Asian Journal of Convergence in Technology *Volume V Issue III*
ISSN NO: 2350-1146 I.F-5.11

Techniques and procedure to be followed for developing fail safe system in complaince with ISO26262

Sreeramulu Pasagadugula[1], Gaurav Verma[2], Jyoti Harmalkar[3]

[1]School of VLSI Design and Embedded Systems, NIT Kurukshetra, Thaesar, India [2]Department of Electronics and Communication Engineering, NIT Kurukshetra, Thaesar, India [3]Product Engineering Services, KPIT Technologies, Pune, India.

[1]srirampasagadugula@gmaill.com [2]gauravnitk13@gmail.com [3]Jyoti.Harmalkar@kpit.com

Abstract— **Advance Driving Assistance System (ADAS) is a future of entire automobile industry, A lot of Embedded Electronic Control Units (ECU's) are integrating into the automobiles to improve the Comfort, Safety and Security like ADAS-Vision, Radar, and Adaptive Cruise Control (ACC) etc. But as number of ECU's are increasing there is a lot of chances for malfunctioning behavior of the system and it is having major effects on the safety of Driver, Passengers and even environment, so there is a need for evolution of system architecture from fail safe to fail operational, For this purpose there is a need of detailed safety analyses need to be carry out for mitigating or completely silencing the obtained malfunctions, ISO26262 describes the steps to be carried out for safety analyses of the system, In this paper ,following the international safety standards for automobiles designing of the fail operational architecture was discussed from the existing fail safe architecture.**

Keywords— ***ADAS, ISO26262, functional safety, fail safe, fail operational, HARA, FSC.***

1. Introduction

Functional safety is getting importance in the automobile industry due to integration of Advance driving assistance systems ,There are lot of stories regarding accidents in industries due to malfunctioning behavior of the system i.e. machine does not stop in time to avoid dangerous harm to a workers of a factory , or of batteries of mobile phone burning up of malfunctions. For the automobile industry, where ECU's are learning how to take over decision taking from human drivers, recognizing and reacting to possible random failures is vitally important. Existing ISO26262 contains 10 Parts which includes vocabulary to guidelines where each part explains process to be followed for developing a product from pre phase to post phase of an production, here we are discussing about the Part-3 of ISO26262 Concept phase which describes about before the design reaching to Original equipment manufacturer what all the requirements to be there in the item we have selected, Here following the concept phase designing of fail operational architecture from existing fail safe architecture is discussed clearly. Here the when the malfunction occurs then it leads to failure of the system existing fail safe architecture are designed in such a way when a failure is detected then reach to safe state like exploding an air bag when severe impact detected by air bag and additionally if any malfunctions occurs during the exploding of air bag which leads to loss of life of passenger or drivers, for resolving these kind of issues the system architecture would be fail operational where in this case if there is the system recognizes that it is receiving the wrong information due to a fault, so the ongoing operation moves to degraded mode

In addition a failure in one component does not stop the whole system from working correctly, the system reconfigures itself to compensate for the fault and in advance it is going to detect that accident is going to happen by comparing the critical distance between vehicles and speed of the vehicles and immediately launching the safety critical operations like ABS (Anti-lock braking system) and pre air bag deploring etc., to protect the life and even environment.

The safety life cycle of ISO26262 is shown below.

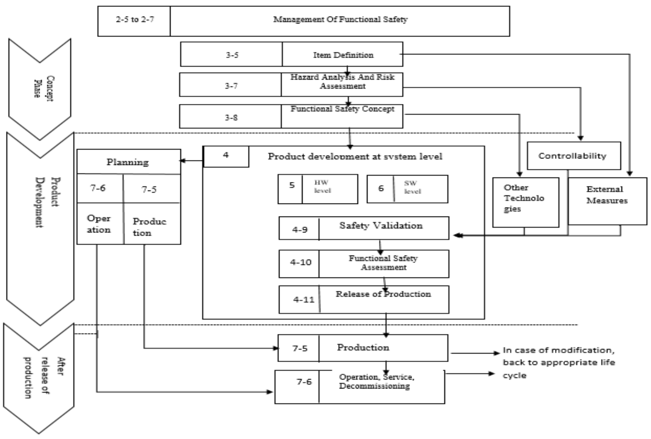
2-5 to 2-7
Management Of Functional Safety
Concept Phase
3-5
Item Definition
3-7
Hazard Analysis And Risk Assessment
3-8
Functional Safety Concept
Product Development
4
Product development at system level
Planning
7-6
7-5
Oper ation
Produc tion
5
HW level
6
SW level
Controllability
Other Technolo gies
External Measures
4-9
Safety Validation
4-10
Functional Safety Assessment
4-11
Release of Production
After release of production
7-5
Production
7-6
Operation, Service, Decommissioning
In case of modification, back to appropriate life cycle

