CHALMERS
UNIVERSITY OF TECHNOLOGY

Implementing ISO 26262-5

A guide to Functional Safety for Product Development at Hardware Level.

Master's thesis in industrial and material science

SOFIA DAHL

DEPARTMENT OF INDUSTRIAL AND MATERIAL SCIENCE

CHALMERS UNIVERSITY OF TECHNOLOGY

Gothenburg, Sweden 2023

www.chalmers.se

MASTER'S THESIS 2023

Implementing ISO 26262-5

A guide to Functional Safety for Product Development at Hardware Level

SOFIA DAHL

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Industrial and Material Science

CHALMERS UNIVERISTY OF TECHNOLOGY

Gothenburg, Sweden 2023

Implementing ISO 26262-5
A guide to Functional Safety for Product Development at Hardware Level
SOFIA DAHL

Examiner: Dag Henrik Bergsjö, Industrial and material science
Supervisor: Stefan Pierrau, System Architecture at Scania

Master's Thesis 2023
Department of Industrial and Material Science
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Abstract

The increasing use of electrical and electronics in road vehicles increases the risk for failures caused by malfunctioning electronic systems. The demand for regulations to ensure functional safety is therefore a fact. The standard ISO 26262 is produced specifically for the automotive industry and presents procedures and requirements for manufacturers to follow. This report focuses on ISO 26262-5 which is product development on hardware level.

Before starting with the ISO 26262-5, the prerequisites need to be defined. The prerequisites are procedures as Hazard Analysis and Risk Assessment, Fault Tree Analysis and safety goal. The safety goals are assigned an ASIL-classification depending on the outcome in case of failure. The ASIL decides the requirements for each safety goal when implementing ISO 26262-5.

A method describing the procedures for implementing ISO 26262-5 is developed. The method guides the developer through the steps presented in ISO 26262-5 and provides the requirement to each procedure. For clarity, an example for following the method is provided to show the context within the procedures.

The example verified that a result can be reached by following the method. The reliability of the result could not be verified and needs to be compared to a result produced by another method. Depending on the outcome of the comparison, improvements may be necessary to ensure the reliability of the method. The main task for manufacturers or developers regarding the implementation of ISO 26262-5 in the development system is providing the necessary documentation to follow the method.

Table of Contents

1 Introduction

This chapter describes the background information of the project and the situation today. The scope of the project is presented together with the aim and the limitations.

1.1 Background

Over the last decades, the implementation and complexity of electrical and electronic systems in road vehicles has increased. Already in 2002, an estimation of 80% of innovations in road vehicles were related to electronics in road vehicles (Leen & Heffernan, 2002). Electrical and electronic systems include all system depending on electronics in the vehicle such as gearbox management systems, braking systems and the lights in the vehicle. The increasing use of electrical and electronic systems directly increases the risk of system failures. This is problematic since unfunctional systems can create uncontrollable situations. System failures in road vehicles can cause hazardous or even life-threatening situations for the driver or other road-users depending on where the failure appears. An example is if a failure appears in the cruise control system and the speed of the vehicle increases without the driver being able to control the speed. This could result in situation where human-life is at risk. Therefore, a standard which regulates the systems and devices used in vehicles is of importance.

Already in 1996, a standard called IEC 61580 was produced to control the development of electrical and electronic systems (International Eletrotechnical Commission, 1996). This standard described in general the requirements to increase the functional safety in all electronic systems. Since the development of electrical and electronic systems continued to increase, a derivative of IEC 61580 specifically for the automotive industry was produced (NI, 2023). The International Organization for Standardization(ISO) released ISO 26262 in 2011 to present the implementation of functional safety in road vehicles.

1.1.1 ISO 26262

ISO 26262 consists of 12 parts presenting the requirements to implement ISO 26262 in the development process (International Organization for Standardization, 2018). The 12 parts presents different areas where the standard needs to be considered to create an ISO 26262 harmonised system. The 12 parts of ISO 26262 are presented in the figure below:

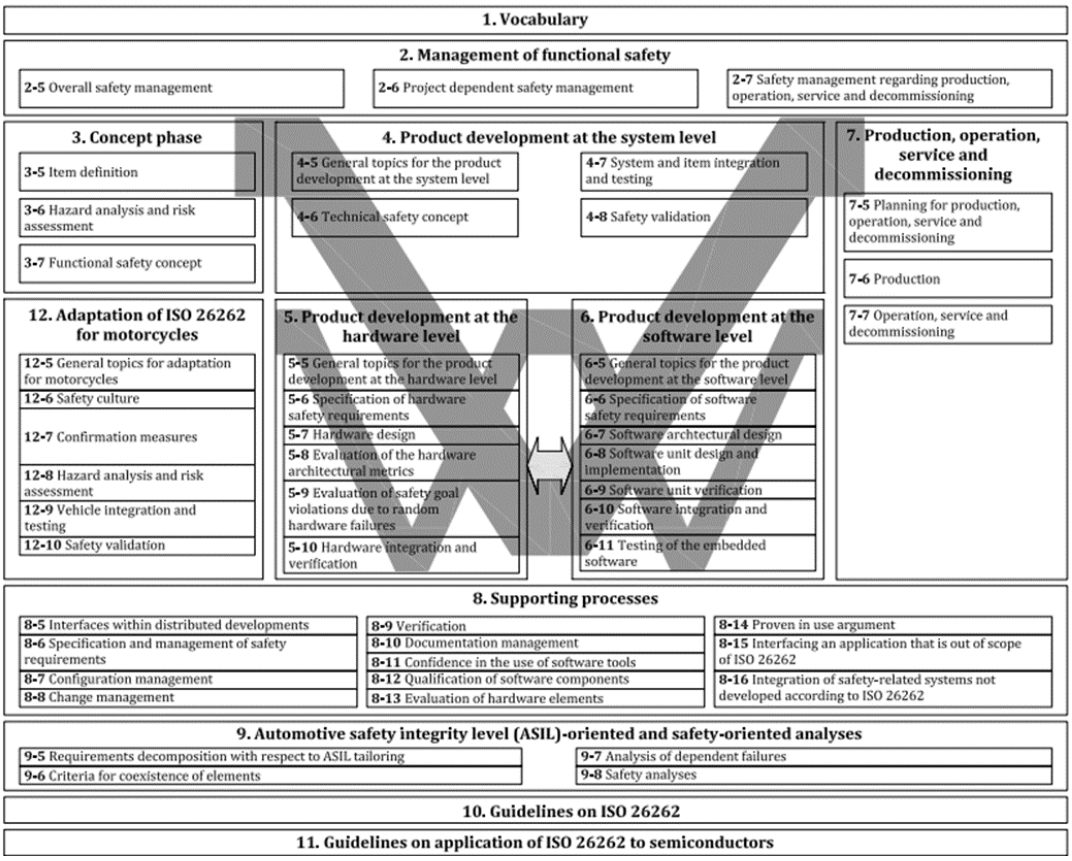

Figure 1. The full process of creating an ISO 26262 harmonised system (International Organization for Standardization, 2018).

The first part, ISO 26262-1 is the vocabulary which presents and describes the meaning of vocabularies specific for the standard. The reason for this is that manufacturers should understand the words when used in the standard and to create common words in the automotive field.

The second part, ISO 26262-2, describes the structure and management for developing procedures. According to the standard, a structural methodical manner increases the functional safety in the developing process. A functional safety manager needs to be designated to ensure that the functional safety procedures are followed. The safety manager is also responsible for documentation of the process to use when finished to argue for the functional safety in the system. The manufacturer needs to select an independent part to evaluate the documentation and decide the procedures achievement of ISO 26262.

ISO 26262 part 3 is the first part related to the vehicle and system development. Part 3 begins with describing the performance of defining the scope of the project which is called the item in the standard. After defining the item, part 3 continues with describing the importance and the performance of a Hazard Analysis and Risk Assessment(HARA). The HARA judge the outcome of a fault in the item. Depending on the outcome, safety goals which defines requirements to be achieved are created. A classification of the importance of functional safety in the safety goal is decided. The Automotive Safety Integration Level(ASIL) consists of 4 levels from ASIL A to ASIL D with ASIL D being the most severe. ASIL D could for example be used for a safety goal where a fault in the functional safety risks human-life and

ASIL A when a fault risks not turning on the lights. The safety goals and the ASIL-classifications are used in the upcoming parts of the standard.

Part 4 of ISO 26262 is about product development at system level. In this part, technical safety concepts and technical safety requirements are produced. Based on the technical safety requirements, safety mechanisms can be constructed to determine faults.

The requirements on system level can be implemented on hardware level or software level. ISO 26262-5 describes the product development at hardware level and ISO 26262-6 the software level. The two parts describes the requirements a product needs to achieve on hardware and software level to ensure functional safety required from the ASIL of the safety goal.

After the development of the hardware and software systems, the production of the system needs to be validated to ensure the functional safety. Part 7 of ISO 26262 describes the production, operation, service and decommissioning of the product. The standard requires the production to be planned an examined to detect defected parts. The parts need to be produced and installed correctly to avoid increasing the functional safety in the developed product. The production phase detects the need of a software update or further development of the hardware is needed.

ISO 26262 part 8 contains information about the supporting processes when developing according to ISO 26262. The part describes the procedure of verification, change in management and other questions which can arise during the process. Part 8 presents the correct methods to manage unexpected situations when developing an ISO 26262 harmonized product.

Part 9 of ISO 26262 describes the safety analysis of the project. Safety analysis performance is parallel to the developing procedure and continues throughout the project. The reason for the parallel performance is to increase the understanding of the functional safety faults and the causes of appearance.

The 10th part of ISO 26262 contains explanations for how to use the standard. Part 10 works as a guidebook for the developer of the implementations of the procedures presented in the other parts. This part gives an overview of the process to create an ISO 26262 harmonised system compared to the more specific areas described in the previous parts.

