ISSN No. 0976-5697

Volume 5, No. 5, May-June 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Safety-Critical Failure Analysis of Industrial Automotive Airbag System using FMEA and FTA Techniques

Dr. M. Ben Swarup
Department of Computer Science and Engineering
Vignan's Institute Of Information Technology, Duvvada,
Visakhapatnam, Andhra Pradesh

K.Amaravathi
Department of Computer Science and Engineering
Vignan's Institute Of Information Technology, Duvvada,
Visakhapatnam, Andhra Pradesh

Abstract: Modern cars are equipped with safety systems that protect the occupants of the vehicle. Airbags are one example of an occupant protection system. Although airbags save lives in crash situations, they may cause fatal behaviour if they are inadvertently deployed. This is because the driver may lose control of the car when this deployment occurs. In developing safety airbag systems 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). In this paper, by applying FMEA safety analysis technique we identify various failure modes of airbag system. These are sensor failures, FET failure, microcontroller failure, Firing Application Specific Integrated Circuit (FASIC) failure. Likewise FTA analysis is performed on the airbag system to identify the various faults that can lead to a top level undesired event, leading to an accident. By employing these two safety analysis techniques the weaknesses in the airbag design can be identified early and necessary interventions taken.

Keywords: safety-critical system, hazard analysis, failure modes, FMEA, FTA.

I. INTRODUCTION

Safety critical systems are those systems whose failure could result in loss of life, significant property damage, or damage to the environment. These systems are used in various fields such as medical devices, chemical industry, traffic control and other military equipment. The important property of a critical system is its dependability. Dependability to cover the related system attributes of availability, reliability, safety, security [1]. To achieve dependability, we need to avoid mistakes, detect and remove errors and limit damage caused by failure.

Many modern systems depend on computers for their correct operation. The future is likely to increase dramatically the number of computer systems that we consider to be safety critical. The reducing cost of hardware, the improvement in hardware quality, and other technological developments ensure that new applications will be sought in many domains.

A. *Traditional Systems:*

Traditional areas that have been considered the home of safety critical systems include medical, commercial aircraft, nuclear power and weapons. Failure in these areas can quickly lead to human life being put in danger, loss of equipment, and so on [2].

B. *Non Traditional Systems:*

The scope of the safety critical system concept is broad, and that breadth has to be taken into account when practitioners and researchers deal with specific systems. Some of the examples of non traditional systems are transportation control, banking and financial systems, electricity generation and distribution, telecommunication and the management of water system [3]. All of these applications are extensively computerized, and computer failure can and does lead to extensive loss of service with consequent disruption of normal activities.

Many modern information systems are becoming safety critical in a general sense because financial loss and even loss of life can result from their failure. Future safety critical systems will be more common and more powerful. From a software perspective, developing safety critical systems in the numbers required and with adequate dependability is going to require significant advances in areas such as specification, architecture, verification, and process. The cost of critical system failure is so high means trusted methods and techniques must be used for development. Example formal methods of software development. The system component where critical system failure may occur:

a. ***Hardware failure:*** It may fail because of its design and manufacturing errors.
b. ***Software failure:*** Software fails due to errors in its specification, design or implementation.
c. ***Operational failure:*** Human operators may operate the system incorrectly [1].

The failure of a safety-critical system can lead to injuries and even loss of life it is extremely important to provide designers with safety assesmentmethods that help to minimise the risk of theoccurrence of such disastrous events. One of these methods is failure mode and effect analysis (FMEA). In FMEA, a team of trained engineers of system designers analyses the cause consequences relationships of component failures on system hazards. After having found such a relation, the occurrence probability of that hazard is computed. It is thenchecked whether this value is above a certain threshold, defined by the tolerable hazard probability rate (THP or THR) [6]. If this is the case measures must be taken to reduce the probability of the undesired event.

This paper is organized as follows: section 2 discusses safety critical hazard analysis techniques, section 3 describes the case study of airbag safety critical system, section 4 presents the failure mode analysis of airbag system using

FMEA and FTA techniques and final section concludes the paper.

