POLITECNICO DI TORINO

Department Of Control And Computer Engineering (DAUIN)

Master's Thesis in Mechatronic Engineering

Politecnico di Torino

Development and analysis of car rearlights in accordance with the standard ISO26262

Internal Supervisor:
Prof. Stefano Carabelli

Candidate:
Alessia Maria D'Onofrio

External Supervisors:
Dott.sa Stefania Maria Collura
Dott. David Sajeva

Academic year 2022-2023

Contents

Acronyms

ACRONYM	EXPLANATION
ISO	International Standards Organization
HW	Hardware
SW	Software
HARA	Hazard Analysis and Risk Assessment
ASIL	Automotive Safety Integrity Level
FSR	Functional Safety Requirement
TSC	Technical Safety Concept
SG	Safety Goal
HWSC	Hardware Safety Concept
MCU	MicroController Unit
HWSR	Hardware Safety Requirement
HSI	Hardware Software Interface
FTA	Fault Tree Analysis
FMEDA	Failure Modes Effects and Diagnostic Analysis
SPF	Single Point Failure
MPF	Multiple Point Failure
SM	Safety Mechanism
RF	Residual Failure
DIA	Development Interface Agreement

1 Introduction

Functional Safety is the branch of engineering that deals with safety systems using electrical, electronic and programmable electronic (E/E/PE) technologies. Functional safety is at the heart of the content of the series of standards IEC 61508. The ISO 26262 series of standards is an adaptation of the IEC 61508 needed to meet automotive-specific requirements. The standard applies to electrical and electronic systems consisting of hardware and software components installed in vehicles. ISO 26262 defines the requirements that must be met for the safety of the system, processes, methods and tools used in their development. It also ensures that sufficient safety levels are met and maintained throughout the entire vehicle life cycle.
First of all, it is important to give some definitions useful to understand the subject matter of this document.

- SAFETY = Absence of unreasonable risk. The residual risk of a system is never equal to 0 but it must be reduced as much as possible until it reaches an acceptable value. The final user must be informed of the final residual risk and the measures to be taken;
- RISK = Product between the probability of an hazard occurring times the severity of the accident itself;
- HAZARD = Any source of potential damage, harm or adverse health effects on something or someone;
- SAFETY RELEVANT SYSTEM = system whose failure may cause injury or death to human beings;
- ITEM = system or array of systems to implement a function at the vehicle level.

The Standard ISO 26262 is composed by 12 parts, each of these refers to a specific area of the project. The norm contains the activities to perform during the whole life-cycle of the project in order to obtain a product which can be defined as ISO-compliant. The Standard is based on the assumption of a V-model as a reference for the different phases of product development (Figure 1).

