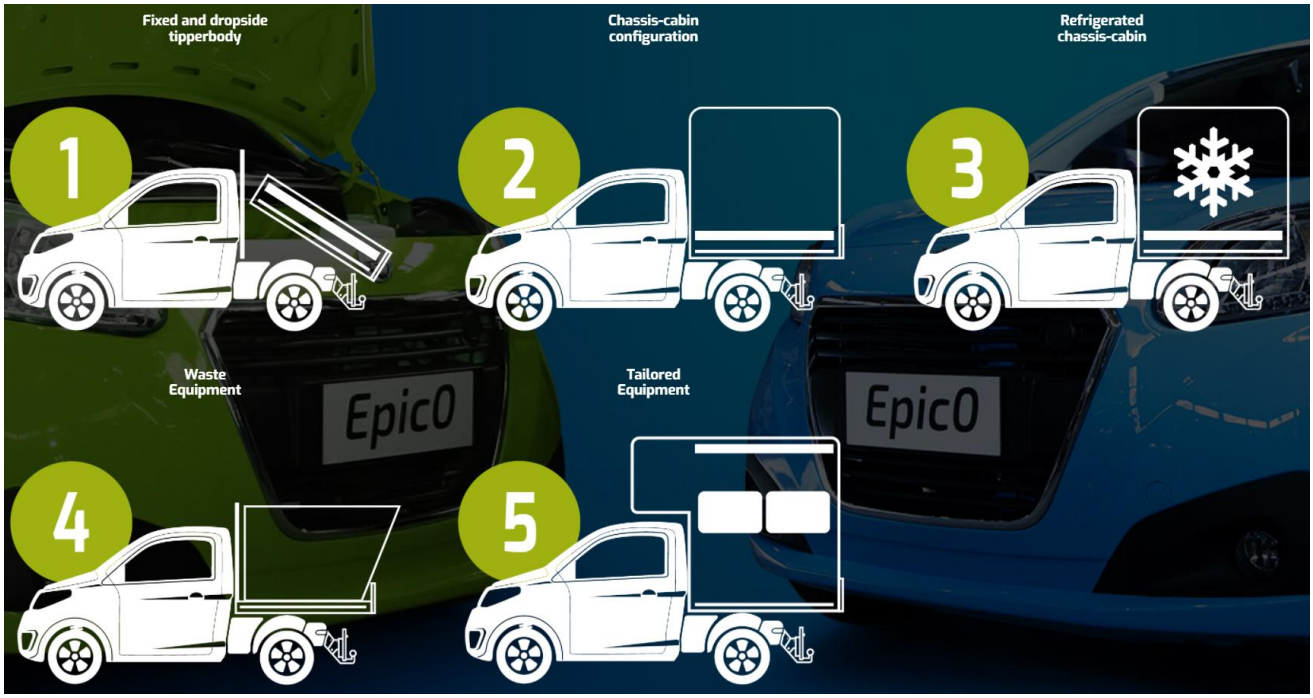


Figure 7: Epic0 configurations

More information about the vehicle can be found on Regis Motor website.

1.5. Thesis work

This thesis has been made in collaboration with Mecaprom Techologies Corporation Italia, an automotive engineering company founded in 1960 and Regis Motor, an Italian company with decades of experience in engineering that produces and sells a whole range of heavy electric quadricycles (L7e-CU vehicle) for Professional use.

Figure 8: Regis Motor logo

Figure 9: Mecaprom Technology Corporation Italia logo

This project aim is about studying Epic0 vehicle LMU, which is one of the safety-critical system in Regis Motor light trucks. Indeed, a wrong behavior of such a system could lead to hazardous events for the driver (such as engine stop or noncorrect torque management) as well for a road user (crash with another vehicle or pedestrian). Moreover, the focus will be on collecting and providing evidence about critical behaviors of LMU during normal operating phases. This is needed to lay the foundations for developing an ISO compliant

version of the LMU. Last part of the thesis is about lay the foundation for a FIDES analysis of a new board developed by a partner of Mecaprom in order to guarantee compliance with ISO 26262.

2. ISO 26262 Part 1: Vocabulary

This section will talk about the Part 1 listed under the ISO 26262 functional safety standard which consists of all the terminologies that are used in all the remaining parts of the ISO 26262. The purpose of this part is to give a clear and schematic view of all the terminology that will be used within the ISO standard.

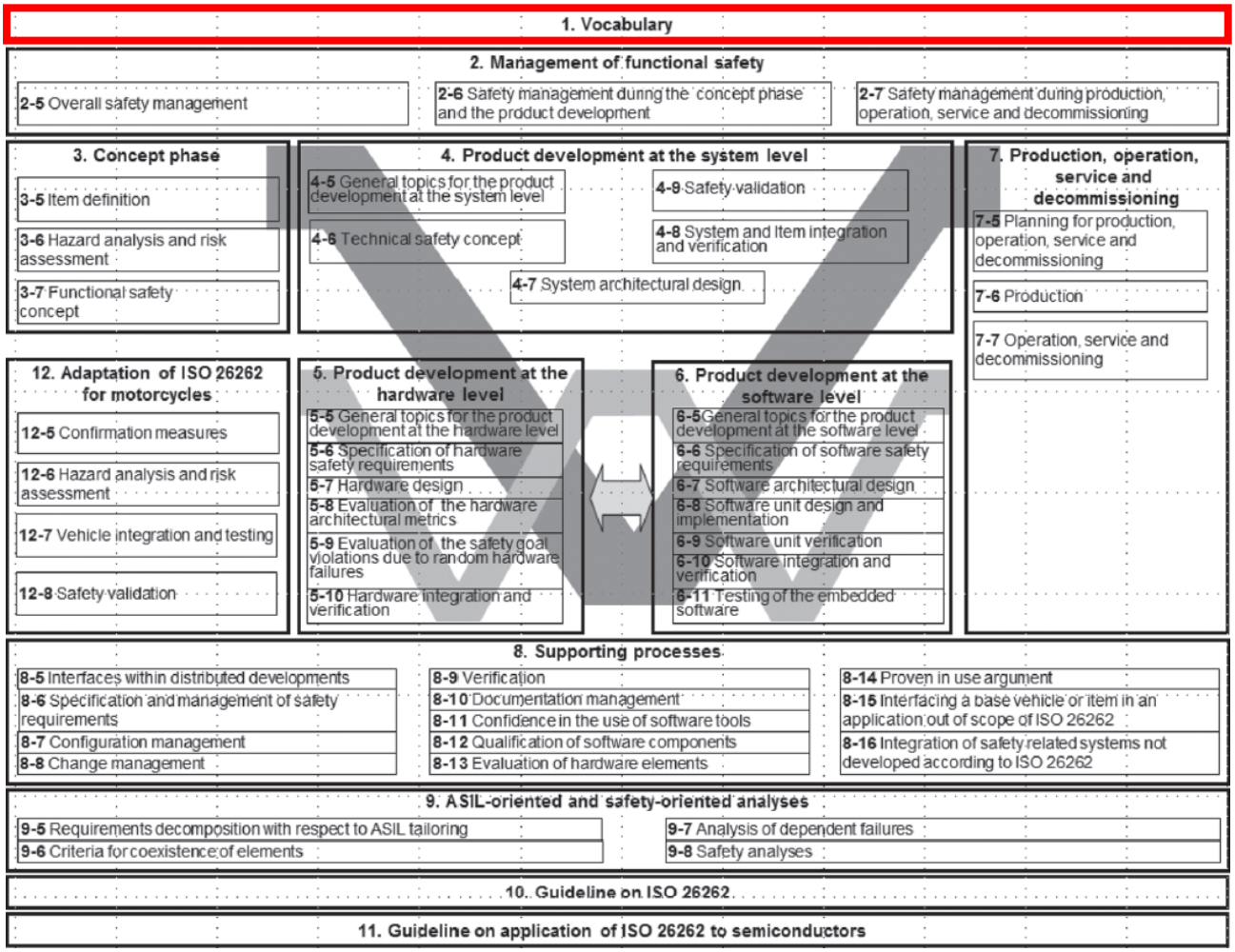


Figure 10: ISO 26262-Part1

2.1. Terms and definitions

Keeping in sight the scope of this thesis, some important and essential terms and definitions are listed from the ISO 26262 Part 1, as follows:

- Architecture – It is the representation of the structure of an item which allows the segregation of building blocks and interfaces involved.
- Automotive Safety Integrity Level (ASIL) – This consists of four levels so as to specify the item's safety measures. These are applied to avoid risk.
- ASIL decomposition - apportioning of redundant safety requirements to elements, with sufficient independence, conducing to the same safety goal, with the objective of reducing the ASILof the redundant safety requirements that are allocated to the corresponding elements
- Cascading failure – This is defined when the failure of an element causes another element to fail.

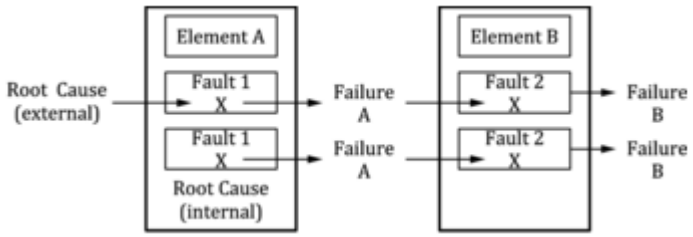


Figure 11: Cascading Failure

- Common cause failure – This is defined when the failure of two or more elements that have a single root cause.

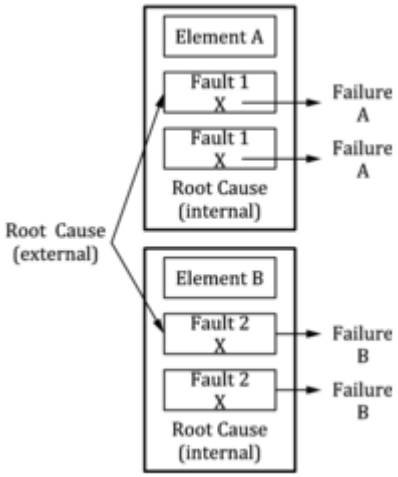


Figure 12: Common cause failure

- Component – It is a level of element that can be logically and technically be separable as it comprises of a number of hardware part and software units.
- System - set of components or subsystems that relates at least a sensor, a controller and an actuator with one another
- Electrical and/or electronic system – These are the systems which consist electrical and/or electronic elements. This may also include programmable electronic elements.
- Error – It is the difference that lies between an observed, computed or measured value against the specified, true or theoretically correct value.
- Element - system, components (hardware or software), hardware parts, or software units
- Failure – It is the inability of an element to execute the required function.
- Fault – abnormal condition that can cause an element or an item to fail
- Fault detection time interval - time-span from the occurrence of a fault to its detection
- Fault reaction time interval – time-span from the detection of a fault to reaching a safe state or to reaching emergency operation
- Fault tolerant time interval - minimum time-span from the occurrence of a fault in an item to a possible occurrence of a hazardous event, if the safety mechanisms are not activated

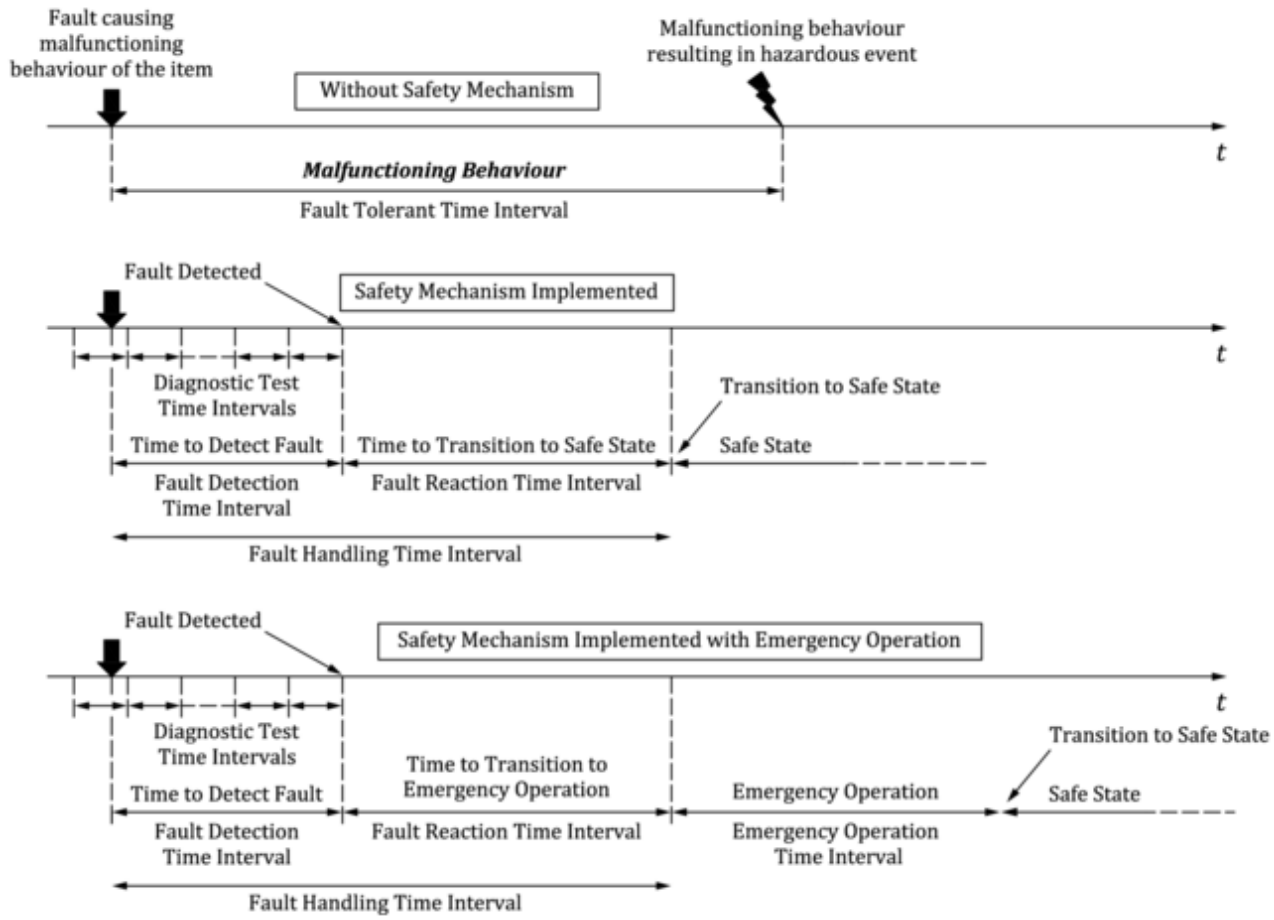


Figure 13: Safety relevant time intervals

- Functional safety concept – It is the detailed specification of the functional safety requirements. This consists of all the important information, allocation to architectural elements and their interaction. These all are highly necessary to achieve the safety goals.
- Functional safety requirement – It is the specification of implementation-independent safety behaviour/measure so as to achieve the safety goal.
- Hazard analysis and risk assessment (H&R) – It is the step that needs to be followed so as to recognize the hazardous events and then specify the safety goals. This is further extended by assigning an ASIL level to avoid any kind of risks.
- Item – It is the array of systems which is used to implement a function to which the ISO 26262 standard is applied.
- Technical safety concept - specification of the technical safety requirements and their allocation to system elements with associated information providing a rationale for functional safety at the system level
- Technical Safety requirement - requirement derived for implementation of associated functional safety requirements
- Safe state - operating mode, in case of a failure, of an item without an unreasonable level of risk
- Risk - combination of the probability of occurrence of harm and the severity of that harm
- Hazard - potential source of harm (physical injury or damage to the health of persons) caused by malfunctioning behaviour of the item
- Functional safety - absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

3. ISO 26262 Part 3: Concept Phase

This section describes all the fundamentals that are included in the Part 3 of the ISO 26262 functional safety standard. This is the part of the standard that lay the foundations for the development of the study carried out during the work of theses.

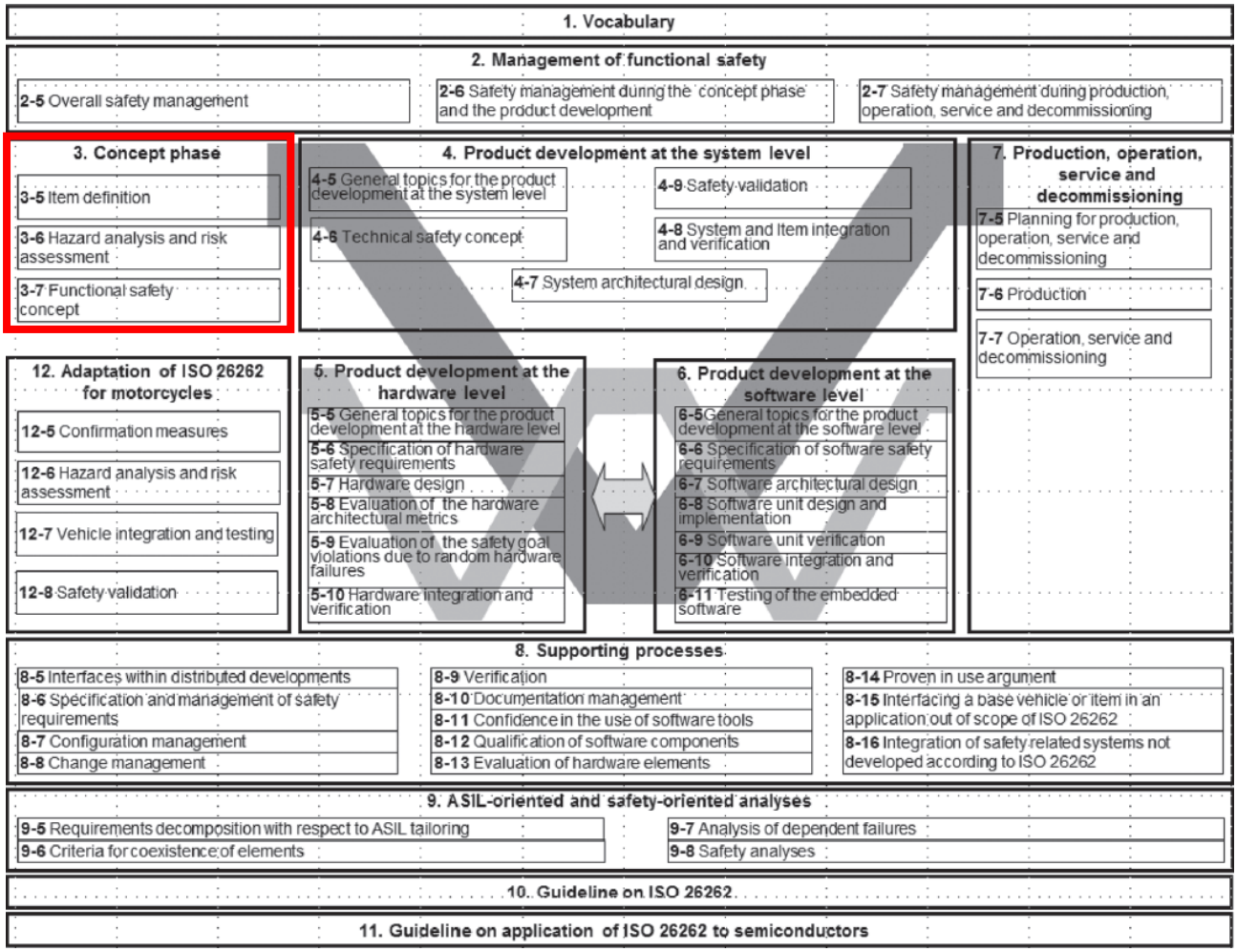


Figure 14: ISO 26262-Part3

As the figure shows, the concept phase consists of 4 individual steps. Each of these steps is described in detail in a separate chapter of part 3 of the norm:

- 3-5: Item definition
- 3-6: Hazard analysis and risk assessment
- 3-7: Functional safety concept

3.1. Item Definition

The foremost task of this sub-section is to first define the item followed by it dependencies and interaction with the environment giving rise to functional and non-functional requirements of the item. They can further

be classified as safety-related once and, in this case, their respective ASIL are declared. Information contained in this first section are the following:

- The functional concept
- The environmental and operational constraints
- Behavioural assumptions of the item
- Consequences of hazards and failure modes
- Scenarios effecting the functionality of the item

Another important differentiation is between a new or a modification of the item. As the system under consideration of this thesis is a new system, all the activities revolving around modifications of the item are ignored.

