ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Software Failure Analysis of Brake-By-Wire Automotive Safety Critical System using FMEA, FTA and MATLAB Techniques

Dr. M. Ben Swarup[1], **B. Hari Prasad**[2]

Dept. of Computer Science & Engg., Vignan's Institute of Information Technology, Duvvada, Visakhapatnam, India[1,2]

Abstract: Safety critical systems are those systems whose failure could result in loss of life, significant properity damage, or damage to the environment. In cars we have common Braking System. The braking system like mechanical and hydraulic braking systems. The replacement of traditional mechanical and hydraulic control systems with electronic control devices or electronic components. The electronic braking system is known has Brake-By-Wire system. Brake-by-wire (BBW) technology in automotive industry is the ability to control brakes through electrical means. The increasing usage of brake-by-wire system in the automotive industry has provided manufacturers with the opportunity to improve both vehicle and manufacturing efficiency. In developing safety Brake-By-System for the automotive industry, potential hazard analysis techniques have to be applied to identify potential failure modes. The commonly used safety analysis techniques are FMEA (Failure Mode Effect Analysis) and FTA (Fault Tree Analysis). The basic design constraint for this application is we are considering the speed of the vehicle, frontal distance of the car and Brake pressure as an input to the application. Considering all these inputs we are calculating the Minimum Brake pressure car. The pressure value convert to electrical signal by VCU, It can transfer to Brake Control Unit(BCU). The Brake Control Unit perform to applied particular pressure to each Wheel that time the vehicle can stop. If the pressure value crosses the Within range value then the System is give a alert message. The purpose of this paper is to discuss Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) based safety-critical approach towards to development of Brake-By-Wire system from a safety perspective. At the same time the safety critical Brake-By-Wire system is simulated in MATLAB to provide safety to the system with Transmission Controller.

Keywords: Safety critical system, safety analysis, failure analysis,, FMEA, FTA

I. INTRODUCTION

Safety critical systems are those systems whose failure could result in loss of life, significant properity damage, or damage to the environment [1]. In safety critical systems, the most important emergent property is its dependability. The term dependability was proposed by Laprie (1995) to cover the related system attributes of availability, reliability, safety and security. The cost of critical system failure is high because trusted methods and techniques must be used for software development.

The system components where critical system failure may occur are:

- **Hardware failure**: It may fail because of its design and manufacturing errors.
- **Software failure**: Software fails due to errors in its specification, design or implementation.
- **Operational failure**: Human operators may operate the system incorrectly.

In FMEA, a team of trained engineers of system designers analyses the cause consequences relationships of component failures on system hazards[2].The role of software has becoming increasingly important and is being use in many critical applications, such as avionics, vehicle control systems, medical systems, manufacturing, and sensor networks. Although it is logical to invert more in the failure analysis of safety critical systems, in general an in-depth failure analysis of any given system will reduce manufacturing cost that may be incurred at following development phases: Design, impl ementation, and post implementation. According to Haapa nen and Helminen[3], the failure modes of the constituent components of mechanical and electrical systems are normally well understood. This is because the reasons for failures are known and their sequences may be studied; some of these reasons are wear, aging and unanticipated stress. However, this does not suggest that the failure analysis of such systems is always easy, but in essence is straight forward. In contrast, the failure modes of software for software-based systems are generally unknown. Software engineering does not only advocate for the development of software that meet user requirement but also one which is dependable as is the case for safety-critical systems[4]. In this case take one case study is Brake-By-Wire System.

This paper investigates the software failure analysis of Brake-By-Wire System Using FMEA And FTA Safety Analysis methods,.