Fig.1

2. Need of migration from fail safe to fail operational architecture

Below shown different analysis techniques explains the need of migration

2A.Table for existing techniques to needed techniques

Previous Generation	Current Generation	Next Generation
Fail-Safe	Safety and Availability	Fail-Operational
Detect Fault	Detect Fault	Detect Fault
Indicate Fault to Safe State System	Indicate Fault to Safe State System and Recover	Indicate Fault to Safe State System

Operation based on architecture

2B.Performance based on level of architecture

Previous Generation	Current Generation	Next Generation
Fail-Safe	Safety and Availability	Fail-Operational
Stop Operation	Continue Operation	Sufficient Vehicle Level Redundancy to Continue Full Operation

Performance based on architecture

Level 0: Fully manual vehicle
Level 1: One single automated aspect
Level 2: Automated steering and acceleration capabilities
Level 3: Environment detection
Level 4: No human interaction required
Level 5: Human driving is completely eliminated

3. ISO26262 Concept phase procedure to be followed on the existing fail safe architecture

The below figure shows the procedure to be followed in concept phase of an ISO26262-Road vehicles standards.

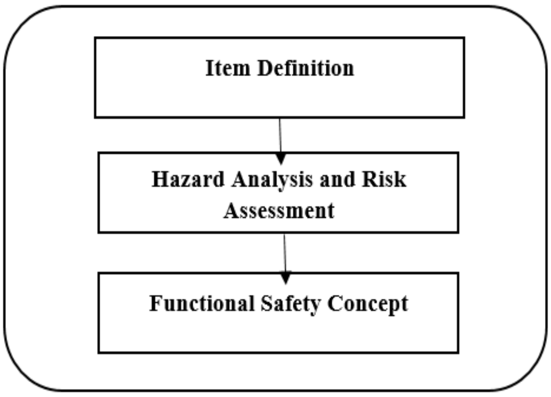
Item Definition
Hazard Analysis and Risk Assessment
Functional Safety Concept

Fig.2

3A.Item definition of existing Fail safe architecture

In the architecture used below there are two king of safety ECU's used one is for power supply and other is for normal operation of the function.

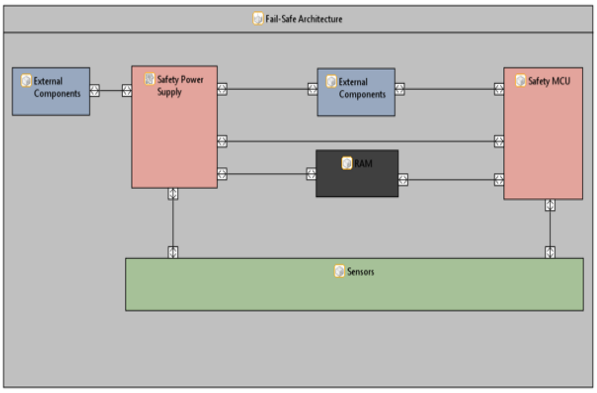

Fig.3

The present architecture is designed in such a way that if a failure in any control units due to malfunctioning behavior then the safety ECU's which are present those are going to detect and allowing the system to go into safe state which is uncontrollable.

In a fail-safe architecture, the power supply delivers and monitors over- and under-voltage to the microcontroller and the other peripherals. It is also in charge of sensing and evaluating the MCU safety operation through the watchdog and HW Error monitoring functions. If a fault is detected, the system goes into safe state (driven by the safety power supply) which promises that the function is maintained in a known and defined state (not uncontrolled).

For the different components included in the architecture, we need to come up with different Component level functions and malfunctions, vehicle level functions and the supporting functions. While deriving the malfunctions of the functions we need to follow the HAZOP checklist keywords.

1. No or not 2.Other than 3.More 4.Early 5.Less 6. Late 7.As well as 8.Before 9.Part of 10.After 11. Reverse (of intent) that we need to map them into the possible HAZARDS, and then we can proceed with HARA.

3B.Hazard Analysis and Risk Assessment

Here the item definition acts an input to the HARA procedure based on the malfunctions obtained in the item definition for different component functions. Here the main motto of this step is to come up with an different safety goals at the vehicle level and determining the Automotive specific integrity level depending (ASIL) depending upon the severity, Exposure and Controllability for the different situations for a particular malfunction caused by the different components present in the architecture such that we clearly knows which component is having the highest ASIL Level.

Depending upon the Effect of severity, Exposure and controllability we will determine the ASIL Level, below table is one of the case for determining the ASIL Level

ASIL	Impact of failure	Exposure	Controllability
A	No injury	Very low probability	Controllable in general
B	Minor injury	Low probability	Simply controllable
C	Fatal/Survival probable	Medium probability	Normally controllable
D	Fatal/Survival uncertain	High probability	Difficult to control or uncontrollable

ASIL Level based on severity, occurrence and controllability

Here the ASIL level determines the impact on the driver/Passenger when the malfunction occurs.