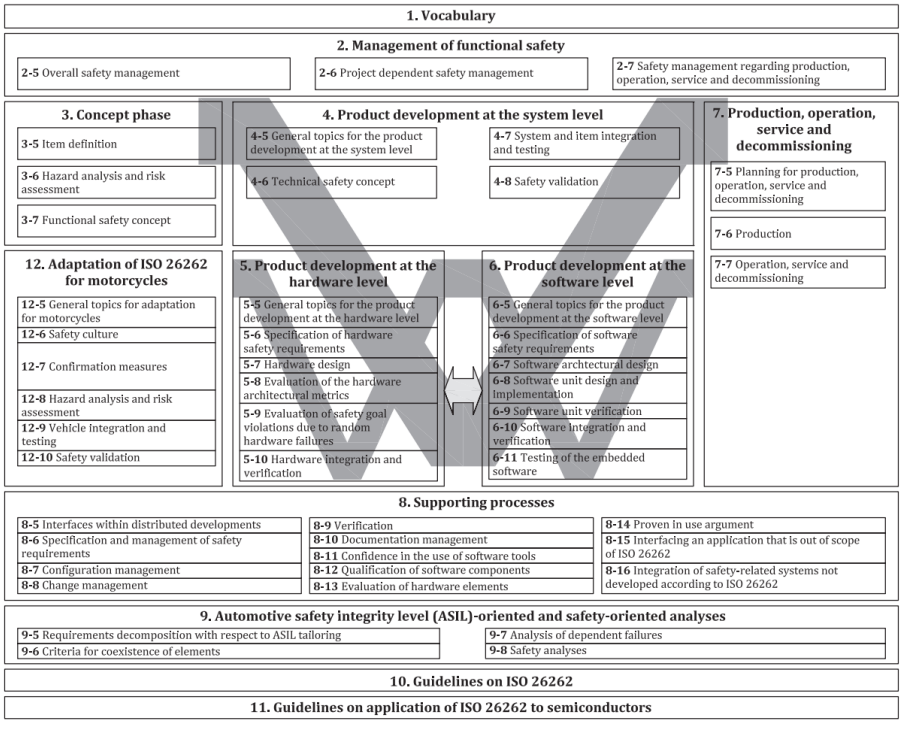

Figure 1: Overview of the ISO 26262 series of standards

This V model also represents the interconnecting among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7. V-Model splits the development process into two parts. The left arm of the V consists of project design while the right arm concentrates on integration of parts and their validation. The two branches interact with each other. HW and SW parts follow two separate v-cycles that are then incorporated into the one concerning the whole system.
The aim of my work/thesis is to implement the lifecycle, according to the ISO26262, for the concept, system and HW parts in order to point out how the safety process impacts on the E/EE parts of a car item. The car item chosen for this project is the car rearlight and its functionalities of stopping, turning and tailing.
This work also includes the safety analyses, both quantitative and qualitative, that provide an evaluation of the robustness of the system. Since the applied analyses and requirements are verified at mathematical and model level, without the possibility of an implementation in a real system (car), the V cycle results completed and confirmed for the verification (test bench, model level...). The validation (on board test) is out of scope for this work.
The structure of this work is based on the V-model discussed above and in particular, it refers to the chapters 3, 4 and 5 of the ISO 26262. It then starts with the "Concept phase" in which the treated item and safety goals related to each function are defined. From the Safety Goals, the Functional Safety Requirements are derived thus concluding the concept phase part.
After that comes the "Product development part at the system level" phase in which provides the writing of a Technical Safety Concept, a document which encapsulates all the most important safety information related to the project. At this stage, the System Architecture and the Technical Safety Requirements, derived from the FSR's, are developed.
Once the System Architecture is defined, we proceed at low-level with the HW part. Therefore, HW requirements, which are more specific than the TSR's, are drawn up and then the actual HW design is done. Once the HW design is defined, we move on to the validation part which is the core of the safety analysis.
The purpose of this project consists on the demonstration that the use of functional safety within a project firstly makes the final product safer but also ensures that the development part of the project is optimized.

2 ISO 26262- 3 : Concept phase

2.1 Item definition

An Item is a set of systems implementing a Vehicle Function. ISO 26262 describes best practice for safe development of items in cars. In this part the item is defined and its functionalities are described in order to support an adequate understanding of the item.
In this project, the vehicle function addressed is 'car rearlights'. The sub-functions that implement it are:

- Brake lights;
- Tail lights;
- Turn lights.

In this particular phase of the development, the functions previously mentioned are defined and generally designed. Stop lights must turn on when the driver requires braking. Turn lights, on the other hand, must turn on when the driver needs to make a right or left turn. Tail lights, instead, must turn on when the daytime running lights are switched on to signal the presence of the vehicle. A problem with one of these functions can lead to a traffic accident.

2.2 Safety goals

In order to determine the safety goals, it is necessary to perform the Hazard Analysis and Risk Assessment (HARA). For each hazardous event evaluated in the hazard analysis, a safety goal and top-level safety requirements shall be formulated. At the end of the analysis, each safety goal is assigned a specific ASIL (Automotive Safety Integrity Level) by a systematic evaluation of the hazardous events. This assignment is based only on the item's functional behaviour, hence the detailed design of the item does not need to be known. The ASIL is determined by considering three specific paramenters: severity (S), probability of exposure (E) and controllability (C). For each paramenter corresponds a specific table on the ISO 26262 which provides a guideline during the assignment.

	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

Figure 2: Classes of Severity

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

Figure 3: Classes of probability of exposure regarding operational situations

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

Figure 4: Classes of Controllability

Once these parameters were assigned the ASIL level can be determined according to the following table (Figure 5).

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure 5: ASIL determination

The safety goal for a specific hazard carries the ASIL requirement. The ASIL D level represents the highest degree of automotive hazard while the ASIL A the lowest. The ASIL QM instead does not dictate any safety requirements.
Usually in projects the safety goals, together with their assigned ASIL, are provided by the client to the developers and the safety analysts. Basing on technical documents related to vehicles on market, the safety goals for this project have been assigned and reported on the TSC. The analysis was consequently structured on the bases of the assigned ASIL in accordance with the instructions given by ISO 26262.

2.3 Functional Safety Requirements

The Functional Safety Requirements (FSRs) are included in the Functional Safety Concept and they are derived from Safety Goals considering the system architectural design. They describe the measures that are to be implemented on a functional level to prevent violation of the safety goals. For each safety goal, at least one FSR has to be specified, although one FSR can cover more than one safety goal. Moreover each FSR inheriting the highest ASIL level from the associated safety goals. Thus there is a hierarchical approach explained below.