Part 11 describes the application of ISO 26262 in semiconductors since the device has different requirements compared to other systems. Part 12 of the standard includes the requirements specifically for motorcycles and differs from the development of other road vehicles.

ISO 26262 is believed to become a legal requirement within the next years by truck manufacturer. Even without being a legal requirement, manufacturers in the truck industry requests ISO 26262 harmonised systems from suppliers to ensure the functional safety in the product. The customers also understand the importance of having a reliable vehicle and therefore the manufacturers need to ensure the functional safety in the vehicle. If the costumers are not convinced that the product is functional safe, the risk of changing to another

manufacturer increases. The reason is risking expensive costs for the costumer in case of a fault appearing in the vehicle.

The process of implementing the standard in the development and products has already begun. Since the standard contains information of the whole procedure to create an ISO 26262 harmonised system, differences of how to interpret and implement the standard occurs. To perform a correct standardisation of products, truck manufacturer requests methods to implement the standard in the existing development methods and systems.

1.1.2 ISO 26262-5

One part in need of a clarification is ISO 26262-5 which describes the product development at hardware level (International Organization for Standardization, 2018). The hardware relevant for functional safety is the hardware related to the electrical and electronic systems. Part 5 describes the requirement for the hardware level and contains information about:

- General topics for the product development at the hardware level
- Specification of hardware safety requirements
- Hardware design
- Evaluation of the hardware architectural metrics
- Evaluation of safety goal violations due to random hardware failures
- Hardware integration and verification

Manufacturers request a method to follow as a guide to achieve the requirements on each step in ISO 26262-5. The method should guide the developer through the process of providing the documentation needed before beginning with ISO 26262-5. After that, the method should guide the developer through the procedures in ISO 26262-5 to be able to perform every step correctly. The method should be based on an existing gearbox management system and how the ISO 26262 can be implemented in the development procedure.

The gearbox management system, also called the transmission control unit, is found in the gearbox in vehicles and cooperates with the engine (MILTA Technology, 2021). The gearbox management system collects data from sensors controlling multiple areas and decides when to shift the gear up or down. Typical data useful for the gearbox management system is data from vehicle speed sensors, wheel speed sensors and traction control sensors. The gearbox management system analyses the data from the sensors at all time and decisions directly which gear should be used. The reason for selecting the gearbox management system as a reference system is because of complexity of the system. Since the system consists of multiple electronic systems, the project will include more requirements in ISO 26262 compared to a system consisting of one electronic system.

1.2 Objective

The aim of the project is to create a method on how to create an ISO26262 harmonised system. The method should be based on a gearbox management system. This is done by understanding and describing ISO26262-5, which is product development at the hardware level. The documentations and actions needed for the manufacturer to follow ISO 26262-5 will be presented in a detailed way to make it easy for a developer to follow. The aim is also to create an example which follows the method to decide the accuracy of the method and if the information in the method is enough to make a system ISO26262 harmonized.

1.3 Limitations

The project will not focus on calculating or estimating Failure-in-Time for each component. The data for failure rate will be assumed as existing from the supplier or the developer. The project will be based on the standard ISO26262 which is about functional safety in electric and electronic systems. The focus will be on ISO26262-5 which is Product development at hardware level and other parts of ISO26262 will only be considered if it affects or are related to ISO 26262-5. The developed method will be designed for the Gearbox Management System and may be applicable for other systems but that is not the purpose of the project.

2 Theory

This chapter explains the prerequisites needed to understand and perform the method presented later in the report.

2.1 Item Definition

The first step in the development process to create an ISO 26262 harmonized system is the item definition (International Organization for Standardization, 2018). This is made by defining which functions a driver requests on the vehicle, so called user functions. The user function can after that be transformed into a technical function which is what needs to happen in the vehicle to provide the function that the driver is asking for. This function is called a system item. Each items functionality, dependencies and interactions with driver or environment is defined.

2.2 Hazard Analysis and Risk Assessment

After the item definition, ISO26262-3 describes how a Hazard Analysis and Risk Assessment (HARA) is performed (International Organization for Standardization, 2018). The goal with the HARA is to answer the following questions (CCOHS, 2017):

1. What can happen and under what circumstances?
2. What are the possible consequences?
3. How likely are the possible consequences to occur?
4. Is the risk controlled effectively, or is further action required?

To respond the first question, hazardous events caused by malfunctioning behaviour of the defined items are identified. This will show connections between hazardous events and malfunctions in the system which is needed to understand the difference in importance to avoid some malfunctions more than other.

Question number 2, 3 and 4 can be translated to that the violation of each hazardous event can be validated in three ways: severity, exposure and controllability. The exposure is how likely the hazardous situation is to occur and can be rated from 0 to 4. The probability for each rate is shown in Table 1 below:

Table 1. Description of rating in exposure. (International Organization for Standardization, 2018)

Rate of exposure	Description
E0	Incredible
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

Severity is how severe the outcome is if the hazardous situation occurs and can be rated from 0 to 3 where 3 is the severest. Table 2 shows the description of the outcomes severity in case of the hazardous situation for each rated value:

Table 2. Description of rating in severity. (International Organization for Standardization, 2018)

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

The controllability is the level of difficulty for the driver to take control over an occurring hazardous situation and can be rated from 0 to 3 where 3 is the most difficult to control. The description of the rates is shown in Table 3 below:

Table 3. Description of rating in controllability. (International Organization for Standardization, 2018)

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

The rating in exposure, severity and controllability for the item combines to find a suitable ASIL-classification for each hazardous event.

Table 4. ASIL-classification depending on exposure, severity and controllability. (International Organization for Standardization, 2018)

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
	E2	QM	A	B
	E3	QM	B	C
	E4	QM	C	D

The combination of the rating for exposure, severity and controllability gives an ASIL-classification for the hazardous event which indicates the severity of the outcome for the hazardous event. If an event is assigned ASIL D, the event has been rated the highest in exposure(E4), severity(S3) and controllability(C3). This indicates that it is of highest importance to avoid the hazardous event to occur. An event could get rated QM which stands for Quality Management. This means that no ASIL-classification is needed since quality management is considered enough because the risk of the hazardous event to violate the safety goal is low.

2.3 Safety goal

When each hazardous event is dedicated an ASIL-classification, safety goals can be identified (International Organization for Standardization, 2018). The safety goals is based on which parts of the system in need of prevention from a failure to avoid the hazardous event to occur. The safety goal should specifically describe which situation in the system that needs to be prevented to avoid the hazardous event. Multiple hazardous events can occur from the same malfunctioning in the system and therefore, their safety goals can be combined to a common safety goal. The safety goal is assigned the same ASIL-classification as the relevant system with the highest ASIL-classification.

2.4 Technical Safety Concepts

After defining safety goals and assigned the ASIL-classification, technical safety concepts need to be created (International Organization for Standardization, 2018). The technical safety concepts are produced on system level and needs information about the relevant systems and components included. According to ISO 26262-4, the systems functionality, dependencies, constraints and properties should be included in the technical safety concept.

The implementation of safety mechanisms in the system also needs to be analysed in a technical safety concept. Safety mechanisms are used to detect faults or to avoid failures and needed if a fault has the possibility to violating a safety goal. The protection from violating a safety goal differs depending on the chosen safety mechanism. One type of safety mechanism could be detection when failure appears while another type could be an additional sensor. The additional sensor gives a stronger protection since the system continues to receive signals even if a failure appears in the original sensor.

2.5 Fault Tree Analysis

A Fault Tree Analysis(FTA) shows the system structure with a deductive approach (International Organization for Standardization, 2018) also called top down approach. The FTA is a graphical model of the system with all faults and events which could possibly occur in the system (NRC, 1981). The predefined undesired event, which is the violation of a safety goal, is in the top showing all the event and faults with possibility to affect it below. The FTA is in most cases carried out in 5 steps (Lundteigen & Rausand, 2014) presented below:

1. Definition of the problem, system and boundary conditions of the analysis
2. Construction of the Fault Tree Analysis
3. Identification of minimal cut sets
4. Qualitative analysis of the Fault Tree
5. Quantitative analysis of Fault Tree

The structure is shown in Figure 1 below with the safety goal in the top and every individual component in the bottom.

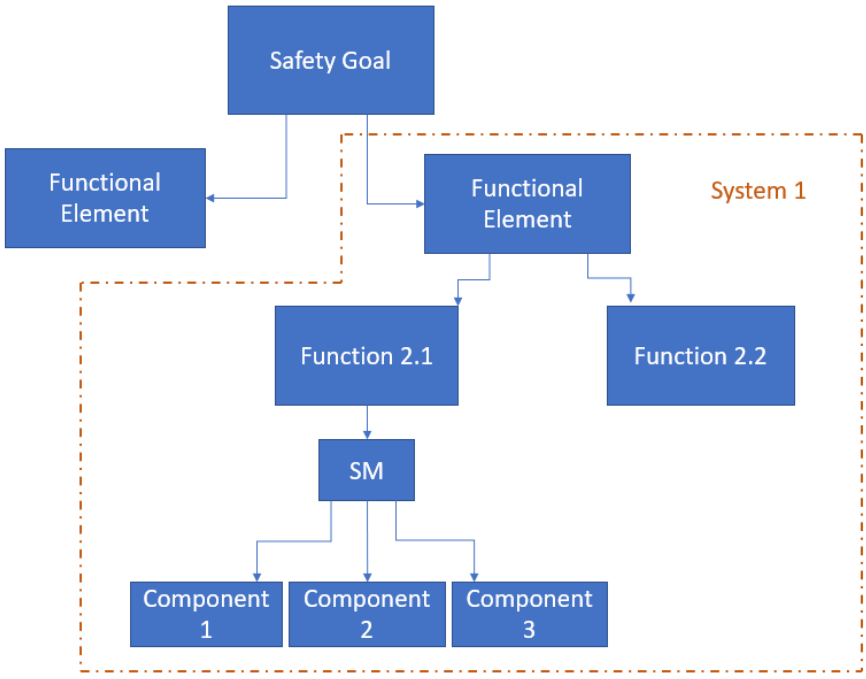

Figure 2.Fault Tree Analysis shows the structure of the functions in the system.