3.1.1. Intended use

In the thesis work the focus was on the Function responsible for the management Torque request. The purpose of the system is to deliver the correct amount of torque (positive or negative) according to how requested by the driver.

The classes of users are:

- All drivers

The possible foreseeable misuses of the item are:

N.A.

3.1.2. Primary Functions

- To apply the correct amount of torque requested

3.1.3. Operating scenarios and environmental constraints

The function shall be available in any driving scenario when driving backward/forward and it shall be when the key is turned ON.

The interfaces of these system are:

- Driver → System:
  - Gas pedal
  - Brake pedal
  - NDR gear
- System → Driver:
  - Torque management function is in fail → Lamp blinking and cockpit error message
- Terrain road types
  All terrain
- Weather and climate conditions
  All conditions

3.2. Hazard Analysis and Risk Assessment

The objective of the hazard analysis and risk assessment is to identify the hazards that may cause malfunctions in the item and falsify the safety goals. So basically, they are used to determine the ASIL levels so as to achieve the safety goals for the item in order to remove the advent of any risks.

The next step is determining the situation analysis along with the hazard identification. The operating modes and the operational situations which lead the item to a hazardous event is described. The operational situation talks about the limits in which the item is in bounds to be safe. The hazardous events are determined so as to get multiple relevant combinations of different hazards and operational situations.

The ASIL is calculated by 4 parameters: severity [S], probability of exposure [E] and controllability[C]. If the classification of a specific hazard in terms of severity, probability of exposure and controllability is becoming a difficult affair then always the higher ASIL level should be assigned.

3.2.1. Severity

The severity can be assigned from one of the following severity classes, namely; S0, S1, S2 or S3 as in table 4. The main focus of this part is on the harm that each person is potentially at along with risks associated to other road users as cyclists or pedestrians. The severity class is based upon the height to which the person is injured.

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

Table 4: Classes of Severity

3.2.2. Exposure

The probability classes are as follows; E0, E1, E2, E3 and E4 as in table 5. The exposure determination is based upon the probability of the likeliness of the hazardous event.

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

Table 5: Classes of probability of Exposure

3.2.3. Controllability

This then needs to be assigned to the controllability classes, namely; C0, C1, C2 and C3 as in table 6. The determination of the controllability is an idea that the driver or the persons probably involved in the risk are able to control and mitigate the same to their fullest capacity. Under this also all the reasonable foreseeable misuses are taken into consideration. In context where the hazardous event is not talking about the vehicle direction and speed, the controllability is judged by the fact that the person at risk is able to mitigate themselves from the hazardous situation.

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

Table 6: Classes of Controllability

3.2.4. ASIL definition

The final step is determining the safety goals and ASIL levels. The ASIL level is determined by severity, probability of controllability and exposure as seen in table 7. There are four ASIL levels and are defined as: ASIL A, ASIL B, ASIL C and ASIL D. Where, ASIL A is the lowest and ASIL D is the highest safety integrity level. Along with these; quality management (QM) specifies no requirement to be implemented in compliance with ISO 26262 standard.

ASIL Rankng Table					
Severity (How Bad)	Probability of Exposure		Controlability by driver		
			C1 Simply Controllable >99% of drivers able to control	**C2** Normally Controllable >90% of drivers able to control	**C3** Difficult to Control <90% of drivers able to control
S1 (Light or Moderate Injury)	**E1**	Very Low	QM	QM	QM
	E2	Low < 1%	QM	QM	QM
	E3	Medium 1~10%	QM	QM	ASIL - A
	E4	High > 10%	QM	ASIL - A	ASIL - B
S2 (Severe Injury / Survival Probable)	**E1**	Very Low	QM	QM	QM
	E2	Low < 1%	QM	QM	ASIL - A
	E3	Medium 1~10%	QM	ASIL - A	ASIL - B
	E4	High > 10%	ASIL - A	ASIL - B	ASIL - C
S3 (Life Treatening Injury)	**E1**	Very Low	QM	QM	ASIL - A
	E2	Low < 1%	QM	ASIL - A	ASIL - B
	E3	Medium 1~10%	ASIL - A	ASIL - B	ASIL - C
	E4	High > 10%	ASIL - B	ASIL - C	ASIL - D

Table 7: ASIL determination

A safety goal is set for each hazardous event along with an ASIL level. Similar safety goals are combined into one goal. And the highest determined ASIL level is assigned to the respective safety goal. In cases where the safety goal can be reached upon by transitioning/maintaining to one or more safe states, then these safe- state have to be defined and specified.

Before starting with the definition of the ASIL level it was necessary, as described in table 8, to clearly define some guideword in order to better understand how the study has been made and what potential malfunction has been analysed.

Primary Function Category	Guidewords	Descripion\Definition
Loss of Function	Does Not	Does not function at all
		Cannot be activated/started
	Stops	Stop functioning prematurely
Unintended Activatio of Fuction	Unintended	The function is activated when not desired, expected or requested
Stuck Function (Activated)	Stuck	The function becomes locked or stuck in the activated state and cannot be de-activated or turned off
Incorrect function \\ The item persforms the function, but incorrectly	Excessive	Function out of specification on the high side (more than desired, expected or requested action occurs)
	Incomplete	Function out of specification on the low side (less than desired, expected or requested action occurs)
	Too Quick	Function outside of specification faster than desired or requested
	Too Slowly	Function outside of specification slower than desired or requested
	Duration Too Long (only if function has specific duration)	Function outside of time duration specification too long
	Duration too short (only if function has specific duration)	Function outside of time duration specification too short
	Delayed	Delay in start of function
	Inverse	Function is performed in the opposite way the desired, expected or requested
	Uneven	A non-uniform distribution of forces/action

Table 8: guidewords for Malfunctioning behavior

Once the terminology is established, the possible malfunctions of the function under analysis are explained, table 9, and the potential hazards resulting from each malfunction are defined, table 10.

Primary Function Description	Guidewords for Malfunctioning Behavior												
	Does Not	Stops	Unintended	Stuck	Excessive	Incomplete	Too Quickly	Too Slowly	Duration Too Long	Duration Too Short	Delayed	Inverse	Uneven
Provide positive torque (D Gear)	M1	M2	M3	M4	M5	M2	N/A	M6	N/A	N/A	M7	M8	M9
Provide negative torque (R gear)	M10	M11	M12	M13	M14	M11	N/A	M15	N/A	N/A	M16	M17	M18
Provide brake torque (Brake pedal)	M19	M20	M21	M22	M23	M20	N/A	M24	N/A	N/A	M25	M26	M27
Provide null torque (N gear or Traction	M28	M29	M30	M31	N/A	M29	N/A	M32	N/A	N/A	M33	N/A	N/A

Table 9: possible malfunction (M)

Function	Malfunction	Hazard	Hazard description
Provide positive torque (D Gear)	M1	H1	Loss of torque
	M2	H1	Loss of torque
	M3	H2	Vehicle destabilization
	M4	H2	Vehicle destabilization
	M5	H2	Vehicle destabilization
	M6	H1	Loss of torque
	M7	H1	Loss of torque
	M8	H1	Loss of torque
	M9	H1	Loss of torque
Provide negative torque (R gear)	M10	H1	Loss of torque
	M11	H1	Loss of torque
	M12	H2	Vehicle destabilization
	M13	H2	Vehicle destabilization
	M14	H2	Vehicle destabilization
	M15	H1	Loss of torque
	M16	H1	Loss of torque
	M17	H1	Loss of torque
	M18	H1	Loss of torque
Provide brake torque (Brake pedal)	M19	H3	Loss of brake torque
	M20	H3	Loss of brake torque
	M21	H2	Vehicle destabilization
	M22	H2	Vehicle destabilization
	M23	H2	Vehicle destabilization
	M24	H3	Loss of brake torque
	M25	H3	Loss of brake torque
	M26	H2	Vehicle destabilization
	M27	H3	Loss of brake torque
Provide null torque (N gear or Traction inhibition ON)	M28	H4	Unwanted movement
	M29	H4	Unwanted movement
	M30	H1	Loss of torque
	M31	H1	Loss of torque
	M32	H4	Unwanted movement
	M33	H4	Unwanted movement

Table 10: Malfunction - Hazard relation

It is now possible to proceed with the definition of HARA. During this phase, all the Hazards and Malfunctions defined above were considered and analysed in the worst possible working scenario, Table 11.

Hazardous Event ID	Malfunctioning Behavior	Mishap Scenario			ASIL Assessment				Safety Goal ID	SG Description
		Potential Hazardous Effect	Vehicle Operation Situations	Persons at Risk	S	E	C	ASIL		
H1	M1, M2, M8, M9	N/A	V>50kph Overtaking Cornering	driver	0	4	0	QM	\	\
H1	M6, M7	N/A	Any speed Junction Low visibility	driver	1	2	1	QM	\	\
H2	M3, M4, M5	Potential vehicle out of road/crash	Urban road Low speed Cornering	driver, road users	3	4	1	**B**	SG1	Avoid vehicle destabilization
H1	M10, M11, M17, M18	N/A	Low speed Urban road Straight driving	driver, pedestrian	1	3	1	QM	\	\
H1	M15, M16	N/A	Any condition	driver,	0	3	0	QM	\	\
H2	M12, M13, M14	Potential pedestrian collision	Urban road Low speed Straight driving	driver, pedestrian	2	4	1	**A**	SG1	Avoid vehicle destabilization
H3	M19, M20, M24, M25, M27	Potential Collision	High speed Traffic condition Straight driving	Driver, road users	3	3	3	**C**	SG2	Avoid loss of brake torque
H2	M21, M22, M23, M26	Potential vehicle out of road/crash	Cornering Any speed Urban road	driver, road users	3	4	2	C	SG2	Avoid vehicle destabilization
H4	M28, M29, M32, M33	Potential pedestrian collision	Urban road Low speed	driver, pedestrian	2	4	0	QM	\	\
H1	M30, M31	N/A	Any Condition	driver	0	4	0	QM	\	\

Table 11: HARA

3.3. Functional Safety Concept

The core fundamental behind the functional safety concept is to extract the functional safety requirements. This is done from the safety goals and then assign them to different architectural elements of the item. The functional safety concept consists of parts that majorly focus on goal of achieving safety, namely; safety measures, safety mechanisms, etc. These are defined in the functional safety concept because they are then executed in the architecture of the item. The functional safety concept talks about the below mentioned points:

- Failure mitigation and fault detection
- Safe state transitioning
- Mechanisms for fault tolerance
- Detection of a fault and warning the driver

Post the H&R the safety goals are thought about as in figure 17. And then the functional safety requirements are derived from them.

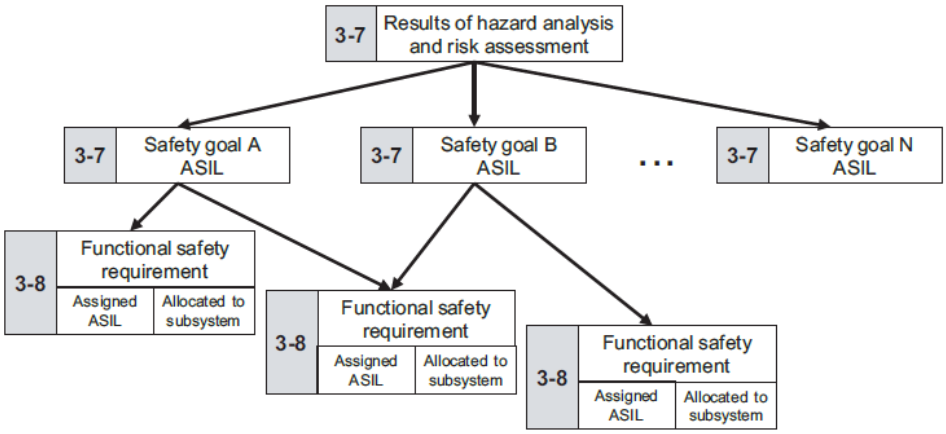


Figure 15: Hierarchy of safety goals and related functional safety requirements

The orientation of the safety requirements in prospect to different parts of the ISO 26262 are illustrated in figure 18. And the functional safety requirements are distributed amongst the elements of the architecture.

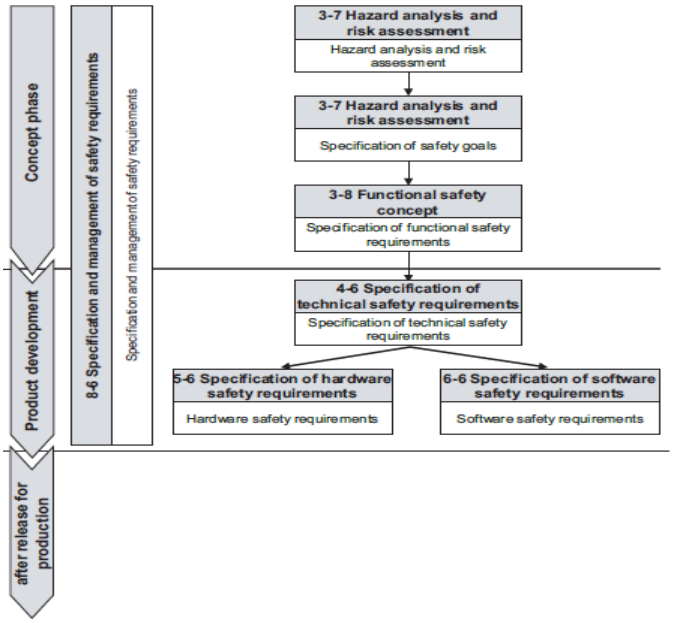


Figure 16: Structure of the safety requirements

As shown in previous tables, ASIL generated by similar condition, were grouped and the highest ASIL level was chosen and then Safety Goals were defined. In order to better describe every Safety Goal, a Functional Safety Requirement (FSR) and a Technical Safety Requirement (TSR) were made. First step was the definition of a safe state (table 12) and then every Safety Goal was divided in various FSR (Table 13).

SAFE STATE	NAME	DEFINITION
SS1	Veh. STOP & Brake	Vehicle unable to move

Table 12: Safe State definition

Safety Goal ID	SG description	ASIL	Functional Safety Requirement	
			ID	Description
SG1	Avoid vehicle destabilization	B	FSR1	If an error occurrs: torque decrasing of 60% until SS1
			FSR2	In case of malfunction the driver must be warned by the use of a cockpit message
			FSR3	Error message must be shown until car is switched OFF
			FSR4	Torque must be correclty generated and actuated
			FSR5	All error message must be saved into an internal storage memory
SG2	Avoid loss of brake torque	C	FSR6	In case of malfunction the driver must be warned by the use of a cockpit message
			FSR7	Error message must be shown until car is switched OFF
			FSR8	All error message must be saved into an internal storage memory
			FSR9	Brake torque must be correctly generated and actuated
			FSR10	If an error occurs: all commands related to a generation of positive torque must be set to 0

Table 13: Functional Safety Requirement description

4. ISO 26262 Part 4: Product development at the system level

This section of the thesis deals with the steps involved in order to proceed with the product lifecycle at the system level.

