Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Safety Analysis of Adaptive Cruise Control System Using FMEA and FTA

M. Ben Swarup[1]
Department of Computer Science and Engineering[1]
Vignan's Institute of Information Technology
India

M.SrinivasaRao[2]
Department of Computer Science and Engineering[2]
Vignan's Institute of Information Technology
India

Abstract— Driver Assistance Systems like Adaptive Cruise Control (ACC) can help to prevent accidents by reducing the workload on the driver. ACC is an automotive feature that allows a vehicle's cruise control system to adapt the vehicle's speed to the traffic environment. A radar system attached to the front of the vehicle is used to detect whether slower moving vehicles are in the ACC vehicle's path. If a slower moving vehicle is detected, the ACC system will slow the vehicle down and control the clearance, or time gap, between the ACC vehicle and the forward vehicle. If the system detects that the forward vehicle is no longer in the ACC vehicle's path, the ACC system will accelerate the vehicle back to its set cruise control speed. This operation allows the ACC vehicle to autonomously slow down and speed up with traffic without intervention from the driver. The purpose of this paper is to describe Failure Modes and Effects Analysis (FMEA) and fault tree analysis (FTA) based safety-critical approach towards to development of Adaptive Cruise Control system from a safety perspective. This approach using FMEA starts at early system design. Thus, weaknesses in the design, leading to potential accidents, can be identified early and necessary interventions taken.

Keywords: adaptive cruise control, safety analysis, speed control, FMEA, FTA.

I. INTRODUCTION

Safety is a property of a system that it will not endanger human life or the environment. A failure of a safety-critical system can lead to injuries and even loss of life it is extremely important to provide designers with safety assessment methods that help to minimize the risk of the occurrence of such disastrous events. There are two safety assessment methods mostly used in the safety analysis. One of the method is failure mode and effective analysis (F MEA) [1]. In FMEA, trained engineers or system designers team analyses the cause consequence relationships of component failures on system hazards. Second method is Fault tree analysis, serves as an effective method in reducing component level testing effort and also plan an effective integration and system testing.

There are many applications that have traditionally been considered safety critical but the scope of the definitionha s to be expanded as computer systems continue to be introduced into many areas that affect our lives.The future is likel y to increase dramatically the number of computer systems that we consider to be safety critical [2]. The droppi ng cost of hardware, the improvement in hardware quality, and other technological developments ensure that new appl ications will be sought in many domains. The cost of critical system failure is so high means trusted methods and techniques must be used for development. Adaptive cruise control (ACC) is an intelligent form of cr uise control that slows down and speeds up automatically to keep pace with the car in front of you. If a slower mo ving vehicle is detected, the ACC system will slow the vehicle down and control the clearance, or time gap, betwe en the ACC vehicle and the forward vehicle. If the system detects that the forward vehicle is no longer in the ACC ve hicle's path, the ACC system will accelerate the vehicle back to its set cruise control speed. Adaptive cruisecontrol is also called active cruise control, autonomous cruise control, intelligent cruise control, or radar cruisecontrol.This is the case because distance is measured by a small radar unit behind the front grille or under the bumper. The Focus of t his paper is to investigate the failures of Adaptive Cruise Control (ACC) system using FMEA and FTA methods. This paper is organized as follows: section 2 deals with safety analysis section 3 describes case study of Adaptiv e Cruise Control, section 4 presents Failure Mode and Effect Analysis of Adaptive Cruise Control (ACC), section 5 presents Fault Tree analysis of Adaptive Cruise Control (ACC)and final section concludes the paper.

II. SAFETY ANALYSIS

Safety analysis is a method for evaluating the hazards and risks posed by a system and ways to minimize them Aha zard is a state or set of conditions of a system that,together with other conditions in the environment of thesystem , will lead inevitably to an accident [3].The primary concern of system safety analysis is the management of hazards: t heir identification,evaluation, elimination and control through analysis, design and management procedures Hazard analy sis is the first stage, in which the system is studied for situation in which potential harm could result,and the frequen cy with which those situation occur. Risk analysis is the second stage, in which the possible outcomes of the hazard and the frequency of appearance of each outcome are determined. This allows sources of potential harm in the system to be prioritized and dealt with to increase the safety of the system. The system safety analysis process can be basically split into thefollowing steps:

Hazard identification: This step identifies the potential hazards in the proposed system.
***Risk assessment**:* This examines each of the identified hazards to determine how much of a threat they pose. This assists in deciding the steps required to reduce the risks to acceptable levels. Many initial safety requirements are set at this stage.