II. SAFETY-CRITICAL HAZARD ANALYSIS TECHNIQUES

Safety is the free from accidents or loss. Safety analysis is a method for evaluating the hazards and risks posed by a system and ways to minimize them. A hazard is a state or set of conditions of a system that, together with other conditions in the environment of the system,will lead inevita bly to anaccident. The primary concern of system safety analysis is the management of hazards: their identification, e valuation, elimination and control through analysis, design a nd management procedures.

Hazard analysis is the first stage, in which the system is studied for situation in which potentialharm co uld result, and the frequency 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 [4]. 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 the following steps:

- ***a. Hazard identification:*** This step identifies the potential hazards in the proposed system.
- ***b. 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.
- ***c. Preliminary system safety assessment (PSSA):*** This phase is concerned with ensuring that design can meet its safety requirements and also with refining these safety requirements as necessary.
- ***d. System safety assessment:*** This stage is concerned with producing the evidence that demonstrates the safety requirements have been met by the implementation [5].

A. Safety Analysis methods:

Failure modes effect analysis (FMEA) is an analysis tool for evaluating reliability by examining expected failure modes to find the effects of failure on equipment or systems. Fault tree analysis (FTA) is a deductive reliability analysis tool for evaluating reliability driven by top level views of what will fail and searches for root causes of the top level event. FTA considers experience and biases such as “every time we build a plant for this product we have these types of failures FTA provides both reliability assessments and fault probability perspectives. Table I shows features of FMEA and FTA analysis methods [7]:

Table I. Features of FMEA and FTA Techniques

Item	***FMEA***	***FTA***
Purpose of analysis	Reliability	Reliability, safety
Analysis starting point	Component failure mode	Product failure, injury
Flow of analysis	Component to product(Bottom up)	Product to component(top down)
Qualitative/quantitative	Qualitative analysis	Both

B. FMEA (Failure Mode Effect Analysis):

Failure modes and effects analysis (FMEA) is a step by step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service. Failures are prioritized according to how serious their 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 table II. FMEA includes review of the following steps in the process.

a. Failure modes (what could go wrong?)
b. Failures causes (why would the failures happen?)
c. Failures effects (what would be the con-sequences of each failure?)

Table 2. Basic Example of FMEA

System	***Component***	***Failure mode***	***Failure Effect***
Electrical	Battery	Discharged	not started
Electrical	Battery Connector	Corroded	Not started
Fuel	Fuel Tank	Empty	No fuel
Fuel	Fuel Pump	Mechanical failure	No fuel

C. FTA (Fault Tree Analysis):

Fault Tree Analysis (FTA) is a popular and productive hazard identification tool. It provides a standardized discipline to evaluate and control hazards. The FTA process is used to solve a wide variety of problems ranging from safety to management issues. This tool is used by the professional safety and reliability community to both prevent 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 Figure 1.

An FTA(similar to a logic diagram)is a deductive analytical tool used to study a specific undesired event such as engine failure. The deductive approach begins with a defined undesired event, usually a postulated accident condition, and systematically considers all known events, faults, and occurrences that could cause or contribute to the occurrence of the undesired event. Top level events may be identified through any safety analysis approach, through operational experience.

The procedural steps of performing a FTA are:

a. Assume a system state and identify and clearly doc ument state the top level undesired event(s).
b. Develop the upper levels of the trees via a top do wn process. That is determining the intermediate fai lures and combinations of failures or events that are the minimum to cause the next higher level even to occur. The logical relationships are graphically generated as described below using standardized FTA logic symbols.
c. Continue the top down process until the root causes for each branch is identified and/or until further decomposition is not considered necessary.

d. Assign probabilities of failure to the lowest level event in each branch of the tree. This may be through predictions, allocations, or historical data.
e. Establish a boolean equation for the tree using bo olean logic and evaluate the probability of the undesired top level event.
f. Compare to the system level requirement. If the re quirement is not met, implement corrective acti on. Corrective actions vary from redesign to analysis refinement.