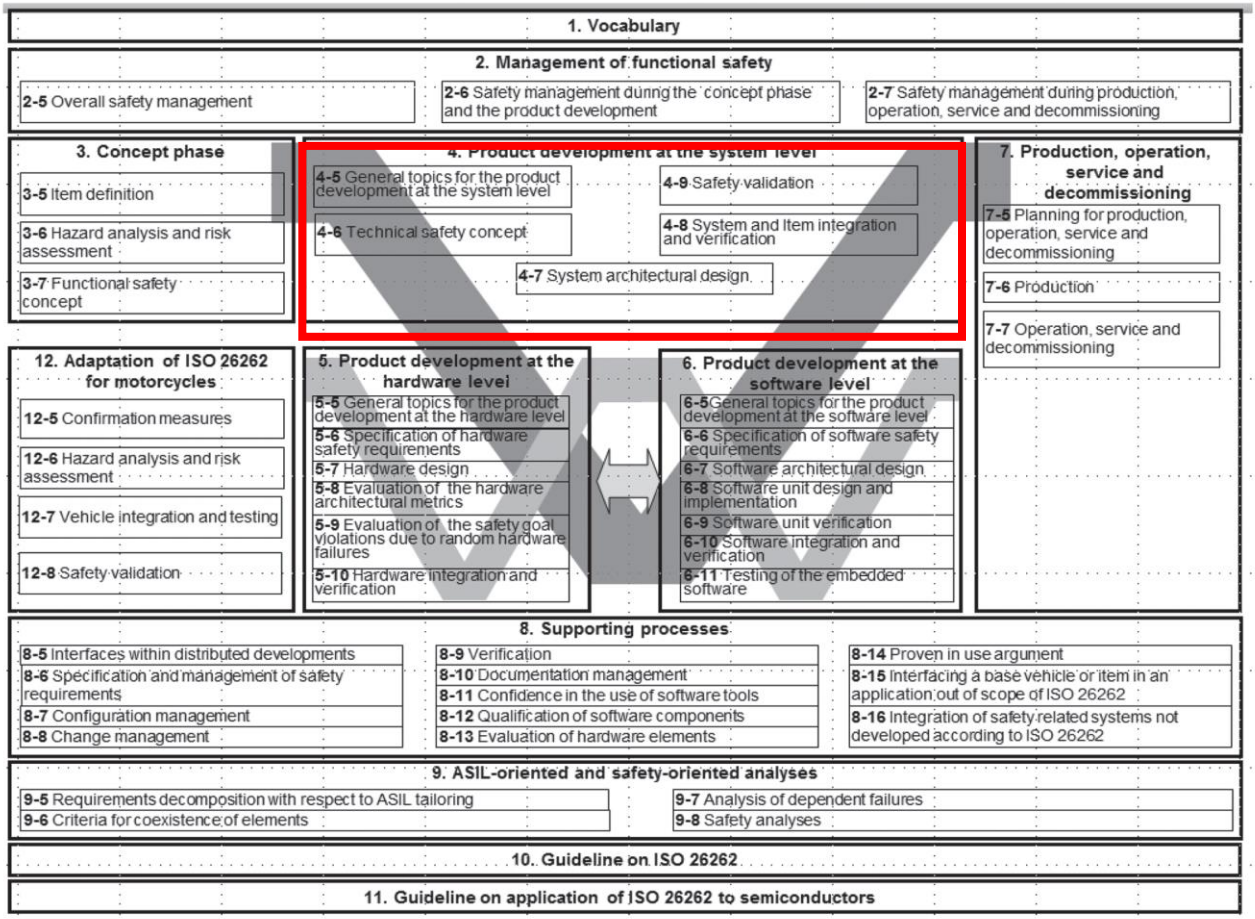


Figure 17: ISO 26262 – Part4

This section will explain all the necessary steps mentioned in the Part 4 of the ISO 26262 functional safety standard about the system level development. This phase finds it place between the concept phase and the simultaneous phases of development at hardware and software. Thus, this is an important part of the ISO 26262 as the decisions made for the system for a particular process governs how the system behaves throughout the lifecycle of the product until it is decommissioned.

4.1. Scope

The requirements needed for the development of the product at the system level of an automotive application is specified under this part of the ISO 26262 and includes the following [21]:

- Initiation of product development at the system level
- Specification of technical safety requirements
- Technical safety concept
- System design
- Item integration and testing
- Safety validation

- Functional safety assessment
- Product release

4.2. Specification of technical safety requirements

The core motive behind initiation of the product development at the system level is to design the activities for functional safety for system development. These activities will be included in the safety plan. All the necessary activities involved during the development of a system are described well in figure 20.

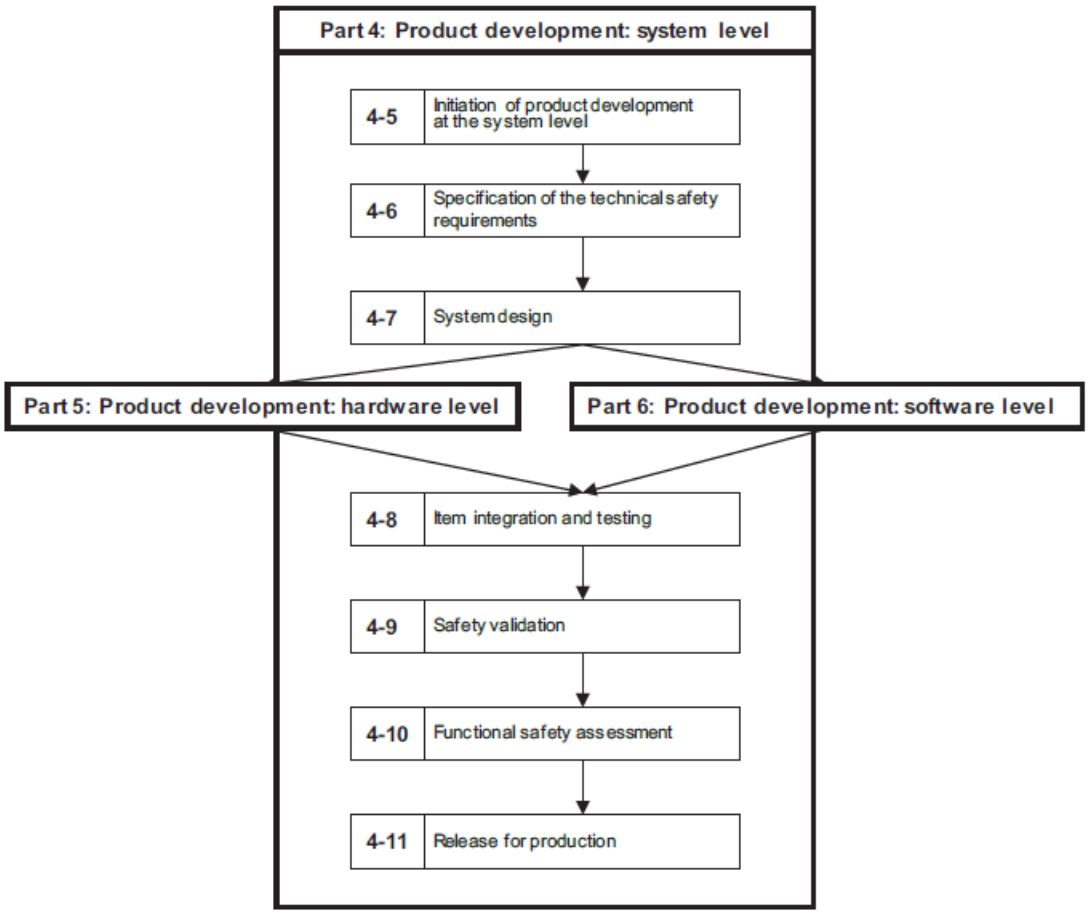


Figure 18: Reference phase model for the development of a safety-related item

In cases where the system consists of multiple levels of integration figure 21 provides an outline about its association with different part of the ISO 26262.

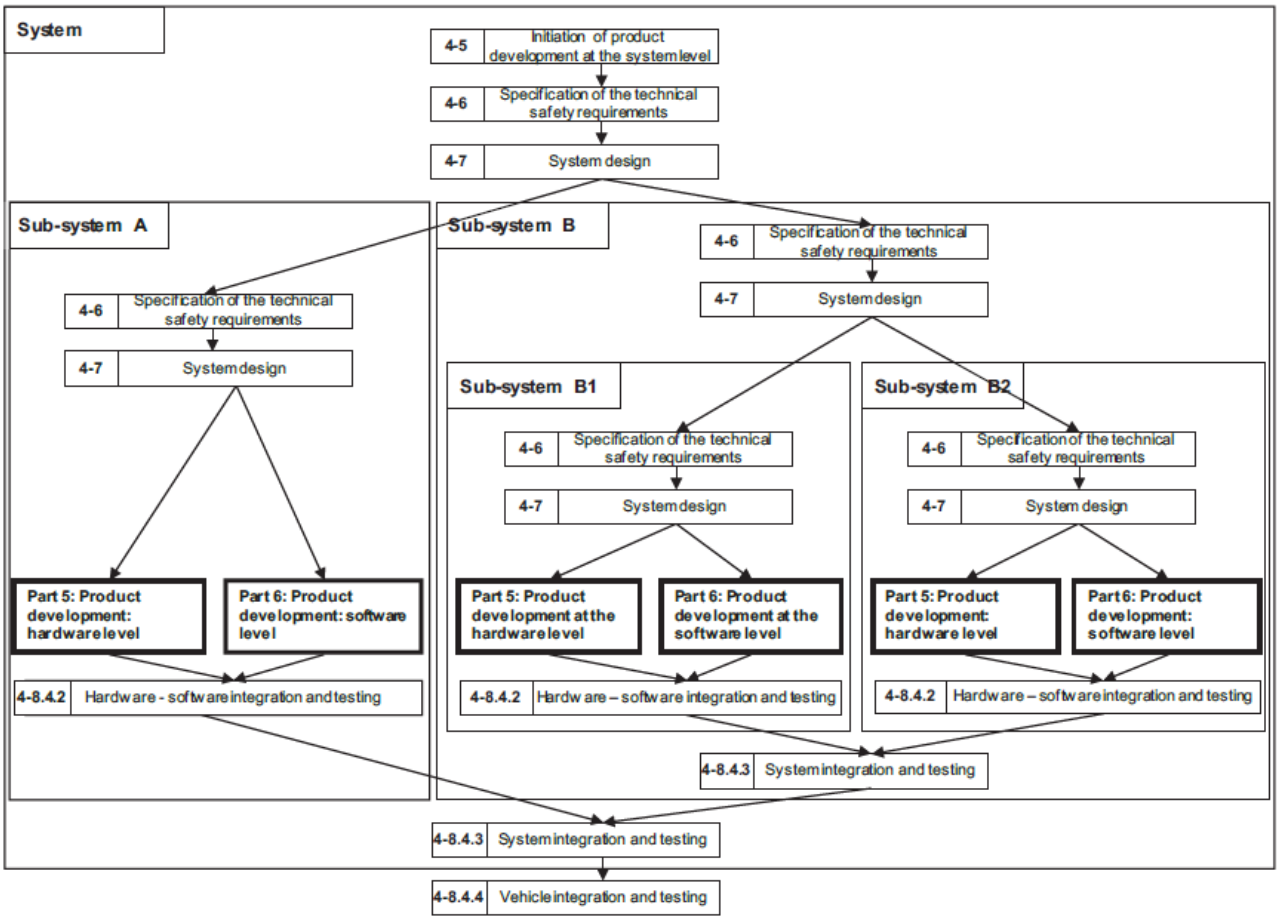


Figure 19:Detailed view of product development at the system level

The first objective is to determine the technical safety requirements. This is refined from the functional safety concept. The second objective is to check whether the technical safety requirements are in par with the functional safety requirements through analysis. As the technical safety requirements are basically the requirements used to implement the functional safety concept, the other goal that lies with it is to assure that the item-level functional safety requirements are parted into the system-level technical safety requirements. While designing the architecture and system properties of the item the following should be taken under consideration:

- All the interfaces required for communication
- Constraints such as functional constraints or environmental conditions
- System configuration requirements

As the technical safety requirements describe the way the elements respond to scenarios that affect the penultimate point of achieving the safety goal, there are certain safety mechanisms to be considered for adhering to the ISO 26262 functional safety standard. These safety mechanisms shall be included in the technical safety requirements along with:

- Measures for detection, direction and control of the system during the event of a fault and/or from external devices
- Measures aiding the system to achieve/maintain a safe state
- Measures for the implementation of the warning and degradation concept
- Measures preventing faults from becoming latent

The measures that aid the system to achieve and then maintain the described safe state the following is to be specified:

- Safe state transition
- Fault tolerant time interval
- Measures to make sure that the safe state is maintained

The technical safety requirements of the requirements for the sample system are mentioned below.

TECHNICAL SAFETY REQUIREMENTS OVERVIEW		
Code	**Description**	**Definition**
TSR1	General signals acquisition	All signals must be phisically acquired twice and compared (redundancy)
TSR2	Gas pedals acquisition	Acquisition of redundant potentiometer signals: different and indipendent signal acquistion made by using 2 potentiometers connected to the same pedal and than compared
TSR3	Signals management	All signal must be manage by using separate microcontroller and compared in different and consecutive instant of time
TSR4	Encoder acquisition	Encoder signal (position) reading must be done separately on Front motor and Rear motor
		F and R acquisition made by using 2 different ABZ encoders with 90 mechanical degrees offset
TSR5	Power supply management	Power supply (both positive and negative) must be correctly protected agains unwanted behavior
TSR6	Error management	When an error occurs in the Torque management function it must be saved in the internal memory
TSR7	Velocity calculation	Velocity value obtained by calculation based on F and R encoder values
		Velocity comparison made when V>5km/h in order to avoid problems related to slipping
TSR8	Hill holding acquisition	Hill holding signal compared with vehicle motion. Aquisition and comparison made separately on Front or Rear axe
		If Automatic parking brake comes (inverter switch off), when the vehicle come back to hill holding mode is necessary a re-calculation of the Torque needed to take the vehicle in balance
TSR9	Gear signal correct acquisition	If concord Gear signals acquisition: Gear signal compared with Front or Rear encoder signal & compared with Hill Holding signal & Velocity value
TSR10	Traction inhibition	Acquisition of redundant Traction inhibition signal: inhibition signal CAN message is acquired twice and than compared
		Acquisition of redundant brake pedal signal: brake signal is acquired twice and than compared
		Acquisition of redundant door and trunk open signal: signal acquired twice and than compared
TSR11	Automatic Parking Brake	Velocity value Front compared with the Rear one
		Brake signal acquired twice at a distance of 1 second and than compared
		Torque value necessary to mantain the vehicle in STOP mode acquired twice and than compared

Table 14: Technical safety requirement of Torque managements functions

4.3. System design

The first objective lies in developing the design of the system and the technical safety concept. The second objective incorporated in this this sub-phase is to verify the design of the system made and the technical safety concept. So to develop a system architectural design for a particular system there are different activities that need to be covered, namely; technical safety requirements, functional safety requirements and non-safety-related requirements. Therefore, both safety and non-safety-related requirements are taken care of.

The activities on which the system design basically depends upon are the functional concept along with the assumptions made about the technical safety requirements and the architecture. Next activity is regarding the system architectural design. The technical safety requirements along with their respective ASIL level should be adhered while designing of the system and subsystem architecture. Then the ISO 26262 talks about the measure so as to prevent the advent of systematic failures. For this a safety analyses needs to be run on the system design which is further elaborated in table 3.5 [21].

All the tables mentioned in this standard follow a level of recommendation for the respective methods and these are categorized as:

- A "++" means that the method is highly recommended
- A "+" means that the method is recommended
- A "o" means that the method has no recommendation

Methods		ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++
[a] Deductive analysis methods include FTA, reliability block diagrams, Ishikawa diagram.					
[b] Inductive analysis methods include FMEA, ETA, Markov modelling.					

Table 15: System design analysis

Once the identification of the external and internal causes for probable systematic failures is achieved, thereafter the ways in which they should be discarded should be though about. And 39 for the same the renowned automotive design principles for the system should be taken into account and including the following:

- Using well-renowned technical safety concepts
- Using well-renowned designs for elements
- Using well-renowned mechanisms for the detection of failures and their control
- Using well-renowned standardised interfaces

The results from the implementation of these on the item then need to be analysed. This applies to all the ASIL levels so as to avoid any failures from architectural design and high complexity. And should exhibit the properties like simplicity, granularity and modularity by the principles mentioned in table.

Properties		ASIL			
		A	B	C	D
1	Hierarchical design	+	+	++	++
2	Precisely defined interfaces	+	+	+	+
3	Avoidance of unnecessary complexity of hardware components and software components	+	+	+	+
4	Avoidance of unnecessary complexity of interfaces	+	+	+	+
5	Maintainability during service	+	+	+	+
6	Testability during development and operation	+	+	++	++

Table 16: Properties of modular system design

4.4. Item integration and testing

This phase basically consists of three phases and two goals: the first phase involves the integration of hardware and software. The second phase talks about the integration process of all the elements to form a complete system. The third phase is about the integration of the item under consideration with various other systems present in the environment of the item.

Looking into the first objective is about the testing of compliancy of every safety requirement with respect to its particular ASIL level. The second objective lies in verifying the system design. The whole integration process is a step-by-step process starting right from hardware-software integration followed by system and

vehicle integration. There are certain tests to prove the accordance of the integrations that happen at all the mentioned stages correctly in this sub-phase of the ISO 26262.

Once there is ample development at the hardware and software the integration at the system level can start. Testing the integration to ensure that the system design is in-par with the technical and functional safety requirements is the next step and the following need to be taken care of during the same:

- Precise implementation of functional and technical safety requirements
- Precise implementation of interfaces
- Robustness

Steeping deeper into system integration the following shall be performed:

- Refined hardware-software integration and testing plan
- Specifications of test at system and vehicle level should be a part of the item integration and testing plans
- Interfaces and the environment must be considered in the system and vehicle level item integration and testing plans

Methods		ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Analysis of external and internal interfaces	+	++	++	++
1c	Generation and analysis of equivalence classes for hardware-software integration	+	+	++	++
1d	Analysis of boundary values	+	+	++	++
1e	Error guessing based on knowledge or experience	+	+	++	++
1f	Analysis of functional dependencies	+	+	++	++
1g	Analysis of common limit conditions, sequences, and sources of dependent failures	+	+	++	++
1h	Analysis of environmental conditions and operational use cases	+	++	++	++
1i	Analysis of field experience	+	++	++	++

Table 17: Methods for deriving test cases for integration testing

For targeting the correct implementation of the hardware-software integration and testing table gives some feasible test methods.

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	++	++	++
1c	Back-to-back test[c]	+	+	++	++

Table 18: Correct implementation of technical safety requirements at the hardware-software level

These are applied to all the ASIL levels. Table talks about the probable effect that the hardware fault detection mechanisms may concur. This also considers the diagnostic coverage of fault models at hardware-software level and can be done by methods present in table

Methods		ASIL			
		A	B	C	D
1a	Fault injection test[a]	+	+	++	++
1b	Error guessing test[b]	+	+	++	++

Table 19: Effectiveness of a safety mechanism's diagnostic coverage at the hardware-software level

This sub-section also entertains the possibility of integration and testing at the system and vehicle level. All the necessary test goals along with their test methods are listed clearly in it. This is also supported by ample number of tables to guide through it. But these are not evaluated in this thesis as it jumps out of bounds.