***Preliminary system safety assessment (PSSA)**:* This phase is concerned with ensuring that a proposed design can meet its safety requirements and also with refining these safety requirements as necessary.
***System safety assessment**:* This stage is concerned with producing the evidence that demonstrates the safety requirements have been met by the implementation.
Safety Analysis methods: FMEA (Failure Mode Effect Analysis) and FTA (Fault Tree Analysis) are typical reliability analysis methods, that are widely used. The failures that are occurred in the Adaptive Cruise Control are identified by using FMEA.

FMEA (Failure Mode Effect Analysis): Failure modes and effects analysis (FMEA) is a step by step approach for identifying all possible failures in adesign, a manufacturing or assembly process, or a productor service. Failures are prioritized according to how serioustheir consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest priority ones. Example of FMEA is shown in Figure 1. FMEA consists of three main phases. In the first phase of identification, one needs to determine what can go wrong. In the second phase of analysis, one is required to identify the probability of failure, its consequences and according to this calculate the risk priority number. In the third phase one should think out how toeliminate the occurrence or reduce the severity of undesired results. Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected.

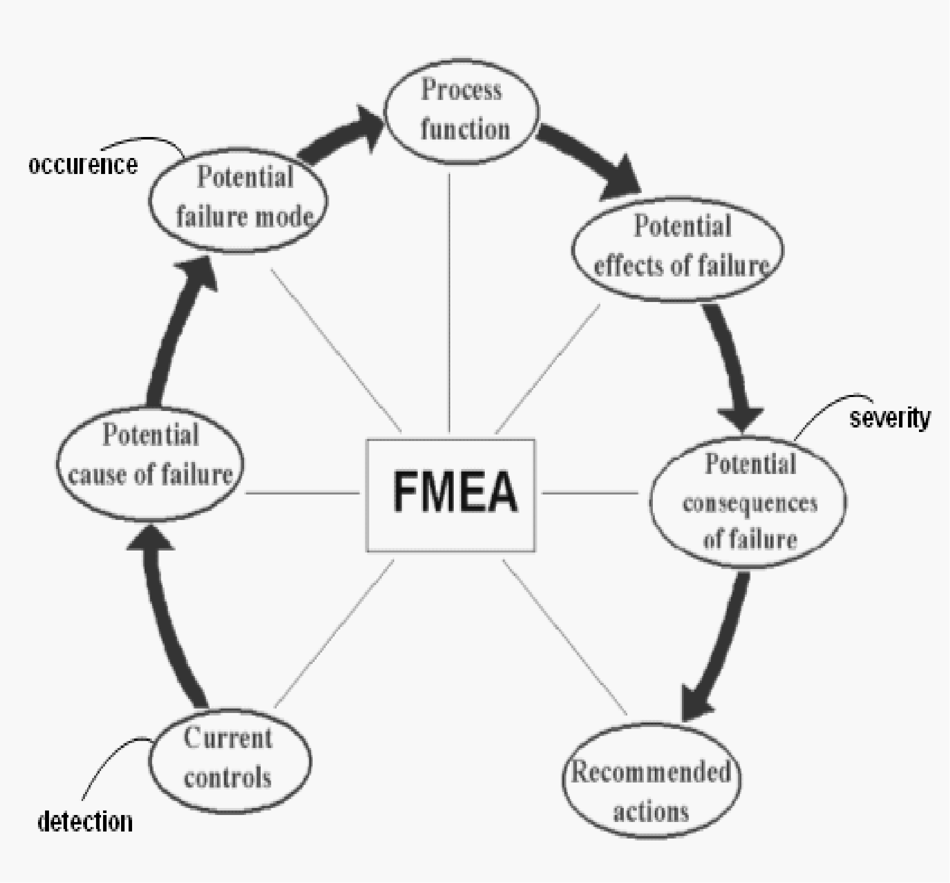


Figure 1: Main phases of FMEA

The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones. Failure modes and effects analysis also documents current knowledge and actions about the risks of failures, for use in continuous improvement. FMEA is used during design to prevent failures. Later it's used for control, before and during ongoing operation of the process. Ideally, FMEA begins during the earliest conceptual stages of design and continues throughout the life of the product or service.
FTA(FaultTreeAnalysis): Fault Tree Analysis (FTA) is a popular and productive hazard identification tool. It provides a standardizeddiscipline to evaluate and control hazards. The FTA process is used to solve a wide variety of