The FTA shows which functional elements that belongs to the safety goal and which functions that belongs to each functional element. The functions can be seen as systems. Each function consists of components which are also shown in the FTA and a safety mechanism if one is implemented.

2.6 Previous Studies

This chapter presents the findings of previous work in the area to increase the knowledge of the problem and the situation.

2.6.1 Texas instruments

Texas instruments' report "Understanding Functional Safety FIT Base Failure Rate Estimates per IEC 62380 and SN 29500" from 2020, instructs the companies developers how to adjust their development according to the functional safety standards produced by the International Electrotechnical Comission(EIC) and the International Organization for Standardization(ISO). Both IEC and ISO require semiconductor manufacturer to address systematic and random hardware failures in their products.

The term Base Rate Failure(BRF) is introduced as an important input to calculate random hardware metrics such as single-point fault metric and latent fault metric (Texas Instruments, 2020). The BRF is a value for reliability on the product working under normal conditions and environment. This value can thereafter be multiplied with factors such as temperature or voltage to make the estimation more realistic. The BRF can be estimated in multiple ways and this report presents the "IEC Technical report 62380" and "SN 29500" as two sources when finding the information to calculate the BRF.

The report continues by defining the difference between systematic faults and random faults. Systematic faults are made in the design, manufacturing or development process and are therefore easier to detect and mitigate before the product is finished. Systematic faults are often eliminated when evaluating the product and the manufacturing process. Random faults depend on the system and the components since all electronic system will fail eventually over time. These faults cannot be eliminated in the design, development or manufacturing process. Therefore, random hardware failure metrics are created to estimate the possibility of a random hardware failure to appear. A certain value are required of the metrics, according to the ISO 26262, to ensure that the functional safety of the system is preventing random hardware failures to occur.

The random hardware failures are connected to the lifetime of the system and components. The lifetime is divided into three periods: Early life failures, Normal life failures and Intrinsic wear-out. The graph below presents how the failure rate change depending on the lifetime.

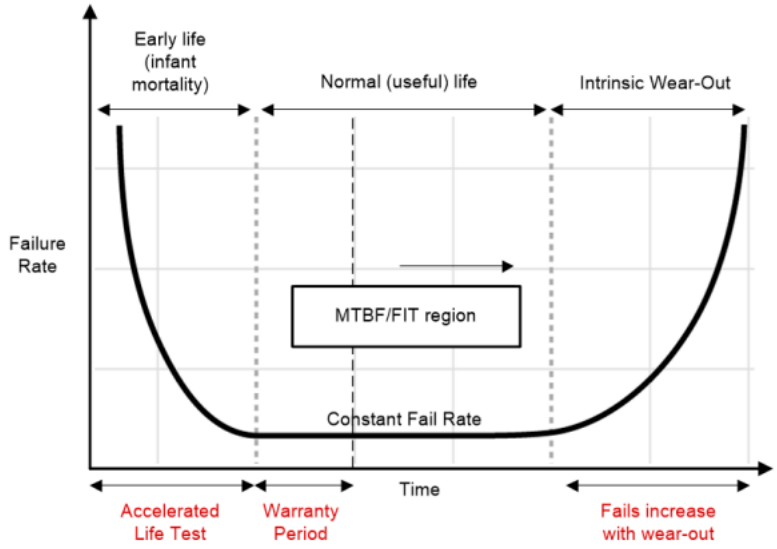

Figure 3. Picture from Texas Instruments report showing the failure rate depending on the lifetime (Texas Instruments, 2020).

The graph shows that a random fault is more likely to appear in the early life phase than in the normal life. By increasing lifetime tests in the manufacturing and development, the early life faults can be reduced since most early life faults would be detected and therefore mitigated. During the normal life phase, the risk of random hardware failures decreases until the intrinsic wear-out phase begins. The Intrinsic wear-out phase begins when the lifetime of systems and components is maximized, and faults begin to appear because of wear-out. The normal life phase for systems and components can be extended by implementing a safety mechanism to correct the fault. The lifetime of the system gives input to the calculation of BRF since the random hardware failures are more likely to appear in the end of the lifetime of the system.

2.6.2 KUGLER MAAG CIE

KUGLER MAAG CIE is a consulting company with expertise within automotive electronics(Källa)). Their consultants support automotive manufacturers in decision making and implementation of safety procedures. One of the experts within ISO 26262 presents the different parts of the standard in videos.

The video presenting the ISO 26262-5 begins with describing the hardware related to the standard. The hardware could be resistors, sensors and microcontrollers or other components related to the electrical and electronic systems. Hardware related to the standard can be programable components or non-programable components.

The product development on hardware level is a part of the functional safety for system development. A prerequisite for ISO 26262-5 is a technical safety concept produced on system level in ISO 26262-4. The technical safety concepts are used to develop hardware safety requirements. The hardware safety requirements needs to include:

- Safety mechanisms
- Detection, indication and control of internal faults
- Failures external to the hardware

- Tolerance times
- Target values for hardware metrics and failure rates

The hardware safety requirements need to be verified before continuing the procedure. Thereafter, possible faults need to be classified depending on the violation of the safety goal. The classifications are directly violating a safety goal, not violating a safety goal and only violating a safety goal together with another fault. Documentation also need to prove that occurring hardware faults are not violating the safety goal and if a fault violating the safety goal exists in the vehicle, evidence for detection needs to be provided.

2.6.3 Toward the application of ISO 26262 for real-life embedded mechatronic systems

The report presents the procedures of implementing ISO 26262 in embedded mechatronics system. The first step is the system definition where the components and systems in the system is defined (Astruc & Becker, 2010). In this phase, all components are included such as mechatronics, mechanical and hydraulic parts. The second step is to perform a HARA on vehicle level to identify possible hazardous events. The safety goal is defined and assigned an ASIL-classification. The HARA is not considering any technologies or components and is only based on hazardous events.

The report continues with describing the functional safety concepts. This is functional safety requirements derived from the safety goal and needs to be implemented on all components and systems related to the safety goal. The functional safety requirements should state the demand for reliability in functionality for the systems. Before going to the next step, the functional safety requirements need to be verified to fulfil the functional safety of the safety goal.

The next step is the technical safety concept which is limited to perform on the electrical and electronic parts of the system. The intention is to apply the functional safety requirements in the system design and verify the implementation is done correctly. The failure of a sensor in the system can cause a violation of the safety goal. Therefore, a decision of the protection against failure in the sensors needs to be made. Safety mechanisms can be applied with different protection depending on the need for each system. For one system, the application of an additional sensor is needed while for another system the detection of a failure in the system could be enough.

After safety mechanisms has been provided, the design of hardware and software is performed. The result of this, an analysis of failure modes in the product needs to be provided. A system designer verifies the analysis if proven that the possible failure modes are covered in the design of the systems. The system designer also verifies that the system design is not introducing new hazards regarding functional safety.

3 Methodology

This chapter explains the chosen methodology and the project following the methodology to reach the result.

3.1 Method Theory

The project follows a design research methodology described in the book DRM, a Design Research Methodology (Blessing & Chakrabarti, 2009). The purpose of the Design Research Methodology is to create a method which increase the chance of creating a successful product. The product is in this case the ISO 26262 harmonized system which needs a method to implement the standard correctly on an existing system.

The Design Research Methodology divides the project in 4 parts: Research clarification, Descriptive study I, Prescriptive study and Descriptive Study II. The process that follows the Design Research Methodology framework is shown in figure 4:

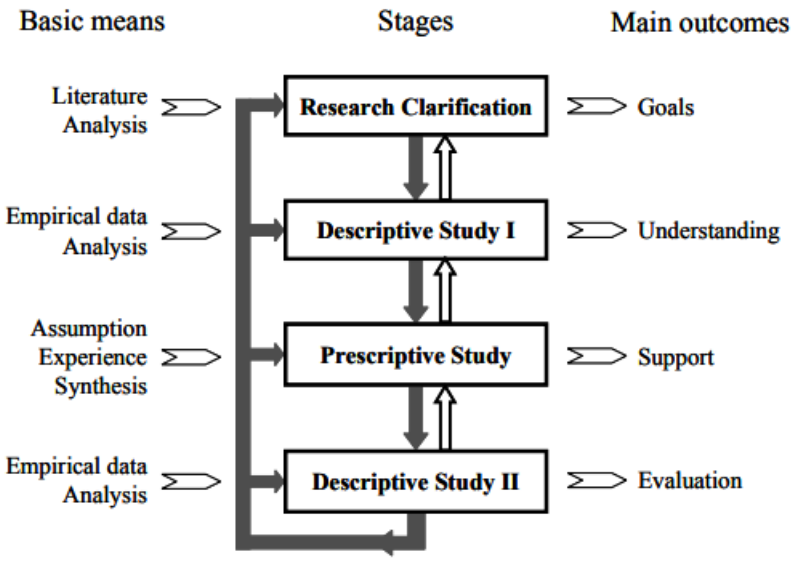

Figure 4. Figure showing the DRM framework. (Blessing & Chakrabarti, 2009)

3.1.1 Research Clarification

The initial step in the Design Research Methodology framework is the research classification which is literature analysis. This part is needed to understand the current situation and the reason for the project to be carried out. As shown in figure 2, the outcome of the literature studies should be the goals in the description of method. This should be measurable criteria which decides the successful product when created according to the method.

3.1.2 Descriptive Study I

When the goal of the project is decided, the next step is to do a descriptive study. With the goal in mind, literature analysis continues but this time the reason is to reach clarification in necessary actions to reach the goals decided in the research clarification. Interviews are held

with people with knowledge in the area to better understand the literature and the current situation. Data analysis is performed to create a connection between the existing data and how it can be implemented in the project.

