A Case Study: Inverter Safety in Compliance with ISO26262

Işıl Coşar Ertaş[1,2], Selin Özçıra Özkılıç[1], Çetin Dalkılıç[2], Osman Can Soygenç[2]

[1]Department of Electrical Engineering, Yildiz Technical University, Türkiye
isil.cosar@std.yildiz.edu.tr, sozcira@yildiz.edu.tr
[2]AVL Türkiye Research and Engineering, Istanbul, Türkiye
isil.cosar@avl.com, cetin.dalkilic@avl.com, osman.soygenc@avl.com

Abstract

Functional safety for inverters is a critical aspect of ensuring the safe operation of modern vehicles, particularly in the context of electric and hybrid vehicles. Inverters' primary duty is to supply the motor with the necessary phase currents so that it can produce the requested torque. The International Organization for Standardization (ISO) 26262 standard has provided a detailed road map for this safety-critical system. The concept stage of the roadmap is the main topic of this article. In this direction, the system is specified and an item definition section for the inverter is constructed. Hazard analysis and risk assessment (HARA) of this system is used to explore potential risks, and fault tree analysis (FTA) is used to look into the root causes of those risks. The foundations of the safety system are formed by carrying out functional safety activities in accordance with ISO26262 for a safer system.

1. Introduction

The way that people view vehicles is changing as a result of the rapid advancement of technology. Users of vehicles are becoming more and more interested in vehicles with smarter and more environmentally friendly features. Since there are more electric vehicles on the road today than ever before, there are also more electrical and electronic components in vehicles as a result of technology's ongoing advancements. With the creation of multiple solutions at the component and subsystem level, electric vehicle technologies are expanding quickly [1].

It is now necessary to incorporate more safety precautions to vehicles due to the rise in electrical and electronic components. As a result of the increasing demand for extra safety measures, international studies on this subject have begun. Accordingly, functional safety for road vehicles has become increasingly evident because functional safety ensures that systems operate safely despite faults, aiming to protect people, the environment and assets. It involves identifying hazards, implementing safety measures and complying with established safety standards throughout the systems lifecycle [2].

The first functional safety standard for the manufacturing of numerous vehicles, ISO26262 was released in the automotive industry. Only safety-related electrical, electronic, and programmable electronic (E/E/PE) systems, comprising motor, electronic, and software components, are covered by ISO26262 [3].

Various approaches have also been developed to help automotive system manufacturers design safer vehicles by facilitating compliance with functional safety standards [4].

Road vehicle functional safety standard ISO26262 was formally released by the ISO in 2011 [5]. The second edition of the ISO26262 standard was released in December 2018, broadening the functional safety standard's scope and strengthening safety development [6]. In addition to these advancements, the Japan Automotive Software Platform and Architecture was established in September 2004 to standardize electronic control systems and software for automotive networks, increasing efficient development and dependability across the entire automotive industry [7].

The initiating functional safety artifact is the item definition [8]. The concept phase section is part three of the ISO26262 standard, the most recent version of which comprises 12 sections. The inverter has been chosen as the subject of this paper, and work is related to its concept phase.

The operating safety of electric vehicles is directly influenced by the inverter [9]. In terms of fragility, power electronic converters are at the top of the list [10].

Functional safety concept development has been carried out for the 380V motor control unit (MCU) and various hazards related to the MCU are highlighted [11]. Based on the understanding of ISO26262, the design of a functional safety concept for torque control of a fully electric school bus has been carried out [12].

Functional safety in vehicles is an issue that needs to be addressed in depth. Functional safety of many different safety-critical systems within the vehicle can be ensured. The inverter system is one of these safety-critical systems. This study is carried out as there are not many studies in the literature on the functional safety of the inverter system, especially for the concept phase which is not included in the literature as much as the development phase.

In this paper, this study till the FTA part to conduct the concept study of the inverter system that can be employed in electric or hybrid vehicles. HARA have been used to establish the risks associated with the most fundamental inverter function that has been chosen, as well as the potential hazards it may present to the vehicle. Automotive Safety Integrity Level (ASIL) was established for this hazard in HARA and the safety objective was established as a result of the safety integrity level of this hazard being calculated concurrently by HARA via assessing the condition of the vehicle in various operating states. Then, the situations that could cause this identified danger are determined by FTA. The emergence of these potential situations may cause the vehicle to accelerate unintendedly, so any work to be done after the concept phase should be done considering the FTA study.