problems rangingfrom safety management issues. This tool is used by the professional safety and reliability community to bothprevent and resolve hazards and failures. Both qualitative and quantitative methods are used to identify areas in a system that is most critical to safe operation. Either approach is effective , the output is a graphical presentation providing technical and administrative personnel with a map of "failure or hazard" paths. FTA symbols are shown in below figur2.

The procedural steps of performing a FTA are:

1. Assume a system state and identify and clearly document state the top level undesired event(s).
2. Develop the upper levels of the trees via a top down process. That is determining the intermediate failures an combinations of failures or events that are the minimum to cause the next higher level event to occur. The logical relationships are graphically generated as described below using standardized FTA logic symbols.
3. Continue the top down process until the root causes for each branch is identified and/or until further decomposition is not considered necessary.
4. Assign probabilities of failure to the lowest level event in each branch of the tree.This may be through predictions,allocations, or historical data.
5. Establish a Boolean equation for the tree using Boolean logic and evaluate the probability of the undesired top level event.
6. Compare to the system level requirement. If the requirement is not met, implement corrective action.Corrective actions vary from redesign to analysis refinement.

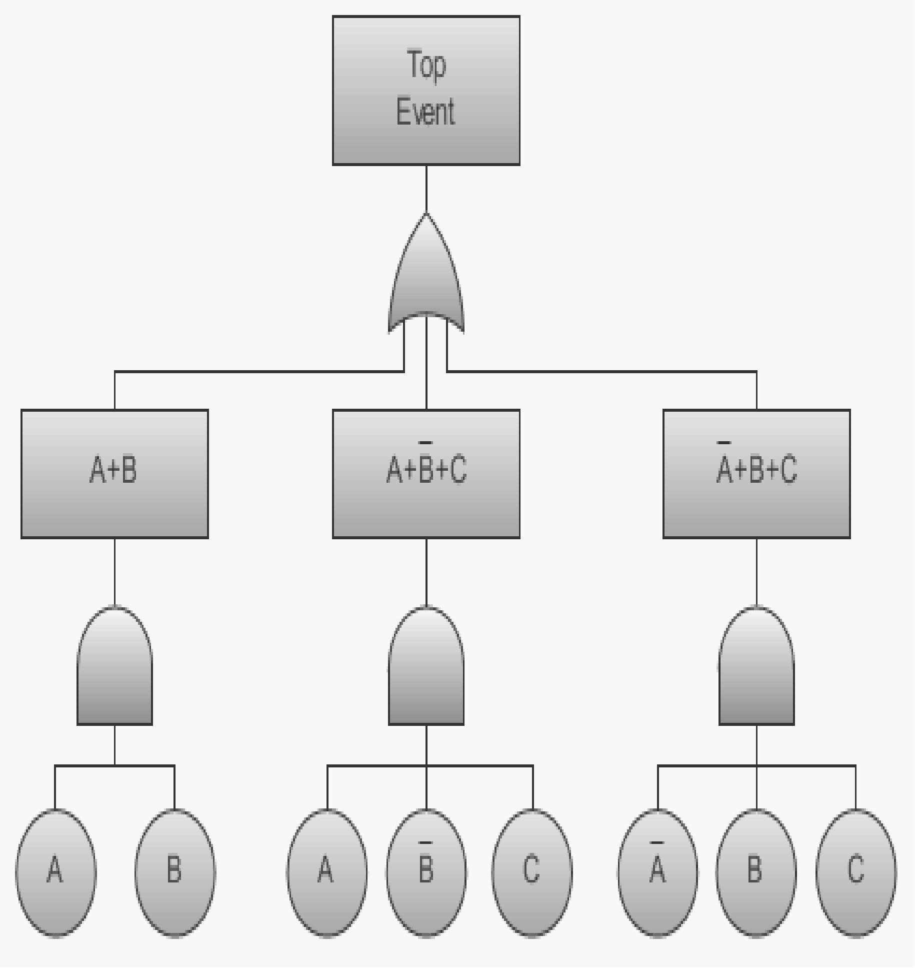


Figure 2: Example of FTA

III. CASE STUDUY: ADAPTIVE CRUISE CONTROL

Adaptive Cruise Control(ACC) is an automotive feature that allows a vehicle's cruise control system to adapt the vehicle's speed to the traffic environment. A radar system attached to the front of the vehicle is used todetect whether slower moving vehicles are in the ACC vehicle's path [4]. If a slower moving vehicle is detected,the ACC system will slow the vehicle down and control the clearance, or time gap, between the ACC vehicle and the forward vehicle [5]. If the system detects that the forward vehicle is no longer in the ACC vehicle's path, the ACC system will accelerate the vehicle back to its set cruise control speed. This operation allows the ACC vehicle to autonomously slow down and speed up with traffic without intervention from the driver [6]. The method by which the ACC vehicle's speed is controlled is via engine throttle control and limited brake operation.

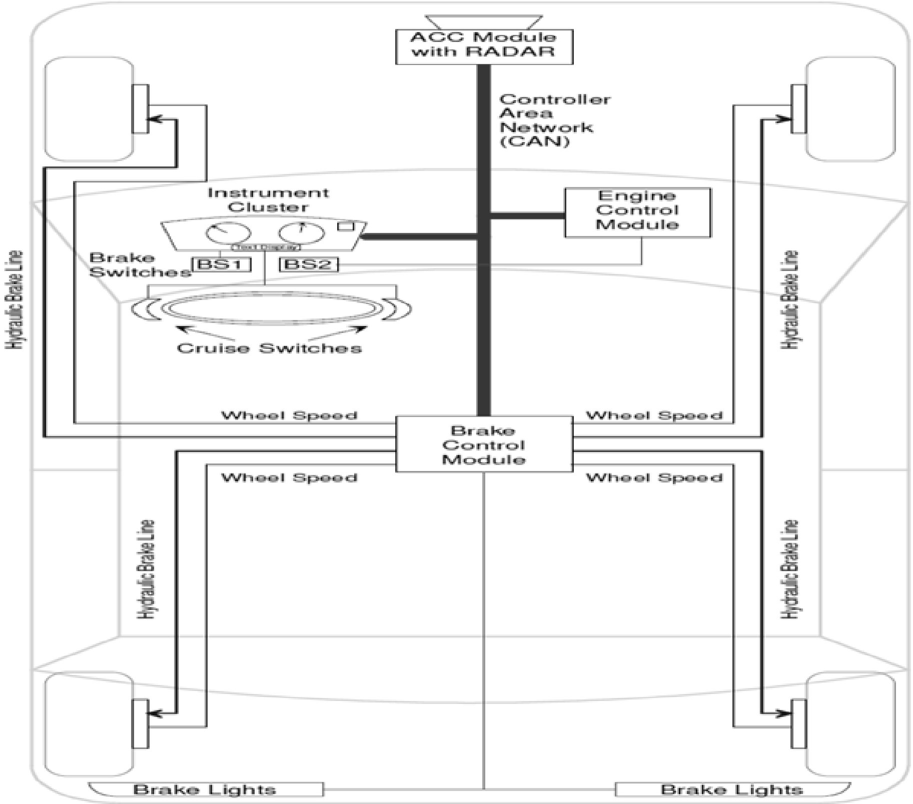
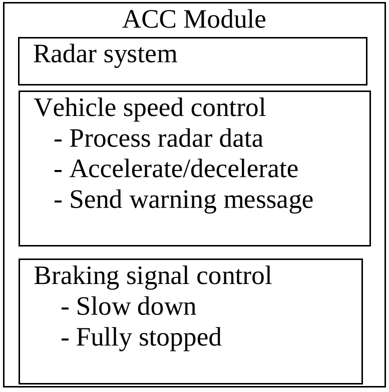


Figure 3: Physical layout of Adaptive Cruise Control System

As shown in Figure 3, the ACC system consists of a series of interconnecting components and systems.The methodof communication between the different modules is via a serial communication network known as the Controller Area Network (CAN).The ACC module is shown in Figure 4.



