Functional safety requirements of traction inverter in accordance to ISO 26262

Bhavana R[1,*], *Omsekhar* Indela[2], and *Mohammed Sajid* Yaragatti[3]

[1] Mtech-CAID, Department of electrical and electronics, MSRIT-Bengaluru, India
[2] Assistant professor, Department of electrical and electronics, MSRIT-Bengaluru, India
[3] Solution Architect, KPIT- Bengaluru, India

Abstract. With the improvement and development in the automotive, the safety related aspects are also becoming more important. Hence there is a stringent demand for the Functional Safety and reliability. In these years, most of the vehicles are made with electrical and electronic components and systems which include lots of Electronic Controller Units (ECUs), electronic sensors, bus systems with coding. Due to the complexity in application of these electrical, electronics and programmable electronics, it is necessary to analyze the potential risk of malfunction for automotive systems. Thus, ISO 26262 has been introduced for automotive electrical/electronic (E/E) systems which ensure the complete safety installation of all ECUs, E/E systems its technical as well as management issues. In this paper, functional safety in accordance with ISO 26262 Part 3 of an electric traction inverter is done, the Functional safety report is generated in MEDINI TOOL and the short circuit fault of traction inverter is considered for Functional safety using MATLAB/SIMULINK.

I. Introduction

ISO 26262, derived from the IEC 61508 ensures the Functional Safety of Electrical and Electronic systems. The Draft International Standard (DIS) of ISO 26262 was published in June 2009. As the automotive industries got advanced and resulted in change over from mechanical to electrical control systems. Electric powertrain, Braking Systems, Electronic Stability, Adaptive Cruise Control, Emergency Brake Assistant, Brake-By-Wire, and Steer-By- Wire, air bags, light control and tire pressure are some of the critical systems where electrical and electronic components and ECUs are highly involved.

Therefore, Functional safety ensures the correct execution of the specific functions of the electrical and electronics involved in vehicles. The ISO 26262 is applicable for the passenger cars up to the gross weight of 3.5T [1]. In this paper the actual procedure involved in Functional Safety Concept – Part 3 for a traction Inverter is explained.

The ISO 26262 is explained by V model as shown in the figure 1.

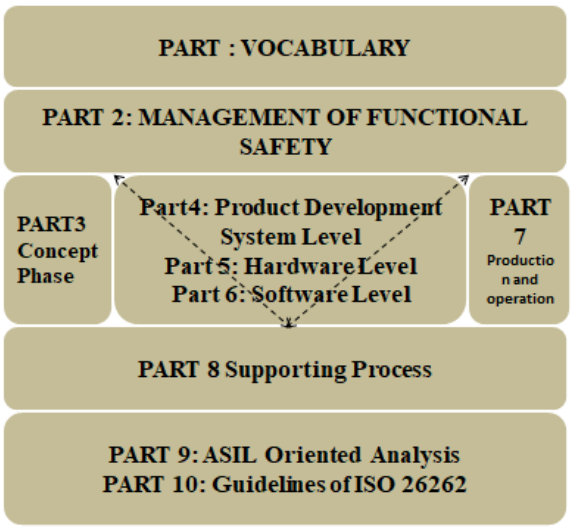

Fig.1.ISO 26262 V model

The part 3 of ISO 26262 goes with, Item Definition, Hazard Analysis and Risk Assessment, giving ASIL, Safety goals and Functional safety concept [1].

Using the term in ISO 26262 the "item" here is a traction inverter which converts Traction Battery DC power to the AC which drives the Electric Motor.

A traction inverter is entirely electric which converts the DC power stored in Traction Battery to AC which has to be fed to AC Electric motors. The traction inverters used are designed in order to control the torque hence the speed of the Electric vehicle. The Traction inverter module is made of the power electronic converter circuit, control unit and feedback circuitry. With the control and feedback circuitry it is possible for the traction inverter to convert the DC power to AC and can provide the require torque as commanded by the Vehicle Supervisory Controller (VSC) at the electric motor output.
IGBTs are widely used as the power converter switch in the circuit. There are different types of traction inverter design philosophies the main two are:

1. Separate Packages "Box Type", frame based silicon gel filled power module placed within the mechanical compartment of the drive train
2. Integrated Inverter design where small and fully encapsulated components.