The paper is organized as follows: Following chapter of the paper contains comprehensive information regarding the steps of the concept phase. The item definition chapter created for the inverter system is detailed in the third chapter, after which the hazard analysis and risk assessment work completed is presented in the fourth chapter. The FTA conducted is presented as the final chapter.

2. Concept Phase According to ISO26262

The ISO26262 standard contains several chapters, one of which is the concept phase. The Fig. 1 displays the stages of the concept phase section as stated by the ISO26262 standard.

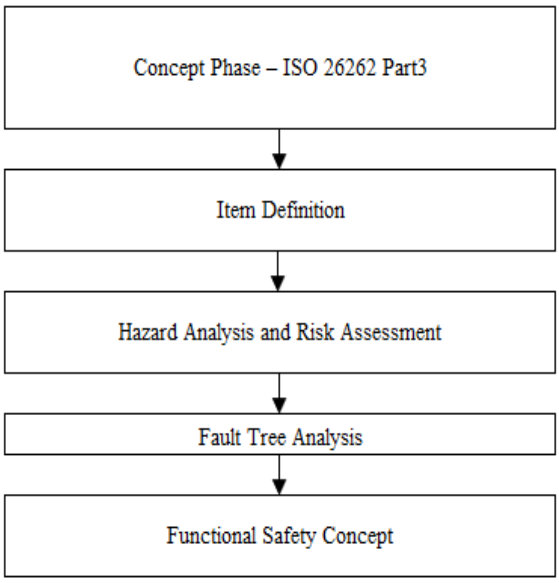

Fig. 1. Steps of concept phase according to ISO26262

The creation of the item definition document is the first step in the concept phase. The main goal of this document, as stated in ISO26262 Part 3, is to describe and explain the item, its functionality, its dependencies, and interactions with the driver, the environment, and other elements at the vehicle level in order to support a sufficient understanding of the subject in order to carry out the activities in the subsequent stages.

HARA is the second stage of the concept phase. In order to avoid risks, HARA section's goals include identifying and categorizing hazardous events brought on by item misbehavior as well as formulating safety objectives for their mitigation or prevention, along with the pertinent ASIL. Hazard classes of hazardous occurrences are established as a consequence of hazard analysis and risk assessment. There are four types of hazards which are ASIL A, ASIL B, ASIL C and ASIL D. When defining these levels, three crucial considerations are taken into account. For the dangerous circumstances, the three factors of severity, exposure, and controllability are assessed.

Table 1. Classes of severity [6]

Class	Description
S0	No Injuries
S1	Light and moderate injures
S2	Severe and life-threatening injures
S3	Life-threatening and fatal injures

In functional safety, "severity" refers to the assessment of the potential harm or damage that could result from a hazardous event or condition. It is a critical factor in determining the level of risk associated with a hazard and in designing safety measures and systems to mitigate that risk effectively. The goal is to ensure that safety-critical systems and processes are designed and operated to prevent or mitigate high-severity events and protect human life and the environment.

Table 2. Classes of exposure [6]

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

Table 3. Classes of controllability [6]

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

The assessment and confluence of these three variables, namely severity, exposure, and controllability, leads to the emergence of an ASIL. The precise determination of these levels is crucial because precautions must be taken according to the level of safety attained as a result of these levels.

Table 4. ASIL determination [6]

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	A	B	C
	E4	B	C2	D

In the FTA, the sub-fractions of the hazard and malfunction's source are broken down and evaluated. The root cause of the risk and malfunction has been sought after. When conducting this analysis, various logic gates are used. A malfunction might be caused by two different failing vehicle parts connected to it, or it might have more than one reason. Logic gates are employed as a result of such circumstances.

The functional safety concept step is the final step of the concept phase. In order to achieve the necessary fault tolerance or to sufficiently lessen the effects of the relevant fault by the element itself, the driver, or external measures, it is necessary to specify the functional or degraded functional behavior of the element in accordance with the safety objectives, determine the constraints for the appropriate and timely detection and control of relevant faults, and obtain the necessary fault tolerance.

3. Item Definition for Inverter System

The item definition of functional safety refers to a comprehensive description and understanding of a specific

component, system, or element within a product or system, detailing its functionality, potential failure modes, and safety-related attributes. This item definition is crucial in the context of functional safety standard ISO26262. Item definition document is created for Power Inverter (PI) system.

The primary purpose of a PI in a vehicle is to supply the engine with the necessary electrical power.