ACC Module

Radar system

Vehicle speed control
- Process radar data
- Accelerate/decelerate
- Send warning message

Braking signal control
- Slow down
- Fully stopped

Figure 4: ACC Module Functions

ACC Module – The primary function of the ACC module is to process the radar information and determine if a forward vehicle is present. When the ACC system is in 'time gap control', it sends information to the Engine Control and Brake Control modules to control the clearance between the ACC Vehicle and the Target Vehicle. The Functions in the ACC are Radar signal, vehicle speed signal and braking signal. The Radar signal transmits the radar information to all interconnecting components and systems.

Engine Control Module – The primary function of the Engine Control Module is to receive information from the ACC module and Instrument Cluster and control the vehicle's speed based on this information. The Engine Control Module controls vehicle speed by controlling the engine's throttle.

Brake Control Module – The primary function of the Brake Control Module is to determine vehicle speed via each wheel and to decelerate the vehicle by applying the brakes when requested by the ACC Module. The braking system is hydraulic with electronic enhancement, such as an ABS brake system, and is not full authority brake by wire.

Instrument Cluster – The primary function of the Instrument Cluster is to process the Cruise Switches and send their information to the ACC and Engine Control Modules. The Instrument Cluster also displays text messages and telltales for the driver so that the driver has information regarding the state of the ACC system.

CAN – The Controller Area Network (CAN) is an automotive standard network that utilizes a 2 wire bus to transmit and receive data.

Cruise Switches –The Cruise Switches are mounted on the steering wheel and have several buttons which allow the driver to command operation of the ACC system. The switches include:

'On': place system in the 'ACC standby' state
'Off": cancel ACC operation and place system in the 'ACC off' state

The driver interface for the ACC system is very similar to a conventional cruise control system. The driver operates the system via a set of switches on the steering wheel. The switches are the same as for a conventional cruise control system except for the addition of two switches to control the time gap between the ACC vehicle and the target vehicle. In addition there are a series of text messages that can be displayed on the instrument cluster to inform the driver of the state of the ACC system and to provide any necessary warnings. The driver engages the ACC system by first pressing the ON switch which places the system into the 'ACC standby' state. The driver then presses the Set switch to enter the 'ACC active' state at which point the ACC system attempts to control the vehicle to the driver's set speed dependent upon the traffic environment. When the ignition key is in the off position, no power is applied to any of the systems.When the key is cycled to the on position, the ACC system initializes to the 'ACC off' st ate.

IV. FAILURE MODE AND EFFECT ANALYSIS (FMEA) OF ADAPTIVE CRUISE CONTROL

FMEA is a bottom up technique used to identify, prioritize, and eliminate potential failures from the system, design or process. The failures of Adaptive Cruise Control (ACC) using FMEA method are listed in Table I.

TABLE I: FMEA of Adaptive Cruise Control(ACC)

ACC Part	Failure Mode	Effects	Cause
Radar	Electrical components failure	sensor output equal to the maximum or minimum of that sensor	Due to hardware failure
	Induced Noise	random variations superimposed on the desired echo signal received in the radar receiver	Reflected signals decline rapidly as distance increases. so noise induces a radar limitation
	Clutter Effect	serious performance issues with radar systems	caused by a long radar waveguide between the radar transceiver and the antenna
Speed Sensor	Power supply to sensor system fails.	No measurement of input signal	Wire defect.
	Crucial electronic components	Incorrect output (e.g. integration might be incorrect).	Due to hardware failure
Brake Sensor	Braking Signal	may result into Accidents.	Delaying (late/Early braking Signals

V. FAULT TREE ANALYSIS (FTA) OF ADAPTIVE CRUISE CONTROL

FTA is a top-down failure analysis used for discovering the root causes of failures or potential failures. A radar system attached to the front of the vehicle is used to detect whether slower moving vehicles are in the ACC vehicle's path. If a slower moving vehicle is detected, the ACC system will slow the vehicle down and control the clearance, or time gap, between the ACC vehicle and the forward vehicle. The radar data is passed to the ACC module and ACC module passes the required signals to each interconnected components and subsystems. The failures that are occurred in the radar are represented using Fault Tree Analysis (FTA) shown in Figure 5.