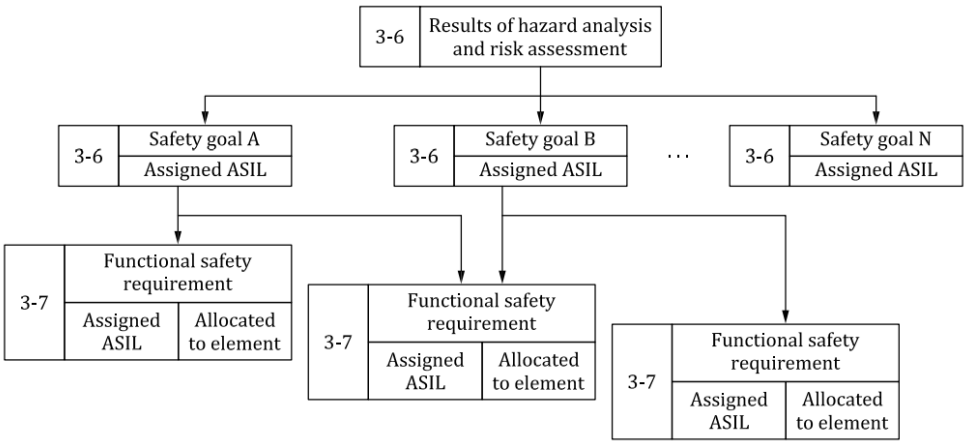

Figure 6: Hierarchy of safety goals and functional safety requirements

The FSRs related to the project are reported in the TSC document and they refer to the safety goals previously discussed. They contain informations about the project system architecture (figure 8) which were derived by taking into account the achievement of the safe states and the assumptions specified in the same document. In particular the FSR give a more in depht description about the trigger signals of the system functions, the range of values of luminous intensity to be respected and the condition to turn off the function. However, all these informations remain at system level and therefore do not give precise indications on the hardware and software to be implemented. That choice is up to hardware and software developers.

3 ISO 26262- 4 : Product development at the system level

The process of the product development at the system level can be schematized as following.

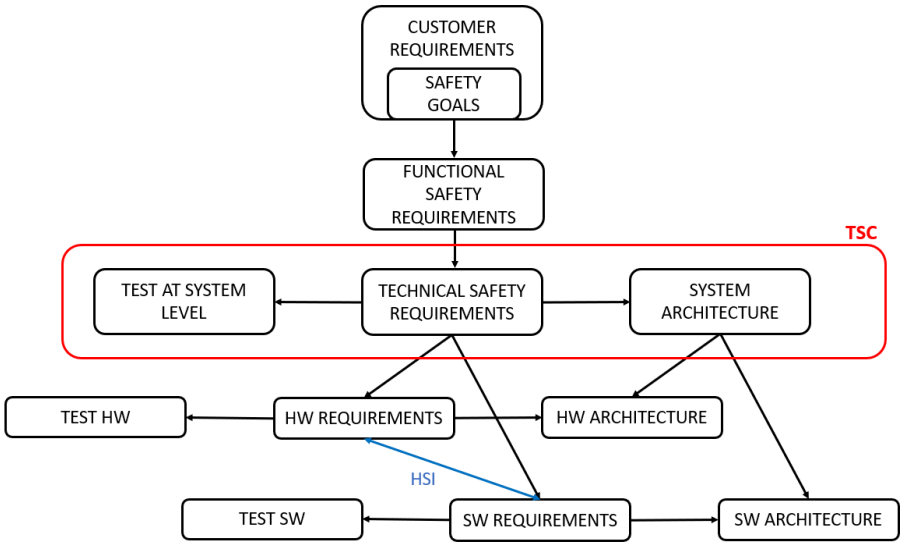

Figure 7: Phase model for the development of a safe-related item

Starting from the customer requirements, the Safety Goals, with their respective ASIL levels, are defined. Derived from SGs, a first more specific information about the system architecture is contained into the FSRs. At that point a TSC document is created. It goes more in depth into the system architecture defining the macro-blocks implementing the relative function. Then, proceeding in parallel, the specific HW and SW requirements and architectures are defined. Once the system is implemented at SW and HW level it is possible to proceed with tests.

3.1 Technical Safety Concept (TSC)

The technical safety concept is an aggregation of the technical safety requirements and the corresponding system architectural design that provides rationale as to why the system architectural design is suitable to fulfil safety requirements resulting from activities described in ISO 26262-3 (with consideration of non-safety requirements) and design constraints.

The TSC of the project is structured as following:

- Document state of art (version, status...)
- Reference document list
- Terms and Acronyms
- General informations (brief system description)
- Safety Concept
  - Safety Goals
  - Safe States
  - Assumptions
  - Functional Safety Requirements
- Technical Safety Requirements
  - TSRs

  - External Requirements
  - External Safety Mechanisms
  - Exit Strategies

- System Architecture (plus explanation of each block composing the subsystems)
- Safety Measure List

To summarise, this document is very important in the field of safety as it keeps track of main informations concerning the project. First of all it contains all the references used for the project and tracks all the changes made to the document itself. It also explains what the objectives of the project are (SGs) and how to achieve them at system level.

3.2 Technical Safety Requirements

The Technical Safety Requirements (TSRs) translate the FSRs at technical level. This means that they provide more details about the interactions between blocks that make up the system architecture but also about stimulus response of the system which affects the achievement of safety requirements. The TSRs are contained in the TSC and comply with the FSRs as required by the standard. They also specify whether a requirement will then be dealt with at software or hardware level, and thus assign a given issue to the field of competence capable of resolving it. Referring to this particular project, only the HW requirements have been treated and specified into another document named Hardware Safety Concept (HWSC).