4.5. Safety validation

The first objective that is stated under this is to assure that whether the functional safety concept and the safety goals concur towards the functional safety of the item. The second objective talks about these goals being true and fully implemented at the vehicle level. This is to make sure that the results deriving from each activity adhere to their respective requirement.
The validation process of the item assures that it sticks to the functionality it was designed for and that it adheres towards the safety measures assigned to it. This plan for validation should include:

- Configuration of the item
- Specification of procedures, driving manoeuvres, test cases for validation purposes
- Required equipment and environmental conditions

This sub-section also entertains the possibility of validating at the system and vehicle level. All the necessary test goals along with their test methods are listed clearly in it. This is also supported by ample number of tables to guide through it. But these are not evaluated in this thesis as it jumps out of bounds. Although the gist for a few methods involved are mentioned below [21]:

- Repeatable tests with highly specific test procedures along with a fail/pass criteria. For instance; black box testing, fault injection, etc.
- Analyses. For instance; FTA, FMEA, etc.
- Long-term tests
- Real-life condition tests
- Reviews

4.6. Functional safety assessment

The objective is to judge the functional safety being led by the item. The entity responsible for the start of this assessment can be the vehicle manufacturer or the supplier. The requirements mentioned in this sub-phase apply to the ASIL levels of ASIL B, C, and D. While conducting the assessment for the functional safety the documentation involved in the same should include the following information [21]:

- Name and signature of the person who is responsible for the release
- Version of the particular item
- Configuration of the particular item
- References to corresponding documents

- Release date

But for the scope of this thesis this sub-section of the ISO 26262 is only analysed within limits. This marks the end of the development at the system level and all the specifications for the same are achieved.

5. ISO 26262 Part 5: Product development at the hardware level

This section gives a slight insight about how the software front is taken care in the ISO 26262 functional safety standard.

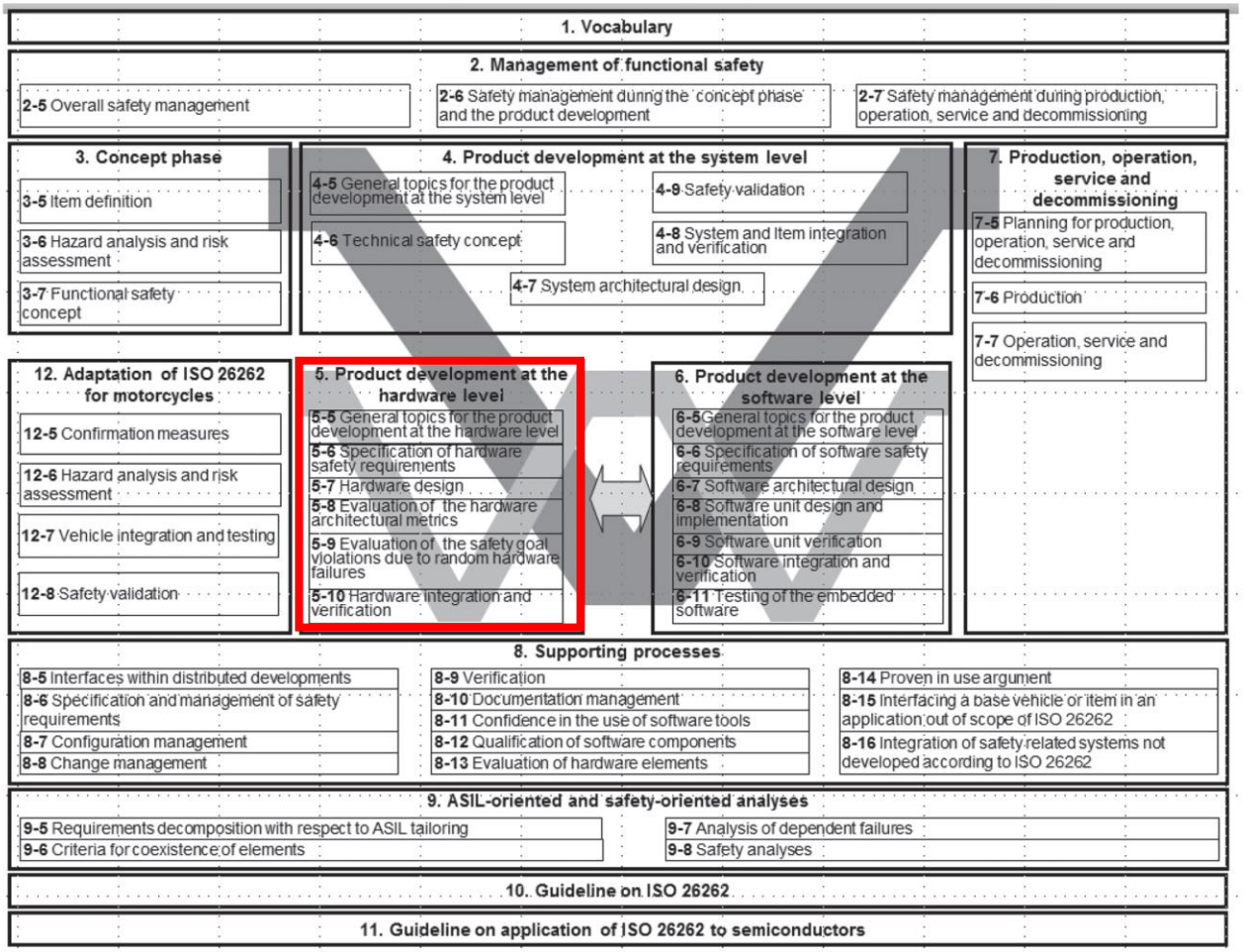


Figure 20: ISO 26262 – Part5

Part 6 of the ISO 26262 lying between the parts those talk about the system and the Part 7. The development at the hardware level goes hand-in-hand with the development at the software level. As these two parts are very closely wound, it is essential to trace and look at the requirements mentioned in the Part 5 with respect to that of the Part 6.

5.1. Scope

This part of the ISO 26262 specifies the requirements for automotive applications of product development at the hardware level consisting of:

- Initiation of product development at the hardware level
- Hardware safety requirements
- Hardware architectural design

- Evaluation of safety goal violation due to random hardware failure
- Hardware integration and testing

5.2. Requirements for compliance

From a safety perspective, hardware should be designed so that it implements the required safety requirements placed on hardware. This design is not just to deliver functional safety, but of course it also has to safeguard the actual function of hardware. Safety mechanisms thus become an integral part of the design. Since we may have to deal with requirements of different ASILs, there may be parts of the hardware with these different ASILs. To avoid “unsafe” parts endangering “safe” parts, ISO 26262 specifies criteria that you must take into account.
In this phase you also have to think about the special characteristics needed for the production and maintenance phase, and ensure they are then implemented.

- Hardware faults must be classified according to whether and how directly they violate safety goals.
- Evidence must be provided that hardware faults that occur do not violate safety goals and are not permanently present in vehicles without being detected.

Depending upon ASIL-dependent requirements certain work products may not be needed as prerequisites. If at all ASIL decomposition has been performed at a previous stage of product development then the resulting ASIL level of the decomposition is complied with it. If any ASIL level is adjoined by parentheses, the respective sub-clause will be considered more as a recommendation rather than a requirement.

6. ISO 26262 Part 6: Product development at the software level

This section gives a slight insight about how the software front is taken care in the ISO 26262 functional safety standard.

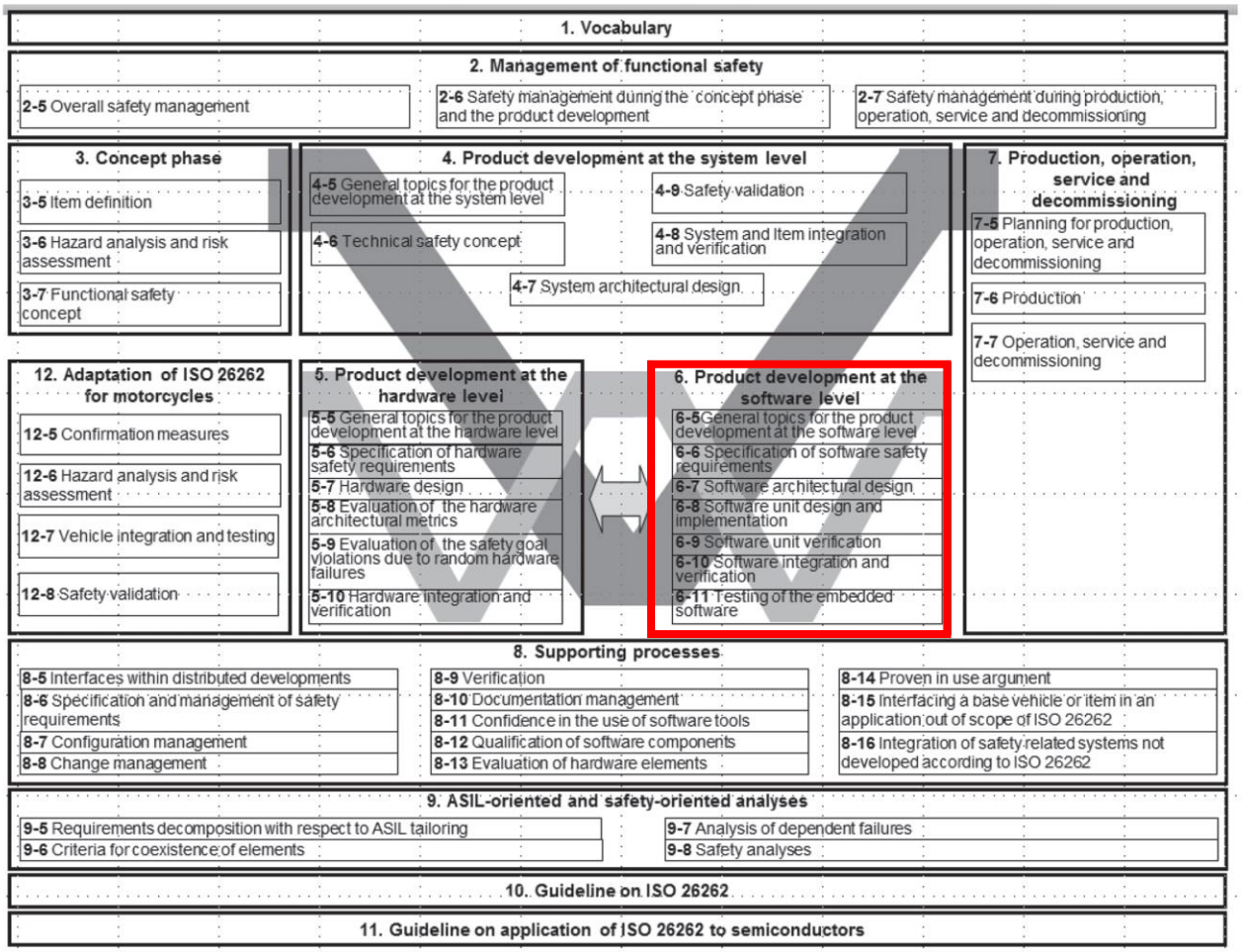


Figure 21: ISO 26262 – Part6

This being the Part 6 of the ISO 26262, lying between the parts those talk about the system and the Part 7. Part 7 talks about the steps involved during the lifecycle of the product during hardware development. Noticeably, the development at the software level goes hand-in-hand with the development at the hardware level. As these two parts are very closely wound, it is essential to trace and look at the requirements mentioned in the Part 6 with respect to that of the Part 5. This is essential so as to absorb the right interpretation of the ISO 26262 standard with respect to all dimensions.

6.1. Scope

This part of the ISO 26262 specifies the requirements for automotive applications of product development at the software level consisting of [22]:

- Initiation of product development at the software level
- Software safety requirements
- Software architectural design
- Software unit design and implementation
- Software unit testing
- Software integration and testing
- Verification of software safety requirements.

6.2. Requirements for compliance

While achieving compliance with ISO 26262 every requirement should obey to it or unless one of the following reasons plays a role:

- the safety activities has been planned in accordance with the ISO 26262
- to accept the non-compliant-ability a rationale is provided and that the rationale is in accordance with ISO 26262

Depending upon ASIL-dependent requirements certain work products may not be needed as prerequisites. If at all ASIL decomposition has been performed at a previous stage of product development then the resulting ASIL level of the decomposition is complied with it. If any ASIL level is adjoined by parentheses, the respective sub-clause will be considered more as a recommendation rather than a requirement. And that this is different from the parenthesis of ASIL decomposition.
The remaining sub-sections of Part 6: Product development at the software level are analysed and elaborated in the following chapters of this thesis so as to maintain a proper workflow.

7. ISO 26262 Part 9: ASIL-oriented and safety-oriented analysis

This section is a highly important part of the ISO 26262 as far as safety of the whole system is considered. As this section provides with the different ways that assists in order to decompose the ASIL levels. The decomposition is slightly complex with due respect to the complexity of the system. This part plays a crucial role when it comes to its linkage with other parts of the ISO 26262. Hence, it becomes essential to have a handsome in-depth look at their decomposition and respective recommendations that need to be followed.

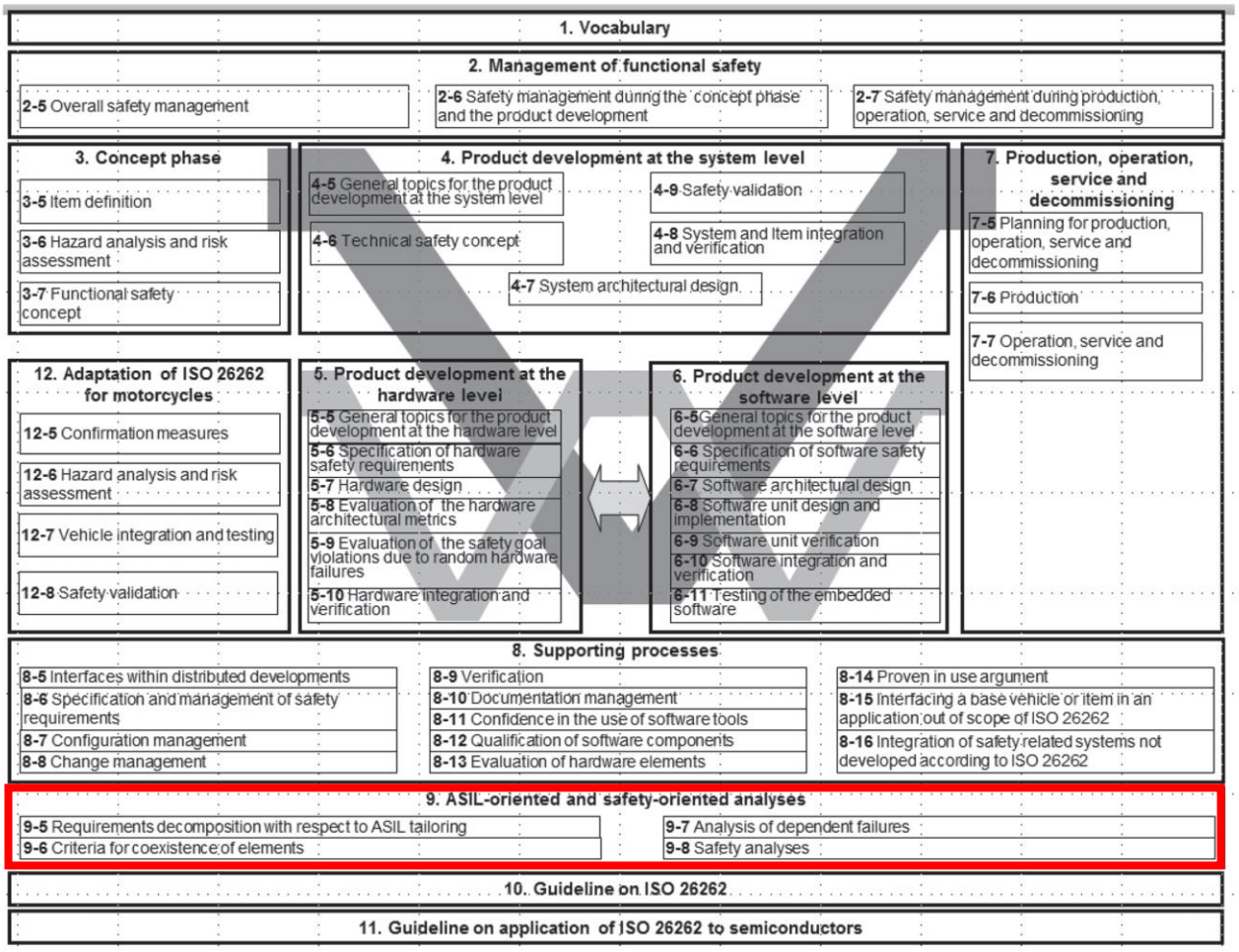


Figure 22: ISO 26262 – Part9

7.1. Scope

This part of ISO 26262 is about the Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses and includes the following:

- requirements decomposition
- coexistence of elements

7.2. ASIL decomposition schemes

For the tailoring of the ASIL levels there are a set of procedures that guide through the decomposition of the safety requirements into redundant safety requirements. So the particular ASIL level is inherited by each following safety requirement. Starting with the functional and technical safety requirements.
Hence, this method of tailoring ASIL levels is termed as "ASIL decomposition". While the allocation process is going on there is a benefit if the architectural decisions has sufficient amount of independent architectural elements. This greatly helps in:

- Execution of safety requirements by the independent architectural elements
- By assigning a lower ASIL to the decomposed safety requirements

So in totality the ASIL decomposition imparts its application to a safety requirement amongst several elements which ensure that it is in par with the same safety requirement in respect to the safety goal. Therefore, the initial safety requirement is to be distributed in terms of redundant safety requirements by the use of sufficient elements.

For the ASIL decomposition at the software level, there has to be enough independencies amongst the elements and should be cross-verified at the system. If at all an ASIL decomposition leads to location of decomposed requirements towards a functionality along with an associated safety mechanism, then the following need to be considered:

- The safety mechanism is to be assigned the highest decomposed ASIL level.
- The safety requirement corresponding to the intended functionality should be implemented with respect to the decomposed ASIL level.