The rest of this paper is organized as follows: section 2 describes the Brake-By-Wire System Architecture section 3describes Safety Analysis of Brake-By-Wire critical system, section 4 describes the MATLAB Simulink Techniques. Section 5 presents simulated results of Brake-By-Wire system and the final section concludes this paper.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

II. DESCRIPTION OF BRAKE-BY-WIRE SYSTEM ARCHITECTURE

Brake-By-Wire technology in automotive industry is the ability to control brakes through electrical means. Brake-By-Wire technology in automotive industry represents the replacement of traditional components such as the pumps, hoses, fluids, belts and vacuum servos and master cylinders with electronic sensors and actuators. The Brake-By-Wire (BBW) system in the context of automotive systems refers to the concept where mechanical or hydraulic system is replaced by electric/electronic systems. The electric/electronic systems are computer controlled and hence are made up of embedded software. Two types of brake by wire systems exist, the wet brake by wire and the dry brake by wire system [5].

The challenge of computer controlled systems is that they introduce new modes of failure that is unfamiliar in hardware failure analysis. To demonstrate the software failure analysis of the BBW, BBW is first introduced and then its user level software design is presented from where the analysis is conducted. The BBW is designed to increase the quality of braking by reducing the stopping distance. The simple form of the BBW is as shown in Figure 3 and is described as follows. The BBW consists of a central controlling unit known as vehicle control unit (VCU) and one brake control unit (BCU) per wheel. The VCU reads as input the braking pressure applied on the brake pedal. It then processes this pressure to send signal to each BCU about the amount of braking pressure to be applied on the respective wheels. Each BCU further processes this signal taking into account wheel conditions in order to establish the needed amount of braking pressure. One of environmental advantages or friendliness of the BBW is that no braking fluid is necessary [5,6].

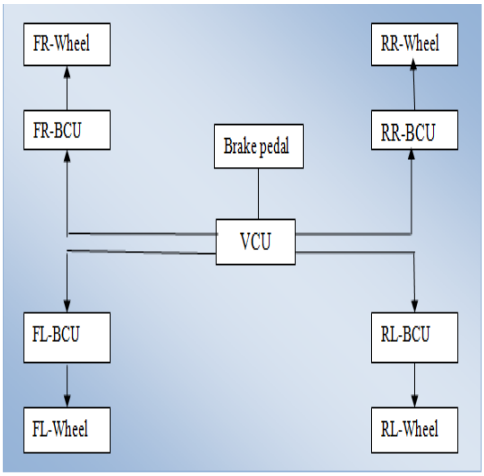

Figure 2.1: Block Diagram Of Brake by Wire System

Where: FL-Wheel refers to front left wheel
FR-Wheel refers to front right wheel
RL-Wheel refers to rear left wheel
RR-Wheel refers to rear right wheel
FL-BCU refers to front left wheel brake control unit
FR-BCU refers to front left wheel brake control unit
RL-BCU refers to front left wheel brake control unit
RR-BCU refers to front left wheel brake control unit

III. SAFETY ANALYSIS OF BRAKE-BY-WIRE SYSTEM

In this system we can perform software failure analysis using Failure Mode Effect Analysis (FMEA) and Fault Tree Analysis (FTA) Techniques.

3.1. Failure Mode and Effect Analysis of Brake-By-Wire (BBW) System:

FMEA is a Safety technique used to identify, prio ritize, and eliminate potential failures from the system, de sign or process. To analyses the BBW system, this paper defines a system failure mode referred to as braking failure.

To this effect braking failure would mean that one of the following events occurs when the brake is applied:
(i) Vehicle stops too early
(ii) Vehicle stops too late
(iii) The brake system fails to deliver its function implying brake failure as explained earlier.

Table 1 mentions some system failure modes related to braking system.

TABLE 1 : Software FMEA of Brake-By-Wire

System Failure Mode: *Braking Failure*			
S.NO	Entity	Failure Mode	System Effect
1.	Driver	Brake not applied – i.e. omission of input	Vehicle cannot Stop
2.	Brake Brake	Low Pressure Input	Vehicle can Stop too late
		High Pressure Input	Vehicle can Stop too early
		Omission of input Value	Vehicle cannot Stop
3.	Brake Control Unit (BCU)	Invalid input(Out of Range)	High or Low Retardation
4.	Vehicle Control Unit (VCU)	Invalid input(Out of Range)	High or Low Retardation

The Brake-By-Wire System contains some failure modes are Brake pressure, Vehicle Control Unit (VCU) and Brake Control Unit (VCU). These failures are reduced by using Sensors.

