ISSN No. 0976-5697

Volume 6, No. 7, September-October 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Safety-Critical Software Failure Analysis of Industrial Automotive Airbag System

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

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

Abstract: An airbag is a safety feature designed to protect passengers in a head-on collision. 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). The basic design constraint for this application is we are considering the speed of the vehicle, frontal distance of the car as an input to the application. Considering all these inputs we are calculating the pressure of the crash and velocity of the car. If the pressure value crosses the threshold value then based on severity the airbag is going to be ignite. If the sensor fails to receive signal then it is passed to another safer sensor for ignition of airbag. At the same time the safety critical airbag system is simulated in MATLAB to provide safety to the system with safety sensor at the time of main sensor failure. Considering speed and velocity as inputs to simulation process, during impact we calculate some physical parameters such as change in speed and seat position of the occupant the airbag is activated to save life of occupant.

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

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.

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].

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 computerfailure 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 assessment methods 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 discuss thecase study of safety critical airbag system, section 3 describes the failure analysis of airbag system, section 4 presents simulation process and section 5 discuss results and discussion and final section concludes the paper.

I. CASE STUDY OF SAFETY CRITICAL AIRBAG SYSTEM

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.

It mainly 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 1 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 main 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.

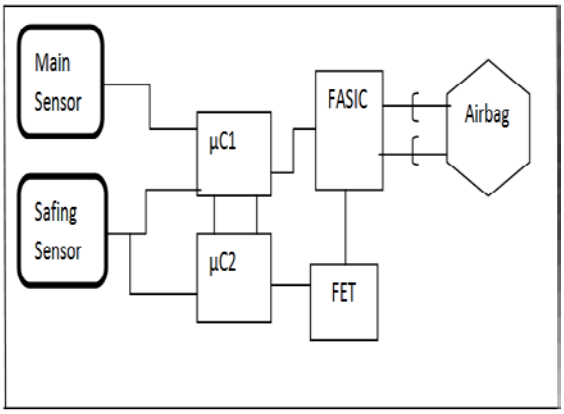

Figure 1. System Architecture for Automotive Airbag System with Safety

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.

II. FAILURE ANALYSIS OF AIRBAG SYSTEM

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 inevitably to an accident. The primary concern of the system safety analysis is the management of hazards:their identification, evaluation, elimination and controlthrough analysis, design and management procedures. Hazard analysis is the first stage, in which the system is studied for situation in which potential harm could result, and the frequency with which those situations occur[4].

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. It is extremely important to provide designers with safety assessment methods. There are two safety analysis methods used in this system. Those are Failure Mode Effective Analysis (FMEA) and Fault Tree Analysis (FTA)

A. FAILURE MODE EFFECTIVE ANALYSIS OF AIRBAG SYSTEM

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].

Sensor Failures:

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

1. Even though both sensors measure the same signal, the amplitude of this signal at both sen sors is different.
2. The sensors deliver wrong amplitudes. This means that the real signals amplitude is corrupted by sensor failures.
3. The sensors function correctly, but since the sensor values are not sampled synchro-nously the delay between the two samples may be so large that the amplitudes are erroneously interpreted as being different.

Microcontroller Failures:

The potential consequences of a microcontroller failure are:

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

FET Failures:

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

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

FASIC Failures

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

1. It is possible that either one or both of the switches close in advertently, or that one or both does not c lose as requested. In the first case, an ignition of th e airbag is not possible as long as the FET is not a ctive-
   ted. In the latter case a correct firing may be suppr essed by the FASIC[5].
2. For diagnostic purposes the FASIC is connected to the voltage supply. If this line is connected to the output line of the FASIC d ue to an internal short circuit, the FET protection be comes useless and the airbag may be fired.

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

Table I. 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

B. 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

Sensor Failure:

An impact is detected by acceleration sensors (front/rear/ side impact) and additional pressure sensors (side impact). Angular rate or roll rate sensors are used to detect rollover accidents. The sensor may fail to receive signals then second sensor is going to work.The sensor may fail due to displacement sensor fault or acceleration sensor fault. The displacement sensor may fail because of incorrect fitting, processor failure or loose cabling.Theacceleration sensor may fail due toaccelometer failure or charge amplifier.

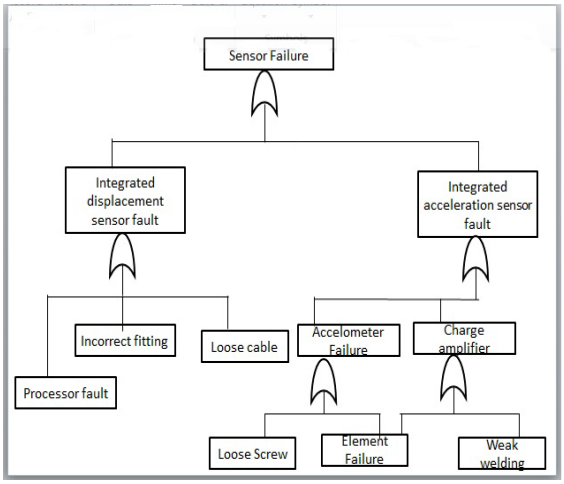

Figure 2. Sensor Failure using FTA

III. SIMULATION

The modelling is done using simulink model in C# with window forms and MATLAB.The task of the airbag system is to minimise the risk of injury to the vehicle occupants following various types of impact. The airbag develops its protective effect depending on the direction from which the impact comes and the resulting vehicle deceleration.

