e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

CONCEPTUAL DESIGN PHASE OF FMEA PROCESS FOR AUTOMOTIVE ELECTRONIC CONTROL UNITS

Venkata Satya Rahul Kosuru*1, Ashwin Kavasseri Venkitaraman*2

*1MS (Electrical And Computers Engineering), Independent Researcher, Sunnyvale, CA, USA.

*2MS (Electrical Engineering), Independent Researcher, Fremont, CA, USA.

DOI : https://www.doi.org/10.56726/IRJMETS30103

ABSTRACT

The main research of this paper describes about deriving safety on Electronic Controller Units or well-known called by (ECU's) in Automotive by conducting a "Failure Mode Effective Analysis" (FMEA's) for ECUS. Often performing FMEA's on ECU are complex [1] due to reason of several components sits on chip and each component interact to every other component on ECU hardware. The main concept of the paper is to derive safety design of electronic systems that are used in automotive and to address to potential failures which cause hazardous events. Automotive Standards are established to underline safety integrity level of electronic systems called as ASIL ("Automotive Safety Integrity Level") Research is conducted by taking ISO 26262:2018 "Functional Safety Guidelines for Road Vehicle-Passenger Cars" standards into consideration to design FMEA's. The behavior of a particular system or ECU shall be identified upfront by conducting effective mode failure analysis whose recommendations can be implemented in design phase of ECU such as for hardware implementing safety design constrains of IC chips and/or for software considering safety redundant logics. To underline the statement of safety design constraints before any FMEA to derive we need to understand that Safety Integrity Level of a particular electronic system. All electronic controllers have specific ASIL level allocated depending on risk [3] and safety integrity factor raising from ASIL A to ASIL level (B, C & D). ASIL A being lowest among safety critical identification when compared high risk level assigned ASIL D to a particular ECU. This research shall focus describing how well FMEA's helps to determine some resolution factors for all ASIL Level controllers. Research also focusses on implementing safety methods from possible outcomes derived from FMEA on ECU's as well propose further resolution that can be considered during design phase of ECU's [2].

Keywords: ASIL Integrity, Functional Safety, Electronic Control Units, FMEA, ISO 26262, Embedded Systems, Fault Tolerant Time Interval.

I. INTRODUCTION

Today when we talk about modern cars, electrical systems or electronic control units plays vital role in occupying or driving any features of vehicle. Every feature of automotive such as steering systems, brakes, suspension systems, body electronics, powertrain controllers are equipped with electronic controller (ECU's) where majority of ECU hardware is "Microcontrollers" 32-bit or 64-bit, Thermal sensors, Pressure sensors and corresponding electrical components. FMEA's shall takes places at various stages of ECU's (at design phase, process phase and as well during manufacturing phase). However, this research paper shall focus on design phase of FMEA (DFMEA) and possible outcomes from FMEA which shall strive for safe implementation of ECUs. The main action from FMEA shall layout three cases which would further help in designing ECU's more safely [2].

a) FMEA identifies possible failures in the Electronic Controller Systems (both Hardware and Software)
b) Severity and Impact of Failures on the Electronic Controller System.
c) Prevent actions or measures that can be taken while designing the Electronic Controller System.

In addition to the above three outcomes of FMEA, FMEA also establishes continuous cycle of "V"-Process that shall help designing the ECUs for further development in future as a learning curve.

Due to the presence of several other electrical components at one place called ECU unit or PCB board there is a high possibility of getting components damaged or not functioning if any faults occurred and are not responded by microcontroller within a specified time interval called "Fault Tolerant Time Interval" (FTTI). To prevent uncertainty of failures where whose faults are known/unknown a need for "failure Mode Effective Analysis" is

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

required to be conducted both on Hardware and Software of Electronic Control Unit (ECU). For any system to conduct FMEA the first identification of system interaction to other systems or sub-systems or units in the car. This paper talks on how independent research carried for one ECU and laying additional failure modes by underling the dependency to other ECU's. FMEA underlines risks and outcomes from the analysis however all known failures that can cause system to be faulted is considered. For Unknown/Uncertainty faults FMEA standalone itself not sufficient and most cases this can be divided into two different segments. For example, working only Automotive Electronics which are non-Autonomous driving systems (such as steering, brakes, suspension controllers) a ASIL on hardware [7] shall assigned by determining failures are single point or latent fault metrics [5]. Based on failures noted a Software redundant logic shall be developed. In case where working Autonomous or self-driving solution controllers we shall consider both Functional Safety standards of ISO 26262 as well Safety of The Intended Functionality ISO-PAS 21448 [4] to determine failures from uncertainty events.