For the radar sensor the failed state is described as "Radar Sensor failure". The next step was to determine how to further expand on this failure. Three separate events, connected by the logic gate "OR" re-express the failure: Electrical component failure, Radar clutter failure , and Noise failure. The primary fault is defined as a defect internal to the sensor, most likely occurring with the electrical components. The resulting outcome of any electrical component failure is a sensor output equal to the maximum or minimum of that sensor. The secondary fault can be expressed as "Radar Sensor Failure due to environmental clutter". The intermediate event of "Radar Sensor Failure due to environmental clutter" can be described by two intermediate events and an undeveloped event. The Radar Failure due to corrosive effects is an attempt to describe the sensor performance near the ocean or any environment where corrosive agents are in the air and can possibly affect the integrity of the electrical components and lead to degradation.

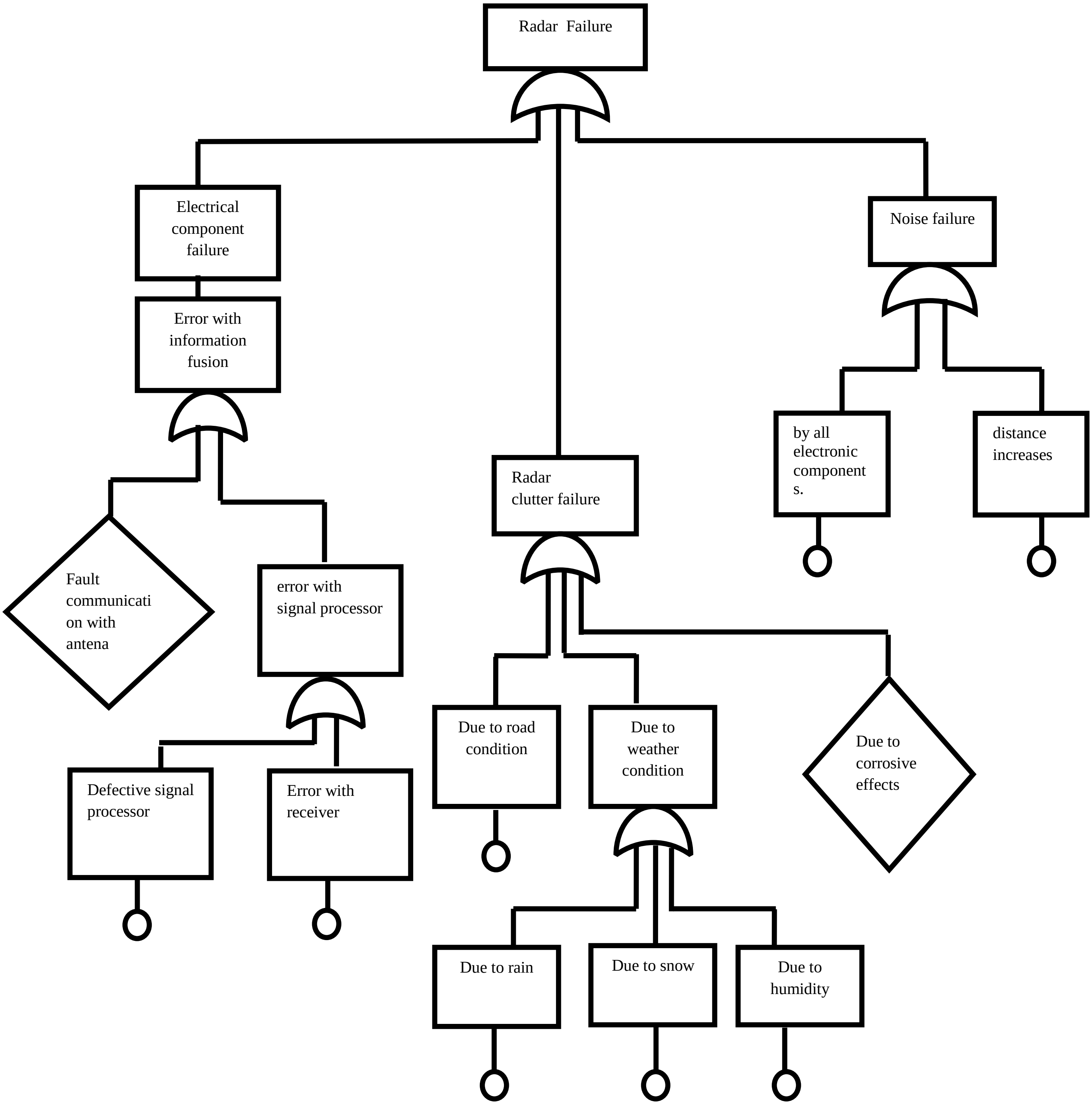


Figure 5: Fault Tree of Radar Failure

This event cannot be described further and is therefore considered an undeveloped event. Clutter refers to radio frequency (RF) echoes returned from targets which a e uninteresting to the radar operators. Such targets include natural objects such as ground, sea, precipitation (such as rain, snow or hail), sand storms, animals (especially birds), atmospheric turbulence, and other atmospheric effects, such as ionosphere reflections, meteor trails, and three body scatter spike. Clutter may also be returned from man-made objects such as buildings and, intentionally, by radar counter measures such as chaff. The third fault is Signal noise, it is an internal source of random variations in the signal, which is generated by all electronic components. Reflected signals decline rapidly as distance increases, so noise introduces a radar range limitation. The noise floor and signal to noise ratio are two different measure of performance that impact range performance. Reflectors that are too far away produce too little signal to exceed the noise floor and cannot be detected. Detection requires a signal that exceeds the noise floor by at least the signal to noise ratio. Noise typically appears as random variations superimposed on the desired echo signal received in the radar receiver. The lower the power of the desired signal, the more difficult it is to discern it from the noise. Noise figure is a measure of the noise produced by a receiver compared to an ideal receiver, and this needs to be minimized. The failures of speed sensor using FTA is shown in Figure 6.