The traction inverter module is mainly comprised of DC-AC converter circuit, Gate driver Circuit, Feedback unit, MCU.
Power electronic converters are ranked as the most fragile components followed by gate drive circuits. The failure of the gate drive circuit, failure of Isolation leads to the failure and the miss operation of the traction inverter. The over current fault is the most common type which may occur in the inverter [2].

PART 3 : CONCEPT PHASE

The part 3 of ISO 26262 is a concept phase which emphasizes on Item definition, Safety lifecycle, Hazard Analysis and Risk assessment and Functional safety concept of the Item [3].

A. ITEM DEFINITION

It gives the introduction of item, the description, interfaces, Boundary, Functional and functional requirements, Vehicle level functions and Malfunction. The Boundary, Interfaces and the item description is explained in the below diagram.

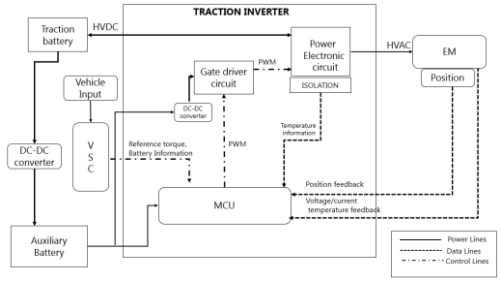

Fig.2.Traction inverter Boundary and Interfaces

The above diagram shows the traction inverter operating Boundary, Interfaces it has and different components in the module.

The Boundary comprise of main MCU (Motor Control Unit) which receives the feedback from the EM and takes the torque command signal from VSC and generates the PWM signal according to the required output. Gate driver circuit will amplify the current signal in order to trigger the IGBTs. Isolation is provided between the High voltage DC and AC and HVDC and LVDC parts. Continuous temperature monitoring of Gate drive circuit, will be done by MCU.

While defining the boundary it is assumed that all the other interfaces out of the traction inverter boundary is working properly and giving the proper and correct inputs. The Malfunctions and hazards could only occur due to the miss operation of the components inside the traction inverter boundary.

The Item definition is summarized as follows:

1) System Functions:
- Convert DC to AC
- Provide required torque as per VSC demand
- Convert AC to DC during Regeneration

2) Operation Conditions:
- Vehicle in Movement and stationary
- With medium and high speed
- Road conditions like, Mud, icy or paved

3) Operating Modes:
- Motoring Mode (DC to AC)
- Regenerative Braking mode (AC to DC)

4) Malfunctions:
- Unintended or Un demanded Acceleration
- Unintended or Un demanded Deceleration
- Incorrect AC to DC conversion

B. HAZARD ANALYSIS AND RISK ASSESSMENT

The HARA analysis is the next step in the Concept phase, which requires the prerequisites of Item definition [1]. By taking the functions and Malfunctions from Item Definition the hazard analysis, Risk assessment is done and for particular malfunction ASIL will be assigned according to the severity, exposure and controllability of the Hazard. FTA will be drawn for the particular malfunction in order to know the root cause of failure at system level. Later the safety goal and functional safety requirements will be drawn.

The detailed steps for HARA is given below,

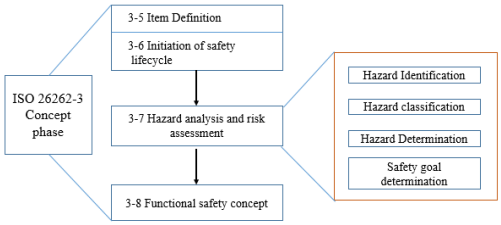

Fig.3. Detailed steps for HARA

The ASIL determination of each malfunction and hazard is depended on the severity, exposure and controllability. The same table is shown below

Table 1.ASIL determination parameters

Classes of **Severity**

Class	S0	S1	S2	S3
Description	No injuries	Light and Moderate injuries	Severe and life threatening injuries (survival possible)	Life threatening injuries (survival uncertain), fatal injuries

Class of **Probability of Exposure** regarding operational scenarios

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

Classes of **Controllability**

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

In the concept phase, the ASIL determination is done by the risk assessment of the potential hazard. That is by evaluating with three components: Severity, Probability of Exposure and Controllability. Table 1 shows the classes of these parameters.