3.1.3 Prescriptive Study

From the Descriptive Study I, the understanding about the project has increased and the initial description of the purpose of the project could need to be corrected or improved depending on the findings. It is of importance to change the description of the goals with the method and what needs to be implemented on the product for it to be successful to avoid complications later on in the project. After the clarification of the project description, the development of the method starts. A Design Research Methodology is selected to support the process of developing the method. Based on assumptions and knowledge from the literature review, the implementations needed to reach the goals of the project are described. An initial evaluation of the method is made by using existing data an evaluate the result.

3.1.4 Descriptive Study II

In the Descriptive Study II, the developed method is evaluated in two steps. The first step investigates how the method is reaching the goals defined in the Research Classification and in the Prescriptive Study. The purpose of this is to investigate if the implementation of the developed method is relevant for creating the successful product. The second step of the evaluation is to investigate the usefulness of the product with the implemented method. The evaluation shows if the implementation of the method is reaching the goals of the project or if modifications of the method are necessary for the project.

3.1.5 Types of research within the DRM framework

In the prescriptive study, a Design Research Methodology is selected for developing the method. The different types described in DRM: a Design Research Methodology are presented in figure 3 below:

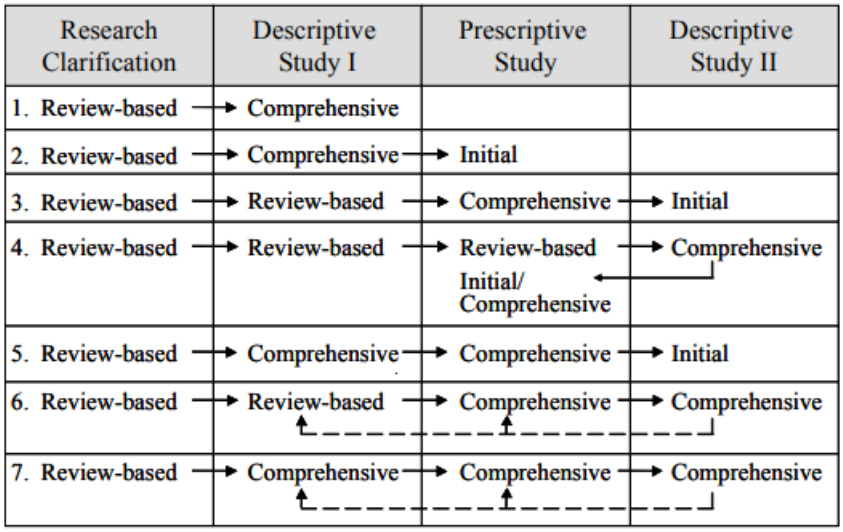

Figure 5. Figure showing the different types of methodology presented in DRM, a Design Research Methodology (Blessing & Chakrabarti, 2009).

Figure 5 shows that every project starts review-based which is the initial literature analysis made to understand the aim and the focus of the project. In this part, a project plan is created according to the available time. In the comprehensive study, the literature analysis continues at the same time as results are produced. The initial study is the final part of the project and is started when results are reached. This part evaluates the results based on the outcome.

3.2 Applied methodology

The following chapter describes the application of the selected methodology in the project.

3.2.1 Research Clarification

The project starts with the research classification which is Literature analysis as shown in figure 2. Literature analysis were started on ISO26262-5 and main information was collected in a document. To increase the knowledge about the ISO26262 and to understand the reason for implementation in truck manufacturing, videos about the functioning of the different parts of ISO 26262(KÜGLER-MAAG CIE by UL Solutions, 2020) were watched to reach an understanding and to get an overview of the standard. When the knowledge about the purpose of ISO26262 and the current situation had increased, Literature analysis continued on the relevant part of the standard which is ISO26262-5. From the literature analysis, goals for what the method should change for the product was defined and described. A background describing the purpose of the project was started to increase the understanding of the purpose of the project.

3.2.2 Descriptive Study I

Literature analysis were performed on the standard ISO26262-5 and ISO26262-3 to understand the structure of the system and the needed input data. A review of a previous made HARA and a FTA together with literature studies on ISO26262-3 was made to understand how safety goals are assigned the ASIL-classification. Thereafter, a meeting was held with a person working with applying the standard on a different system to understand how safety goals, user functions and item definitions are connected to each other.

The literature analysis continued on ISO26262-5 about different kinds of faults and hardware metrics. To gain a deeper understanding of hardware metrics, a meeting was held with a person experienced in performing hardware metrics. With knowledge from the meeting and from literature studies on the ISO26262-5, a review of a previously performed hardware metrics was made. This was made by calculating the hardware metrics from the provided data to understand how the data is used to achieve the correct answer. An example was reviewed of how to calculate hardware metrics which is provided in ISO26262-5.

When information about the project is gathered by literature studies, requirements of what the method should perform to meet the goals of the project was defined.

3.2.3 Prescriptive Study

In the prescriptive study, a clarification of the goals of the method was made since the knowledge of the area had increased during the Descriptive Study I. The development of a method which makes the product reach the goals are started. A Design Research Methodology is selected to support the process. Based on the requirements of the method, the necessary information was described in the results. The initial evaluation of the method was made by comparing the results to examples in ISO26262-5 and to previously performed hardware metrics.

3.2.4 Descriptive Study II

The evaluation of the method started with investigating if the implementation of the method makes the product reach the goals defined in the Research Classification. This was done by implementing an example of a system, based on the information provided in ISO 26262-5, into the method. The outcomes of the method could thereafter be analysed and compared to the requirements on the system requested from the standard in order to be ISO 26262 harmonized. The findings were described and analysed before the result was modified to improve the validity of the method.

4 Results

In this part of the report, the results of the project will be presented based on the methodology for the project.

4.1 Research Clarification

The literature analysis in in the Research Clarification resulted in that the methods purpose is to make an existing hardware system ISO 26262 harmonized. The analysis also resulted in description of the current situation described in chapter 1. The research for previous studies resulted in information regarding ISO 26262, as described in chapter 2.

4.2 Descriptive Study I

Before the result can be implemented on a system, an item definition, a HARA and a FTA needs to be performed according to the description of ISO26262-3 in chapter 2 of this report. The system needs to have defined safety goals assigned an ASIL-classification to be able to perform the steps presented in this chapter.

The actions required in the method to create an ISO26262 harmonized hardware system are:

• Describing prerequisites needed to use the method.
• Describing how existing data is used to make the system ISO 26262 harmonized.
• Presenting the requirements for the system and how to reach them.

4.3 Prescriptive study

This chapter presents the result from the prescriptive study of the methodology. The result presents the procedures and requirements in ISO 26262 for product development at hardware level. The method presented begins with the assumption of correctly performed and provided documentation of the prerequisites

4.3.1 Types of Faults

In this section, the different types of faults that can appear in a system is presented together with how a safety mechanism can affect the violation of a safety goal.

- **Safety Mechanism**
  A safety mechanism(SM) is a function which prevents the violation of a single-point fault (International Organization for Standardization, 2018). When applied, a single-point fault can become a multiple-point fault which decrease the risk for violation of a safety goal.

- **Single-Point Fault**
  Faults that directly violate a safety goal and there is no safety mechanism to avoid the failure. A single-point fault can lead to a hazardous situation depending on where the fault appears and which safety goal it is violating.

- **Residual Fault**
  A residual fault has a safety mechanism, but the fault can in some cases escape the safety mechanism. When escaping the safety mechanism, the residual fault is violating the safety goal with the same severity as a single-point fault. A value for failure mode coverage shows the percentage of the faults escaping the safety mechanism.

- **Multiple-Point Faults**
  A multiple-point fault is a fault which is not violating a safety goal by itself because there is one or several safety mechanisms. The multiple-point fault violates the safety goal when a fault appears in the original functionality and the safety mechanisms. In most cases, Multiple-Point Faults are Dual-Point faults which means that the function has one safety mechanism. This means that a Dual-Point fault can only violate the safety goal if two independent faults appear at the same time. There are three types of multiple-point faults:

  – **Latent Multiple-Point Faults**
  Faults which are prevented by one or several safety mechanisms but cannot be detected by the driver or the safety mechanism. The safety mechanism is constantly active and can therefore not detect the failure. This can appear in a situation where two sensor is measuring the same value to make sure the signal is correct. If a failure appears in one sensor, the other sensor will keep sending the correct signals until a failure appear in that sensor.

  – **Detected Multiple-Point Faults**
  Faults that are detected and directly gets corrected by the safety mechanism. The fault can therefore not violate the safety goal if there is no fault in the safety mechanism that corrects the fault.

  – **Perceived Multiple-Point Faults**
  Faults that has a safety mechanism and can only violate a safety goal with at least two independent faults appearing at the same time. The fault is not detected by the safety mechanism but is perceived by the driver who can correct the fault by activating a safety mechanism.

- **Safe Faults**
  A Safe Fault can appear without violating a safety goal and can therefore not put the vehicle in a hazardous situation. No safety mechanism is necessary for a safe fault. The faults violation of the safety goal is visualized in figure 4 below. The figure shows that the single-point faults and the residual faults directly violates the safety goal which is in the middle while the safe faults appear in the area without violation of the safety goal.