3.2. Fault Tree Analysis:

Fault tree developed in the aerospace industries, but have found uses in many areas, most recently software analysis. Fault trees operate by developing a list of the faults that can occur in a system, and attempting to trace them back to their root causes. The reason that they are called fault trees, is that there is a tree like formal notation that accompanies the analysis, in which different types of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

events are specified by differently shaped containers, and the events are linked logically in tree like structures to lead up to the eventual fault of the system. While this method can be used to show complicated interactions, it is still subject to the danger of over looking aspects of the system as these are mostly enumerated.

In Brake-By-Wire System We can perform the Fault tree analysis. In this case failures are occurred at low level to high level. The braking System failure may depend on the low level failure to high level failures.

Brake failure depends on some failure modes like Driver, Brake pressure, VCU, and BCU .in this case driver not applied the brake that may be cause of brake failure.

The brake pressure failure may be depend on the High pressure, Low pressure and omission of invalid input pressure. The VCU and BCU are may be failure depend on input value. Any one of failure occurred at low level to high level that time entire system is failure, this failure is cause of accidents.

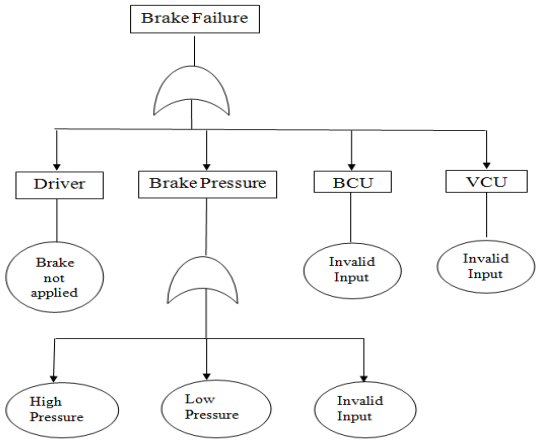

Figure 3.2: Fault Tree Analysis of BBW System

IV. MATLAB DESCRIPTION

MATLAB is the main software used for computation, model implementation, and simulation.The MATLAB simulation tool Simulink, Which is used for modelling and simulating dynamics systems, has been playing a major role during this work.

MATLAB/Simulink is a high-level technical computing language and object oriented environment for algorithm development, data visualization, data analysis and numerical computation. MATLAB/ Simulink allows the development of a solution to technical computing problems faster than with traditional programming languages, such as C, C++ and FORTRAN.

The easy of development along with the extensive toolboxes and functions available were the major reasons for selecting MATLAB/ Simulink as the simulation environment. The Simulation environment starts as an overview of the implementation of the PID controller to the BBW (Brake By Wire)System. Next, we can maintain the look table and then perform the calculation of Throttle, Engine RPM and vehicle Speed of the model by using with Controller.