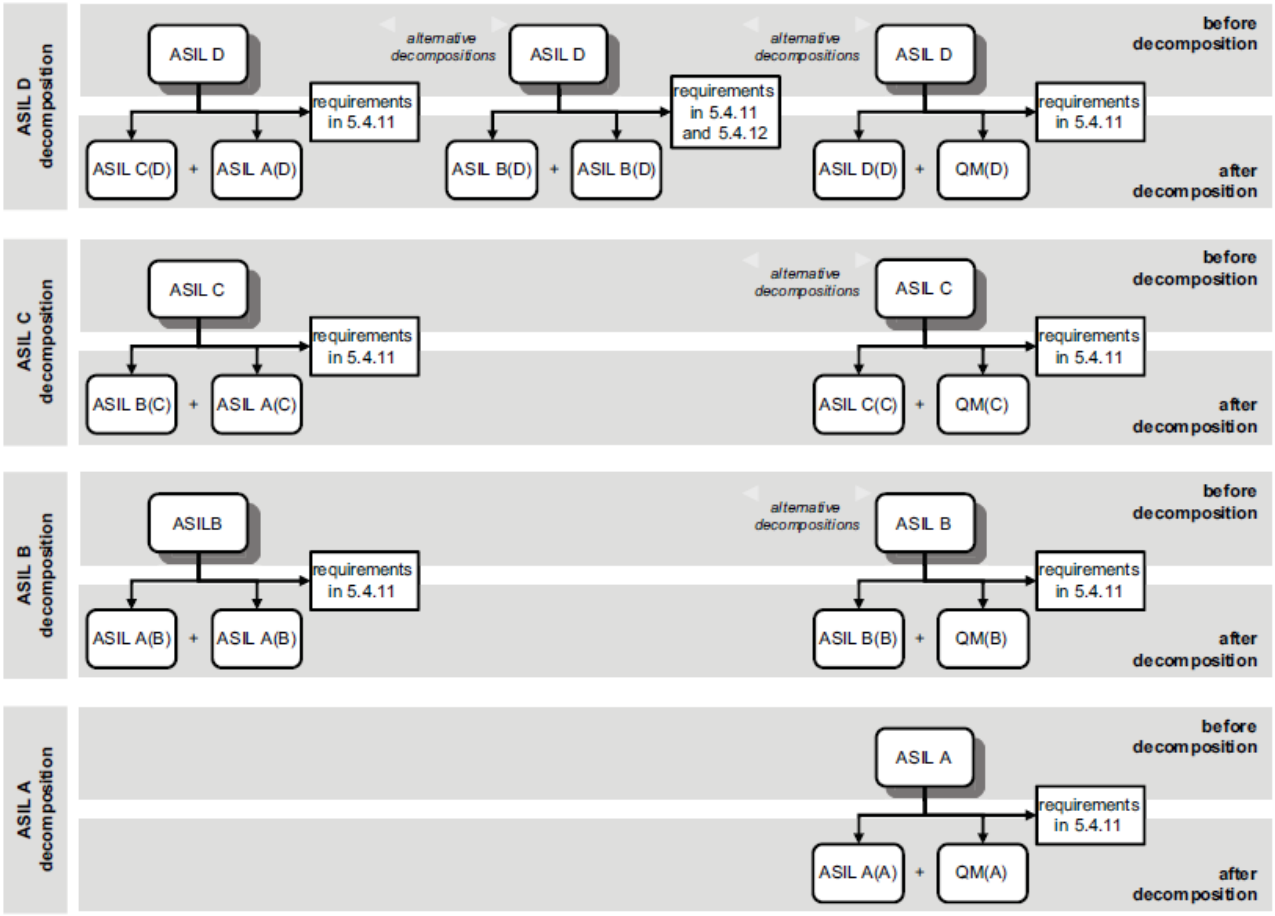


Figure 23: ASIL decomposition scheme

If at all there is an issue with an initial safety requirement then the availability of sufficient independent elements that implement the decomposed safety requirements have to be considered. The following figure 3.19 [23] shows the different decomposition schemes that are mentioned in the ISO 26262 functional safety standard. A single decomposition of the ASIL level is defined when there is a transition from one step of one level to the lower next level and the following always needs to be kept under check:

- To comply the ASIL level with respect to the safety goal
- After decomposition there should be a sufficient independence of the elements

Utmost care need to be taken while using the decomposition scheme for ASIL D. And the following needs to be considered during the same time:

- The decomposed safety requirements should be in par with that of ASIL C requirements so as to avoid any systematic failures
- The same software tools that were used for the development of the decomposed elements should also be used for the development of the ASIL D elements

8. Implementation

As the title suggests this section deals with the aspect of implementation undertaken during thesis work. After defining characteristics and working conditions of the generic Torque generation function, the work focused on the characterization of the vehicle control unit (LMU). During this phase, mainly parts 4 and 5 of ISO 26262 were used. As a functioning LMU was already available, not all points were considered, but only relevant points for the thesis work.

8.1. ISO 26262 Part 4.7: System architectural design

In this section we focused on the study and definition of the LMU present on the current vehicle thanks to the analysis of the documentation made available by the company.

8.1.1. LMU functionalities overview

LMU is an electronic logical device powered by 12V vehicle battery. Its electronic components must be energized only when the key switch is turned on, furthermore LMU implements a power latch that enable it to remain active even after vehicle shutdown. All its functions are controlled by an internal microcontroller.
LMU is designed for:

- Receiving digital and analogic inputs from vehicle components such as:
  - Brake pedal,
  - brake hydraulic pressure sensor,
  - accelerator pedal,
  - direction stick,
  - key switch,
  - BMS signals (RUN and RGN).
- Communicate with other logics devices through a dedicated CAN line.
- Implement power supply outputs for vehicle components and loads such as:
  - Inverter logic,
  - buzzer,
  - back up light,
  - accelerator pedal.
- Ensures a security insulation of battery pack in case of vehicle fault activating, through an external Emergency Relay, a dedicate BMS input.
- Storage detected fault in a dedicate memory module.

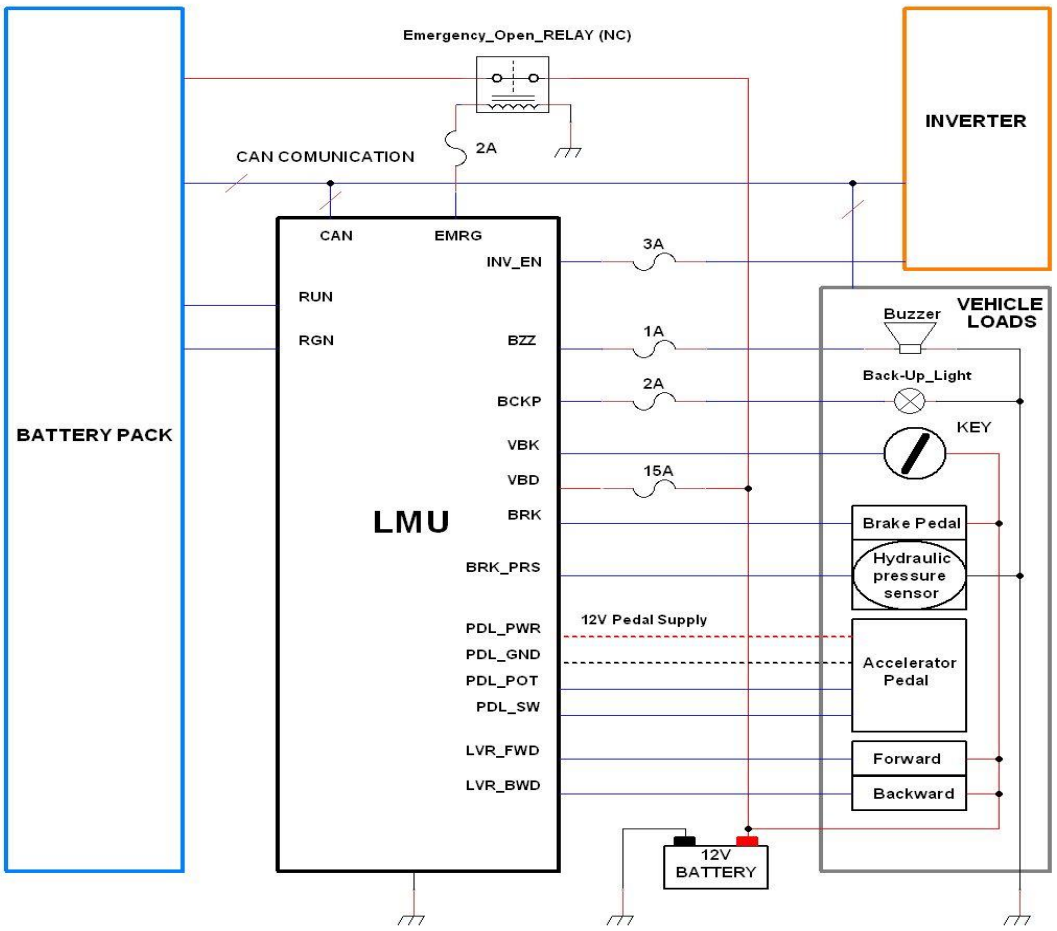


Figure 24: LMU functional scheme

Power supply block is protected against incorrect polarity (LMU hardware shall be compliant to international road vehicles standard) and, if the vehicle key is turned off, LMU internal electronic component shall not be powered.

As shown in figure 26, LMU board shall manage: 8 digital inputs, 2 analog input and 5 power outputs, and shall be capable to properly manage the power outputs drivers and input values coming from digital and analog inputs.

Furthermore, stored parameters shall be read even in case of braking of the board and also when the board in disconnected to the vehicle.

Table 20 lists all pins that shall present an external box connection and its functions.

Name	Function	Type	Dir	From/To
VBD	Direct battery positive pole.	P	I	VEH
BATT_GND	Battery ground.	P	I	VEH
RUN	RUN signal from BMS (vehicle able to move).	D	I	BTPK
RGN	Regeneration enable signal from BMS (regeneration is allowed).	D	I	BTPK
VBK	Keyed battery positive pole.	D	I	VEH
CANL_IN	CAN line, low, in.	C	I/O	VEH
CANL_OUT	CAN line, low, out.	C	I/O	VEH
CANH_IN	CAN line, high, in.	C	I/O	VEH
CANH_OUT	CAN line, high, out.	C	I/O	VEH
PDL_POT_1	Accelerator pedal signal.	A	I	VEH
PDL_POT_2	Accelerator pedal signal. (NOT USED)	A	I	VEH
BRK	Brake signal from pedal.	D	I	VEH
PDL_SW	Accelerator pedal switch.	D	I	VEH
BRK_PRS	Brake hydraulic circuit pressure sensor.	D	I	VEH
LVR_FWD	Forward signal.	D	I	VEH
LVR_BWD	Backward signal.	D	I	VEH
EMRG	Emergency relay activation.	P	O	REL/VEH
BCKP	Back up light activation.	P	O	VEH
BUZZ	Passenger compartment buzzer activation.	P	O	VEH
PDL_PWR	Accelerator pedal power source.	P	O	VEH
PDL_GND	Accelerator pedal ground.	P	O	VEH
INV_EN	Inverter enable.	P	O	INV

Table 20: LMU external pin connections

8.2. ISO 26262 Part 5

In this section hardware characteristic of LMU will be deeply analyzed.

8.2.1. ISO 26262 Part 5.5: General topics for the product development at hardware level

A first scheme of the electronic board is shown in Figure 28

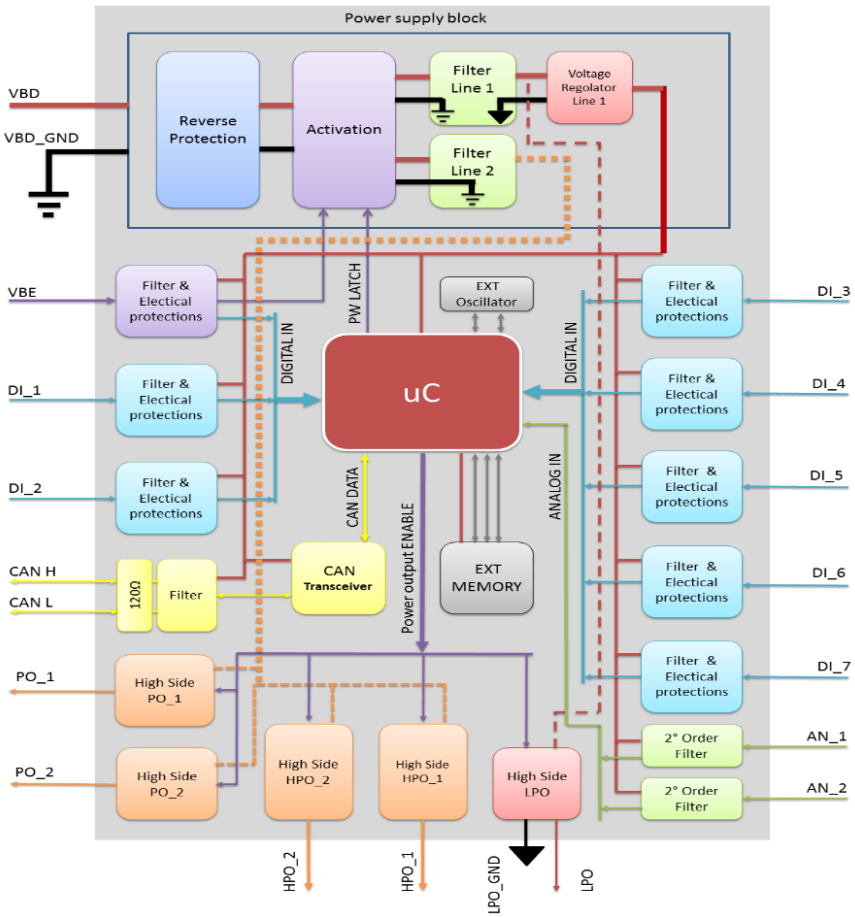


Figure 25: LMU hardware architecture

LMU unit is connect to vehicle wiring trough a Delphi (type HCCPHPE24BKA90F) connector shown in figure 28

Figure 26: Connector

Table 21 lists all connector pins association whit vehicle signals request, LMU HW pins and the respective functionality.

Vehicle signals request Errore. L'origine riferimento non è stata trovata.	Vehicle signal Description	LMU HW #Pin
BCKP	Back up light activation.	HPO_1
INV_EN	Inverter enable.	HPO_2
EMRG	Emergency relay activation.	PO_1
PDL_SW	Accelerator pedal switch.	DI_4
CANH_IN	CAN line, high, in.	CANH_1
CANL_IN	CAN line, low, in.	CANL_1
PDL_POT_2	Accelerator pedal signal 2.	AN_2
PDL_POT_1	Accelerator pedal signal 1.	AN_1
BATT_GND	Battery ground.	VBD_GND
BUZZ	Passenger compartment buzzer activation.	PO_2
CANH_OUT	CAN line, high, out.	CANH_2
CANL_OUT	CAN line, low, out.	CANL_2
LVR_FWD	Forward signal.	DI_1
LVR_BWD	Backward signal.	DI_7
VBD	Direct battery positive pole.	VBD
VBK	Keyed battery positive pole.	VBE
PDL_PWR	Accelerator pedal power source.	LPO
PDL_GND	Accelerator pedal ground.	LPO_GND
BRK_PRS	Brake hydraulic circuit pressure sensor.	DI_3
BRK	Brake signal from pedal.	DI_2
RGN	Regeneration enable signal from BMS.	DI_6
RUN	RUN signal from BMS.	DI_5

Table 21: Connector pin association

8.2.2. ISO 26262 Part 5.7: Hardware design

The LMU V1.0 board is equipped with a MC9s12ZVM NXP family microcontroller which implement the control logic for:

- manage enable digital input signal
- manage all digital input signals
- manage all analogic inputs signals
- manage the CAN communication
- enable power outputs
- storage data in external microcontroller memory.

Microcontroller firmware can be programmed connecting, PEMicro Multilink Universal programmer BDM PORT C, to P1 printed board connector highlighted in Figure 29. For improve microcontroller performance, LMU IS equipped whit an 8MHz oscillator opportunely connected to microcontroller pins. LMU is equipped with an 8 kB storage memory, used for storage faults data history or other parameters. In case of damage or microcontroller inactivity, data stored in memory shall be directly accessible by a dedicate connector P3 highlighted in Figure 29. For external directly memory data access is mandatory to physically remove R60, R61, R62, R63, R65 resistors (highlighted in Figure 30) from LMU PCB. Memory is directly supplied by VDDF microcontroller 3.3V power output.

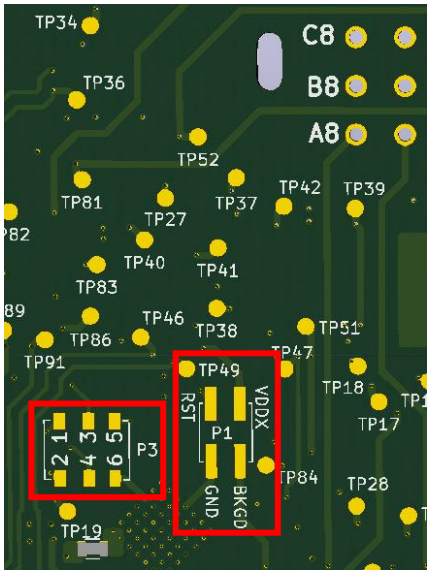


Figure 27: LMU P1, P3 connectors.

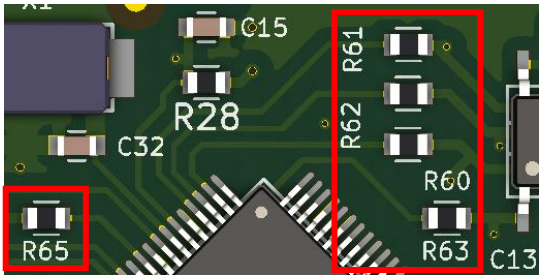


Figure 28: LMU memory resistors

8.2.3. Power supply block

The Power Supply block receive the 12V external supply positive voltage, connected to VBD pin, and negative ground pole connected to VBD_GND. Those pins generate board voltage references for supply all internal electronic components and the external loads connected to the 5 power outputs. When enable board signal pin (VBE) is low, only the electronic components located in "Reverse Protection" block are powered. When Enable Board signal pin goes high "Activation" block powers the "Filter" blocks. "Filter line 1" and "Voltage regulator line 1" blocks generate the reference voltages for all internal blocks and "LPO" power output. The other 4 power output blocks ("PO_1", "PO_2", "HPO_1", "HPO_2") are powered by "filter line 2". After board power on, if the enable signal turns low, the LMU remain powered and board power down is controlled by the internal microcontroller through power latch line.
The "Reverse protection" block protect LMU from reverse polarity apply on **VBD** and **VBD_GND** pins, in order to properly remove reverse polarity condition when met.
The "Activation" block is powered by the "Reverse Protection" block (see Figure 28). When a enable event occurs on pin VBE the "Filter line 1" and "filter line 2" blocks are powered. In this condition all LMU electronic component are powered and the microcontroller starts to manage all board functionality. Microcontroller is informed of the **VBE** state on its **PAD7** digital input pin. LMU power off is carried out by the internal microcontroller activating **PW LATCH** line (**PAD8** digital output pin). This function allows the microcontroller to save internal data and to bring itself in a security state before power off the board. Figure 33 shown the LMU power ON/OFF procedure.