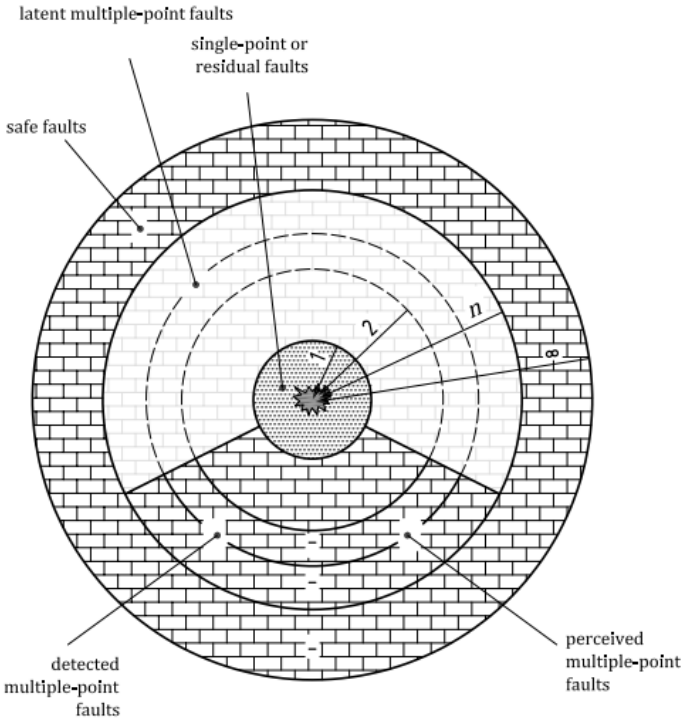

Figure 6. Figure from ISO 26262-5 (International Organization for Standardization, 2018) showing different faults violation of the safety goal.

4.3.2 Failure-In-Time

Failure-In-Time(FIT) is a unit to describe the frequency of a fault to appear in a system or in a component. 1 FIT means that a failure is likely to occur once in a billion hours. Every component in a system has their own FIT value and the total FIT value for the system is the sum of the FIT values for all components in the system. The FIT value for a system is needed for proving the system to fulfil the desired ASIL-classification.

4.3.3 Total FIT

the total FIT is the sum of the FIT for all components in a system. This gives the FIT value for the system which means how many times a failure is likely to appear in a system in a billion hours.

4.3.4 Total Safety Related FIT

The total safety related FIT for a system gathered from the sum of all components in a system except from the safe faults since they are not violating a safety goal or violating the function of the system. The safe faults are excluded from the analysis because of irrelevance to the functional safety of the vehicle for the specific safety goal.

4.4 Hardware Metrics

This chapter will present the different types of hardware metrics, their use and how to find them.

4.4.1 Failure mode

A fault in a component can appear in different ways which is called failure modes. To be able to calculate hardware metrics, these failure modes and their distribution needs to be identified. This is needed to understand FIT for the different kinds of fault that can appear in the component which is needed when calculating the hardware metrics. The total FIT for a component is the sum of the FIT for all different faults for a component.

4.4.2 Single-Point Fault Metric

After the performed HARA, each safety goal is assigned an ASIL-classification. The ASIL-classification of the system decides the requirements for functional safety that a system needs to reach to be able to be ISO26262 harmonized. One of these requirements is the Single-Point Fault Metric. The calculation of the Single-Point Fault Metric shows the coverage of safety mechanisms preventing Single-Point and Residual Faults to appear in a system.

The requirements for Single-Point Fault Metric for the system to be ISO26262 harmonized is:

- ASIL D: ≥ 99%
- ASIL C: ≥ 97%
- ASIL B: ≥ 90%

To be able to calculate the single-point fault metric, the sum of all the single-point faults needs to be found. This is done by calculating the possibility for single-point fault by multiplying the FIT for each component with the failure mode related to a single-point fault and finally multiplying with the distribution of faults which can escape the safety mechanism.

The SPFM for a system can be found by the equation:

$$SPFM = 1 - \frac{\sum \lambda_{SPF}}{TotalSRFIT}$$

where:
$\sum \lambda S\ P\ F$ =Sum of the FIT for single-point faults
TotalSRFIT = Total FIT of components related to violation of a safety goal in a system

If the SPFM is lower than the required value according to ISO26262, a safety mechanism needs to be inserted to decrease the risk of a single-point fault.

4.4.3 Latent-Fault Metric

The Latent-Fault Metric works in the same way as the Single-Point Fault Metric but for Latent Multiple-Point Faults instead of Single-Point and Residual Faults. The Latent-Fault Metric shows the coverage of avoiding Latent Faults in the system when the Single-Point Faults are not considered.

Depending on the ASIL-classification for a safety goal, the requirement on the Latent-Fault Metric is:

- ASIL D: ≥ 90%
- ASIL C: ≥ 80%
- ASIL B: ≥ 60%

The Latent-Fault Metric can be estimated with equation:

$$LFM = 1 - \frac{\sum \lambda_{MPFlatent}}{TotalSRFIT - \sum \lambda_{SPF}}$$

where:

$\sum \lambda_{MPFlatent}$ = Sum of latent multiple-point faults in a system
TotalSRFIT = Total FIT of components related violation of a safety goal in a system
$\sum \lambda_{SPF}$ = Sum of FIT for single-point faults

4.4.4 Probabilistic Metric for Hardware Failure

The Probabilistic Metric for Hardware Failure(PMHF) is a metric for calculating the probability of a safety goal to be violated by a random hardware failure. ISO26262-5 gives requirements on the probability value in a system depending on the safety goals ASIL-classification. The PMHF is found by using the equation:

$$PMHF_{est} = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPFdet} \times \lambda_{MPFlatent} \times T_{lifetime}$$

Where:

λ_{SPF} =FIT for Single-Point Fault
λ_{RF} =FIT for Residual Fault
λ_{MPFdet} =FIT for Detected Multiple-Point Fault
$\lambda_{MPFlatent}$ =FIT for Latent Multiple-Point Fault
$T_{lifetime}$ =The percentage of the total hours in operation out of 1 000 000 000 hours

The calculated PMHF is an estimation of the probability for violation of a safety goal by a random hardware failure and for the system to be ISO26262 harmonized, the $PMHF_{est}$ needs to fulfil the requirement for the safety goal's defined ASIL-classification which is:

ASIL D	Requiring	$< 1\times10^{-8}$/hour	10 FIT
ASIL C	Requiring	$< 1\times10^{-7}$/hour	100 FIT
ASIL B	Recommending	$< 1\times10^{-7}$/hour	100 FIT

4.4.5 Probabilistic Metric for Hardware Failure for item consisting of multiple systems

As described in chapter 4.2, each item is assigned a safety goal and, if possible, multiple items can be assigned the same safety goal. The safety goal gets assigned the same ASIL-classification as the item with the highest ASIL-classification. The items connected to the safety goal are assigned a PMHF budget decided on the ASIL of the safety goal. The budget is divided between the functional elements and the systems within the functional elements. The sum of the functional elements PMHF needs to be lower than the PMHF requirement for the safety goal.

Figure 7 below shows a safety goal with ASIL D. This gives that the total PMHF for the functional elements is allowed to be 10 FIT. Functional element 1 has PMHF 4 FIT. Functional element 2 includes two functions, one with PMHF 2 FIT and one with PMHF 4 FIT. The total PMHF for functional element 2 is 6 FIT. The sum of PMHF for functional element 1 and 2 is 10 FIT which is the requirement for ASIL D.

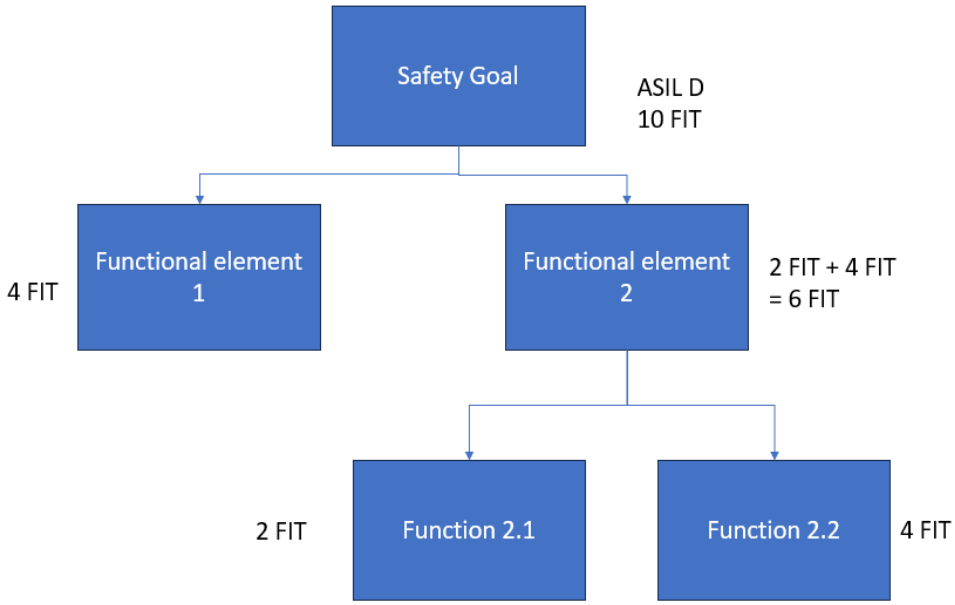

Figure 7. FTA showing the combined PMHF FIT for safety goal depending on multiple functional elements.

4.4.6 Diagnostic Coverage

Diagnostic coverage is a value for the percentage of the detection and mitigation of a faults for a hardware component or element in a system. Each components diagnostic coverage shall not be lower than 90% according to ISO26262-5(chapter 9.4.1.3) which means that more than 90% of the faults needs to be detected and mitigated by a safety mechanism. If the percentage for a component or element is lower than 90%, a motivation for why the lower diagnostic coverage is acceptable needs to be made.