Traditional way of conducting FMEA uses excel template and excel tab formula to determine single point, residual fault metric as well to determine risks, causes, severity and implement suggestions. In this research methodology we shall outline the FMEA calculation and possible outcomes and resolution for failure modes that are identified.

This paper describes how to perform FMEA for hardware, software, and ways to addressing failures within the system. Research has adapted methodologies (where detailed description noted in following section) and objective on conducting FMEA.

II. DESIGN PHASE FMEA METHODOLOGY

The important point of consideration before conducting FMEA on an ECU is to determine overall system importance of ECU. For example, a steering or brakes control must require a FMEA to determine failures that can impact system level similarly a FMEA on single component (such as resistor, transistor, or diode) is not required unless the component is integrated to other components or sub-systems that has potential hazard of failing the system [6]. To start FMEA on ECU we shall follow the product development cycle also called as V-cycle in automotive field of domain. Below figure shall demonstrates Design Phase FMEA how it can get started and process of design through concept before implementation

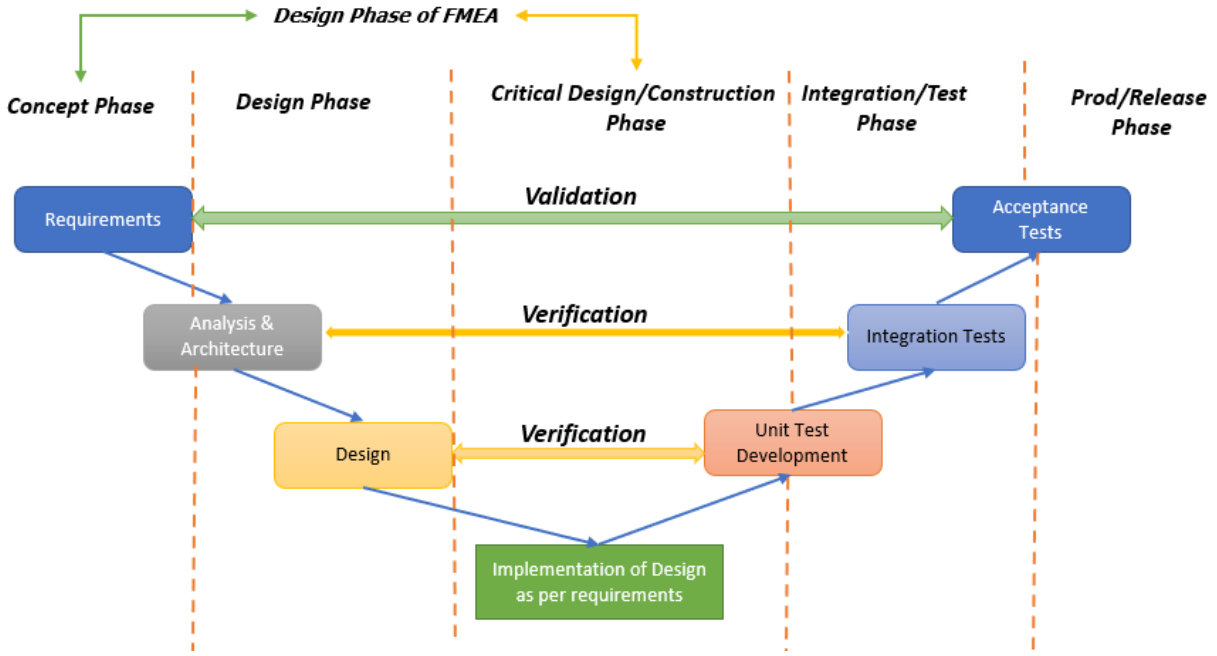

Figure 1: Product Development Cycle – Design Phase FMEA.

Scope of FMEA

Performing FMEA at design phase of system is little tricky. Some questions arise such as

a) Is FMEA constructed contributed to complete system level?