3.3 System Architecture design

In the Figure 8 it is showed the system architecture related to the project. It is structured as following: there is a macro block representing each function (FZ_BR, FZ_TL, FZ_TN) and all three are located within the block representing the project item (LH_REARLAMP). The latter interfaces with a microcontroller that manages the switching on and off of each function. Each function consists of:

- a power management block that manages the power supply and adapts it for the other blocks
- a light management block that deals with the light intensity of the rearlamp
- a diagnostic block to detect any problems in the function and communicate them to the MCU, which will then deactivate the function itself

As it is possible to notice in the scheme below, each block contains the corresponding ASIL level as required by the standard. For the sake of clarity only the diagram of the left rearlamp has been developed but the development of the right one is exactly the same.

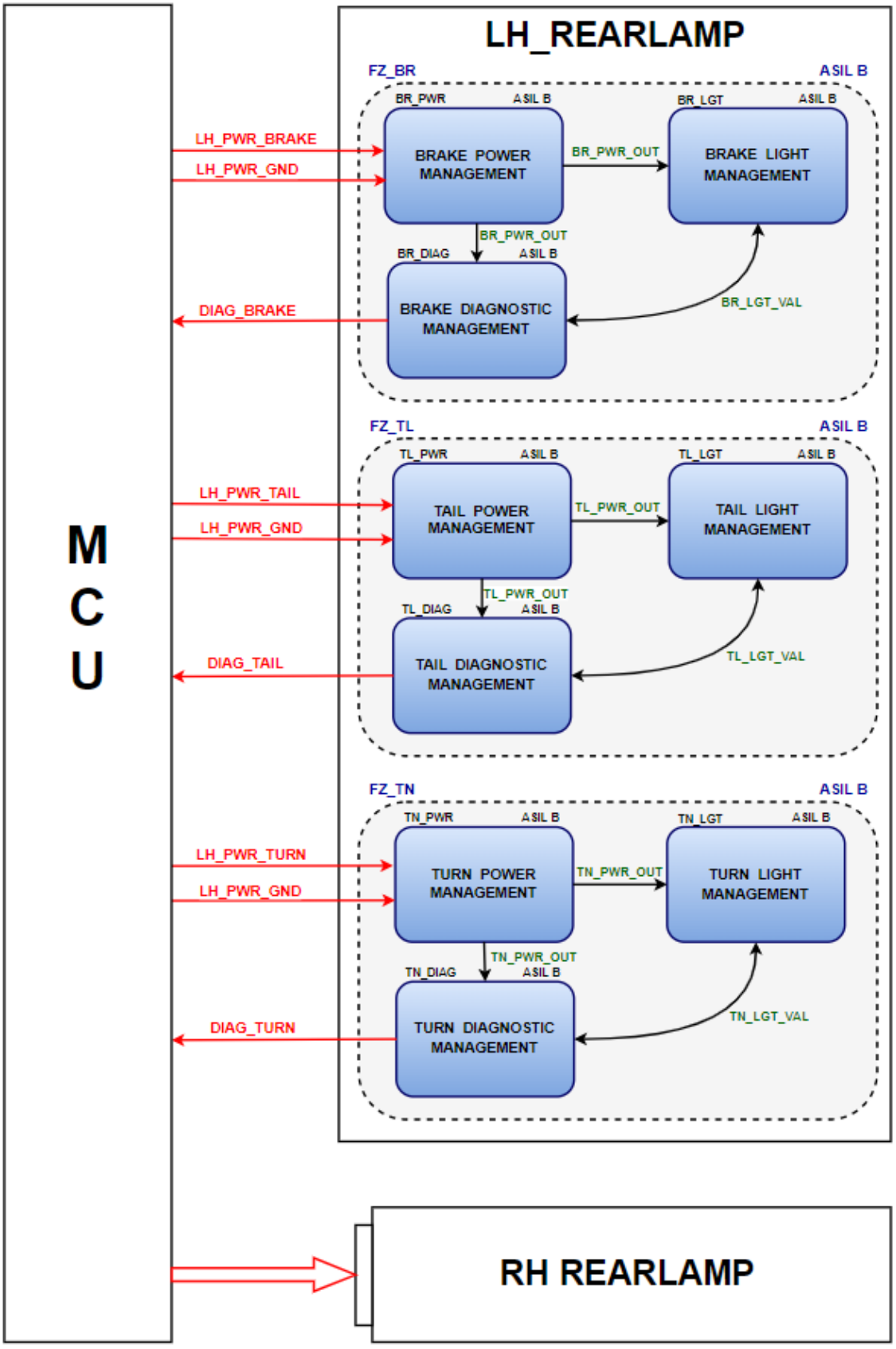

Figure 8: System architecture

4 ISO 26262- 5 : HW part

4.1 HW Requirements

Starting from TSR's allocated to hardware, the Hardware Safety Requirements (HWSR's) are derived. They contain specifications for hardware elements of the item and they shall include:

- safety mechanisms to control internal/external failures of/to the element hardware;
- requirements and relevant properties of safety mechanisms both to comply with the safety requirements of other elements and to detect and signal internal or external failures;
- the hardware safety requirements not specifying safety mechanisms as for example: target values to meet in order to avoid random failures, requirements to avoid specific behaviour of the function or to implement the intended functionality, requirements specifying design measures on cable harnesses or connectors.