A hybrid or fully electric vehicle may be the one in which the inverter is employed. In electric propulsion systems, traction is provided by an electric motor, electrical power is provided by a battery or generator, and engine performance is controlled by a motor control unit (MCU). AC inverter included within MCU. A semiconductor switch for DC connection and a capacitor with a high ripple current capacity are both included in the circuit Voltage Source Inverter (VSI) topology of the voltage source inverter of the PI. Under a variety of voltages and environmental factors, the PI is calibrated to precisely control the electric motor.

The gate drivers in the inverter receive Pulse Width Modulation (PWM) signals from the motor control unit, which are then used to generate the necessary phase currents for the electric machine. To better understand this system, the interfaces of the system are given in Fig. 2.

The process begins with the vehicle control unit sending a torque request, which is then received and processed by the motor control unit. This processing step is crucial for determining how to manage the motor's operation. Subsequently, a signal is generated at the motor control unit's output and sent PWM to the gate drivers. These gate drivers control switches within the inverter, allowing it to generate phase currents required to drive the motor effectively. This entire sequence of operations ensures that the motor receives the necessary phase currents to operate as intended in response to the initial torque request.

The inverter component of the vehicle carries out a variety of functions. Torque control is the inverter's primary function. The torque is modified using the phase currents that the inverter supplies to the electric motor in response to the torque request that is sent over Controller Area Network (CAN) to the inverter system.

Field oriented control is one of the methods used in torque control. Motor control unit block diagram is given in detail in Fig. 3.

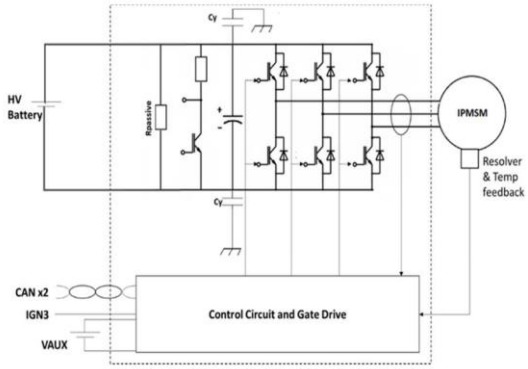

Fig. 3. Motor control unit block diagram [11]

The active discharge functions of the inverter system bear significance as well. The active discharge function gives you the chance to bring the high voltage value down below 60V within a predetermined amount of time.

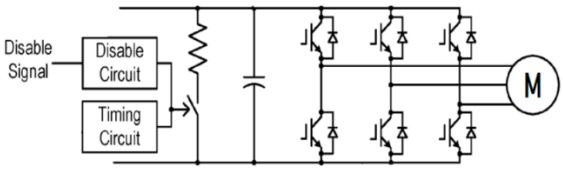

Fig. 4. Active discharge block diagram

Apart from these roles, it is equally critical for the inverter system to identify errors and reset PWM signals when problems occur in the motor control unit.

The item definition document holds paramount importance in comprehending a system or component thoroughly. In this study, it is meticulously crafted by considering the system as a holistic entity. Accurate item definition is an important initial step that enables us to identify potential hazards within the system effectively and is crucial for guiding subsequent safety-related actions and analyses.

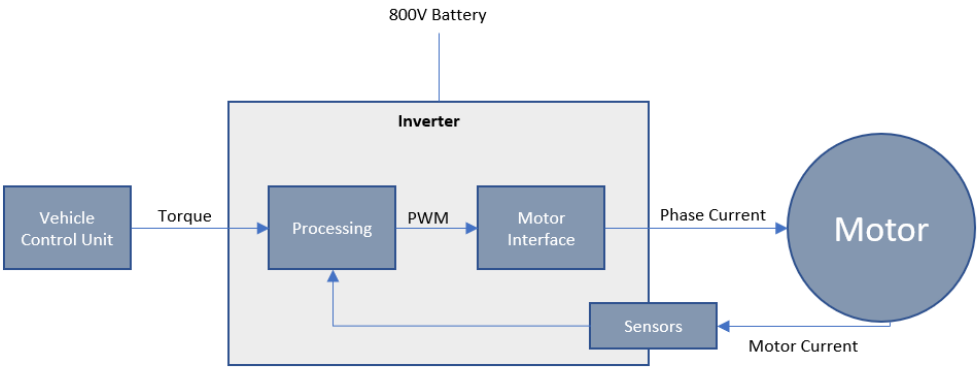

Fig. 2. Interfaces of inverter at system level

4. HARA for Inverter System

HARA in accordance with ISO26262 involves a systematic process. It starts with the identification of potential hazards, followed by assessing their severity and likelihood. These hazards are then classified into risk classes, and safety goals are established to set acceptable risk levels. A functional safety concept is devised to address these hazards, leading to the derivation of safety requirements. The safety goals are validated, and the process may be iterative to accommodate changes and new information. Overall, HARA serves to methodically identify and mitigate safety risks in the development of electrical and electronic systems in road vehicles.