Here ISO26262 defines a table for determining the ASIL Level.

Severity	Exposure	Controllability		
		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

Fig.4

From the HARA we will get the safety goals and from item definition we will get the HAZARDS now these are acts as input to the Functional safety concept where we come up with an design ,this design may contain hardware redundancy or software redundancy depending upon the Hardware and Software Requirements Step which was explained in the ISO26262 Part-5 and Part-6 ,Now before starting with functional safety concept we need to do the deductive failure analysis which is used to determine the basic event which is responsible for the malfunction to occur i.e., Fault tree analysis .

Here the fault tree analysis acts as an input to the Functional safety concept

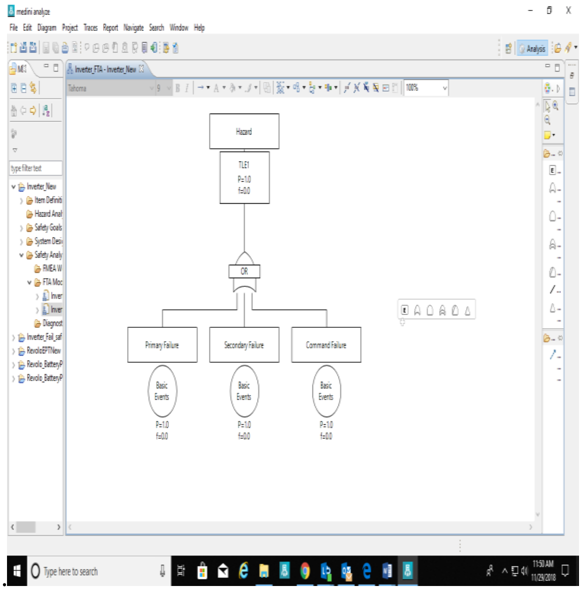

Fig.5

3C.Rough model on Functional Safety Concept

It includes two steps

1.Functional safety requirements

2.Technical safety requirements

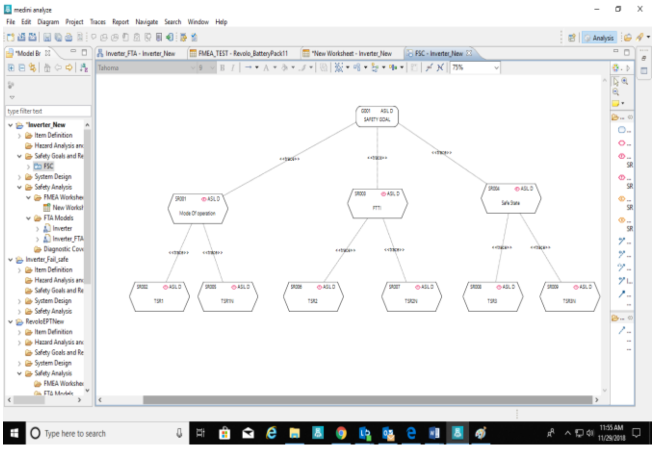

Fig.6

Functional Safety Requirements: Each functional safety requirement shall be specified by considering the following, if applicable.

1. Mode of operation of the Item:

It defines about whether the item used is in operating mode or not

2. Fault Tolerant Time Interval

It includes all the critical time information that when the fault occurs which leads to failure there would be some time interval to mitigate the fault either by self-diagnosis through software or by using an hardware redundancy based on severity integrity level and if that self-diagnosis fails within the time interval then it will reach to safe state and if reaching to fail state is not happened then immediately operating the Emergency operation within the FTTI

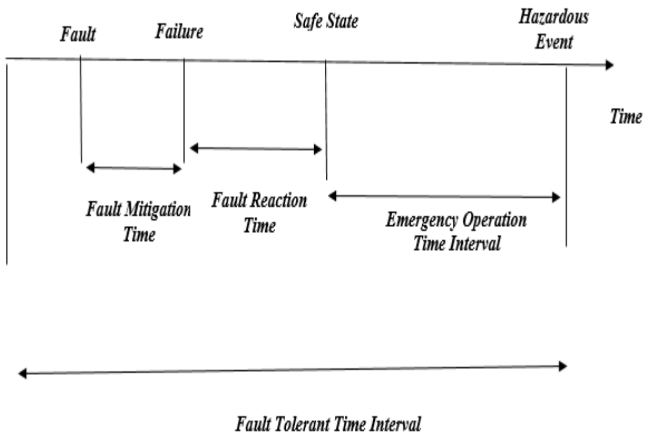

Fig.7

3. Time to come out of the safe state

If after fault if it reaches to safe state within the fault reaction time then in functional safety requirements we should mention about the time that should come out of the safe state.