4.5 Descriptive Study II

Based on the information in ISO 26262-5, an example of a system was provided. From the prerequisites described in the theory chapter, a safety goal was provided. The safety goal is ”Avoid unintended drive off” and is dedicated ASIL C. The safety goal can be violated by multiple functional elements and one of them is “Avoid unintended clutch engagement”. The system function to the functional element is “Gearbox must be in neutral” which means that the system needs to be able to identify a request of standstill, put the gearbox into a neutral position and signalize correctly when the request is performed. The structure of the Safety Goal, functional element and the system function is shown in the FTA in figure 5 below:

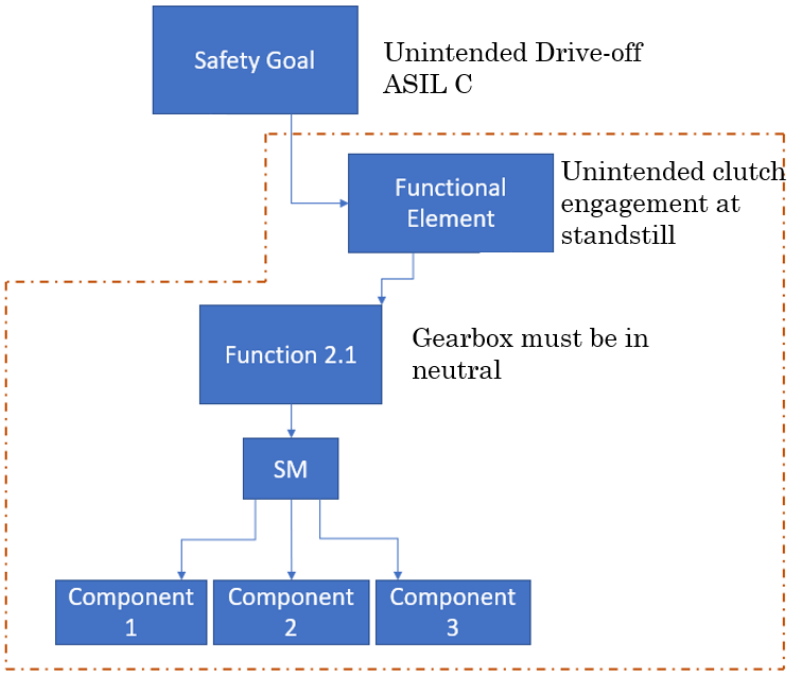

Figure 8. FTA showing the structure of the safety goal used in the example.

The components used in the system function “Gearbox must be in neutral” is shown in Figure 6 together with the information needed according to ISO 26262-5. The system consists of 1 ECU, 5 Resistors, 2 Inductors and 3 Capacitors. The second column shows each components FIT which is the number of times in a billion hours a fault is likely to appear in the component. In the third column, it is shown if the component is safety related which means if a fault in the component can violate the safety goal. If the component is dedicated a “YES” in this column, a failure in the component can violate safety goal. If it instead is dedicated a “NO”, the fault is a safe fault and cannot violate the safety goal. The 4th and the 5th column show the components different failure modes and failure mode distribution which means in which way a failure can appear in the component and how likely each failure mode is to appear.

Column 6 to Column 9 is related to residual faults and single-point faults. In column 6, the failure modes with potential for a Residual fault or a single-point fault is shown with an “X”. The next column shows if a safety mechanism is implemented to avoid violation of the safety goal. The failure mode coverage shows the percentages of faults avoided by the safety mechanism. The FIT for residual faults or single-point faults which did not have a safety mechanism or escaped the safety mechanism is shown in column 9.

The four following columns are connected to multiple-point faults in the same way as the residual faults and the single-point faults. The first column shows in which failure mode there is a probability for a multiple-point fault to appear. The safety mechanism shows if there is a safety mechanism and which one in that case. The failure mode coverage with respect to latent failures shows the percentage of latent faults avoided by the safety mechanism. The latent multiple-point fault FIT is how many times in 1 billion hours a latent fault is likely to appear and escape the safety mechanism and therefore create a latent multiple-point fault in the component.

The last column is the detected multiple-point faults which is a result of the FIT for the component, the failure mode and the residual faults or single-point faults. The value in this column describes how many faults that could be detected and avoided before the safety goal was violated.

A list of the components and their properties are shown in Table 5 below:

Table 5. List over components with properties used in the example.

Component name	FIT	Safety related component	Failure mode	Failure mode distribution	Failure mode with potential to violate the safety goal in abscence of safety mechanism	Safety Mechanism	Failure mode coverage	Residual or Single-Point Fault FIT	Failure mode that may lead to Multiple-Point Fault	Safety Mechanism	Failure mode coverage with respect to latent failures	Latent Multiple-Point Fault FIT	Detected Multiple-Point Faults
ECU	100	YES	Open	30%	X	SM1	95%	1,5	X	SM1	100%	0	28,5
			Closed	35%									0
			Drift 0.5	30%	X		90%	3	X		100%	0	27
			Drift 0.2	5%					X		0%	5	0
R1	3	YES	Open	80%	X	SM2	99%	0,024	X	SM2	100%	0	2,376
			Closed	20%	X		99%	0,006	X		100%	0	0,594
R2	2	YES	Open	90%	X	none	0%	1,8				0	0
			Closed	10%	X		0%	0,2				0	0
R3	3	YES	Open	50%	X	SM2	90%	0,15	X	SM2	100%	0	1,35
			Closed	50%									0
R4	2	NO	Open	90%									0
			Closed	10%									0
R5	2	Yes	Open	90%					X	none	0%	1,8	0
			Closed	10%					X		0%	0,2	0
I1	5	YES	Open	70%	X	SM3	99%	0,035	X	SM3	100%	0	3,465
			Closed	20%	X		99%	0,01	X		100%	0	0,99
			Drift 0.5	5%	X		99%	0,0025	X		100%	0	2,475
			Drift 0.2	5%									0
I2	4	YES	Open	50%	X	SM3	99%	0,02	X	SM3	100%	0	1,98
			Closed	30%	X		99%	0,012	X		100%	0	1,188
			Drift 0.5	15%	X		99%	0,006	X		100%	0	0,594
			Drift 0.2	5%									0
C1	2	YES	Open	20%	X	SM2	95%	0,02	X	SM2	100%	0	0,38
			Closed	80%	X		95%	0,08	X		100%	0	1,52
C2	2	YES	Open	20%					X	none	0	0,4	0
			Closed	80%									
C3	4	YES	Open	70%	X	SM2	99%	0,028	X	SM2	100%	0	2,772
			Closed	30%	X		99%	0,012	X		100%	0	1,188
							Σ	6,9055			Σ	7,4	76,372

The following results could be summarized from Table 5:

1.	Total FIT	129
2.	Total non-safety related FIT	2
3.	Total safety related FIT	127
4.	ΣSPF and ΣRF FIT	6.9055
5.	ΣMPF_lat FIT	7.4
6.	ΣMPF_det FIT	76.372

The total safety related FIT, ΣSPF and ΣMPF_lat inserts in the equations presented for calculating Single-Point Fault metric and Latent Fault Metric. The Single-Point Fault Metric and the Latent Fault Metric for the system are presented below:

Single-Point Fault Metric	$1 - \frac{6.9055}{127} = 0.94562598 \approx 94.56\%$
Latent Fault Metric	$1 - \frac{7.4}{127-6.9055} = 0.93838186 \approx 93.84\%$

The ΣMPF_{lat}, ΣSPF and ΣMPF_{det} inserts in the equation presented for calculating the PMHF. The operational lifetime was assumed to be 100 000 hours. The calculated Probabilistic Metric for Hardware Failure for the system is presented below:

Probabilistic Metric for Hardware Failure	$6.9055+7.4\times76.372\times\frac{100\,000}{10^9} = 6.9620$ FIT

Since the safety goal is assigned ASIL C, the requirement for PMHF is < 100 FIT. The PMHF was calculated to 6.9620 and fulfils the requirements. The latent fault metric for the example is 93.84% which meets the requirement on latent fault metric for ASIL C which is >80%. The Single-Point Fault Metric for the example is 94.56% which is below the requirement on > 97%.

5 Analysis

In this chapter, the results presented in previous chapter is discussed. Before the result can be implemented on a system, the procedure described in chapter 2 needs to be followed. This is needed for understanding the systems relevant for each safety goals since that determines which failures it is of importance to avoid.

5.1 Research Clarification

failures it is of importance to avoid. The literature studies resulted in deeper knowledge about ISO 26262 and the importance of implementation in development processes. The information found on ISO 26262-5 was general descriptions of the requirements for product development at hardware level. A concrete method guiding the developer in each procedure of the implementation of ISO 26262-5 was not found. This confirms the need for a method to be developed for guidance through the standard.

5.2 Descriptive Study I

The descriptive study I resulted in 3 requirements on the method. The first one is describing the prerequisites needed to use the method which means presenting the actions required to start following the method. This includes documentation of HARA, FTA and safety goals.

The second requirement is to describe the data needed for following the method. This could be information of system design and information of the components used in the systems. Before following the method, the data needed for the method should be provided to ease the procedure. The method should also guide the developer which data is used in every step.

The last requirement is describing the procedures stated in ISO 26262-5. The procedures should be presented in a detailed way and should be simple for a developer to follow step-by-step. The requirement from ISO 26262 on each procedure should be clearly presented so the developer can compare the result to the requirement after the procedure.

5.3 Prescriptive study

This chapter presents the findings about the procedure to implement ISO 26262-5 in systems.

5.3.1 Types of Faults

The first part of the result describes what types of faults that can appear in a component or in a system. The faults affect the components in different ways and not all faults are necessary to avoid to have a fully functioning vehicle. It is of importance for the truck manufacturer to identify which type of faults and where the fault is in need to be avoided to decrease the possibility of the fault to violate the safety goal. The faults and components that are relevant for the system depends on the safety goal which is based on the HARA.

5.3.2 Hardware Metrics

The hardware metrics consist of 3 requirements which a system needs to fulfil to be ISO 26262 harmonized. That is the single-point fault metric, the latent fault metric and the probabilistic metric for hardware failure.

The calculated single-point fault metric shows the percentage of single-point faults or residual faults that are avoided in the system. This means that for ASIL D which has the requirement <99% for the single-point fault metric, a maximum of 1% of the faults appearing in the system is allowed to be a single-point fault or a residual fault. If the system is not fulfilling the requirement, safety mechanisms can be added to the components to decrease the risk of the fault to appear or creating a multiple-point fault which make the fault less likely to violate the safety goal. The other option for increasing the single-point fault metric is to evaluate the components which contributes to the single-point fault metric and compare them to similar components on the market. A replacement of one or several components can be considered if there are components which contributes less to the single-point fault metric compared to the components used in the analysis.