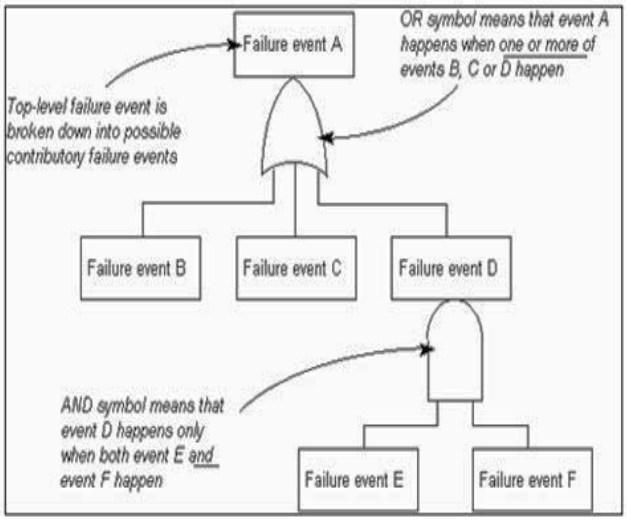

Figure 1. Basic Example of FTA

III. CASE STUDY OF AIRBAG SAFETY CRITICAL SYSTEM

Modern cars are equipped with safety systems that protect the occupants of the vehicle. Air bags are one examples of an occupant protection system. In case of a crash, the air bags system will deploy airbags that will reduce the risk of serious or even fatal injuries for the occupants. Current airbag systems consist of not only the front airbags but also of side, head, knee and a number of further airbags to protect both the driver and the passengers.

An airbag system can be divided into three major parts: sensors, crash evaluation and actuators. An impact is detected by acceleration sensors (front/rear/ side impact) and additional pressure sensors (side impact)[6]. Angular rate or roll rate sensors are used to detect rollover accidents. The sensor information is evaluated by two redundant microcontrollers (mc) which decide whether the sensed acceleration corresponds to a crash situation or not The deployment of the airbags is only activated if both microcontrollers decide that there was indeed a critical crash. The redundancy of the microcontroller system layout decreases the hazard of an unintended airbag deployment, which is considered to be the most hazardous malfunction of the system.

Our case study focuses on two variants of the air bag system. It consists of two acceleration sensors whose task is to detect front or rear crashes, either one microcontroller or two microcontrollers to perform the crash evaluation, and an actuator that controls the deployment of the airbag. Figure 2 gives a schematic overview of the system architecture using the two microcontroller variant. Notice that redundant acceleration sensors are mounted into different directions so that one is measuring the acceleration in the x direction (also referred as main sensor) of the vehicle and the other one is measuring the acceleration in they (safing sensor) direction.

The microcontrollers read the sensor values of the safing sensors (microcontroller 1) or the safing sensor (microcontroller 2) in a cyclic fashion. The two sensor values (x and y acceleration) are compared after they have been read by microcontroller1.They are then separately used for crash discrimination which is normally done by calculating mean values of the acceleration measured over certain intervals of time. If a certain number of thresholds in a given time frame are exceeded, the microcontrollers will synchronize their fire decisions and only if they both come to the conclusion that a critical crash occurred the airbags will be deployed.

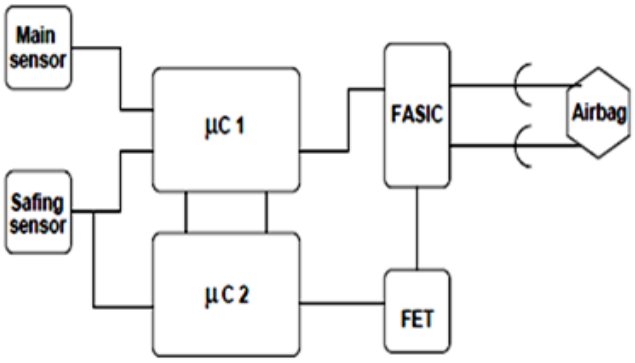

Figure 2.System Architecture for Automotive Airbag System [6]