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

b) Will hardware and software FMEA's can be separated at concept phase.
c) What value it adds if FMEA's are separated instead of doing system level FMEA

To answer above open questions, we shall first understand scope of FMEA. At first, for hardware only identifying the failures "FMEDA" (Failure Mode Effective Design Analysis") is considered instead of FMEA. Since Hardware faults can contribute to either single point failure or dual point failure by performing FMEDA to calculate Permanent and Transient fault metrics percentage or PMHF factor

Below table flow diagram highlight scope of FMEA flowing from conceptual phase to system to sub-system or component level failure mode analysis

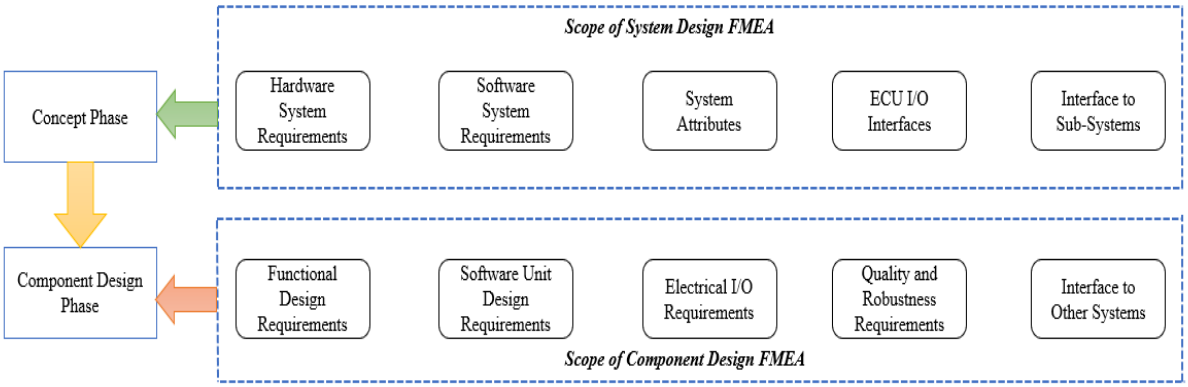

Figure 2: Scope of System and Sub-System FMEA Analysis.

The key aspects of conducting FMEA requires below actions to be thoroughly identified on ECUs

- To determine what Systems and/or Sub-systems or components considered
- To determine possible functions for systems and sub-systems
- To determine all possible list of failures from functions listed in point 2
- To determine effects from failures listed in point 3
- To determine causes of failures identified from point 4
- To list current actions or controls for failures
- To determine recommended action from list of failures noted
- To determine any other relevant actions or necessary modification in design

Process Flow of Failure Mode Effective Analysis

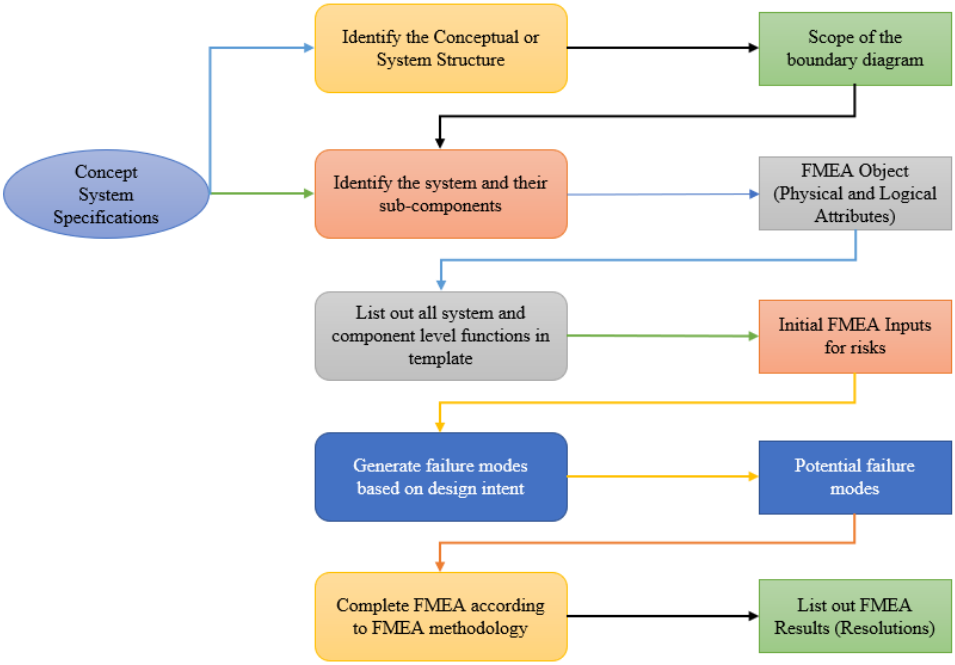

Figure 3: Flow Chart of Failure Mode Effective Analysis.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

The diagram below illustrates high level design adaption in accordance while conducting FMEA on electronic controller units. Behavior of any ECU shall first be analyzed by list of failures that a system can cause thus there is a need for FMEA process to establish supporting concept phase in "V" or Product Development cycle.