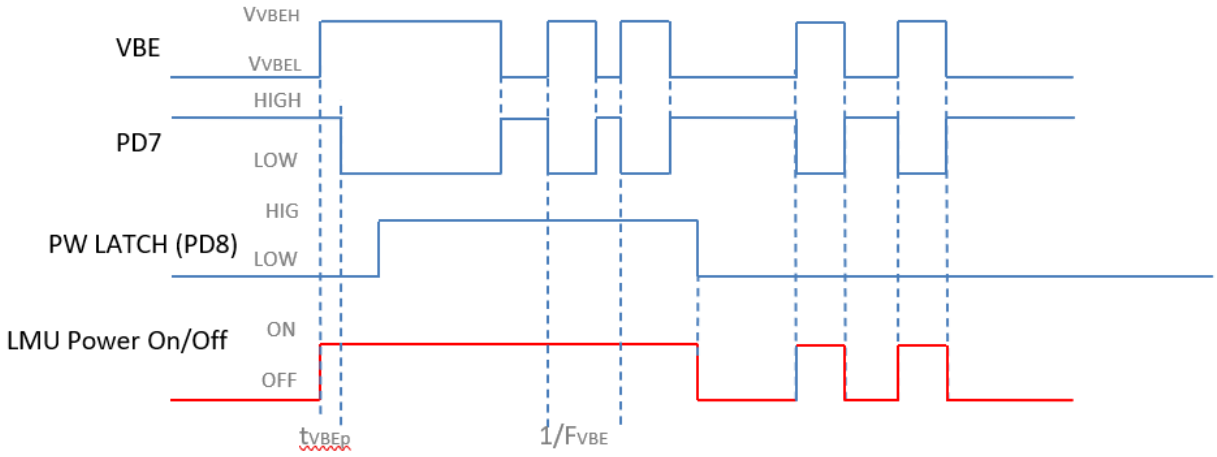


Figure 29: LMU power ON/OFF procedure

The "Filter line 2" block filter the power supply line coming from the "Activation" block (see Figure 28), and it ensure protection from overvoltage spike to all loads connected to the 4 power output blocks ("PO_1", "PO_2", "HPO_1", "HPO_2").

The "Filter line 1" and the "Voltage regulator line 1" blocks provide to:

- filter the power supply line coming from the "Activation" block,
- ensure overvoltage protection caused by spike,
- stabilize the voltage for supply all electronic component,
- ensure an appropriate GND line filtering.

"Voltage regulator line 1" block (Figure 34) is an 5V linear voltage regulator **enabled** by **BCTL** microcontroller output pin. It provides to supply all 5V internal blocks and is connected to Vddx microcontroller pins. If BCTL pin is disabled, 5V are supplied directly by Vddx microcontroller pin.

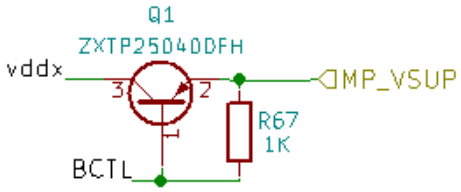


Figure 30: 5V voltage regulator

8.2.4. Digital input

All the 8 Digital Inputs blocks shall be designed for managing signals coming from vehicle and BMS units. All inputs blocks shall be filtered, electrical insulated, protected from reverse polarity and compliant to ISO tests. A pulldown resistor shall be present on all digital input pins.

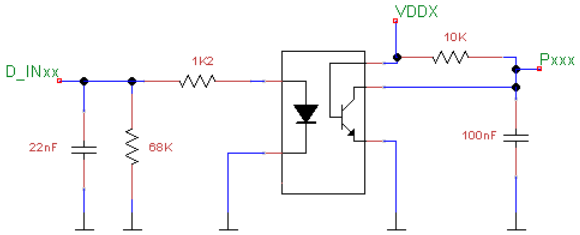


Figure 31: Digital input block

8.2.5. RGN input (Regeneration enable signal)

Regeneration enable signal from BMS (RGN) is a digital input. When RGN input goes high regeneration is allowed, microcontroller is informed to this event on its DI# digital input pin. Figure 3 show the DI# microcontroller pin activation signal.

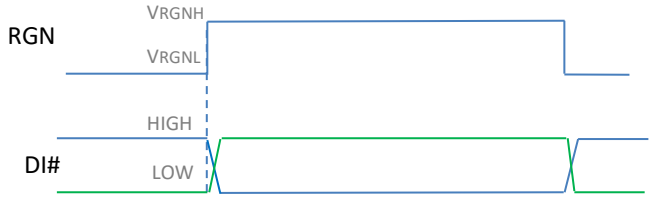


Figure 32: RGN activation signal.

8.2.6. RUN input

Run signal from BMS (RUN) is a digital input. When RUN input goes high LMU can allow traction, microcontroller is informed to this event on its DI# digital input pin. Figure 4 show the DI# microcontroller pin activation signal.

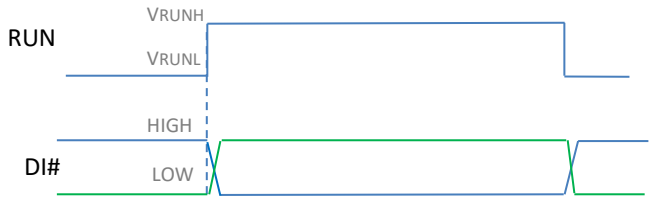


Figure 33: RUN activatio signal

8.2.7. VBK input (Key signal)

When the vehicle key is turned on, and consequently voltage on VBK digital input goes high, “Power supply” power block shall be enabled.

8.2.8. BRK input (Brake pedal signal)

Brake pedal signal from vehicle (BRK) is a digital input. When brake pedal is pressed the voltage on BRK digital input goes high, the microcontroller shall sense, through DI# pin, when this event occurred. Figure 5 show the DI# microcontroller pin activation signal.

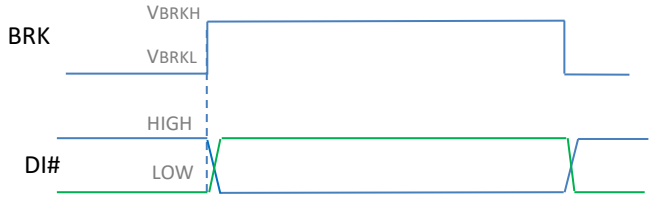


Figure 34: BRK activation signal

8.2.9. BRK_PRS input (Brake hydraulic circuit pressure sensor signal)

Brake hydraulic circuit pressure signal from vehicle (BRK_PRS) is a digital input. When a fault, in the brake hydraulic circuit, occurs the voltage on BRK_PRS digital input goes high. Board microcontroller shall sense, on its DI# pin, when this event occurred. Figure 6 show the DI# microcontroller pin activation signal.

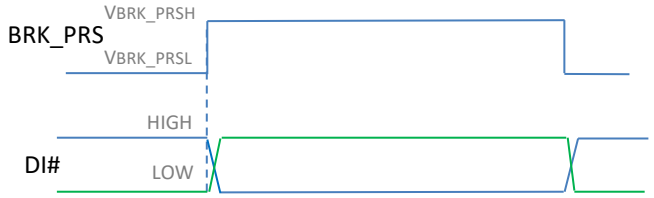


Figure 35: BRK_PRS activation signal

8.2.10. LVR_FWD (Forward direction stick signal)

Forward direction stick signal from vehicle (LVR_FWD) is a digital input. When the direction stick is in Forward position the voltage on LVR_FWD digital input goes high. Board microcontroller shall sense, on its DI# pin, when this event occurred. Figure 7 show the DI# microcontroller pin activation signal.

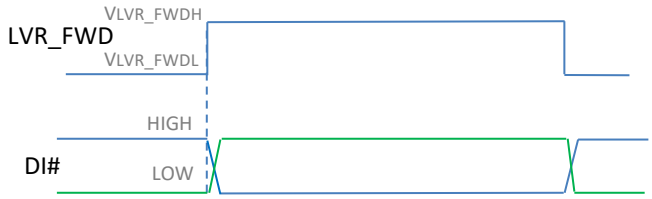


Figure 36: LVR_FWR activation signal

8.2.11. LVR_BWD (Backward direction stick signal)

Backward direction stick signal from vehicle (LVR_BWD) is a digital input. When the direction stick is in Backward position the voltage on LVR_BWD digital input goes high. Board microcontroller shall sense, on its DI# pin, when this event occurred. Figure 8 show the DI# microcontroller pin activation signal.

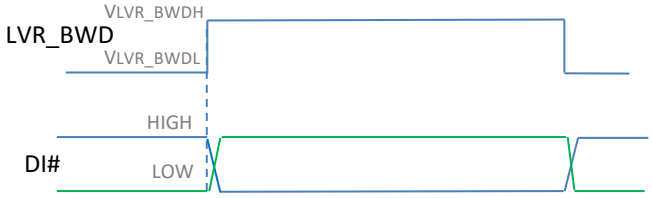


Figure 37: LVR_BWD activation signal

8.2.12. PDL_SW (Accelerator pedal switch signal)

Accelerator pedal switch signal from vehicle (PDL_SW) is a digital input. When the accelerator pedal is start be pressed the voltage on PDL_SW digital input goes high. Board microcontroller shall sense, on its DI# pin, when this event occurred. Figure 9 show the DI# microcontroller pin activation signal.

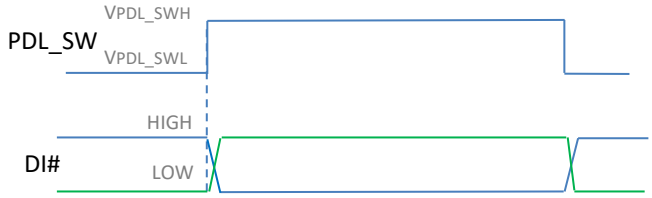


Figure 38: PDL_SW activation signal

8.2.13. Analog Input

All Analog Inputs blocks shall be designed for managing accelerator pedal signals coming from vehicle. All analog inputs shall be protected from reverse polarity, overvoltage and compliance to ISO tests. A pull-down resistor shall be present on all digital input pins. More over all analog inputs shall be filtered, at least, whit filter having:

- Gain =1 V/V,
- Allowable PassBand Ripple =1dB,
- Passband Frequency =100Hz,
- Corner Frequency Attenuation = -3dB,
- Stopband Attenuation =-45dB,
- Stopband Frequency =5Kz.

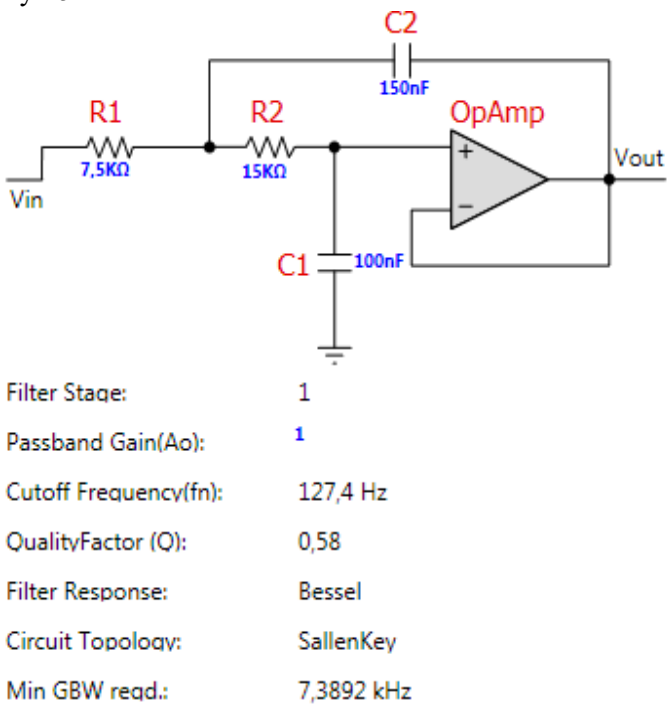


Figure 39: ADC input filter

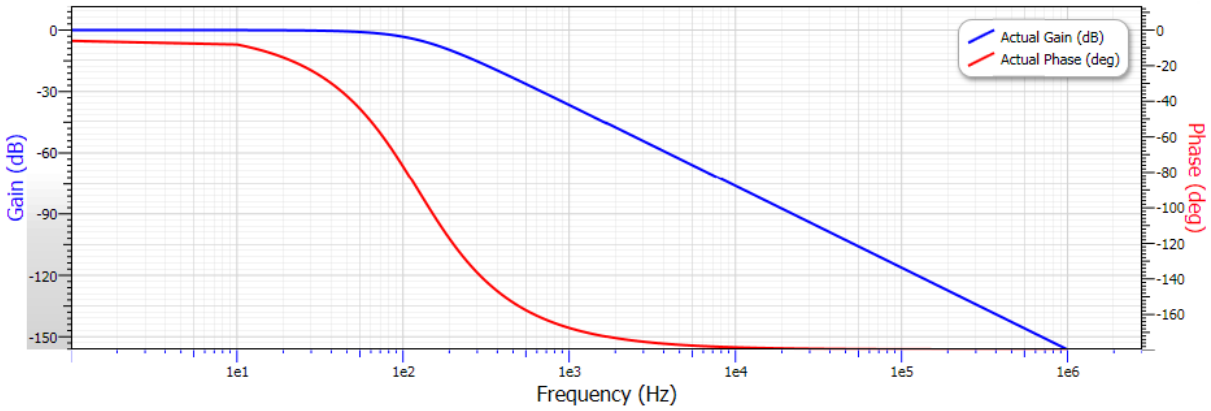


Figure 40: ADC inputs filter Gain and Phase

8.2.14. PDL_POT_1 (Accelerator pedal signal 1)

When the accelerator pedal is pressed the voltage on PDL_POT_1 analog input change, microcontroller, on its AI# pin, shall properly acquire this signal.

8.2.15. PDL_POT_2 (accelerator pedal signal 2)

When the accelerator pedal is pressed the voltage on PDL_POT_2 analog input changes, microcontroller, on its AI# pin, shall properly acquire this signal.

8.2.16. Communication block

The communication block shall implement a proper CAN interface for allow the communication among LMU, vehicle, inverter and BMS. Communication signals shall be properly filtered and protected against overvoltage. **CANH** and **CANL** signals shall be managed by high speed CAN transceiver connected to specific microcontroller pins and supplied by VDDX. CANH_1 pin is directly connected to CANH_2 pin and CANL_1 pin is directly connected to CANL_2 pin. CAN communication line is internally terminated using two 60Ω resistors placed through CANL and CANH pins. To exclude CAN termination R19 and R18, highlighted in figure 45, must be physically removed from LMU PCB.

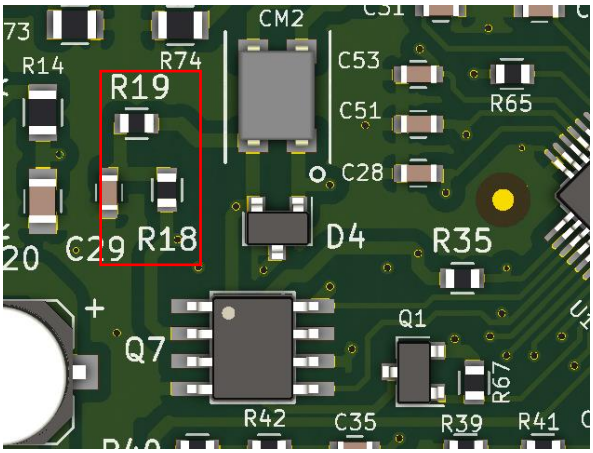
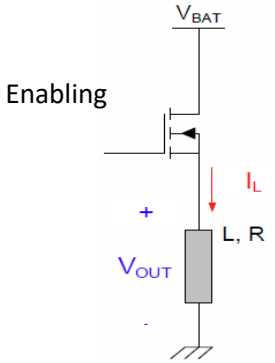


Figure 41: CAN resistors

8.2.17. Power output blocks

Power out blocks shall supply external loads and it shall be in high-side switches configuration as shown in the figure 10. All outputs shall be compliant with ISO tests therefore protected against:

- short circuit to ground,
- over temperature,
- reverse polarity,
- overvoltage,
- battery ground loss.



Moreover, EMRG, BCKP, BZZ and INV_EN power outs (PO_1, HPO_1, PO_2 and HPO_2) shall be enabled and disabled by LMU microcontroller.

The “Low power output” block (LPO / LPO_GND) supply external low power loads with a dedicated power line, this is the only power output block supplied by “Filter line1”. LPO / LPO_GND power out line is protected against short circuit to ground by PTC RESETTABLE FUSE and incorrect polarity.

Figure 42

8.2.18. PDL PWR (Pedal Power Supply)

The “Pedal power supply” power out block (PDL_PWR) shall supply the throttle pedal with a dedicated power line. This shall be the only power output block supplied without microcontroller enable and shall be in accordance with the throttle pedal specifications.
PDL_PWR power out line shall be protected against short circuit to ground by PTC RESETTABLE FUSE and incorrect polarity.

8.2.19. EMRG (Emergency relay activation)

The “Emergency relay activation” power output block (EMRG) shall be designed for managing emergency relay, which is of NC type, connected to BMS. When LMU wants to force HV contactor opening it shall activate EMRG output. DO# microcontroller pin manage EMRG power output as shown in figure 11. Moreover EMRG power output shall be comply with ISO tests.

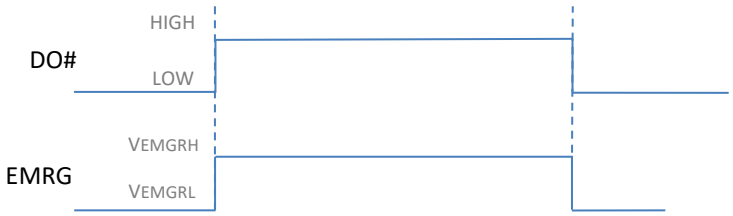


Figure 43: EMGR power output activation

8.2.20. BCKP (Back up light activation)

The “Back up light activation” power output block (BCKP) shall be designed for managing back up light. When the direction stick is in Backward position a DI# microcontroller pin change its status. When the microcontroller state machine is in a state allow the vehicle to proceed backward, a DO# microcontroller pin shall activate. In this condition BCKP power out shall be enabled (Figure 12 show the BCKP pin activation signal). This action permits to switch on the back up light powered to VBCKP voltage.