The HWSR's of the project are gathered within the Hardware Safety Concept (HWSC), a document organized as the TSC but which goes more in detail about how the functionalities of the system have to be implemented at hardware level. The HWSR's contain specific values to be imposed and thus enforced on the system such as voltage/current values, number of LEDs to be used and in which configuration... As requested by the ISO, there is a direct correspondence between TSRs mapped on hardware and HWSRs.

4.2 Design HW

The main focus of the design at hardware level is making an HW architecture that:

- supports the safety-oriented analyses and takes into account its results;
- fulfils the hardware safety requirements and the hardware-software interface (HSI) specification;
- is consistent with system architectural design specification and satisfies the required hardware design properties.

A single hardware design is created to satisfy both safety and non-safety requirements so that only one development process is involved to handle both.
The HWSC of the project includes only the hardware architectural design; the hardware detailed design, instead, is contained into the file of the FMEDA analysis. The former represents all hardware macro-components and their interactions with one another. The latter is at the electrical/electronic level, i.e. the actual schematics, representing the interconnections between hardware parts implementing the hardware components.
In the ISO26262 chapter 5, paragraph 7.4.1 there are rules that must be respected for the design and therefore based on these rules the hardware design of the functions was created. Below there are the hardware architectural designs concerning the functions composing the item.

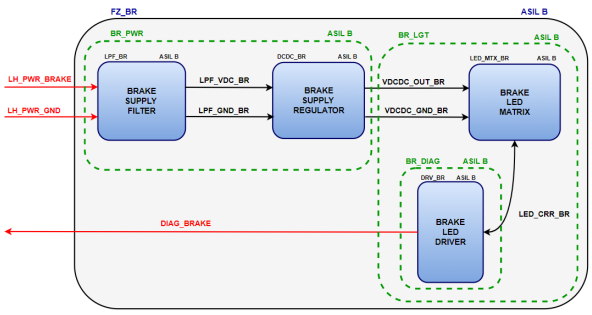

Figure 9: Brake function hardware architectural design

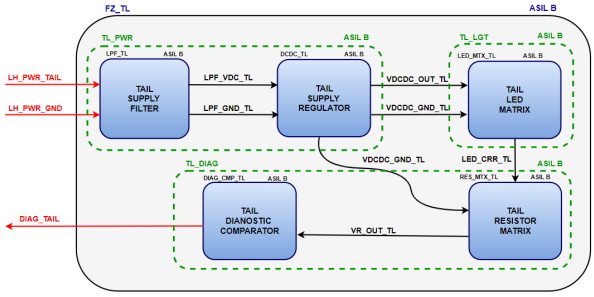

Figure 10: Tail function hardware architectural design

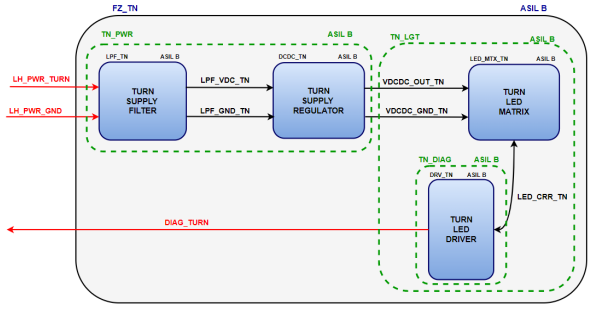

Figure 11: Turn function hardware architectural design

4.3 HW Design Verification

The HW design verification is needed to ensure the compliance of the developed hardware with the hardware safety requirements. In order to satisfy this task, the following test methods shall be applied:

- Functional testing: aims at verifying that the specified characteristics of the item have been achieved, i.e. proper inputs and outputs, functionality of the system...;
- Fault injection testing: aims at simulating a fault or a certain number of faults in order to evaluate the diagnostic coverage of safety mechanisms or, more in general, the damages on the system;
- Electrical testing: aims at verifying compliance with hardware safety requirements within the specified voltage range (out of content of the project).

4.4 Safety Analyses at HW level

The HW design safety analysis aims at identify the causes of failure and the effects of faults that may affect the system. In order to perform this search, there are two possible methods which can be used: Deductive Analysis or Inductive Analysis.
For each safety-related hardware component or part, the safety analysis shall identify the following for the safety goal under consideration:

a. safe faults

b. Single-Point Faults or Residual Faults (SPF or RF)

c. Multiple-Point Faults (MPF)

Concerning the ASIL level assigned to each Safety Goal, the ISO26262 gives a guideline about which types of analysis have to be done. For this project, having all ASIL B level for the safety goal, both qualitative (FTA) and quantitative (FMEDA) analyses have been done. The first with a

deductive approach (top-down) starts from the undesired system behaviour and goes to the causes of this behaviour. The latter instead has an inductive approach (bottom-up) directly considering the effects of the individual faults.

