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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

FMEA-based Failure Analysis of Brake-By-Wire Automotive Safety-Critical System

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

Department of Computer Science and Engineering, 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 properityda mage, or damage to the environment. Brake-by-wire (BBW) technology in automotive industry is the ability to contr ol brakes through electrical means. It can be designed to supplement ordinary service brakes or it can be a standalone brake system. The increasing usage of brake-by-wire system in the automotive industry has providedma nufacturers with the opportunity to improve both vehicle and manufacturing efficiency. The replacement of traditional mechanical and hydraulic control systems with electronic control devices presents different potential vehicle-level safety hazards than those presented by conventional braking system. The purpose of this paper is to discuss Failure Modes and Effects Analysis (FMEA) based safety-critical approach towards to development of brake-by -wire 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. The FMEA investigates failure of each entity of the BBW design component.

Keywords: safety critical system, safety analysis, failure analysis, hazard analysis, FMEA

I. INTRODUCTION

Safety can be defined as freedom from accidents or losses, In a safety critical system failure can lead to significant economic losses, physical damage or threats to human life [1]. There are three main types of critical systems (i) safety critical systems (ii)mission critical systems (iii) business critical systems. 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 applica-tions, 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, implementation, and post-implementation. According to Haapanen 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 straightforward. 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. This paper investigates the failure analysis of software at its architecture level by employing a traditional failure analysis technique used for mechanical, electrical and electronic systems. The rest of this paper is organized as follows: section 2 deals with safety analysis, section 3describes the case study of brake by wire critical system, section 4 presents failure mode and effect analysis of brake by wire system and the final section concludes this paper.

II. SAFETY ANALYSIS

In safety-critical systems, we have to perform the safety analysis. Safety analysis is a method for evaluating the hazards and risks posed by a system and ways to minimize them. Hazard analysis is the first stage, in which the system is studied for situations in which potential harm could result, and the frequency with which those situations occur. Risk analysis is the second stage, in which the possible outcomes of the hazards and the frequency of appearance of each outcome is determined.

Hazard Analysis: A hazard is a situation in which there is actual or potential danger to people or the environment Hazard analysis, accordingly is a method for examining a system to examine how it can cause hazards to occur, and in some cases, how to prevent those hazards from occurring. While the actual techniques may vary in their approaches, they all have certain aspects in common.

Risk Analysis : Risk is a combination of the frequency or probability of a specified event, and its consequence. Risk analysis is the counter part to hazard analysis, taking a list of hazards and producing a list of possible outcomes and their likelihood of happening. The first part of risk analysis is an examination of the possible results of a hazard.

Available Tools and Techniques:There are many forms of safety analysis, and someof the major ones are discussed below. Some are useful tools or techniques, while others are designed to be comprehensive. All of the analytical methods listed below have been used to good effect in the past.
The following are the various safety analysis tools:

- Failure Mode Effective Analysis(FMEA)
- Fault Tree Analysis(FTA)
- Event Tree Analysis(ETA)

Failure Mode and Effects Analysis: Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects and Criticality Analysis (FMECA) function much like a checklist, only a more organized one. There is a standard form which must be filled out, in which each subsystem or component is listed, along with the different ways in which that particular component can fail. Once these failure modes have been listed, the effects of that failure are listed. In the criticality analysis, each failure mode is associated with a frequency, and each effect with a 'danger rating'. These numbers are used to provide some idea of exactly how much risk that failure mode places upon users or the environment. Once these have been collected, each failure mode has a possible protective measure listed with it. Criticality analysis adds a cost of protection number here. This provides a list of hazards, risks, and possible counter measures, and the criticality analysis orders them according to the level of danger they represent. The danger here is, again, that of leaving something out in the course of listing the possibilities. In practice the answers are searched in FMEA through an iterative analysis process, for which the main phases are illustrated in Fig.1.

The analysis process starts from the identification of the scope of the system and the functions the FMEA is to be applied on. The development process flowchart and design plans of the system are used to support the identification. After the subject for the FMEA is confirmed the next step is to identify the potential failure modes in a gradual way. The technique of brain storming has often proven to be a useful method for finding failure modes. In FMEA, a team of trained engineers of system designers analyses the cause consequences relationships of component failures on system hazards [4]. After having found such a relation, the occurrence probability of that hazard is computed. There exist so many different work sheets to support the brain storm procedure and the documentation of FMEA overall. In the following phases the effects and causes of potential failures are determined. So called cause and effect diagrams can be used to help in these phases.The final step is to document the process and take actions to reduce the risks due to the identified failure modes.