III. OBJECTIVE FOR DESIGN FMEA

In order to determine the objective of FMEA this paper uses steering case of ECUs to perform research on possible effects from failures identified by calculating risk factor [3]. ECUs considered for listing out failure modes are rated as highest safety integrity level whose ASILs are of ASIL D [7].

Use Case on Steering Electronic Controller Unit

Most cars today are occupied electronic steering controller i.e., when there's a loss of power steering (due to some failures on electrical systems or software logic) user or driver shall still be able to steer the wheel manually. However, this scenario of driving is considered safety critical i.e., when there's a loss of electronic steering action from column controller to steering ECU hence this is rated as Automotive Safety Integrity Level of highest which is (ASIL D).

Construction FMEA on Steering Controller ECU is little tricky by considering all possible cases of what might go wrong that would make loss of electronic steering command. However, with the help of excel FMEA layout one would be able to list of failure modes as well mode of action required for faults that are noted from FMEA. Below FMEA table for steering ECU shall identify the list of failure modes and potential action for failure modes that are noted.

Table 1. Steering ECU Failure Mode Effective Analysis Calculation for Possible List of highest Failures

FUNCTION	FAILURE MODE	EFFECT	SEVERITY	CAUSES	OCCURANCE	DETECTION	DETECTION CRITERIA	RPN = S*O*D	PREVENTION
Provide Supply voltage to Steering ECU	Loss of 5V supply to Microcontroller	Loss of Power Steering	9	Electrical HW failure to ECU	10	10	Startup Tests to conduct on ECU the check Power Supply	900	Design need for redundant supply voltage for controls code to run
Provide required operation ECU conditions	Overheating of ECU and/or Low temperature	Loss of Thermal sensitivity Monitor on ECU	9	Overheating of ECU or no cooling run across ECU to maintain temperature	10	8	Startup tests as well continuous sensor monitoring for temperature checks	720	Design need for vehicle level temperature monitoring system to monitor several ECU's thermal sensitivity

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

Provide continuous health check Monitoring	Loss of CAN communication from steering ECU to Vehicle System	Disrupt in CAN communication due to a) E2E checks are failed or b) delayed in receiving CAN signal	7	CAN transistor failure or Can communication Logic corrupted	8	8	To Perform BIST tests, run-time tests to continuously monitor CAN communication	448	Design to have redundancy in software logic and design for error reporting strategy
Provide continuous health check Monitoring	Corruption of Memory in ECU	Loss of steering action as well effect on other sub-components that communicates	8	Design constraints does not consider for Freedom from Interference (FFI)	8	8	To Perform MBIST, LBIST tests to check Memory interference at start of tests	512	Memory checks need to be continuously monitored on ECUs that share same RAM
Inform users or driver on steering failure	An electrical failure in system of Software functionality failure	Loss of driver notification about steering failure	7	Instrument Cluster software failure for not displaying malfunction	7	8	Logical tests, Startup test shall be able to detect the failure notifications	392	In the event of driver notification failure users shall still be able to receive the faults by using DTC methods

Severity, Occurrence and Detection criteria numbering are from Industry standards of Automotive whose values are underlined from table below

Table 2. Severity Rating Derivation used for FMEA

Severity Rating	Determination	Explanation
10	Very High	Causes in non-recoverable faults
9	Very High	Noncompliance with regulations.
8	High	Loss of primary vehicle function

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

7	High	Degradation of primary vehicle function necessary for normal driving during expected service life.
6	Moderate	Loss of secondary vehicle function.
5	Moderate	Degradation of secondary vehicle function.
4	Moderate	Very objectionable appearance, sound, vibration, harshness, or haptics.
3	Low	Moderately objectionable appearance, sound, vibration, harshness, or haptics.
2	Low	Slightly objectionable appearance, sound, vibration, harshness, or haptics.
1	Very Low	No discernible effect.