4.4.1 FTA

The Fault Tree Analysis (FTA), as introduced before, is a safety analysis using a deductive approach, which means that it goes from the highest level to the lowest one. In particular, this kind of analysis starts from a "top event" which corresponds to an undesired behaviour of the system (Safety Goal violation) considered as root of a logic tree and it continues through all the possible causes which can lead to this event. Through this type of analysis it is easier to find all the Multiple Point Failures (MPF), i.e. the set of all those failures that, if occurring, they lead to the violation of the Safety Goal. Thus the advantages of this kind of analysis can be schematized as following:

- Top-Down approach: starts with a macroscopic catastrophic event that violates the safety goal up to the microscopic cause;
- Visual Analysis: since it is an analysis built from blocks connected by logic gates, it is easy to see which paths are dangerous and weak. By looking at the diagram, it is therefore possible to visualise the problems of the entire structure;
- At high level: it allows to modify the structure adding or deleting branches, inserting Safety Mechaninsm (SM) thus looking if a certain design is better in terms of safety than another;
- Minimal Cutset computation: by using software tools it allows to see which are the most critical events, i.e. the events with the shortest path from the end of the tree to the top event;
- Applicable to complex system: since it is a visual analysis, staying at a high level it is possible with just a few blocks to completely define the functions of the system and find its weakest points. Whereas using an FMEDA analysis on a complex system would means to analyse thousands of components trying to understand the effects of them at a high level thus needing more time.

Being a qualitative analysis, it does not introduce numerical evaluations but only the creation of the tree structure.
In order to perform an FTA analysis, the first step is to decide at what level of abstraction it should stop. There are four abstraction levels:

a. Functional Level: usually used for very complex systems, is limited to a functional knowledge of the system, i.e. how it works, without defining which components will make up the device;

b. System Level: at this level the system requirements are already draft thus giving a more detailed scheme. It is also possible to know what is present at the HW level and at SW level;

c. HW Level: this is the recommended level for an FTA because it goes into the system block level, i.e. it considers the macroscopic components and not the singular electrical component such as a resistor, a capacitor...

d. Component Level: investigates the possible causes of the negative event into the individual failure modes of the components. This is a very deep level of abstraction and it is not recommended for complex systems which contain a lot of components.

Once the level of abstraction has been chosen the next step is to decide the top event which is usually identified as the violation of the Safety Goal. Then, through a deductive analysis, the causes leading to the violation are found and subsequentially the causes of these last too. Thus proceeding in sequence it arrives at the primary causes of the event itself that will be found at the bottom of the Fault Tree. From the tree structure is possible to identify different cutsets. A cutset is defined as a group of events which, if it occurs, leads to the violation of the safety goal. At the end of the analysis, all the minimal cutsets are identified, thus giving an idea of how much safe the system is.

For what concern the project, a system-level abstraction was chosen in order to not obtain a too huge tree structure. The Fault Tree of the project is contained into the document "FTA report" which has been made thanks to the Isograph Reliability Workbench tool. A small extract from the FTA analysis report is shown in the figure below (Figure 12).