Table 2.ASIL determination from S, E and C

		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	C	D

According to ISO 26262 there are four ASIL levels are identified: ASIL A, ASIL B, ASIL C and ASIL D [4]. The ASIL D will provide the highest safety integrity level and the ASIL A the lowest. There is another class called QM which do not dictates any Functional Safety requirement, they can be handled in the normal way.

The Table 2 gives the ASIL level according to the S, E and C classes.

C. ASIL Determination and HARA

With the consideration of operating scenarios, the Malfunctions and hazards are listed for different scenarios of EV operation like, Acceleration, Deceleration and cursing.

Here the Table 3 gives the summary of HARA and ASIL determination for various Malfunctions at different operating scenarios.

The Unintended and Un-demanded acceleration is the hazard caused due to the malfunction of more torque production, similarly the Unintended and Un-demanded deceleration is caused due to the Less Torque production.

Table 3.HARA and ASIL Determination

EV operating Scenario	*Malfunctions*	*HAZARDs*	*S*	*E*	*C*	*ASIL*
1. Stationary	Unintended Movement	*EV hits other Vehicles *EV hits obstacles *People inside get severe injuries	S3	E4	C3	D
2. Acceleration	Un-demanded Acceleration	*EV hits other Vehicles *EV hits obstacles *People inside get injuries *Loss of stability *EV may crash and catch fire	S2	E4	C3	C
	Unintended Deceleration	*EV hits other Vehicles *People inside get injuries	S1	E4	C2	A
	Unintended Lateral motion	*loss of Stability	S2	E4	C3	C
3. Cruising	Unintended Acceleration	*EV hits other Vehicles *EV hits obstacles *People inside get severe injuries *Loss of stability *EV may crash and catch fire	S2	E3	C3	B
	Unintended Deceleration	*EV hits other Vehicles *People inside get severe injuries	S2	E3	C2	A
	Unintended Lateral motion	*loss of Stability	S2	E4	C3	C
4. Deceleration	Unintended Acceleration	*EV hits other Vehicles *EV hits obstacles *People inside get severe injuries *Loss of stability *EV may crash and catch fire	S2	E2	C3	A
	Un-demanded Deceleration	*EV hit by other Vehicles	S1	E2	C2	QM
	Unintended Lateral motion	*loss of Stability	S1	E2	C2	QM
5. Any	Electrical malfunctions	*Service person gets severe electric Shock	S3	E3	C2	B

The highest ASIL rating is provided for Unintended Movement of vehicle from stationary condition which will take the highest severity of S3 as the Traffic participants may get fatal and survival difficult injuries, Exposure for the hazard will also be more as the vehicle will be stationary condition and the sudden movement with acceleration causes the increase in severity. The controllability will also be difficult extra maneuvering will be required from the driver. The same analysis is also done by taking the road conditions into consideration like, Low friction Wet or Icy road, Normal Paved road and Sand or Mud road. The ASIL rating is given for the hazards and malfunctions by taking these considerations.

D. Safety Goals

The safety goal for the all malfunctions and hazards are derived. For malfunctions with ASIL QM the functional safety will not be required and no safety goal will be derived [1]. Table 4 shows the Safety goal written for the Malfunctions of More Torque production, less torque production and incorrect AC-DC conversion.

Table 4.Safety goals for malfunctions and Hazards

Malfunction/Hazards	Safety Goals
More Torque Production	Avoid More torque production
Less Torque production	Avoid Less Torque production
Incorrect AC-DC conversion	Ensure the proper DC-AC conversion and energy restoration

According to the Safety goals written the Functional safety requirements will be drawn. Further FTA, the Top Down approach is done to know the root cause of the hazard at function level and to derive the functional safety requirements.