Airbag System simulation: In this airbag activation process the speed and velocity of the car are given as inputs to the system to calculate the belt force of the car during collision.A complex sensor system and evaluation unit is required to control the system. Thetriggering unit, which is usually located in the centre of the vehicle, measures the deceleration recorded by one or several acceleration sensors during an impact and calculates physical parameters such as the deceleration, change in speed. The airbag is triggered when a threshold value is exceeded which is determined by the collision conditions, the seat position and the passenger compartment.

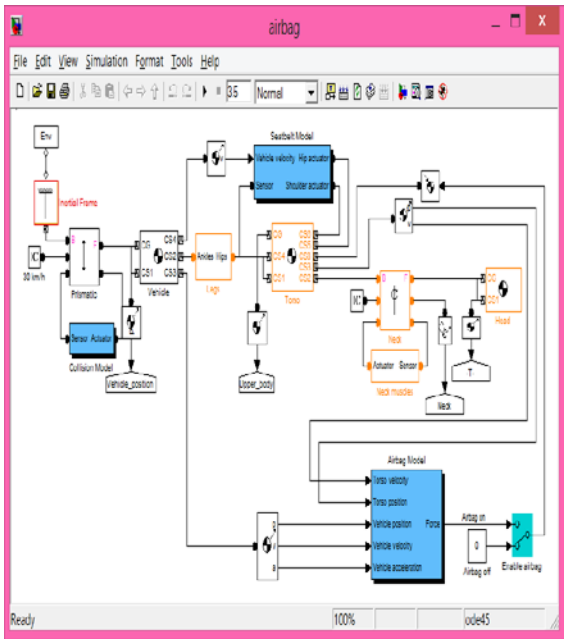

Figure 3. Airbag Activation System without Safety

Airbag Force Calculations: Considering vehicle position, vehicle acceleration, vehicle velocity, torso position and velocity as inputs to the system to calculate force of the impact during crash. The force value is exceeded the basic threshold value then airbag is ignited during crash to save life of occupant.

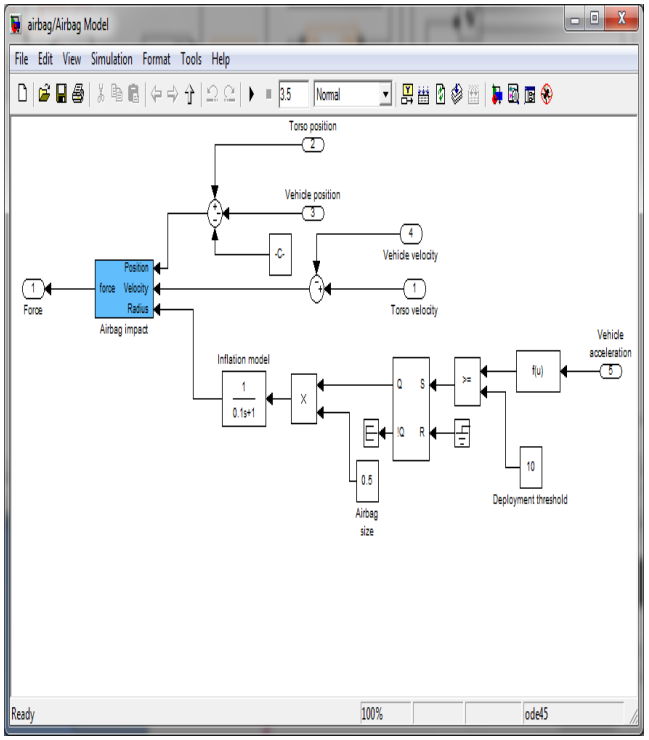

Figure 4. Airbag Force Calculator Based on Impact**Dual Sensor Approach for Airbag Activation:** The airbag system is activated by considering inputs such as throttle, speed, pressure to the system. If the first sensor may fail to activate the airbag during crash then it bypasses the signal to safing sensor to ignite the airbag. In figure 5 we are using two PID controllers to provide safety to the vehicle. The first sensor may fail due to over speed then it is unable to receive signal. So, the safety sensor will receive data to ignite the airbag.