The latent point metric gives the requirement for the percentage of faults needed to be protected from latent faults when single-point faults are not considered. For ASIL D, which has the requirement < 90%, only 10% of the faults beside the single-point faults are allowed to be latent faults. The reason for the lower requirement for the latent fault metric compared to the single-point fault metric depends on the risk of violation of the safety goal. To reach the requirement for the latent point metric, the manufacturer can implement a safety mechanism with higher coverage for latent faults. Another option is to implement a detection system which change the latent fault to a perceived multiple-point fault or a detected multiple-point fault.

A single-point fault or a residual fault violates the safety goal directly while the latent fault needs at least two faults to violate it. The reason for the existence of the latent fault metric and not the other multiple-point faults, the detected multiple-point faults and the perceived multiple-point faults, depends on the information to the user when one fault appear. When a perceived or detected multiple-point fault appear, the user or manufacturer are noticed in time to correct the fault before the violation of the safety goal. A latent fault appears without notification to the user or the manufacturer which means that the fault will not get corrected immediately when the fault appears. This increases the chance of another fault appearing while one fault already exists which creates a multiple-point fault leading to violation of the safety goal.

5.4 Descriptive Study II

The descriptive study II is the part of the project where the provided method evaluates in order of finding out the validity of the method. Before the implementing of the method, the prerequisites described in Chapter 2 needed to be performed. Since this project is about creating a method to implement when developing gearbox management systems, a safety goal related to this system was chosen.

To be able to follow the method described in the result, a list of components for every system needs to be provided. Since this part of the project is about evaluating the methodology and no existing list of components for this system was provided, the components provided in Table 5 are not the actual components needed for the system function and is only used as an example. The components and their properties are based on an example provided in ISO 26262-5.

By following the method, the Single-Point Fault Metric, Latent Fault Metric and the Probabilistic Metric for Hardware Failure was calculated. The ASIL-classification on the safety goal was ASIL C which means that the requirements on the system in order to be ISO 26262 harmonized is:

Single-Point Fault Metric	≥ 97%
Latent Fault Metric	≥ 80%
Probabilistic Metric for Hardware Failure	100 FIT

The result of the example showed:

Single-Point Fault Metric	94.56 %
Latent Fault Metric	93.84 %
Probabilistic Metric for Hardware Failures	6.9620 FIT

This indicates that the system fulfils the ASIL C requirements for the Latent Fault Metric and for the Probabilistic Metric for Hardware Failure but not on the Single-Point Fault Metric. This means that the system is not safe enough to be ISO 26262 harmonized and a safety mechanism needs to be implemented. To be able to do this, the component in the component list which contributes most to violation of the safety goal with a single-point fault or a residual fault needs to be identified. In the example, the ECU is the component contributing the most to the single-point fault. The ECU violates the safety goal with single-point or residual fault in two failure modes and the existing safety mechanism protects the safety goal from 90% of the single-point faults in one failure mode and 95% of the single-point faults for the other failure mode. To make the system ISO 26262 harmonized, a new safety mechanism which would increase the coverage for avoiding single-point faults to 99% for both failure modes could be implemented. This implementation would decrease the FIT for single-point faults to 0.3 for each failure mode since more of the single-point faults becomes multiple point faults instead because of the safety mechanism.

The Latent Fault Metric and the Probabilistic Metric for Hardware Metrics both fulfils the ASIL C requirements for the system to be ISO 26262 harmonized if there is no more functional elements or system functions related to the safety goal. If there are more than one functional element or system function, the Latent Fault Metric will still fulfil the requirements for ASIL C while the Probabilistic Metric for Hardware Failure becomes dependent on the other functional systems Probability Metric for Hardware failure. The reason for this is that the requirements for Single-Point Fault Metric, Latent Fault Metric and the Probability Metric for Hardware Failure is set on the safety goal. The Single-Point Fault Metric and the Latent Fault Metric are in percentage and therefore they will not change if the metrics for the other system functions fulfil the requirement for ASIL C.

The requirement for Probabilistic Metric for Hardware Failure is a value and the sum of all system functions cannot exceed the requirement in order to have an ISO 26262 harmonized system. Therefore, an FTA needs to be created showing all functional elements and system functions relevant to the safety goal. A list of components needs to be provided for each system function in the FTA and the system function’s Probability Metric for Hardware Failure needs to be found. The sum of all these Probability Metric for Hardware Failure cannot exceed the requirement based on the ASIL-classification. Figure 9 below shows an example

of what the FTA for the systems functions can look like together with an assumption of their Probabilistic Metric for Hardware Failure.

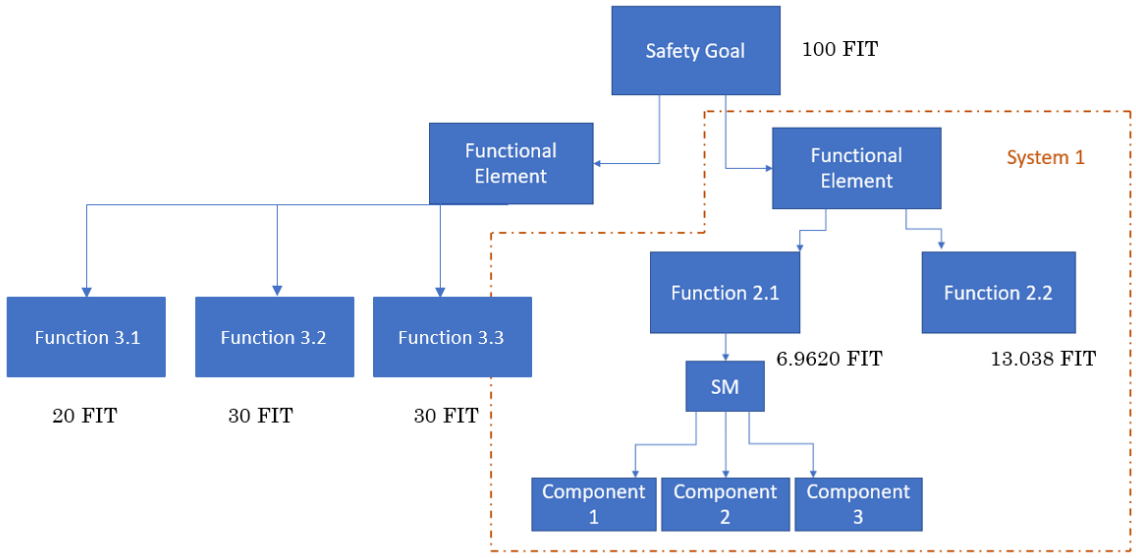

Figure 9.FTA showing the PMHF for a safety goal with multiple functional elements.

Figure 9 shows an example of a safety goal consisting of multiple functional elements. The safety goal is classified ASIL C which gives a PMHF budget of 100 FIT. The sum of PMHF FIT for the functional elements should not exceed 100 FIT. In this example, the sum of PMHF for the left functional element is 20+30+30=80 FIT. The PMHF FIT for the right functional element is 6.9620+13.038=20. The total PMHF FIT for the safety goal is 80+20=100 FIT. This is the maximum PMHF FIT allowed for the system which gives that the example fulfils the requirement.

6 Discussion

The standard ISO 26262 was produced to increase the functional safety for electrical and electronic system for the automotive industry. This puts a pressure on the automotive manufacturer to implement the standard in their development of electrical and electronic systems and devices. The standard is complicated to understand, and manufacturer requests a simplified guideline with steps to follow for creating ISO 26262 harmonised systems.

The previous studies research resulted in findings of ISO 26262 and especially ISO 26262-5. The studies described the content of ISO 26262-5 and the requirements to achieve. For manufacturers, there is information in previous studies about the requirements when implementing ISO 26262 but a method or guide to follow every step in ISO 26262-5 could not be found. This is the reason for developing a correct method to follow.

6.1 The Developed Method

This report presents a method for how to implement ISO 26262-5 in manufacturers development of electrical and electronic systems. The report first presents the prerequisites which is the input to follow the method. The first step is the item definition where the user functions of the vehicle is defined. After that, the process of creating a HARA based on the item definition is explained together with the production of safety goals and their ASIL-classification. The process continues with describing the designing of an FTA based on the safety goal and the relevant system. These steps are common in the development of systems and some manufacturers may already have the prerequisites for the system to follow the method presented in this report. For other manufacturers without the prerequisites for the system, this report explains the processes to design the needed input to proceed to the method for creating an ISO 26262 harmonized system.

The method is a simplified version of the standard ISO 26262-5 which the developer or manufacturer can follow step by step to increase the functional safety in systems. The method describes the classification of different fault with risk to appear in the system in a simplified way to increase the possibility of correct fault classification. The method continues with describing the process of creating hardware metrics based on the fault classifications. The inputs and the calculations for the hardware metrics are described with examples which makes it easy to follow the calculating process. The requirements from the ISO 26262 on the hardware metrics are presented for a clear and simple respond to if the system reach the goal for each metric.

For clarity, an example is provided in the report to show the different processes in the report. The intention of this is to present exactly how to perform the steps and how the steps correlate to each other. The example also works as an evaluation since it shows that the method is possible to follow. On the other hand, the evaluation is not enough to confirm a reliable result. The result from the method needs to be compared with the result from another method to see if the same result is given. More examples can also be an alternative to find out if the method gives a similar result or if the result is unlikely to be correct. This way would only show major

faults in the method while the comparison with a result from another method can show both major and minor faults in the method.

The example showed a likely result which means no modifications to the method was needed after the initial evaluation. The PMHF for items consisting of multiple system was not evaluated in the example. This can affect the result for safety goals which consist of multiple systems and are therefore in the need of being evaluated.