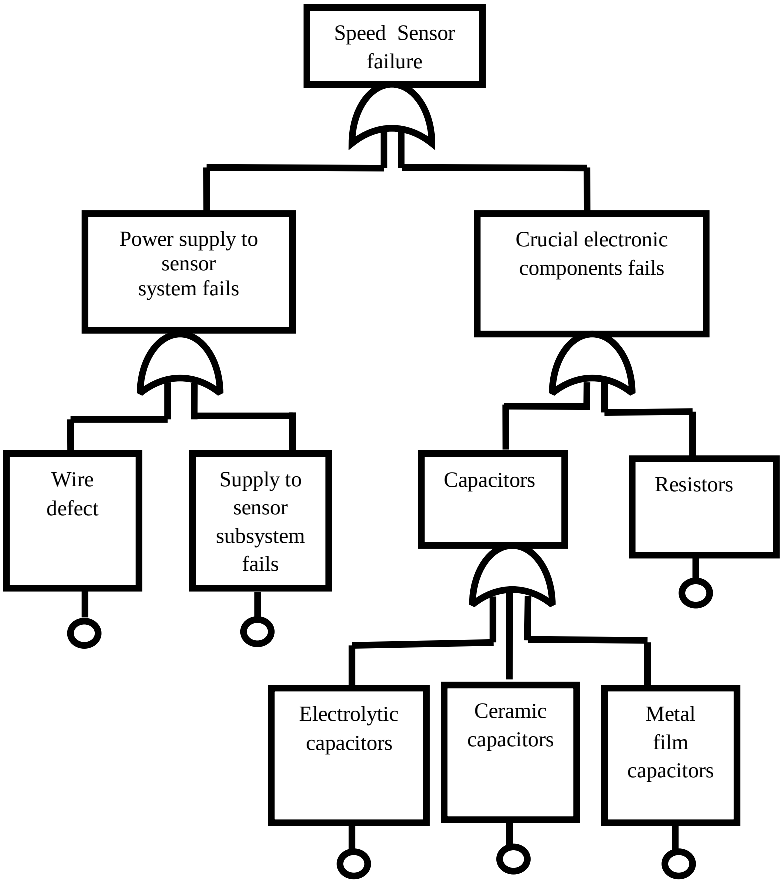


Figure 6: Fault Tree of Speed Sensor

The Vehicle Speed sensor measures transmission output or wheel speed. The speed sensor faulted due power supply to sensor system fails and also faults in the crucial electronic components. When wiring of the speed sensor was defect then there is no power supply to sensor and also subsystems connecting to the sensors fails. The crucial electronic components of any sensor are resistors, electrolytic capacitors, ceramic capacitors, metal film capacitors, power MOSFETs. Failure of these components leads to sensors failure which in turn causes catastrophic problems when these sensors used in critical application. Sudden component failure generates enough heat due to fault current to damage and carbonize the sensor's insulating material. This carbonization can lead to conduction between traces at different potentials and may cause sensor to fail.

***Recommendation To Designer**:*

To overcome radar sensor failures:

a) Radar sensor is failed due to failures of Electrical components , induced noise and clutter effects. The clutter effects are occurred due change in weather condition and road condition. So components used in the radar should be resistible to weather condition and road condition. The electrical components used in the radar should re liable and properly worked.

b) The radar sensor in the front shall detect small objects (e.g. a motorcycle) or a vehicle driving far off center. An extra radar sensor should be added in the back of the vehicle to detect the speed and distance of vehicles behind.

To overcome speed sensor failures:

a) Placing components strategically can help limit damage to the sensors when components fail thermally or heat due to large amounts of power dissipation.
b) Robust design for environmental stresses is needed.
c) Components that generate heat should be placed away from fault sensitive parts such as the power
d) supply or input
e) Components that may fail exothermically, such as power FETs can be strategically placed such that a failure does not propagate beyond the component.

VI. CONCLUSION