All inverter functions are listed initially when the inverter system begins the HARA operation and from these functions safety critical functions are selected. This section will cover the inverter's most fundamental purpose, which is to provide or restrict phase currents in accordance with the requested torque. This function is one of the safety-critical functions. The function responsible for delivering or limiting phase currents is thoroughly evaluated by scrutinizing different malfunction scenarios. For instance, an example of such a malfunction could involve supplying phase currents that exceed or fall short of the intended levels. In order to identify potential hazards arising from these malfunctions, a collective brainstorming and teamwork approach is employed to compile a list of possible risks that might affect the vehicle. These hazards are listed in Table 5. For providing/limiting phase currents function, four hazards are found. The safety integrity level for the Hazard-2 is then determined after evaluating several operational scenarios.

The exposure part of HARA in ISO26262 involves assessing the likelihood and extent of exposure to specific hazards during the operation of a vehicle.

Table 5. Vehicle hazards

Vehicle Hazards	
Hazard-1	Unintended Deceleration
Hazard-2	Unintended Acceleration
Hazard-3	Loss of Acceleration
Hazard-4	Overheating

It considers factors such as the frequency and duration of exposure to various scenarios and conditions in which hazards could manifest. By quantifying exposure, HARA helps determine the level of risk associated with each hazard.

For unintended acceleration, ASIL is found as ASIL D. The safety integrity level's standards must be met by the measures to be implemented in response to this hazard. The safety goal determined for this hazard is to prevent unintended acceleration.

HARA yields a comprehensive understanding of safety-related risks, including identified hazards, their severity, and probability, resulting in the categorization of hazards into risk classes. Safety goals are established to define acceptable risk levels, alongside the development of a functional safety concept outlining safety mechanisms and requirements. The process culminates in validated safety goals, ensuring the systematic mitigation of safety risks and compliance with relevant safety standards and regulations.

Table 6. Hazard analysis and risk assessment

Hazard	Operational Situation	Severity		Controllability		Exposure		ASIL
Unintended Acceleration	Vehicle approaching pedestrians using the crosswalk	3	Because of the pedestrians or high speed, life-threatening injuries can happen.	2	Because of the approaching to pedestrians, situation is less controllable.	4	Vehicle approaching crosswalk with pedestrians	ASIL C
Unintended Acceleration	Parking on the side of the road	3	Since there may be high speed vehicles around, life threatening injuries can happen.	2	Because of the oncoming traffic, it is less controllable.	4	Vehicle is parking	ASIL C
Unintended Acceleration	Different highway situations	3	Since vehicle speed is high speed, life threatening injuries can happen.	3	Because of the high speed, it is hard to control.	4	Vehicle driving on the highway	ASIL D
Unintended Acceleration	Driving on a straight road in urban area, with parked vehicles and oncoming traffic in the environment and low speed	2	Because of the low or very low speed, severe and life-threatening injuries can happen but survival is possible.	2	Since pedestrians and parked vehicles exist around the vehicle, situation is less controllable.	4	Driving in urban area	ASIL B

5. Fault Tree Analysis for Inverter System

FTA is a systematic method used to analyze the causes of complex system failures, using logic gates to represent the relationships between events. The top-level event, which is the undesired outcome under investigation, is analyzed in terms of the logical connections between various events. AND gates require all input events to occur for the top-level event to happen, OR gates allow the top-level event to occur if any of the input events happen, and NOT gates signify the event's non-occurrence as a factor. Probability assessments are assigned to events to calculate the likelihood of the top-level event, facilitating the identification of critical paths and informing strategies for risk mitigation and system improvement.

Each FTA contains the potential causes for the indicated hazard.

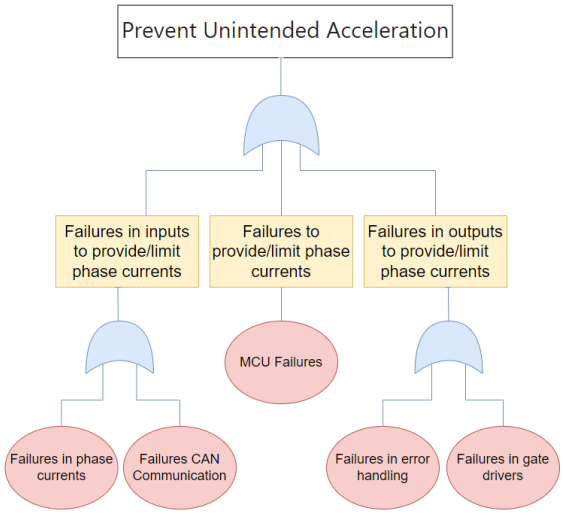

Fig. 4. Fault tree analysis for unintended acceleration

Three areas were looked at in the analysis of this function: the components that feed data into the inverter system, the mistakes within the function itself, and the outputs associated with this function.