E. Fault Tree Analysis

Fault tree analysis is the Top down approach which goes on reasoning the cause of the hazard and malfunction occurred. It is done based on the logic gates. Figure 4 shows the FTA of Unintended Acceleration. Where the malfunction, Unintended Acceleration is taken in the Top level and other will be listed in the next level. Here OR gate is used to connect the reasons and causes [4]. In the Figure it tells that, the traction inverter may cause Unintended Acceleration with the Fault in power Electronic circuit OR Isolation Failure OR Fault in gate drive circuit OR due to MCU faults. In the next level the causes of these higher level interfaces will be listed. The Fault in Power electronic circuit will be due to the Hardware faults OR Interface failures. Further next level the Interface failure is may be due to Communication faults OR HVDC failure OR Incorrect PWM. Finally the incorrect PWM will be due to the fault in Gate drive circuits.

Similarly, for the Isolation Failure, MCU faults and Gate drive failure the causes to the function level will be written and the safety requirement will be written for each step.

The same type Bottom down approach of FTA is written for the Unintended Deceleration and Incorrect AC-DC conversion. Further the Functional Safety Requirements will be derived.

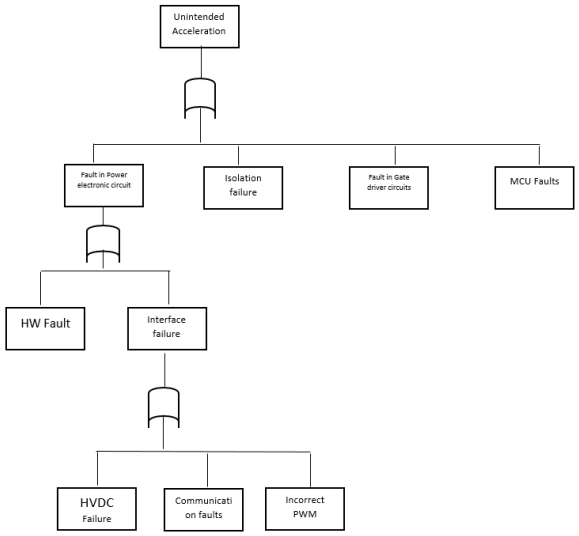

Fig.4. FTA of Unintended Acceleration

II. Simulation and Results

The Inverter model is simulated in the Matlab\Simulink environment. Different Malfunctions are listed in the table 3, in that one of the malfunctions of electric shock which can occur in any operating conditions is taken. The three phase inverter is taken fed by SPWM technique. The DC source is of 400V and connected to the three phase RLC load. The SPWM technique helps in producing the PWM signals to the IGBT gates [5]. Three Sine wave of power frequency with phase difference of 120 degree is compared with the high frequency wave of 1K hertz.

Figure 5(a) shows the Simulink model of the three phase inverter with SPWM technique. Figure 5(b) and 5(c) shows the phase voltage, line voltage and line current.