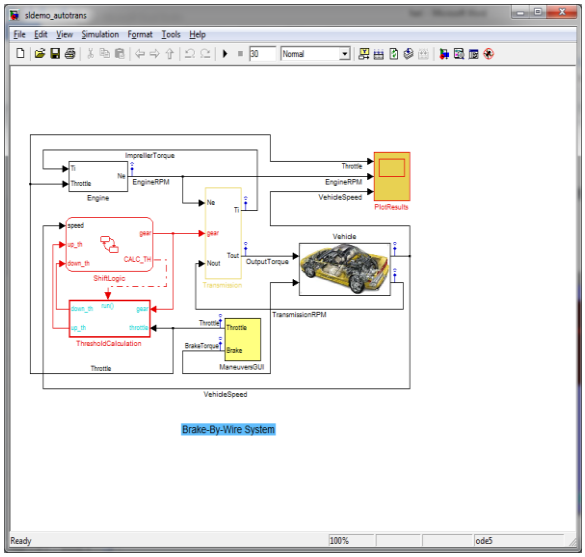

Fig: 4.1MATLAB Simulink model

V. SIMULATED RESULTS FOR BRAKE-BY-WIRE SYSTEM

Safety analysis methods are applied to the Brake-By-Wire(BBW) system to identify failure modes of BBW system. The safety analysis methods are failure mode effect analysis (FMEA) and fault tree analysis(FTA). By applying FMEA we identified the failure modes like Brake pressure failure, micro controller failure and basic switch failures. FTA is used to discover the root cause of the failure of speed sensor and microcontroller failure.

We now present the result of the application as with safety and without safety. These are tested by considering the inputs of the Brake-by-Wire system are Brake Pressure, speed of the vehicle, Brake Force and frontal distance of the vehicle.From these input file, The Vehicle control unit(VCU) calculate the Signal Noise ratio. The brake pedal signal parameters user interface as shown below

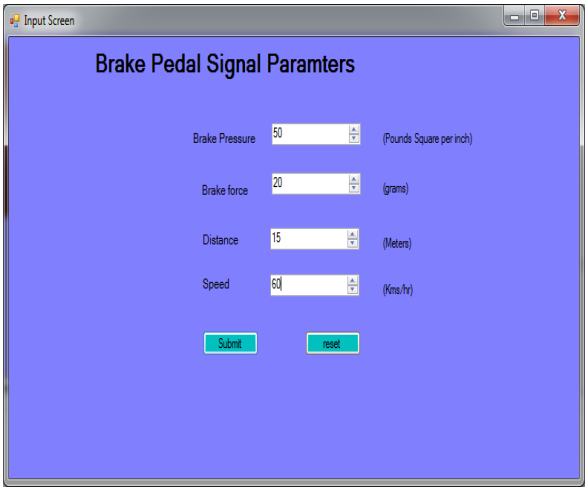

Fig 5.1: Brake pedal Signal Parameters

In this case the vehicle control unit(VCU) calculate the pressure value and moment value using brake pedal signal parameters.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

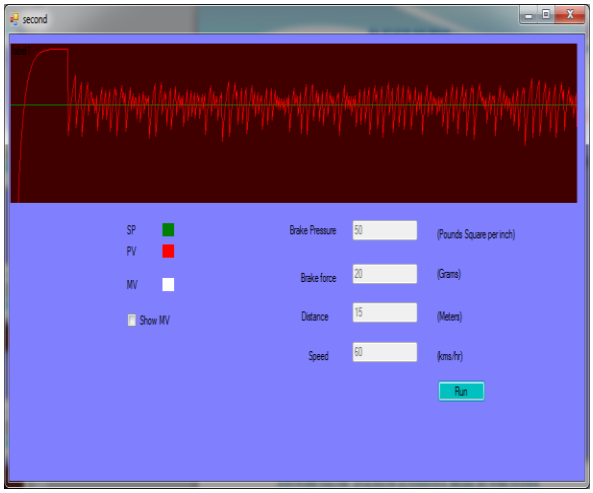

Fig 5.2: Result of Noise Signal Ratio

In this project, when the driver applied the brake pressure on the brake pedal. Brake pedal connected with sensor, here sensor take the inputs brake pressure , Brake force, speed and distance of front vehicle. The VCU take these brake pedal signal parameters then calculate the Minimum pressure and moment value. It then processes this pressure to send signal to each BCU about the amount of braking pressure to be applied on the respective wheels. Each BCU further processes this signal taking into account wheel conditions in order to establish the needed amount of braking pressure. Then that time vehicle was stopped.