Adaptive Cruise Control system was developed for the purposes of driving safety and comfort. It reduces the number of brake and switch operations that are required of the driver. As a result, the system reduces the driving burden so that the driver can drive in comfort. This paper has investigated the possible failures in Adaptive Cruise Control (ACC) system using FMEA and FTA in the failure analysis of safety-critical system. We have identified the failures that commonly occur in the working of the Adaptive Cruise Control (ACC) system. The failures parts in the ACC system are radar failures, speed sensor failures and brake sensor failures. The effects and causes of these ACC parts are identified by using Failure Mode Effective Analysis(FMEA) and root causes of these failures are analyzed by using Fault Tree Analysis(FTA). The combined results of FMEA and FTA provide input for analysis of temporal or causal justification for prioritization of verification or validation test systematic approach from system down to subsystem

.

ACKNOWLEDGEMENT

Thanks are due to AICTE, New Delhi. The research presented in this paper is supported by AICTE-RPS Project sanctioned to Vignan's Institute of Information Technology (VIIT), Visakhapatnam, in July 2013 (Ref.No:20/ AICTE/ RIFD/RPS(Policy-1) 49/2013-14) with Dr. M. Ben Swarup as Principal Investigator.

REFERENCES

[1] International Electrotechnical Commission. Analysis Techniques for System Reliability Procedure for Failure Mode and Effects analysis (FMEA), IEC 60812, 1991.

[2] Flex Redmil, Tom Anderson "*Current Issues in Safety-Critical Systems*" , Bristol, UK February 4, 2003.

[3] Sommerville, Ian. Software Engineering.Boston: Pearson .ISBN 0-13705346-0, 2011.

[4] H. Soma, Y. Shiraishi, T. Watanabe, Y. Takada, and Y. Takae, "Trust in low speed adaptive cruise control syms analysis of trust structure," *Review of Automotive Engineering*, vol. 26 no.2, pp. 211-212, 2005

[5] I. K. Moon and K. S. Yi, "Vehicle tests of a longitudinal control law for application to stopand go cruise control," *KSME International Journal*, vol. 16, no.9, pp.1166 - 1174, 2002

[6] G.N. Bifulco, F. Simonelli, R.D. Pace, Experiments toward an human like adaptive cruise control, Proc. IEEE Intelligent Vehicles Symposium, Eindhoven, pp.919 - 924, 2008.