The complicated part about implementing ISO 26262 in existing development is not to follow the method described in this report, it is to provide all information to use as input to the method. The challenge for manufacturers is to create a HARA, safety goal and FTA on all their systems and user functions. Manufacturers also needs to gather all components to every system together with the components FIT and failure mode. This can seem time consuming to provide for a simple method as described in this report, but it is what the ISO 26262 requires. The standard is produced to increase the functional safety in electrical and electronic systems and requires manufacturer to know which components they use in their products. Especially when it comes to components which could create a hazardous event in case of failure. This standard ensures that the manufacturers take responsibility for the components they use in their product even if the component was developed at a supplier.

6.2 Impacts of the Method

The standard gives the manufacturers an opportunity to understand the systems and where an upgrade could be needed. The component lists discover the probability of failure in each component which can facilitate the decision of replacing components with a high failure rate. This can increase the time to failure of the whole product which benefits the manufacturer and the brand.

An aspect of increasing the functional safety in road vehicles is to reduce the risk of causing hazardous situations for the driver and other road users. In a worst-case scenario, a hazardous situation could threaten human life. Therefore, the standard is produced to minimize the risk of hazardous situations. The mandatory HARA gives the developers information about the events of importance to avoid. The ASIL-classifications on the following safety goals indicates in which systems manufacturers need to invest time and highly reliable but more expensive components. If there was no economic aspect for manufacturers, all safety goals could be assigned ASIL D for maximum functional safety. Since manufacturers usually have economical aspects, the standard presents for the manufacturer which systems in need of expensive components.

Another aspect to consider is the environmental aspect. When analyses of functional safety are produced, the information of components and systems lifetime will be discovered. This will increase the knowledge of when a component or system needs to be replaced to avoid faults to appear. Even if the faults appearing are not random hardware faults but systematic failures since they appear because in the end of the lifetime, there is still a relevance for functional safety. A system or component malfunctioning can cause harm to other systems.

That can result in a major replacement instead of replacing the malfunctioning system or component. A major replacement requires more components which are made from different resources and needs to be produced. Therefore, a replacement before failure could have a less impact on the environment.

6.3 Methodology Discussion

The Design research methodology used was relevant to the project. The initial literature review to understand the problem and the current situation was time consuming but necessary for being able to start the project. Before the research for ISO 26262 could start, information about functional safety and electrical or electronic systems needed to be gathered to understand the existing process. Since the ISO 26262 is an unknown area, developers interpret the standard in different ways. This made the planned interviews confusing because of conflicting information gained in the interviews. The decision to focus more on the information in the actual standard was made to create a method based on the requirements in ISO 26262. A method influenced by developers would be easier to implement in the existing development because of the knowledge about the processes and the system. The risk with basing the method on developers is that information from the standard can be interpreted in a suitable way for the already existing process. A method which guides the developer directly to an ISO 26262 harmonized system may be time consuming but assures reaching the requirements from the standard.

The evaluation of method was made with an example showing the different actions required to reach an ISO 26262 harmonised system. The example shows that it is possible to follow the method and reach a result in the specific case used in the example. The problem is the uncertainty if the results is correct since there is nothing to compare the result to. For further evaluation, the method needs to be used on ISO 26262 harmonised systems to compare the method presented in this report to other methods. This would increase the credibility of the method if shown that the same result can be reached with this method as with a more complicated method. The evaluation could also be made on multiple systems with different components and designs. This would give a deeper understanding of coverage of the methodology so modifications to the method can be made.

One different approach to this project would be to begin with an example from the beginning. The starting point could be a user function which is decided in the item definition. Following the ISO standard, the next step could be researched, and after that proceed to the HARA. The HARA could be produced based on the user function and safety goals with ASIL-classification would be the outcome. The example continues through the FTA until the ISO 26262 is complete. This approach would increase the understanding and knowledge of each step in the process since each step needs to be solved before moving on to the next step. The risk of missing parts of process decreases because after each step, the next step needs to be found without knowing the end goal. The problem with this approach is the absence of an overview of the problem. This could lead to focusing on the wrong areas. For example, performing a HARA is time consuming and probably not needed since it is common process and may already exist for the system. The time consumption to perform the HARA is unnecessary to solve the overall problem. The uncertainty of where to focus without the overall picture makes this approach not likely to use as a methodology.

6.4 Future Work

As described in previous chapter, an evaluation of the method is needed to verify the reliability of the method. The evaluation would discover eventual faults in the method or an incomplete method missing important procedures. The findings could after that be implemented in the method to increase the reliability and simplify the procedures for the developer.

After finishing the method for implementing ISO 26262-5, there are other parts of the standard in need of a guide. Part 6 with information about product development at software level and part 7 containing information about production, operation, service and decommissioning, could need clarifications in a similar way as ISO 26262-5. To develop and manufacture ISO 26262 harmonised products, the whole standard needs to be followed in the process. This means that different developers may be involved in different parts while developing the product. Therefore, a guide for how to follow the standard when changing developer could be in need for the company. This would increase the knowledge of how to continue the developing of the product.

The innovations and use of electrical and electronic systems in road vehicles will continue to increase and consequently, the need of functional safety will increase. This will request manufacturers to implement ISO 26262 as a natural part of the development process to avoid mistakes in the required documentation. Since the procedure is time consuming, avoiding mistakes is of importance to make it as efficient as possible.

Creating a time efficient method for implementing the ISO 26262 will probably be requested by manufacturers. The problematic procedures presented in this report was to understand which components a system consisted of. This is an area with opportunity to become more efficient. All components in a system should be compiled into document together with the FIT value. Manufacturers also need to ensure that suppliers have tested the components and given the components a FIT. The procedure of assigning FIT needs to be improved since most FIT values today are decided from comparisons to similar components. This is not a valid method because the component used in the comparison was probably assigned the FIT in the same way. Testing of the components needs to be implemented in the development of components before a component can be assigned a reliable FIT.

When the procedures for implementing ISO 26262 are completed, the manufacturer also needs to evaluate the methodology of the development. This is done to understand if all the procedures are correctly followed in the process, if something is missing in the documentation and how to improve the process until the next development project.

7 Conclusion

The increasing request for functional safety in electrical and electronic systems, forces the implementation of ISO 26262 in development prosses. Since ISO 26262 fully covers the development process, the explanations for the performance of each procedure are complicated. ISO 26262-5 describes the implementation of ISO 26262 in the development process at hardware level. Truck manufacturers requests a guide for this part of the standard to ensure a correctly performed implementation of ISO 26262 on hardware level.

This report presents a method to use as guidance while implementing ISO 26262 on hardware level. The method presents the procedures of reaching the documentation of the correctly performed prerequisites. The method explains the provided prerequisites contribution in each procedure required by ISO 26262-5. The method continues with guidance for reaching reliable results according to ISO 26262-5.

To ensure the reliability of the method, evaluation is needed. For this project, an example was created and confirmed the possibility of following the method through the procedures. To be able to confirm that each procedure is described correctly and gives reliable results, comparison to other methods needs to be made. This would confirm the reliability to reach the correct result with the method or if improvements are necessary.

The difficulties with implementing ISO 26262-5 are to provide the required documentation. Before beginning with ISO 26262-5, procedures as Item definition, HARA and FTA need to be performed. Documentation of components included in systems needs to be provided with the required properties like FIT, failure mode and failure distribution. Technical safety concepts need to be verified and safety mechanisms needs to be motivated.

As a conclusion, the developed method needs an evaluation to verify the reliability of the results. The results from the example used indicates that guidance from the method gives correct performance of the procedures. When the method is verified, the guidance to create an ISO 26262-5 harmonised system can be performed correctly if all documentation of prerequisites is provided.

Bibliography

Astruc, J.-M., & Becker, N. (2010). *Toward the application of ISO 26262 for real-life embedded mechatronic systems.* Retrieved from https://hal.science/hal-02264389/document

Blessing, L., & Chakrabarti, A. (2009). *DRM, A Design Research Methodology.* London: Springer-Verlag.

CCOHS. (2017). *Hazard and Risk - Risk Assessment.* Retrieved from https://www.ccohs.ca/oshanswers/hsprograms/hazard/risk_assessment.html

International Eletrotechnical Commission. (1996). *Methods of measurements for waveguides.* (IEC 61580:1996).

International Ogranization for Standardization. (2018). *Road Vehicles - Functional Safety.* (ISO 26262:2018).

International Organization for Standardization. (2018). *Road Vehicles - Functional Safety - Part 3: Concept Phase.* (ISO 26262-3:2018).

International Organization for Standardization. (2018). *Road Vehicles - Functional Safety - Part 4: Product Development at the System Level.* (ISO 26262-4:2018).

International Organization for Standardization. (2018). *Road Vehicles - Functional Safety - Part 5: Product Development at Hardware level.* (ISO 26262-5:2018).

Leen, G., & Heffernan, D. (2002). *Expanding Automotive Electronic Systems.* Retrieved from https://www.researchgate.net/publication/2955571_Expanding_automotive_electronic_systems

Lundteigen, M., & Rausand, M. (2014). *Fault Tree Analysis.* Retrieved from https://www.ntnu.edu/documents/624876/1277046207/SIS+book+-+chapter+05+-+Introduction+to+fault+trees/fa8ba01a-3baf-4bb8-94ed-116bf5bc6b44

MILTA Technology. (2021). *Inside the Mind of Your Automatic Gearbox: Everything About the TCU.* Retrieved from https://milta.co/2021/06/09/inside-the-mind-of-your-automatic-gearbox-everything-about-the-tcu/

NI. (2023). *What is the ISO 26262 Functional Safety Standard.* Retrieved from https://www.ni.com/en/solutions/transportation/what-is-the-iso-26262-functional-safety-standard-.html

NRC. (1981). *Fault tree handbook.* Retrieved from https://www.nrc.gov/docs/ML1007/ML100780465.pdf

Texas Instruments. (2020). *Understanding Functional Safety FIT Base Failure Rate Estimates per IEC 62380 and SN 29500.* Retrieved from https://www.ti.com/lit/wp/sloa294/sloa294.pdf?ts=1695726054901