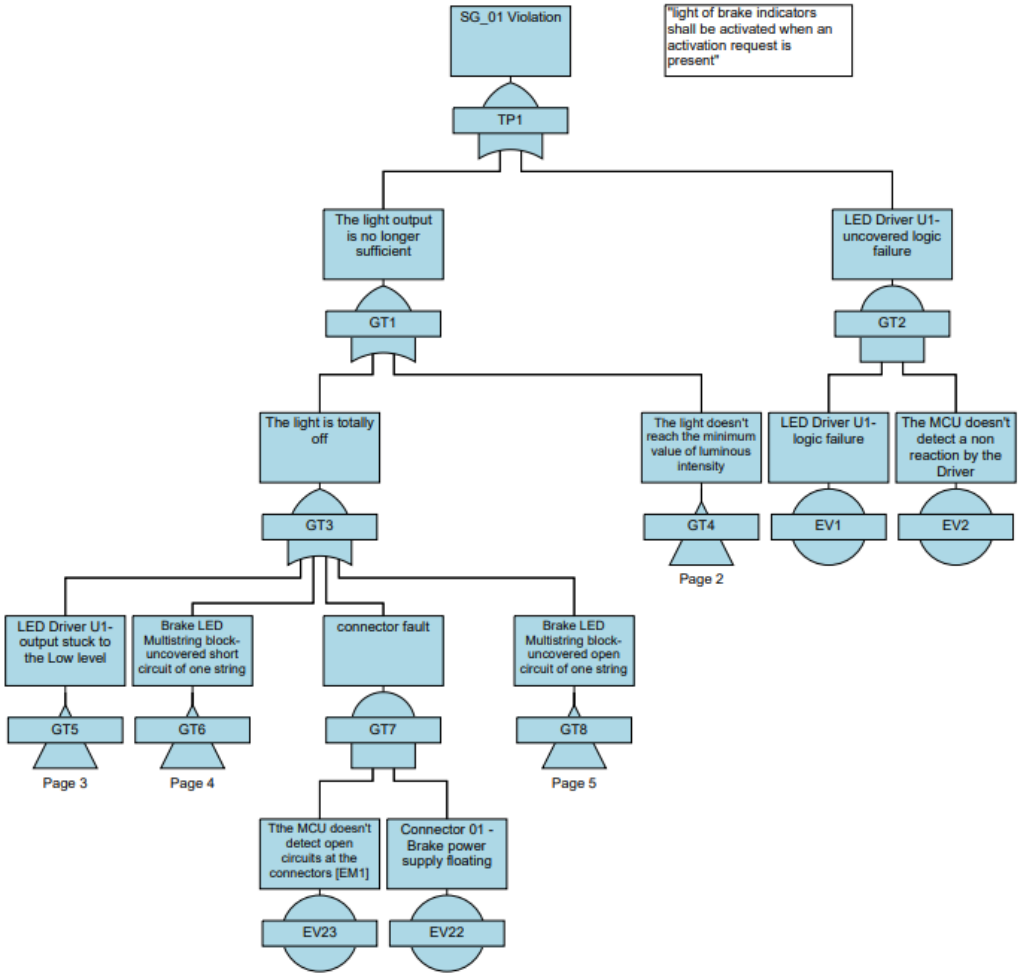

Figure 12: Abstract of FTA thesis report

From the figure is possible to notice a certain simbology which is typical of this analysis. At the top of the fault tree there is the top event named by the acronym "TP" followed by a number which uniquely identifies that particular event. The other blocks identified by the acronym "EV" are the events. They can be primary or intermediate events. The first are the ones at the bottom of the tree, i.e. that events that cannot be developed further. The latter instead are the ones between the top event and the primary ones and they are identified by the acronym "GT" which stands for "Gate". A gate is the link between output and corresponding input events and it can be one of the type: logic AND, logic OR or PRIORITY AND (the output event occurs only if the input events occur in sequence from left to right).
Thanks to the same tool used for the tree structure, a search and then an analysis of all the minimal cutsets relating to each SG have been carried out. This analysis is contained into the document "FTA cutset analysis". Each cutset has an associated order which corresponds to the number of events associated to the path. Cutsets with an order equal to 1 are considered as Single Point Failures and they are the most dangerous ones. Therefore, in order to have a system with a good level of safety, it is better to limit cutsets of order 1 as much as possible.

4.4.2 FMEDA

The acronym FMEDA stands for "Failure Modes, Effects and Diagnostic Analysis". As introduced before, this particular type of analysis uses an inductive approach, i.e. it goes from the lowest level to the highest one. It is possible to notice that this kind of approach is complementary to the one used by the FTA. FTA and FMEDA can be combined to provide the safety analysis with the right balance of top-down and bottom-up approach without redundancies or duplicate work.
Thanks to the FMEDA, the possible diagnostics of failure and its effectiveness by the system under investigation is studied more in detail. This analysis gives an estimate of how much the system is able to detect a failure. In order to do this, three specific parameters are computed:

- SPFM (Single Point Fault Metric)
- LFM (Latent Fault Metric)
- PMHF (Probabilistic Metric for Random Hardware Failures)

To have an acceptable level of safety, the value of these parameters must fall within a certain range imposed by the standard.

	ASIL B	ASIL C	ASIL D
SPFM	$\geq 90\%$	$\geq 97\%$	$\geq 99\%$
LFM	$\geq 60\%$	$\geq 80\%$	$\geq 90\%$
PMHF	$>10^{-7}$ h^{-1}	$>10^{-7}$ h^{-1}	$>10^{-8}$ h^{-1}

Table 1: Range values for SPFM, LFM and PMHF imposed by ISO26262

The FMEDA analyses the random hardware failures at the component level. It assigns a failure rate and a distribution to each component failure mode. Hardware architectural metrics (single-point fault metric and latent-fault metric) shall be calculated and reduced by the application of diagnostic coverage. The scope is to lead the minimum target requested by ISO 26262 according to the safety goal ASIL. In order to assign the correct values of failure rate and distribution to each component a reference is made to the following documents: SN29500 and IEC62380. These documents provide elements to calculate failure rate of mounted electronic components, in particular they refer to passive components (resistors, inductors and capacitors).
The FMEDA related to this project, it has been set with an Excel document named "FMEDA" with a table cointaining all the informations needed for the analysis. At each component belonging to the system it has been assigned a value of failure rate taken from the documents mentioned above. The failure rate is defined as the number of times that an item fails in a specified period of time and its value represents the reliability of the product. It is represented with the symbol λ and it is quantified with the unit of measurement of FIT. A FIT is defined as the number of failures over 10^9 hours of work.
Starting from the failure rate, the failure rate fraction has been computed taking into account the respective failure modes relative to the specific component with their distribution. Then for each failure mode of each component the analysis leads to evaluate whether or not in case of failure it goes to violate the safety goal. If the failure mode of a specific component directly violates the safety goal, the value of that specific failure rate is considered as SPF (single-point failure rate). All the values of SPFs relative to the components are used for the computation of the SPFM through the following formula:

$$SPFM = (1 - \frac{\lambda_{SPF} + \lambda_{RF}}{\lambda_{tot}}) \tag{1}$$

Where λ_{SPF} is the sum of all the SPFs, λ_{RF} is the sum of all the residual failure rates and λ_{tot} is the sum of all the failure rates. The weight of the parameter λ_{RF} depends on the diagnostic coverage of the safety mechanism applied. Basing of the coverage percentage of the safety mechanism applied the impact of the failure changes. The safety mechanism can have:

- high coverage (99%)
- medium coverage (90%)

- low coverage (60%)

So basing on these level of coverage the parameter λ_{RF} relative to each component can impact on the computation at the 1%, 10% or 40%.

Similarly, it is assessed whether the breakage of that component, added to other faults at other components, violates the safety goal. In this case, the corresponding failure rate should be considered as LF (latent fault) and it is used to compute the LFM using the following formula:

$$LFM = (1 - \frac{\lambda_{LF}}{\lambda_{tot} - \lambda_{SPF} - \lambda_{RF}}) \tag{2}$$

Where λ_{LF} is the sum of all the LFs, λ_{SPF} is the sum of all the SPFs and λ_{tot} is the sum of all the failure rates.
Once these parameters have been calculated, it is necessary to check that they fall within the safety values imposed by the ISO. Referring to this particular project, the computed values comply with the ones imposed so no design changes had to be made to the project. In the case that these values did not meet those imposed by the standard, there would be a need to insert safety mechanisms in order to increase the system's ability to detect faults.
After the computation of SPFM and LFM, the PMHF is calculated using the following formula:

$$PMHF = \lambda_{SPF} + \lambda_{RF} + \lambda_{DPF_{det}} * \lambda_{DPF_{lat}} * T_{lifetime} \tag{3}$$

Where:

- $\lambda_{SPF} + \lambda_{RF}$ = sum of all the failure rates relative to single point failure
- $\lambda_{DPF_{det}}$ = sum of all the failure rates relative to the multiple point failure with fault coverage
- $\lambda_{DPF_{lat}}$ = sum of all the failure rates relative to the multiple point failure without fault coverage
- $T_{lifetime}$ = 10'000 working hours

Also in this case, referring to the project, the values of PMHF fall within the range imposed by the ISO.

5 Conclusions

When speaking of functional safety, it is important to specify that it does not mean that there is no risk of malfunctioning, but functional safety implies the absence of unacceptable risks due to hazards caused by incorrect behaviour of electrical and electronic systems. Automotive Functional Safety is the implementation of protective measures to eliminate or mitigate hazards caused by the failure or unintended behavior of a vehicle-level system.
The main purpose of this project aims to demonstrate how much the Functional Safety impacts on an automotive project both in terms of safety and optimisation of the development process. As treated in this work, Functional Safety involves transversally all the stages of the product development process which constitute the V-cycle mentioned in the introduction. By intervening during the design and development, verification and validation, production, operation and disposal of the product, the Functional Safety allows to guarantee a final product capable of avoiding or mitigating the possible risks due to malfunctions of electrical systems-electronic devices on board the vehicle. So the first proven result is a safe product for users according to a certified standard. The other fundamental aspect of functional safety can be seen in the optimisation of the product development process. As demonstrated in this thesis, applying a safety analysis during the development and design phase makes it possible to limit the number of changes that need to be made to the item architecture, thus avoiding costly product recalls. It also ensures that there is no unnecessary redundancy at component level so it avoids "overdesign" of components that have no impact on functional safety.
Currently, ISO 26262 is not a certification standard and therefore does not contain clauses governing certification. From the point of view of the standard, there is no obligation to certify systems, components or processes. Experience with the implementation of the ISO 26262 standard by experts in the field has reported that most cases where the standard is implemented a valid external assessment and certification is obtained. The content of these checks is currently being defined by the relevant certification bodies. From a regulatory point of view, ISO 26262 does not entail any direct change in the legal situation for type approval. In fact, the provisions concerning liability for defective products are still applied. Explicit agreement at the technical level, in particular on safety targets, classification of safety targets and safety measures to be implemented, etc., is necessary. The purpose of the Development Interface Agreement (DIA) is to detail the explicit agreement between the companies involved in the development of E/E systems or components. This document is necessary to guarantee the development of a product respecting safety requirements beyond the sales goal. There is, however, a consideration to be made regarding ISO26262: ISO26262 terminology can lead to misunderstandings that impact, in particular, on the writing of requirements. The optimal solution lies in making the standard as objective as possible and then making it mandatory in automotive production processes.