Technical Safety Requirements:

Each Technical safety requirement shall be specified by considering the following, if applicable

The measures relating to the detection, indication and control of faults in the system itself;

NOTE1. This includes the self-monitoring of the system or elements to detect random hardware faults and, if appropriate, to detect systematic failures.

NOTE2.This includes measures for the detection and control of failure modes of the communication channels (e.g. data interfaces, communication buses, wireless radio link).

b) The measures relating to the detection, indication and control of faults in external devices that interact with the system;

EXAMPLE External devices include other electronic control units, power supply or communication devices.

c) The measures that enable the system to achieve or maintain a safe state;

NOTE3.This includes prioritization and arbitration logic in the case of conflicting safety mechanisms.

d) The measures to detail and implement the warning and degradation concept;

e) The measures which prevent faults from being latent.

After coming up with Functional safety requirements and Technical Safety Requirements we need to follow the inductive analysis to differentiate the safety levels from fail operational architecture to fail safe architecture. For this reason we need to do a Failure Mode Effect Analysis

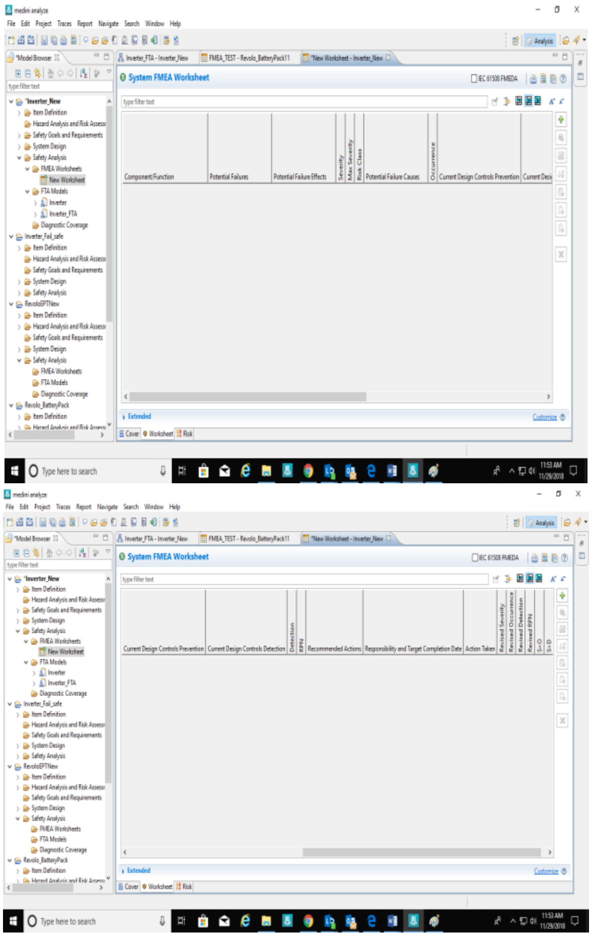

Fig.8

From the above analysis we get to know the Risk Priority Number of the existing detection and prevention techniques based on severity, occurrence and detection of the potential failures of the component. And we need to recommend new detection and prevention techniques following ISO26262 standards and then Original equipment manufacturers calculate the Risk Priority Number of the proposed techniques if they are satisfied with the result original equipment manufacturers are going to implement the proposed architecture in the existing architecture.

Conclusion:

The proposed method would achieve many benefits to the automobile industry in the long term.It may take some time to fully integrate the above procedure for the existing fail-safe architecture by following the above procedure we will have such kind of an fail-operational architecture which can overcome the failures by early recognizing the fault and reaching to degraded mode and even completely calm the hardware and random failures in existing architecture,Eventhough ISO26262 does not describe in details the proper process to be applied for obtaining the automotive safety requirements.A lot of research can be done explaining about the process to be follow.By According to European automotive electroncis Systems ISO26262 is going to be future for the automobile industry.

References:

[1]. ISO26262-Road vehicles Functional Safety Part-3 Concept Phase,Licensed to KPIT Technologies.

[2]. ISO26262-Road vehicles Functional Safety Part-4 Product Development at System Level,Licensed to KPIT Technologies.

[3]. ISO26262 automotive functional safety:issues and challeneges by Azianti Ismail ,Liu Qiang.International Journal of Reliability and Applications.

[4]. https://blog.nxp.com/automotive/automotive-functional-safety-the-evolution-of-fail-safe-to-fail-operational-architecture

[5]. https://blog.nxp.com/automotive/three-things-to-know-about-functional-safety

[6]. The Research Of Electric vehicle's MCU System Based on ISO26262-2017 2nd Asia-Pacific Conference on Intelligent Robot Systems.