The development of the airbag is also secured by two redundant protection mechanisms. The Field Effect Transistor (FET) controls the power supply for the airbag squibs that ignite the airbag. If the Field Effect Transistor is not armed, which means that the FET Pin is not high, the air bag squib does not have enough electrical power to ignite the airbag. The second protection mechanism is the Firing Application Specific Integrated Circuit (FASIC) which controls the airbag squib. Only if it receives first an arm command and then a fire command from the microcontroller1 it will ignite the airbag squib which leads to the pyrotechnical detonation inflating the airbag.

IV. FAILURE MODE ANALYSIS OF AIRBAG SYSTEM USING FMEA AND FTA TECHNIQUES

In this section we describe possible failures of the system components and their respective consequences for the safe functionality of the system. The hazards, we consider in this paper is either the suppression of airbag ignition when required or the unintended deployment of the airbag, in case no crash occurs [6].

A. FMEA Technique Sensor Failures:

For the sensors, we have identified the following failure modes:

a. Even though both sensors measure the same signal, the amplitude of this signal at both sensors is different.
b. The sensors deliver wrong amplitudes. This means that the real signals amplitude is corrupted by sensor failures.

c. The sensors function correctly, but since the sensor values are not sampled synchronously the delay between the two samples may be so large that the amplitudes are erroneously interpreted as being different.

B. Microcontroller Failures:

The potential consequences of a microcontroller failure are:

a. A fire command is needlessly sent to the FET and FAS IC, thus causing an unintended deployment of the airbag.
b. A fire command in case of the critical crash is suppressed, thus preventing the airbag from being ignited.
c. The fire command for the airbag in case of a crash is delayed, thus causing the airbag to be ignited too late.

C. FET Failures:

The Field Effect Transistor (FET) can be compared to a switch.

a. It can close inadvertently and hence enable the FASIC to fire.
b. It can be open instead of being closed as requested and hence suppressed ignition of the airbag.

D. FASIC Failures:

The Firing Application Specific Integrated Circuit (FAS IC) consists of two internal switches (High side and Low side switch)

a. It is possible that either one or both of the switches clos e in advertently, or that one or both does not close as re quested. In the first case, an ignition of the airbag is not possible as long as the FET is not activeted. In the latter case a correct firing may be suppressed by the FASIC.
b. For diagnostic purposes the FASIC is connected to the voltage supply. If this line is connected to the output line of the FASIC due to an internal short circ uit, the FET protection becomes useless and the airbag may be fired.

Although airbags save lives in crash situations, they may cause fatal behaviour if they are inadvertently deployed. This is because the driver may lose control of the car when this deployment occurs. It is therefore a pivotal safety requirement that an airbag is never deployed if there is no crash situation. These are the inputs to the designers to overcome all these failures:

a) By using two microcontrollers instead of one microcontr oller reduced the failure effect.
b) The usage of sensor also reduces the failure effect.
c) By using FET and FASIC and with help of two microco ntroller to reduce the failure.

The failures commonly occur in the working of the airbag systems are shown in table III.

Table 3. Failure Modes of Airbag System using FMEA Technique

System	***Component***	***Failure mode***	***Failure Effect***
Airbag System	Sensor failure	Wrong amplitude	accident
	Microcontroller failure	Fire command is delayed	accident
	FET failure	Missed deployment	accident
	FASIC failure	Unintended deployment	accident

E. FTA Technique:

Fault Tree Analysis involves identifying the undesired event and working backward from the event to discover the possible causes of the hazard. We describe possible failures of the system components and their respective consequences for the safe functionality of the system using Fault Tree Analysis technique. Figure 3 describes the specific failure of airbag system. Microcontroller failure is considered as a undesired event or top level event. It may fail because of failure in hardware or software. The software of the microcontroller may fail due to algorithm/logic problem or programming error.