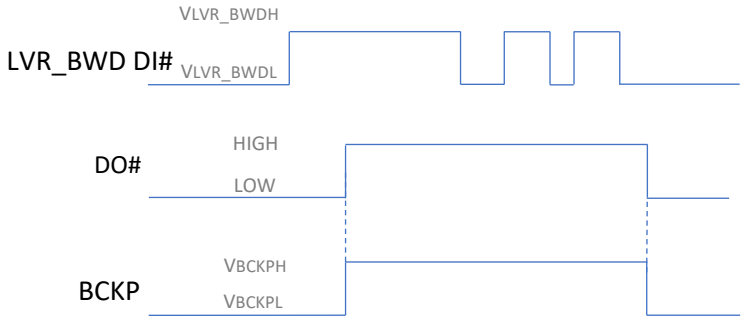


Figure 44: BCKP power output activation

8.2.21. BUZZ (Buzzer activation)

The “Buzzer activation” power output block (BUZZ) shall be designed for managing acoustic signal buzzer load present in the car passenger compartment. The LMU microcontroller shall activate the buzzer when necessary. DO# microcontroller pin manage BUZZ power output as shown in the figure 13.

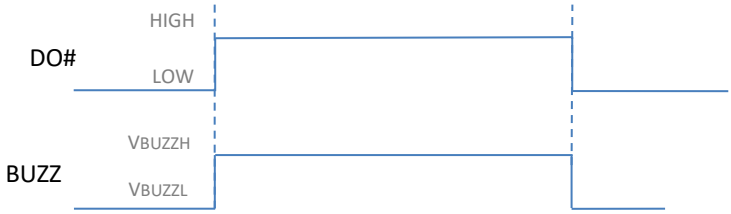


Figure 45: BUZZ power output activation

8.2.22. INV_EN (Inverter logic enable)

The “Inverter enable” power output block (INV_EN) shall be designed for enabling inverter logic. When DO# microcontroller pin goes high the INV_EN power out became activate and inverter electronic logic shall be powered to VINV_EN. Figure 14 show the INV_EN output activation signal.

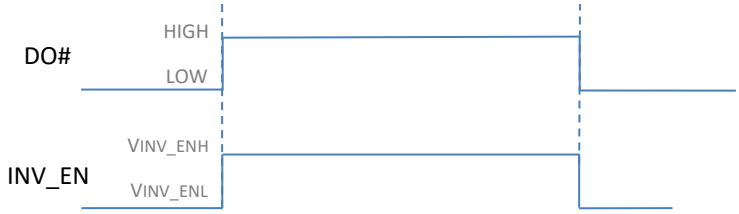


Figure 46: INV_EN power output activation

9. ISO 26262 Compliance verification

In this part a comparison was made between what is required by the ISO standard and what is actually present on the LMU fitted on the Epic0 vehicle.

In order to carry out this study it is necessary to clearly know the Functional Safety Requirements (FSR) and the Technical Safety Requirements (TSR) obtained following the application of the ISO26262 standard on the Torque Management function and, of course, the structure (both HW and SW) of the LMU card.

In Table 21 below you can see how this comparison was made. In the left column are indicated the HW and SW features that the LMU board must implement in order to comply with ISO 26262. The central column shows the functions performed by the current version of the LMU, while the results of this comparison are shown in the right column.
In the last column are also indicated the possible improvements that can be made on the board to make it compatible with the standard and the critical points results after comparison.

HW & SW Requirements	LMU_StateOfArt	Comparison result	Comments
Redundant gas pedal acquisition	Pedal acquisition is carried out through a 12 volt analog signal and a digital switch signal. The LMU carries out a debouncing on the digital signal and there is also an interface to the diagnostic machine. There is a second Analog input pin, but it is not used	NOK	Redundancy possible, by adding the second analog input
Comparison btw gas pedal request and Torque operating range	The gas pedal generates a signal that is translated into torque request by an algorithm that has input beyond the gas pedal also: -Speed signal -State of the brake pedal -State of closing doors -Time The torque control thus created is sent to the inverter that actuates it with rate limiter. Ranges are calculated in which the feedback torque must be according to the request (tollerance in value and time)	OK	
Redundant signal management	All signals are managed by using a single microcontroller	NOK	HW must be modify
Torque needed for hill holding calculated twice before switch to Hill Holding or Parking mode	There is a specific SW-Component that manages the hill holding: hill holder, if enabled, allows the electric motor to produce the amount of torque needed to keep the vehicle in stationary condition. Usually this feature is obtained by using brake circuit pressure on brake caliper instead of electric motor. Actually, hill holder logic works as follows: • Hill holder will be enabled only if brake pedal is pressed, driver status is in forward or reverse condition and vehicle speed is under a certain threshold. This condition must be maintained for a certain amount of time and only after that time hill holder will be activated. A variable is used in order to enable or not this functionality. If one of this condition is not maintained, hill holder must be disabled. • If previous conditions are verified, hill holder is active even if the vehicle is not running. In order to have real effects on the vehicle a brake pedal release should occur. • Once a brake pedal release occurs, hill holder will be kept enabled for a certain amount of time and till vehicle speed not became greater than a certain threshold. • If a pedal torque request is greater than inverter torque feedback and this condition is maintained for a certain amount of time hill holder should be disabled. Hill holder will be disabled also if vehicle speed will be greater that a certain threshold. This logic part could be disabled throughout an enable variable. This logic is used for forward and reverse driver status separately. • The logic could understand also if the vehicle is in one of the following particular condition: a) Positive slope with reverse driver status selected and a inverter feedback torque greater than a certain threshold (case 2) b) Negative slope with forward driver status selected and a inverter feedback torque greater than a certain threshold (case 3) Hill holder will be disabled if this condition occurs for more than a certain time threshold or if a driver status change occurs. This logic part could be disabled throughout an enable variable.	NOK	Problem: during the hill holding phase I can get off the vehicle and the car remains in that state -> engine overheating + consumption There are no problems to calibrate the system if I increase the load during the hill holding phase
Hill holding compared with motion signal			
Hill holding acts automatically when D gear and vehicle go backward			
Redundant Position signal (Front and Rear)	The position signal comes from Inverter through CAN. LMU only acquires that signal(we have just one electric motor).	OK	
Gear verification made by double acquisition of the same digital value with a certain time interval	The gear is read on two wires : D and R. Possible states 00 N 01 D 10 R 11 Error Forward gear does not always correspond to positive torque, no verification is possible. Ignition shall be at 0, otherwise error	NOK	OK, l'acquisizone avviene tramite 2 fili
Check btw Gear and Torque request			Only when the system is fully observable
Gear actuation made only if Gear choerent with Velocity and Torque and Hill Holding OFF			Not present, but possible implementation
Brake pedal signal acquired twice	Brake pedal acquired by a single relay and related to a digital input	NOK	
Error signal cause traction inhibition	The LMU high level state machine goes to fault state when a Fault on inverter is detected or when the BMS is not able to allow the traction. When in Fault state, it publishes an error code on CAN and on the dashboard.	OK	
Timing management	The time to go to the Fault state is determined in the state machines of the inverter and high level SM. During MIL and HIL tests, a faults injection is carried out and the diagnostic system is tested.	NOK	Not implemented in SW

Table 22: Comparison LMU vs Safety Requirements

As can be seen the current board has basic features and a logic compatible with ISO, however many functions cannot be properly implemented.
Because of this Mecaprom decided to contact a third company with which to develop a new LMU that fully satisfies how needed from the Epic0 vehicle and from ISO26262.

HW and SW development of the board was managed entirely by the partner company and, therefore, is outside the work of the thesis.
My final task, however, was to carry out all the preliminary consideration in order to permit the Company to make a FIDES analysis on the new LMU in order to certify compliance the ASIL level resulting from the application of ISO26262.

10. LMU v2.0 – Future development

The comparison made in the previous chapter highlighted a series of security issues related to board design. It is therefore necessary to rethink the board starting, however, from the correct features implemented in the old version.
In this section will be given the general specifications that must have the updated and safety compliant version of the LMU developed by Mecaprom Technologies Italia in collaboration with an external company.

10.1. LMU v2.0 block diagram

The core of the latest LMU is the TC297TA Aurix microcontroller combined with the TLF35584 power supply providing safety support as SEooC, up to ASIL D in order to cover even other functions (with greater ASIL level) that might be allocated to LMU.
The board includes: 4+1x CAN-FD for the connection with the vehicle buses; 1x 100 Mbit Ethernet in order to exchange information with the FusionBoard and the outside word; Level Shifter interface that provide a voltage level translation of the signals exchanged between the two board; 1x USB for software development; GPIOs, Analog Input and Output which allows to use the board as a TC29 evaluation board with the Arduino shield compatibility.
Figure 47 shows the SafetyBoard block diagram.

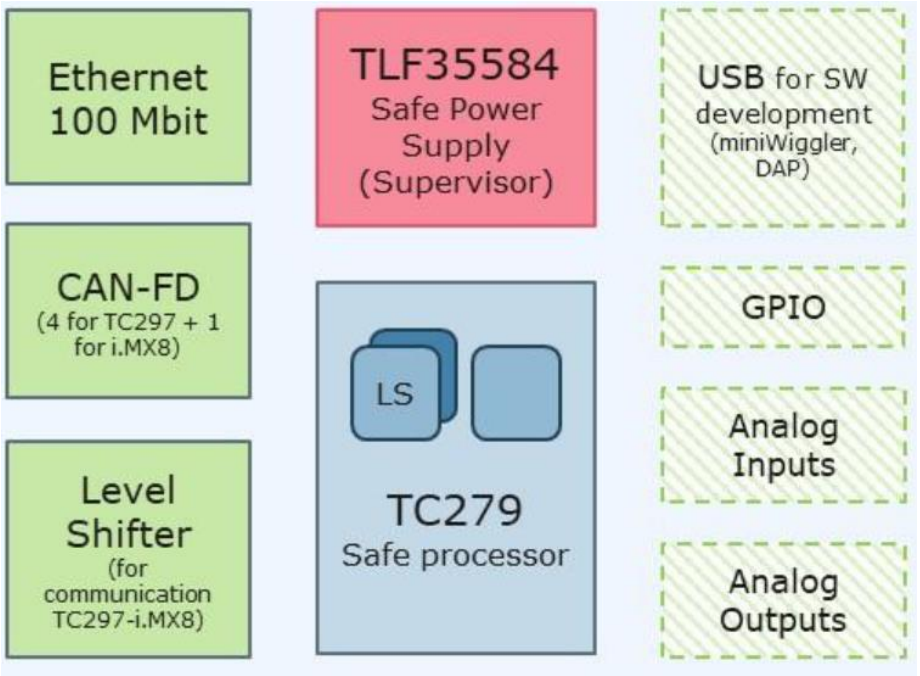


Figure 47: LMU v2.0 - Block Diagram

10.2. LMU v2.0 Microcontroller

The Infineon TC297TA is an automotive 32 bit microcontroller based on a Tricore Architecture, it combines three powerful technologies within one silicon die, achieving new levels of power, speed, and economy for embedded applications:

- Reduced Instruction Set Computing (RISC) processor architecture;
- Digital Signal Processing (DSP) operations and addressing modes;
- On-chip memories and peripherals.

The main features of the TC297TA are:

- Triple TriCore™ with up to 300MHz and DSP functionality
- Supporting Floating Point and Fix Point with all Cores
- Dedicated FFT HW Acceleration Unit
- Up to 8MB Flash w/ ECC protection
- 384 KB EEProm @125k cycles
- Up to 728 KB + 2MB RAM w/ ECC Protection for RADAR/Camera Image Storage
- 4x 12bit SAR ADC Converter
- Ethernet 100Mbit
- FlexRay, CAN, CAN FD, LIN, SPI
- Redundant and Diverse Timer Modules (GTM, CCU6, GPT12)
- Programmable HSM (Hardware Security Module)
- External Memory Interface
- High Speed Serial Interface for Interprocessor Communication
- High Speed Trace Port 2.5Ghz for Real Time Vision and Radar Data Tracking
- Single Voltage Supply 5V or 3.3V
- LFBG A-292 Package

The block diagram of TC297TA is reported in Figure 2.

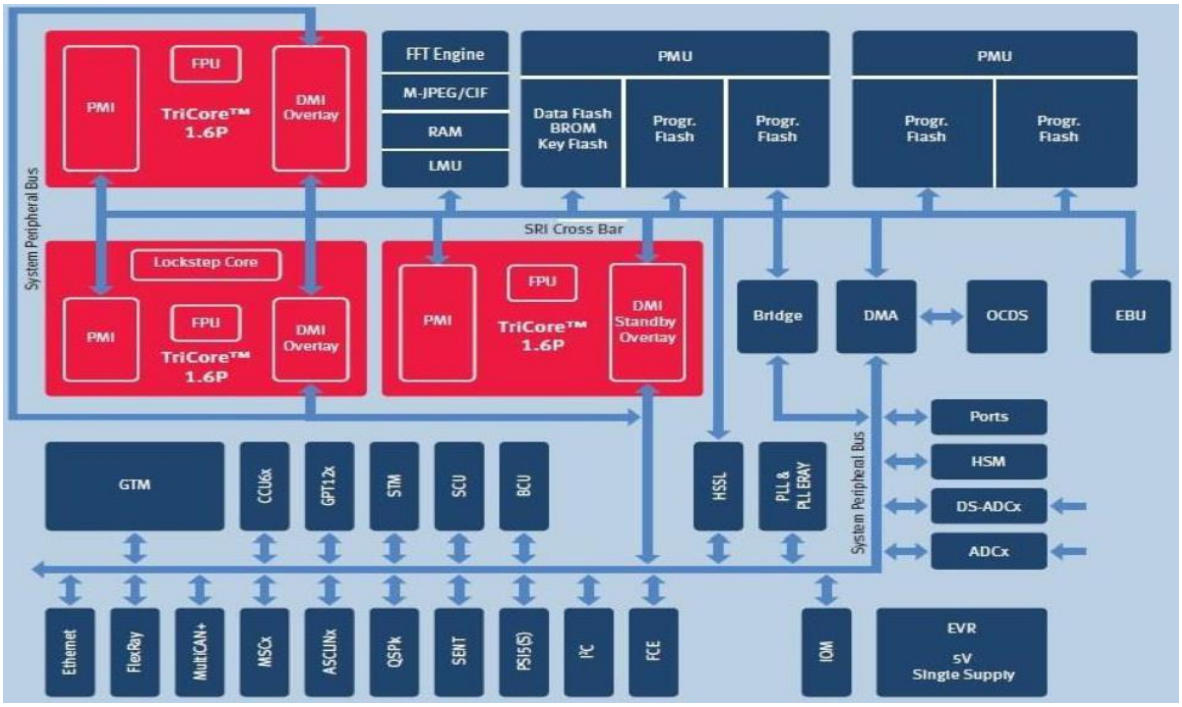


Figure 48: TC297TA block diagram

The main functions of the board are the following:

- Power Supply:
    - Safe state control;
    - External supply identification (12V via SEAM connector and power connector, or 5V via USB connector);
    - Power ON the FusionBoard.
- 1x 100 Mbit Ethernet;
- 4+1x CAN-FD:
    - 4x CAN-FD channels of the TC29 (CAN0 with wake-up functionality);
    - (1x CAN-FD channel of the i.MX8 (the SafetyBoard integrates the transceiver for the second CAN i.MX8 channel)).
    - All can lines are protected against:
        - Short to battery
        - Short to ground
        - Short between lines
- 2x SPI channels connected to two SPI of the i.MX8 processor;
- 1x USB interface for easy debugging;
- GPIOs, Analog Input and Output in order to make the the SafetyBoard the usable as TC297 evaluation board, compatible with the Arduino shields.

10.2.1. Operating voltage

Battery voltage requirements of a standard powertrain application have been targeted:

- Safety Board:
    - Nominal battery voltage: 12V system
    - Operating battery voltage range (full performance): $3V \leq Vbatt \leq 40V$.

10.2.2. Operating temperature range

Safety board temperature range: -40 to +85° C;

10.2.3. Technical Specifications

The board is designed in order to take into account the future developments of the Hyper SDF platform and to be used as a TC297 evaluation board Arduino shield compatible.

10.2.4. Board Connectors

The LMU mounts the following connectors (Figure 49):

- SEAM connector 500 ways: it is an High-Speed High-Density Open-Pin-Field Array Terminal used for connect the SB with the FB;
- The standard 9 pin D-sub connectors:
    - DE09_A for the CANs 0 and 1, the CAN0 is the FD-CAN with wake-up function and the CAN1 is the FB FD-CAN line;
    - DE09_B for FD-CAN2 and FD-CAN3.
- RJ-45 connector for the 100 Mbit Ethernet communication;
- J1, J2, J3, J4, J5 and J6 dual in-line connectors: used as a GPIOs for the TC29 and ARDUINO compatible;
- Micro USB_AB_1 connector for software development;
- Micro USB_AB_2 only for power supply;
- Micro USB_AB_1 connector for software development;

- Micro USB_AB_2 only for power supply;
- SPOX connector.