The events of the FTA indicate that several factors can lead to unintended acceleration. Unintended vehicle acceleration is caused by situations such as errors in the phase currents supplied to the electric machine or errors in the torque request received via communication. Sensors may experience errors in phase currents, such as the sensor state being stuck or the sensor value being measured incorrectly.

Internal issues with the motor control unit itself could also prevent the electric machine from receiving the requested torque, which could result in unintended acceleration. Gate drivers may experience hardware issues that result in unintended acceleration. The safety requirements in the next step, the functional safety concept stage, are also derived from FTA.

6. Conclusions

Concept study of the inverter system on paper is carried out up to the FTA step according to the ISO26262 standard. The inverter is a critical safety element for electric and hybrid vehicles. The dangers that may occur if the torque control, which is the basic function of the inverter, is not performed properly and the phase currents are not transferred to the electrical machine correctly, have been identified and one of these hazards, unintended acceleration, has occurred. A safety target has been set to prevent unintended acceleration and the safety integrity level of this hazard under different operating conditions has been determined. Then, what could cause this danger is examined through FTA, and as a result of this analysis, it is determined that it could be caused by errors that may occur at the input/output of the system or in the engine control unit itself. Situations such as errors in phase currents or incorrect torque request signals from the CAN communication may cause unintended acceleration in the vehicle. The initial steps of functional safety operations have been thus carried out in accordance with the ISO26262 standard created for road vehicles in order to improve the system's safety, eliminate hazards. In the future stages of the study, the functional safety concept phase will be completed and the software safety requirements of the system will be extracted and the system will be modeled in MATLAB Simulink.

7. References

[1] Karamuk M., “Review of Electric Vehicle Powertrain Technologies with OEM Perspective”, 2019 Int. Aegean Conf. Electr. Mach. Power Electron. 2019 Int. Conf. Optim. Electr. Electron. Equip., IEEE; pp. 18-28, 2019.

[2] Liu B, Li Y., “Research on Vehicle Control Unit based on functional safety”, 2017 2nd Asia-Pacific Conf Intell Robot Syst ACIRS 2017, 2017:160–4.

[3] Xie G, Li Y, Han Y, Xie Y, Zeng G, Li R., “Recent Advances and Future Trends for Automotive Functional Safety Design Methodologies”, IEEE Trans Ind Informatics 2020;16:5629–42.

[4] Gharib M, Ceccarelli A, Lollini P, Bondavalli A., “A cyber–physical–social approach for engineering Functional Safety Requirements for automotive systems”, J Syst Softw 2022; 189:111310

[5] ISO, ISO 26262:2011 - Road Vehicles – Functional Safety, International Organization for Standardization in ISO 26262, Nov. 2011.

[6] ISO, ISO 26262:2018 - Road Vehicles – Functional Safety, International Organization for Standardization in ISO 26262, Dec. 2018.

[7] “Japan automotive software platform and architecture - JASPAR,”2019.[Online].Available: https://www.jaspar.jp/en

[8] Schranner FS, Misheni AA, Warnecke J., “Deriving a representative variant for the functional safety development according to ISO 26262”, Reliab Eng Syst Saf 2021;209:107436.

[9] Bo L, Xiaochen W, Yue F., “Research on functional safety of drive motor system for electric vehicle”, Proc - 2021 Int Conf Artif Intell Electromechanical Autom AIEA 2021 2021:84–7.

[10] Bhavana R, Indela O, Yaragatti MS., “Functional safety requirements of traction inverter in accordance to ISO 26262” E3S Web Conf 2020;184:1–5.

[11] Sabbella RR, Arunachalam M., “Functional Safety Development of Motor Control Unit for Electric Vehicles”, 2019 IEEE Transp Electrif Conf ITEC-India 2019, 2019:6–11.

[12] Yi F, Zhang W, Zhou W., “Functional Safety Design for Torque Control of a Pure Electric Vehicle”, 2021 9th Int Symp Next Gener Electron ISNE 2021, 2021:1–4.