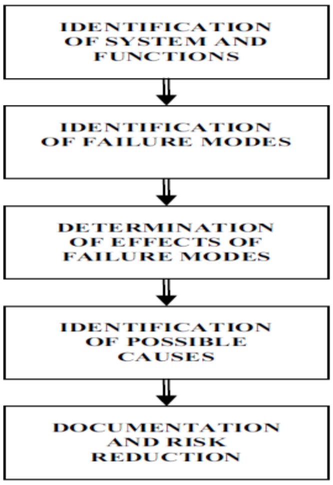

IDENTIFICATION OF SYSTEM AND FUNCTIONS
IDENTIFICATION OF FAILURE MODES
DETERMINATION OF EFFECTS OF FAILURE MODES
IDENTIFICATION OF POSSIBLE CAUSES
DOCUMENTATION AND RISK REDUCTION

Fig 1:Main phases of FMEA

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 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. An example is shown below [4].

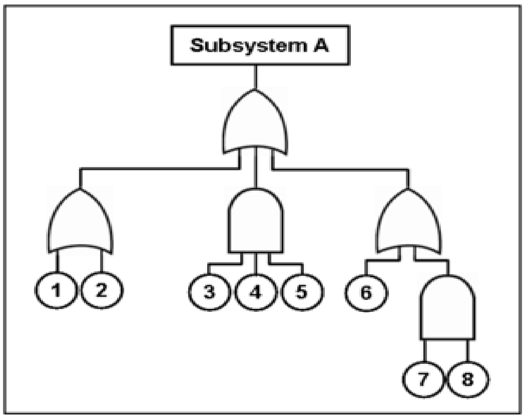


Fig 2:Example of Fault Tree Analysis

Event Tree Analysis: Event trees function similarly to fault trees, but in the opposite direction. An event tree attempts to enumerate a list of components and subsystems and determine the result of their operation or non operation. In this way all sequences of possible events are covered involving those components. An example is shown below in Fig.3.

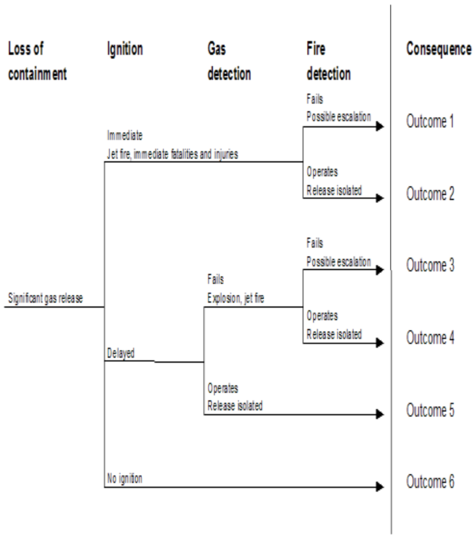


Fig: 3 Example of Event Tree Analysis

III. CASE STUDY : BRAKE-BY- WIRE CRIT ICAL SYSTEM

Brake By Wire(BBW) technology in automotive industry is the ability to control brakes through electrical means. It can be designed to supplement ordinary service brake or it can be a standalone brake system. 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. Drive by wire technology in automotive industry replaces the traditional mechanical and hydraulic control systems with electronic control systems using electromechanical actuators and human machine interfaces such as pedal and steering feel emulators [5]. Some x by wire technologies have been already installed on commercial vehicles such as steer by wire, and throttle-by-wire. Brake by wire technology is still under development by some automobile and automotive parts manufacturers industry worldwide and has not been widely commercialized yet [6].This is mainly due to the safety critical nature of brake products.

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 [7]. The electric/electronic systems are computer controlled and hence are made up of embedded software. Embed of software offers the possibility to introduce functions that were either originally impossible or costly with mechanical or hydraulic system components. It also reduces size and weight. However, with the brake by wire system still being new, a mechanical/hydraulic system may be used in conjunction with the brake by wire system. This can be used as a backup to strengthen safety measures.

Two types of brake by wire systems exist, the *wet brake by wire* and the *dry brake by wire* system [8]. The former is a combination of the electronic brake system and the hydraulic brake system as a backup while the latter represents systems consisting of electronic brake system where no master cylinder or hydraulic lines are needed and therefore there is no mechanical backup. Sequel to the focus of this paper on software failure analysis, the dry brake by wire system is used and subsequent references to brake by wire will imply the dry brake by wire system. 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 brake by wire system considered in this paper is similar to the one described in Wilwert et al [9]. 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 4 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 the environmental advantages of the BBW is that no braking fluid is necessary [8, 9].