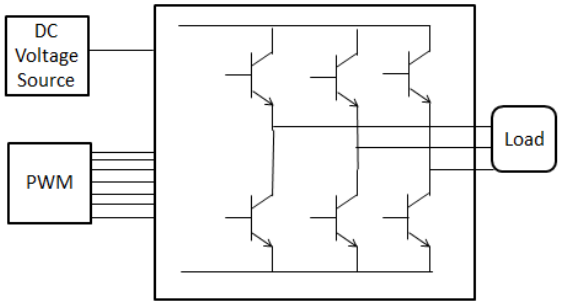

Fig.5(a). Simulation model of three phase Inverter

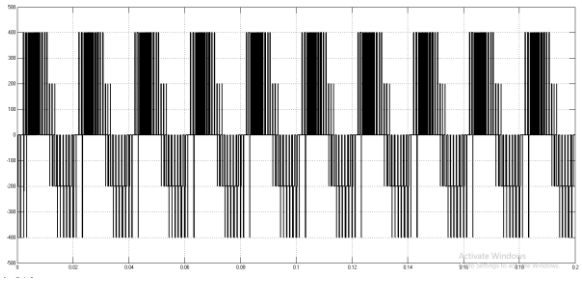

Fig.5(b). Phase to Phase three phase voltage at RLC load

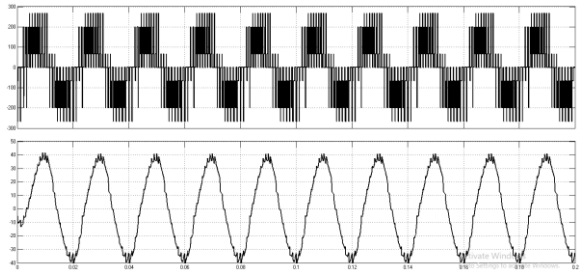

Fig.5(c). Line Voltage and Line Current at RLC load

During normal operating condition, when there are no faults and the output is within the range as shown in Figure 5(b) and 5(c), the MCU will continue to work in the normal operating condition. This determines the vehicle in the safe operating level QM condition. Similarly, the same model is simulated for the IGBT short circuit condition and the raised in line current is observed. The current will increases from 40A to 90A which is twice the original current that the load can handle. Figure 6 shows the increase in line current As a result of this the torque will raises and leads to the unintended acceleration. Also it may cause the severe electric shock for the driver or the passengers.

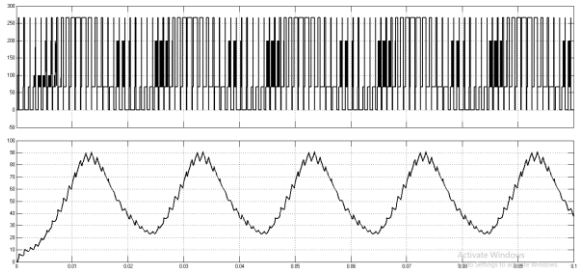

Fig.6. line current of 90A during IGBT short circuit condition

Once MCU detects the change in the output and the hazards event by the traction inverter, the Functional Safety concepts will be introduced into the Vehicle system according to the raised hazard and malfunction depending on the risk, severity and controllability of the hazard [6].

III. CONCLUSION

The Functional Safety Requirements for traction inverter is drawn in accordance to part 3- Concept phase of ISO 26262. The Item Definition, Hazard Analysis and Risk Assessment is derived for few faults and hazards in inverter and respective Safety goals are derived with the help of Fault Tree Analysis and came up with the safety requirements. The three phase Inverter model is simulated in the Matlab\Simulink environment for one of the malfunction and respective safety outcome is seen in concept phase.

References

[1] "26262:2011, ISO DISRoad Vehicles-Functional safety," *International Organisation for Standardization,* vol. Vol.43.040.10 26262.

[2] G. Zhiwei, C. Cecati, and S.X. Dingi, "A survey of fault diagnosis and fault-tolerant techniques—part II: fault diagnosis with knowledgebasedand hybrid/active approaches," *in Industrial Electronics, IEEE Transactions on,* Vols. vol.62, no.6, pp.3768-3774, June 2015.

[3] "ISO 26262-3:2011 Road vehicles - Functional safety - Part3: Concept".

[4] Kuen-Long Leu, Hsiang Huang and Yung-Yuan Chen, Li-Ren Huang and Kung-Ming Ji, "An Intelligent Brake-By-Wire System Design and Analysis in Accordance with ISO-26262 Functional Safety Standard," *International Conference on Connected Vehicles and Expo (ICCVE),* 2015.

[5] L. Bin, and S.K. Sharma, "A literature review of IGBT fault diagnostic and protection methods for power inverters," *in Industry Applications, IEEE Transactions on,* Vols. vol.45, no.5, pp.1770-1777, Sept.-oct. 2009.

[6] M.A. Ravindra Reddy Sabbella, Maheswaran Arunachalam "Functional Safety Development of Motor Control Unit for Electric Vehicles," in *IEEE Transportation Electrification Conference (ITEC-India)*, 2019.