Table 3. Occurrence Rating Derivation used for FMEA

Occurrence Rating	Determination	Explanation
10	Very Low	Prevention controls not able to predict field performance or do not exist
9	Very Low	Prevention controls not targeted to identify performance to specific requirements.
8	Low	Prevention controls not a reliable indicator of field performance.
7	Low	Standards, best practices, and design rules apply to the baseline design, but not the innovations.
6	Moderate	Standards and design rules exist but are insufficient to ensure that the failure cause will not occur.
5	Moderate	Practices re-evaluated for this design but have not yet been proven.
4	High	Predecessor design and changes for new design conform to best practices, standards, and specifications.
3	High	Design expected to conform to Standards and Best Practices, considering Lessons Learned from previous designs.
2	High	considering Lessons Learned from previous designs, with significant margin of confidence.
1	Very High	Failure eliminated through preventive control and failure cause is not possible by design

Table 4. Detection Rating Derivation used for FMEA

Detection Rating	Determination	Explanation
10	Extremely high	Test procedure yet to be developed.
9	Very high	Test method not designed specifically to detect failure mode or cause.
8	Very high	New test method; not proven.
7	High	Test failures may result in production delays for re-design and/or re-tooling.
6	High	Test failures may result in production delays for re-design and/or re-tooling.
5	Moderate	Test failures may result in production delays for re-design and/or re-tooling.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

4	Moderate	Planned timing is sufficient to modify production tools before release for production.
3	Low	Planned timing is sufficient to modify production tools before release for production.
2	Very Low	Planned timing is sufficient to modify production tools before release for production.
1	Extremely Low	Prior testing confirmed that failure mode or cause cannot occur, or detection methods proven to always detect the failure mode or failure cause.

IV. RESULTS AND DISCUSSION

From the research study conducted on steering electronic controller unit it noted that, performing failure mode effective analysis on system level ECU shall lists of potential faults due to failure of system (both hardware and software) that could cause while vehicle is driving and FMEA lists out potential safety measures that can be adopted while designing the ECU at concept phase. For Systems that are higher ASIL rated such as for brakes, steering it is very crucial to conduct FMEA at concept and as well during process or implementation stage of system to analyze the faults that could occur during implementation phase.

From the FMEA design table it can be clearly noted that FMEA has high potential is listing out all potential failures that could cause to make system fail however, preventive measures are identified based on the severity, occurrence, and detection of a failure.

V. CONCLUSION

A detailed FMEA analysis on use case study for steering ECU layered out structure where, requirements shall be adjusted to adapt preventive measures. FMEA is a qualitative analysis and performing FMEA at conceptual phase allows users to save on time and cost of ECU and add a learning graph in designing fail safe hardware and software ECU requirements. Although there are many proven techniques of conducting FMEA but it when comes to Automotive electrical systems and electronic controller unit it is very much required to draft each and every possible potential failure that can be derived from functions or functional requirements of ECU. Going further deep dive in study shall give us a wider view aspect of what better ways of resolving potential failures that are identified by FMEA, how to address failure modes for complex systems and how fast the failures can be resolved timely. This research outlines the need for FMEA for ECU though the systems are not ASIL rated but QM conducting FMEA always helps to avoid potential hazardous situations.

VI. REFERENCES

[1] Henshall, E., Campean, I., and Rutter, B., "A Systems Approach to the Development and Use of FMEA in Complex Automotive Applications," SAE Int. J. Mater. Manf. 7(2):280-290, 2014.

[2] Teng, S.H. and Ho, S.Y., 1996, “Failure Mode and Effects Analysis: An Integrated Approach for Product Design and Process Control,” International Journal of Quality and Reliability Management, Vol. 13, No. 5, pp. 8-26.

[3] Dobryden, A.D., Rutter, B., Hartl, D., & Bramson, E.D. (2017). Failure Mode Avoidance Approach for Hybrid Electric Vehicle Systems. SAE International journal of engines, 10, 222-226.

[4] A. Ismail and W. Jung, "Research trends in automotive functional safety," 2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), 2013, pp. 1-4, doi: 10.1109/QR2MSE.2013.6625523.

[5] Chang, K. H., Chang, Y. C., & Lai, P. T. (2014). Applying the concept of exponential approach to enhance the assessment capability of FMEA. Journal of Intelligent Manufacturing, 25(6), 1413–1427.

[6] Van Eikema Hommes, Q., "Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety," SAE Technical Paper 2012-01-0025, 2012.

[7] Hamann, R., Sauler, J., Kriso, S., Grote, W. et al., "Application of ISO 26262 in Distributed Development ISO 26262 in Reality," SAE Technical Paper 2009-01-0758, 2009.