F. Microcontroller Failures:

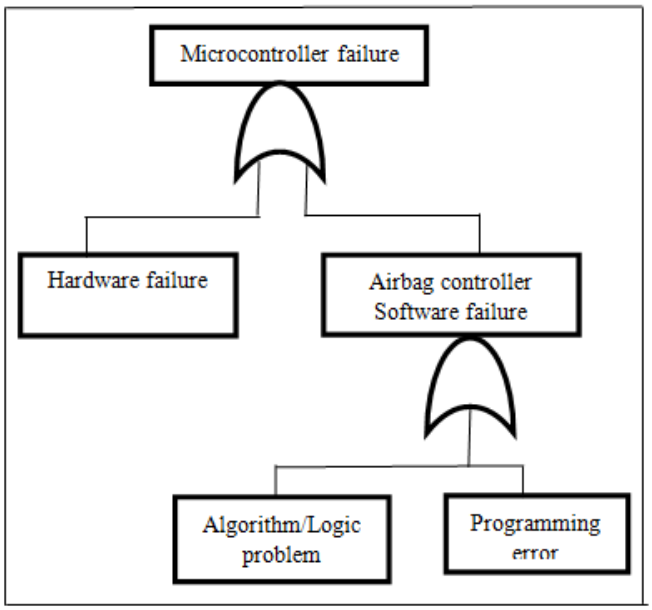

Figure 3. Microcontroller Failure using FTA

V. CONCLUSION

In this paper we have considered the airbag system which is a safety critical system. We have applied FMEA and FTA techniques to airbag to identify potential failures. With the help of FMEA, we can determine of the effect of failures on the system and with Fault Tree Analysis, design changes may be proposed early-on to address concerns over initial system reliability. We have presented a case study for applying FMEA to an industrial air bag system. We have considered a system with two different configurations (one and two microcontrollers). By applying FMEA the two system configurations were checked whether they comply with the upcoming safety standard for road vehicles with respect to a large number of possible component failures. We have identified the failures that commonly occur in the working of the airbag system. The failures are sensor failure, microcontroller failure, FET failure, FASIC failure. FTA technique is also applied on the airbag system to identify potential failures. By using these inputs the designer can reduce the failures in the airbag system resulting in a safer architecture.

VI. ACKNOWLEDGEMENT

Thanks are due to AICTE, New Delhi for sponsoring this research. This research presented in this paper is

supported by AICTE-RPS Project sanctioned to Vignan's Institute of Information Technology (VIIT), Visakhapatnam, in July 2013 with Dr. M. Ben Swarup as Principal Investigator.

VII. REFERENCES

[1]. Somerville Ian (2011), Software Engineering, Boston Pearson. ISBN0137053460.

[2]. John C. Knight, "Safety Critical Systems: Challenges and Directions," Proceedings of the 24th International Conference on Software Engineering (ICSE), Orlando, Florida, 2002.

[3]. K. Amarendra, A. Vasudeva Rao, "Safety Critical Systems Analysis," Global Journal of Computer Science and Technology, Volume 11, December 2011.

[4]. Robert Slater, "Safety Critical System Analysis", Spring1998, Available: http://users.ece.cmu.edu/ ~koopman/des_s99/safety critical.

[5]. Richard Hawkins, Ian Toyn, Iain Bate, "An Approach to Designing Safety Critical Systems using the Unified Modelling Language," Available: ftp://pisa.cs. york.ac.uk/pub/hise/finalUML.pdf.

[6]. H. Aljazzar, M. Fischer and L. Grunske, "Safety Analysis of an Airbag System using Probabilistic FMEA and Probabilistic Counter Examples," IEEE Computer Society Press, 2009.

[7]. Hiroshi Wada, "Safety analysis methods and applications at the design stage of new product development-Introducing the FMFEA and S-H Matrix Methods," Available: http://www.espec.co.jp/english/tech-info/tech_info/pdf/a4/e_24.pdf.