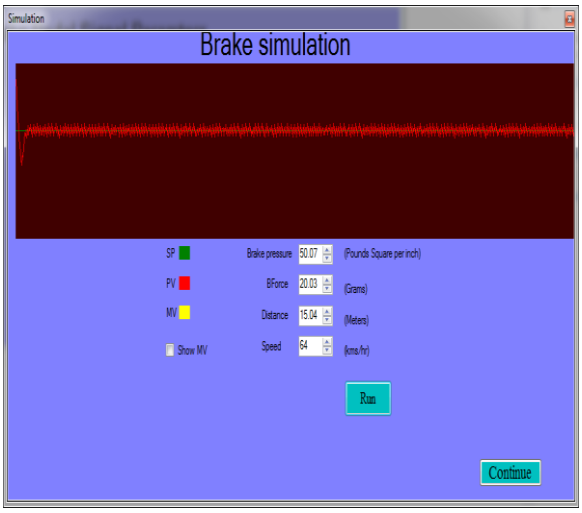

Fig 5.3 : Brake Simulation Result

Brake-By-Wire System is ability to control the vehicle through electrical means. It is designed for standard alone braking system. Brake By Wire System was developed for the purposes of driving safety and comfort. It reduces the stopping distance. The entire braking system was simulated in MATLAB Simulink using Some brake signal parameters.

In this model, we use the three modules there are Threshold calculation, Shift logic and engine. In GUI ,system was take the throttle and brake torque. Threshold calculation take that throttle value calculate the throttle _up and throttle _in values.

These values pass to the Shift logic, here calculate gear and speed. These inputs pass to transmission control. Transmission control can maintain in look_up table.
In look_up Table we maintain the gears and speed values. The System can be depend upon these values the vehicle can stop particular distance.Brake By Wire System was developed for the purposes of driving safety and comfort. It reduces the stopping distance.

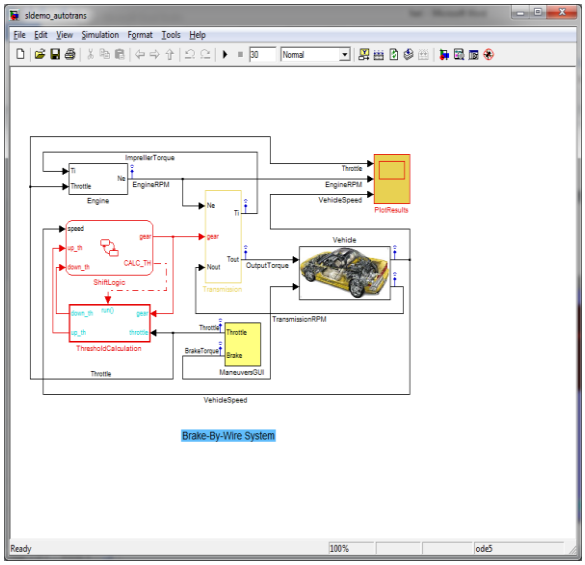

Fig 5.4: Model For Brake-By-Wire System

Plot results:
After you import data into the MATLAB® workspace, it is a good idea to plot the data so that you can explore its features.
An exploratory plot of your data enables you to identify discontinuities and potential outliers, as well as the regions of interest.
The MATLAB figure window displays plots. See Types of MATLAB Plots for a full description of the figure window. I
t also discusses the various interactive tools available for editing and customizing MATLAB graphics.

Load and Plot Data from Text File
This example uses sample data. The file consists of three sets are Throttle, Engine RPM and Vehicle speed. In this result contains three plot results. In this diagram contains X-axis as Time and Y-axis as speed, Engine RPM and Speed of the vehicle.
When the vehicle travel at 80km/ that time driver applied the brake the vehicle reduce the throttle value in 5seconds gradually stop the vehicle within 30 seconds. The vehicle speed starts at zero and the engine at 1000RPM.
The Engine RPM increases up to 4000 RPM at 80km/hr. when brake applied the Engine RPM reduces at 8 seconds the vehicle can stop within 30 seconds.
The Vehicle speed increases up to 80km/hr. when brake applied the the Vehicle speed reduces at 10 seconds the vehicle can stop within 30 seconds.
This process is shown in graphical representation.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