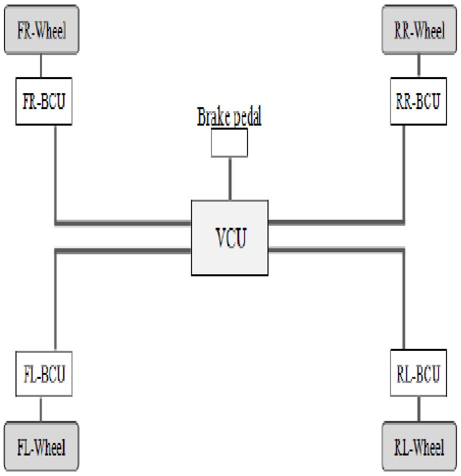


Fig 4: Simple Brake by Wire (BBW) System [9]

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

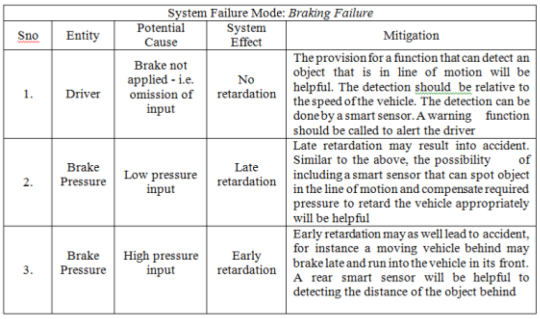
IV. FAILURE MODE AND EFFECT ANALYSIS OF BRAKE-BY-WIRE SYSTEM

To analyses the BBW system, this paper defines a system failure mode referred to as braking failure. It should be noted that this is different from brake failure in that the term brake failure may refer to the inability of the brake system to deliver its function on demand. 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 BBW



System Failure Mode: *Braking Failure*				
Sno	Entity	Potential Cause	System Effect	Mitigation
1.	Driver	Brake not applied - i.e. omission of input	No retardation	The provision for a function that can detect an object that is in line of motion will be helpful. The detection should be relative to the speed of the vehicle. The detection can be done by a smart sensor. A warning function should be called to alert the driver
2.	Brake Pressure	Low pressure input	Late retardation	Late retardation may result into accident. Similar to the above, the possibility of including a smart sensor that can spot object in the line of motion and compensate required pressure to retard the vehicle appropriately will be helpful
3.	Brake Pressure	High pressure input	Early retardation	Early retardation may as well lead to accident, for instance a moving vehicle behind may brake late and run into the vehicle in its front. A rear smart sensor will be helpful to detecting the distance of the object behind

The analysis shows that hardware design modifications could be informed by the result of software failure analysis, for instance the introduction of sensors. The analysis has also shown that functions required to prevent failure can be identified at the user level architecture. In a further design, these identified functions could be included in the class diagram of the system. In a typical system development environment, teams of engineers may be given different failure modes to work on where firstly each engineer within a team will work independently. Secondly a collective review and collation in each team is performed and thirdly the work of all teams is reviewed.

V. CONCLUSION

This paper has investigated the possibility of using FMEA in the failure analysis of safety-critical software systems by considering the case study of brake-by-wire (BBW) system which is a recent design consideration in the automotive industry. In both software and hardware systems, failure analysis should begin from the infancy stage of design through to completion stage. The analysis shows that the use of FMEA to analyzing software systems is possible and that results of the analysis such as mitigating interventions would reveal further design considerations to improve dependability of software systems.

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] Sommerville, Ian (2011). Software Engineering. Boston: Pearson. ISBN 0-13-705346-0.

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

[3] 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

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

[5] Hoseinnezhad, R., Bab Hadiashar, A., "Missing Data Compensation For Safety Critical Components In A Drive by wire system" (2005), IEEE Transactions on Vehicular Technology, Volume 54, Issue 4, pp. 1304–1311.

[6] 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.

[7] 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

[8] 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

[9] C.Wilwert,N. Navet,Y.Q.Song, and F. SimSonot Lion, "Design of automotive X by Wire systems," in the Industrial Communication Technology Handbook, R Zurawski, Ed. Boca Raton, FL: CRC