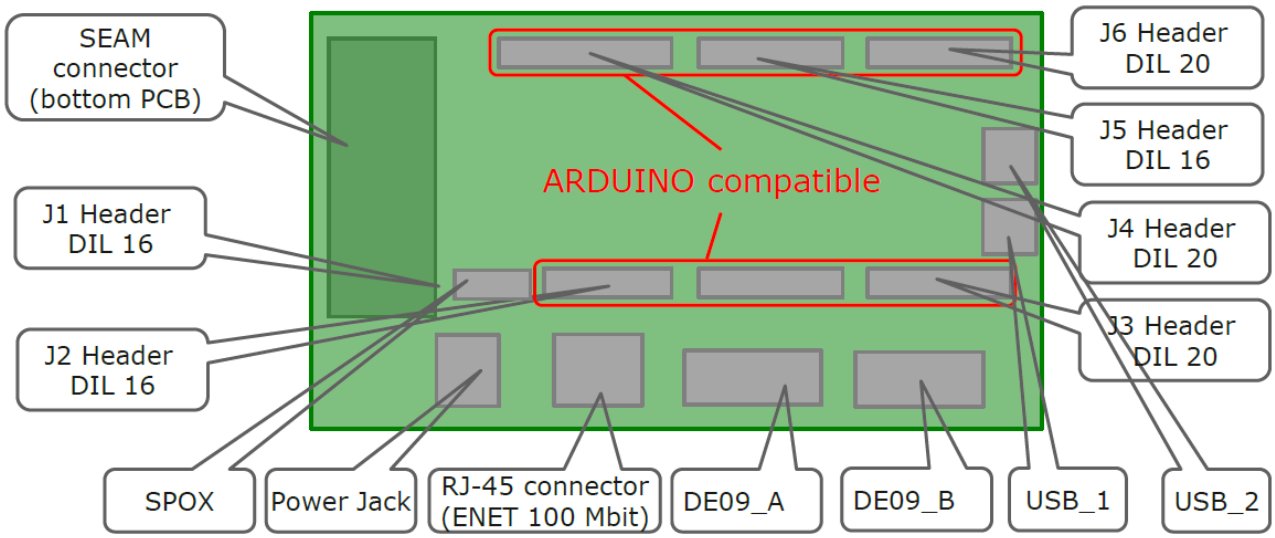


Figura 49: Board connectors

10.2.5. Power supply

The microcontroller needs 3 different supply voltage. Voltages are generated via Infineon's Multi Voltage Safety Micro Processor Supply TLF35584QVVS1 (+5V) and via the microcontroller itself (+3,3; +1,3V). The +5V are also used for power the CAN transceivers and to generate +3,3V for the PHY KSZ8051MNLV supply.

Applying a stable supply voltage causes the power on reset after a short period.

There are 3 possibilities for power the board from external:

- the 2.1mm jack socket;
- dedicated pins on the SEAM connector;
- micro-USB.

All the power supply are protected against:

- Polarity inversion
- Simultaneous power supplies connections

All other features will be implemented according to the future developments and characteristics developed by Mecaprom Technologies Corporation

11. FIDES Analysis

In this section will be given an overview of what a FIDES analysis is, how it is carried out and what output it provides.

Figure 49: FIDES Logo

11.1. Application domains

The FIDES methodology is applicable to all domains using electronics:

- Aeronautics.
- Navy.
- Military.
- Production and distribution of electricity.
- Automotive.
- Railway.
- Space.
- Industry.
- Telecommunications.
- Data processing, home automation, household appliances

11.2. Model coverage

The FIDES methodology models failures with origins intrinsic to the studied items (item technology or manufacturing and distribution quality) and extrinsic (specification and design of the equipment, selection of the equipment procurement, production and integration system).

The methodology takes account of:

- Failures derived from development or manufacturing errors.
- Overstresses (electrical, mechanical, thermal) related to the application and not listed as such by the user (the occurrence of the overstress remained concealed).

Failures not dealt with by the methodology include:

- Software failures.
- Unconfirmed failures.
- Failures related to preventative maintenance operations that were not carried out.
- Failures related to accidental aggressions when identified or proven (failure propagations, use outside specifications, bad manipulations: the occurrence of the overstress is known).

11.3. General case

Reliability predictions given by the FIDES methodology are failure rates denoted λ.

Experimental observations show that the way in which the failure rate varies as a function of time is usually represented by the following "bathtub curve".

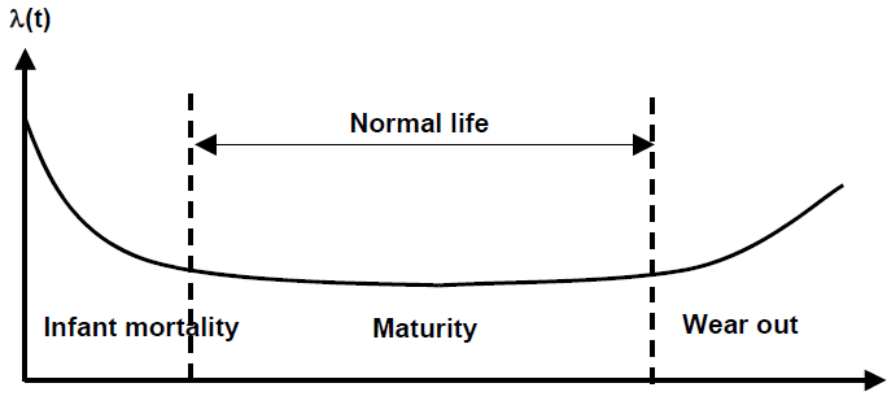


Figure 50: Failure rate distribution

Therefore the life of a product can be broken down into three periods:

- Infant mortality period, early failures.
- Period of useful life, approximately constant failure rate.
- Wear out period, wear failures.

The failure rate reduces during the infant mortality period. The reliability of a product increases with time. This is the period during which failures are due to problems with setting up processes and debugging the design and components.

The useful life period is represented by a constant failure rate. The failure rate is independent of the number of functioning hours of the product (this is why these failures are often described as random). This period is often non-existent for mechanical products, but is the reference case for electronics.

The reliability during the wear out period decreases with the number of hours of functioning; the older the product, the more probable a failure becomes. This type of behaviour is characteristic of items subject to wear or other progressive deterioration and is related to an increasing failure during this period.

The FIDES evaluation method includes an evaluation of the reliability at constant failure rate (in fact, at an average failure rate). Infant mortality and wear out periods are excluded from the prediction (with a special case for some subassemblies). This is due to the following reasons:

- Firstly, the infant mortality period is representative of the development of an equipment or a system. Control over increasing reliability during this phase is a crucial step towards quickly obtaining good reliability.

- The wear out period is also excluded from FIDES because in principle it is sufficiently far in the future compared with the useful life of electronic systems covered by FIDES. However, checking this assumption during the design of the product is a key point. If items do not have a sufficiently long life, approaches other than predicted reliability alone must deal with this aspect, for example such as the definition of preventative maintenance.
- There is no doubt that microscopically, very few failure mechanisms strictly satisfy a "constant rate" type occurrence law. However:
    1. The dispersion of many failure mechanisms, although they are accumulative and therefore increasing with time, is such that they can be deemed to be constant over the periods considered.
    2. The accumulation of the large number and diversity of components, even on a single board, will be close to a constant.
    3. Age differences between equipment in the same system or a stock of equipment will tend to make the rate constant for an observer at system level.

For these reasons, use of a constant failure rate is still the most relevant approach for estimating the predicted reliability of a system.

The physics of failures is used in some special cases to predict probabilistic life values (Time To Fail). This type of prediction is complementary to the reliability prediction, but cannot replace it.

11.4. Failures related to wear out in the case of subassemblies

In most cases, the life for electronic components is sufficiently long compared with the operational usage period and therefore its impact is negligible, but, for example, this is no longer the case in the presence of wear phenomena caused by moving mechanical parts.

Failures related to wear out of some subassemblies, for which the life is significantly shorter than the complete system, may make a non-negligible contribution to reliability. Particular modelling is proposed for these cases.

11.5. Confidence in the prediction

Evaluations made using the FIDES methodology are aimed at providing realistic values of reliability levels, similar to usually observed average values (not pessimistic or conservative values).

One essential question after making an estimate of the predicted reliability is to know what confidence should be assigned to the estimate. This question is particularly important because users do not have confidence in raw results provided by previous methodologies and reliability control (quantification and engineering) in projects has become essential.

One of the objectives of the FIDES project is to build up this confidence. However, the accuracy of the prediction is not the only purpose of the FIDES methodology. Identification and control of factors influencing reliability may be considered as being even more important objectives.

As a general rule, an isolated estimate of the predicted reliability cannot be combined with a confidence interval in the same way as is possible when a failure rate is measured from feedback from operations. In the case of FIDES, while it might be possible to calculate a confidence interval on some basic failure rates, it is practically impossible to estimate confidence in all correcting parameters, even in the case of known and widely used physical acceleration laws.

The representativeness of the prediction increases with the number of items considered. Predictions are generally not applicable for a single item. It is recommended that the level considered should be at least the equipment level (set of electronic boards).

A comparison between a predicted reliability and a reliability measured from feedback from operations is always a difficult approach, because there are also uncertainties in measuring reliability in service. For example, these uncertainties are related to:

- The change in reliability with time.
- Poor knowledge of the real life of the product.
- The separation of failures that are due to the product from those that result from non-product sources.
- Cases of batch effects, which are difficult to take into account for the reliability calculation.

One prerequisite for the comparison between a predicted reliability and a reliability measured from feedback from operations is to assure that the life profile actually experienced by the product is sufficiently close to the life profile used to make the prediction. Otherwise, the comparison applies to the relative severity of the two life profiles (predicted and real) and not to the reliability itself.

11.6. Covered items

The FIDES methodology covers items varying from an elementary electronic component to a module or electronic subassembly with a well-defined function. Coverage of item families by FIDES is not absolutely exhaustive. However, the coverage is broadly sufficient to make a representative evaluation of reliability in most cases.
The methodology is applicable to COTS (Commercial Off-The-Shelf) items.
With this term is denoted any item bought from a catalogue with a supplier reference and for which the customer has no control over the definition or production, and available on the domestic or foreign market. This item may be modified, and production or maintenance may be stopped without the customer having any control. A single supplier or several suppliers may be available for the same item.
FIDES deals with the following COTS:

- Components such as printed circuit boards, discrete semiconductor circuits or passive components.
- Subassemblies such as hard disks and screens.
- Assembled COTS boards.

11.7. Origins of reliability data

Data used for the construction of models originate from:

- Failure analysis databases in the weapon systems domain and the civil aeronautical domain
- Reliability data for component and subassembly manufacturers.
- Existing reliability collections when they are relevant and can be used.

These data were used to develop and calibrate models, based on three methods:

1. Method 1: Use of operational databases (aeronautical and military) on failure mechanisms.
2. Method 2: Use of test data from component and subassembly manufacturers (environmental tests, technological data, etc.).
3. Method 3: Use of mixed data (manufacturer data, feedback from operations, test results). This method is used mainly to build subassembly models.

11.8. FIDES approach

The FIDES reliability approach is based on the consideration of three components (Technology, Process and Use). These components are considered for the entire life cycle from the product specification phase until the operation and maintenance phase.

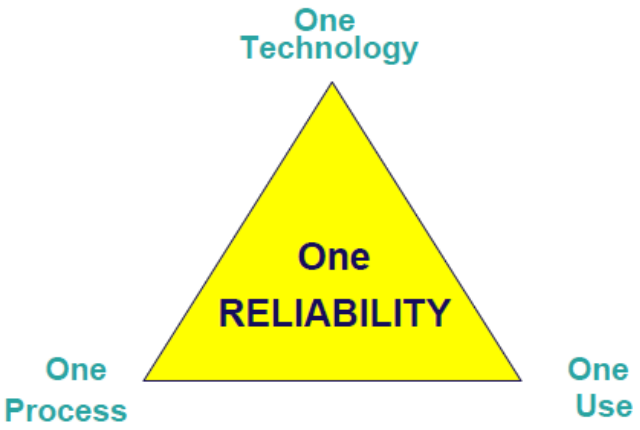


Figure 51: FIDES approach

Technology covers the technology for the item itself and also for its integration into the product.
Process considers all practices and the state of art from the product specification until its replacement.
Use takes account of usage constraints defined by the product design and by operation at the final user.
These models consider a technology faced with usage constraints based on a failure mechanism approach and associated contributing factors. Those particularly balance the risk of failure by all process contributing factors that can activate, accelerate or reduce these mechanisms.

11.9. Generic input data

Input data are as follows, generically:

11.9.1. Data on environments and product usage conditions.

These are typically:

- Operating temperature.
- Amplitude and frequency of temperature cycles.
- Vibration amplitude.
- Relative humidity.
- Ambient pollution level.
- Exposure to accidental overstress (application type).

These data should be broken down for each product life phase. The level of detail at which the product life profile is described within an operational system controls the accuracy of the reliability evaluation. Therefore, this step in the prediction analysis should be carried out with the utmost care.

11.9.2. Data on the product definition.

These are typically:

- Parts lists.
- Technical or technological characteristics of items derived from manufacturer datasheets.

Information related to the application shall be evaluated for each phase in the life cycle:

- Stress or overstress levels on items (dissipated powers, stress under power, etc.).
- Local aggravation (or moderation) to the temperature or another environmental parameter.

In practice, these data are often constant or assumed to be constant for all operating phases, but this is not always the case.

11.9.3. Data on the product life cycle.

These data must be collected through an audit of the process. This audit deals with the control of the reliability. It concerns the phase of specification, design, equipment manufacturing, integration into system, product operation, maintenance process and the support activities. Obviously, the thoroughness and extent of this audit shall be matched with the required reliability level.

11.10. Mission Profile

After internal discussion with Mecaprom engineers has been defined a mission profile with approximate trend to a Gaussian, as shown in figure 52.

LIFE PROFILE

Standard life profile

Phase name	On / Off	Calendar time (hours)	Temperature	Temperature cycling				Humidity	Mechanical	Chemical			
			Ambient temperature (°C)	Δt (°C)	Cycle duration (hours)	Number of cycles (/phase)	Maximum temperature during cycling (°C)	Relative humidity (%)	Random vibrations (Grms)	Saline pollution	Environmental pollution	Application pollution	Protection level
Standby	OFF	2.000 h	-20,00 °C	10,00 °C	24 h	80	-15,00 °C	30	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	3.000 h	-10,00 °C	10,00 °C	24 h	125	-5,00 °C	30	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	6.000 h	0,00 °C	10,00 °C	24 h	200	5,00 °C	50	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	8.000 h	10,00 °C	10,00 °C	24 h	330	15,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	14.000 h	20,00 °C	10,00 °C	24 h	580	25,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	20.000 h	25,00 °C	10,00 °C	24 h	800	30,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	14.000 h	30,00 °C	10,00 °C	24 h	580	35,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	8.000 h	40,00 °C	10,00 °C	24 h	330	45,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Standby	OFF	5.000 h	50,00 °C	10,00 °C	24 h	200	55,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Total Stanby hours		80.000 h											
Operative	ON	50 h	-20,00 °C	15,00 °C	4 h	12	-13,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	100 h	-10,00 °C	15,00 °C	4 h	25	-5,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	200 h	0,00 °C	15,00 °C	4 h	50	7,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	500 h	10,00 °C	15,00 °C	4 h	125	17,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	1.000 h	20,00 °C	15,00 °C	4 h	250	27,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	2.000 h	25,00 °C	15,00 °C	4 h	500	35,00 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	1.000 h	30,00 °C	15,00 °C	4 h	250	37,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	500 h	40,00 °C	15,00 °C	4 h	125	47,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic
Operative	ON	200 h	50,00 °C	15,00 °C	4 h	50	57,50 °C	80	0,00 Grms	Low	Moderate	Low	Hermetic

Figure 52: Mission Profile

To proceed with FIDES analysis it is necessary to know in detail the HW of the LMU, in order to insert each component in the simulation tool and then be able to obtain a failure rate as reliable and realistic as possible.

12. Conclusion

The focus of the Final Thesis was on understanding the scenarios in which the Epic0 vehicle is operating and, in particular, on understanding the functioning of the torque management function, in order to clearly develop an Item Definition and, as a result, a Hazard Analysis Risk Assessment (HARA).

The ASIL level resulting from the HARA analysis was used to understand whether the state-of-the-art features of the LMU present in the Epic0 vehicle currently in production were consistent with the requirements of the ISO.

The comparison showed that the current version of the LMU does not meet the safety requirements imposed by an ASIL C.

At this point Mecaprom Technologies Corporation in agreement with Regis Motor have decided to entrust the development of the new control unit to an external company, providing as initial input for the design of the board the data obtained from this analysis.

It is therefore necessary to implement several measures both HW and SW in order to comply with the requirements of the ISO and, subsequently, test the HW by using the FIDES tool, briefly described in the document, inserting all the electronic components mounted in the board and all the usage data deriving from the definition of the mission profile, so as to obtain a probability of failure rate as reliable as possible.

This document therefore aims to be the starting point for the future development of the LMU of the vehicle and, more generally, for the development and evolution of the vehicle Epic0.

13. References

[1] "WHO | Global status report on road safety 2018", WHO, 2021.

[2] "WHO | Save lives: a road safety technical package", WHO, 2017.

[3] R. Bell, "Introduction to IEC 61508", Conference in Research and Practice in Information Technology Series, 2005.

[4] IEEE Spectrum "How Software is Eating the Car", Robert N. Charette, 07 June 2021.

[5] N. A. Peper, "Systems Thinking Applied to Automation and Workplace Safety by", 2017.

[6] International Organization for Standardization, \ISO 26262 Part 1: Vocabulary," p. 26, 2009.

[7] H.-L. Ross, "Functional Safety for Road Vehicles", Springer International Publishing, 2016.

[8] Y. Luo, "From conceptual models to safety assurance: applying model-based techniques to support safety assurance" Ph.D. Department of Mathematics and Computer Science, 2016.

[9] REGULATION (EU) No 168/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Official Journal of the European Union, 15 January 2013

[10] FIDES guide 2009, Edition A, Reliability Methodology for Electronic Systems, September 2010

[11] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-1, 2016 edition

[12] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-3, 2016 edition

[13] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-4, 2016 edition

[14] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-5, 2016 edition

[15] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-6, 2016 edition

[16] DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-9, 2016 edition

[17] A Reference Example on the Specification of Safety Requirements using ISO 26262, Jonas Westman1 and Mattias Nyberg, Royal Institute of Technology (KTH)

[18] Formalization of the ISO 26262 standard, Master Thesis, Dennis van den Brand

[19] FUNCTIONAL SAFETY MODEL FOR E/E COMPONENT OF AN AUTONOMOUS VEHICLE, Mukul Anil Gosavi

[20] Analysis and Specification of an AUTOSAR based ECU in compliance with ISO 26262 Functional Safety Standard, Vibhu Layal

[21] How to ensure functional safety, according to ISO 26262, Christian Brenner, December 2019

[22] ISO 26262 Functional Safety Requirement Types, Nabile Khoury, February 2021

[23] Functional Safety Requirements for Battery Management Systems in Electric cars, Nordbatt, September 2019

[24] Practical experiences in applying the "concept phase" of ISO 26262, Dr David Ward, November 2012

[25] Functional safety and IEC 61508 - A basic guide, IEC, November 2002

[26] Provision of information and services to perform an initial assessment of additional functional safety and vehicle construction requirements for L7e-A heavy on-road quads, M Edwards, M Seidl, J Carroll & A Nathanson, April 20014

[27] EU Regulation on the Approval of L-Category Vehicles, Adrian Burrows, International Vehicle Standards, December 2013