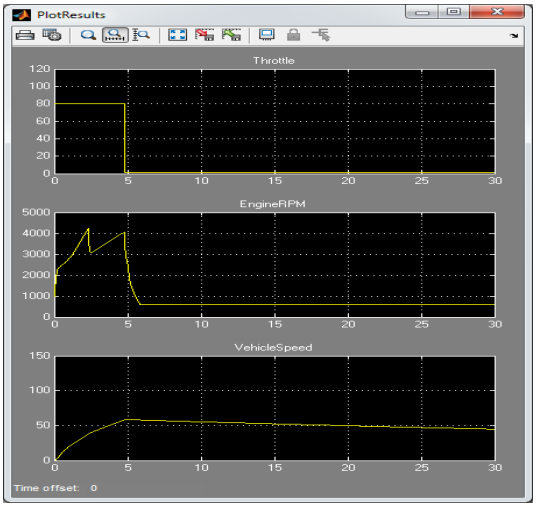

Fig : 5.4 plot results for Brake-By-Wire System

VI. CONCLUSION

This project is mainly focused on providing safety to the occupant in case of critical crash. Brake By Wire System was developed for the purposes of driving safety and comfort. Airbag system is a vehicle safety device designed to protect occupant from accidents. Although Brake-By-Wire system saves lives in crash situations. In this system we perform the software failure analysis.The safety analysis methods are failure mo de and effect analysis (FMEA) and fault tree analysis (FTA). The failures are identified and analysed to detect root cause of the hazard. 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. These values were given as inputs to sensor, depending upon the Brake pressure, speed, frontal distance of the car and Brake Force value. The vehicle controller (VCU) take these inputs and calculate the minimum pressure value. The Pressure value applied to each wheel by Brake control unit (BCU) then the vehicle stop at particular distance within time. The Results of this safety Brake-By-Wire system has simulated using C# with Window Forms and MATLAB-Simulink.

ACKNOWLEDGMENT

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, inJuly 2013(Ref.No:20/ AICTE/ RIFD/RPS(Policy-1) 49/2013-14) with **Dr. M. Ben Swarup** as Principal Investigator.

REFERENCES

[1] Shawulu Hunira Nggada,"Software Failure Analysis at architectural using FMEA", International Journal of Software Engineering and Its Applications,Vol.6.no.1,January,2012.

[2] P.Haapanen, and A.Helminen, "Failure mode and Effects Analysis of Software based Automation Systems",STUK YTO TR190,Helsinki,2002,Available:http://www.fmea infocentre.com/handbooks/softwarefmea.pdf, Accessed: (2011)July

[3] N. Leveson, "A New Accident Model for Engineering Safer Systems", Safety Science (2004) Vol.42,No.4, pp. 237-270 .

[4] Hoseinnezhad,R.Bab Hadiashar, A.," Fusion of redundant information in brake by wire systems, using a fuzzy Voter" (http:/ /www.isif.org/ 2075D04.pdf) (2006), Journal of Advances in Information Fusion (JAIF), Volume 1, Issue 1, pp. 35–45.

[5] P.Sinha, "Architectural Design and Reliability Analysis of a Fail Operational Brake by Wire System from ISO 26262 Perspectives", Reliability Engineering & System Safety, Vol.96, Issue 10 (2011)pp. 1349-1359

[6] H.T.Dorissen, K. Dürkopp, "Mechatronics and Drive by Wire Systems Advanced Non contacting Position Sensors", Control Engineering Practice, Vol. 11, Issue 2 (2003) pp. 191-197

[7] C.Wilwert,N. Navet,Y.Q.Song, and F. SimSonot Lion, "Desig n of automotive X by Wire sys tems," in the Industrial Co mmunication Techno logy Handbook, R Zurawski, Ed. Boc a Raton, FL: CRC