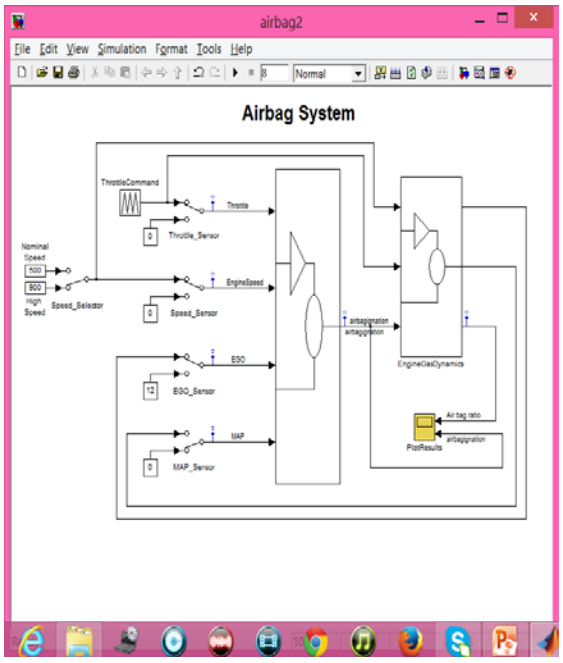

Figure 5. Airbag Activation with Safety

IV. RESULTS AND DISCUSSION

Since the acceleration curve has to be considered for a safe decision on any airbag deployment and the system must be monitored to guarantee the function, the use of purely mechanical sensors proves difficult. Mechanical and electromechanical systems can only detect the transgression of a previously defined maximum acceleration, a diagnosis is complicated. A continuity check of the spring, for example, is possible to detect a broken spring.

The safing sensor is used as a safety switch to prevent an unintentional triggering. Its switching thresholds are set so that no closure is possible in normal driving conditions. This sensor only switches early in the event of a crash and thus enables triggering.The inputs car position, speed and frontal distance of the car are shown in figure 6. The coefficient value is the threshold value which is constant. The acceleration values that need to trigger is as default value 0.2 which must be less than threshold value. From this the weight of the car is calculated.

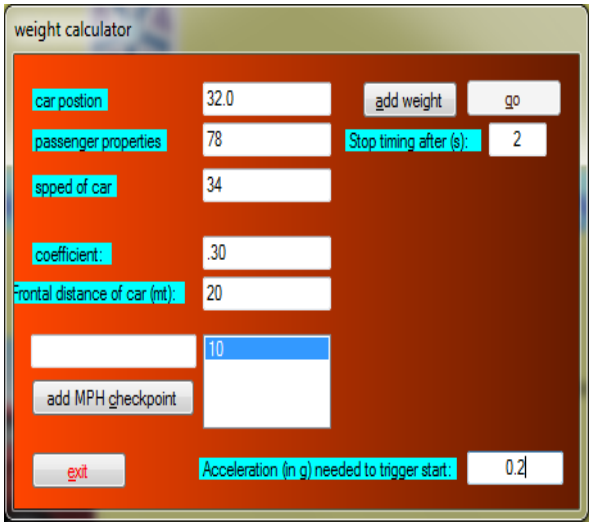

Figure 6. Inputs of Airbag Activation (Weight Calculator)

The airbag is activated with respect to main sensor or safety sensor is shown in figure 7. The sensor will receive signal during impact measures acceleration of the vehicle, change in speed and belt force.If the threshold value is exceeds the range (0.3 to 0.55) then airbag is activated with the help of safety sensor.

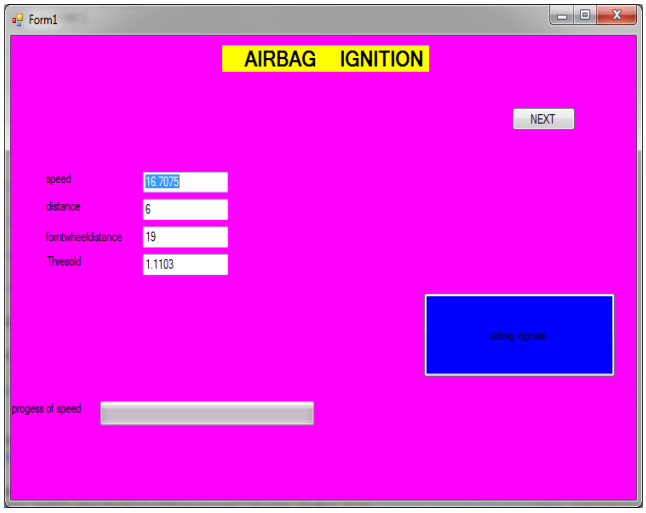

Figure 7. Airbag Activation with Safety in window form

The output form shows the flow of the logic with respect to safety sensor means if the main sensor is unable to ignite the airbag during crash then safety sensor will receive the data to ignite the airbag during critical crash. Based on the severity the airbag will activated means the particular pressure range the main sensor will activate if that exceeds the safety sensor will take care about ignition during crash.It shows the flow of control logic with respect to safety sensor.

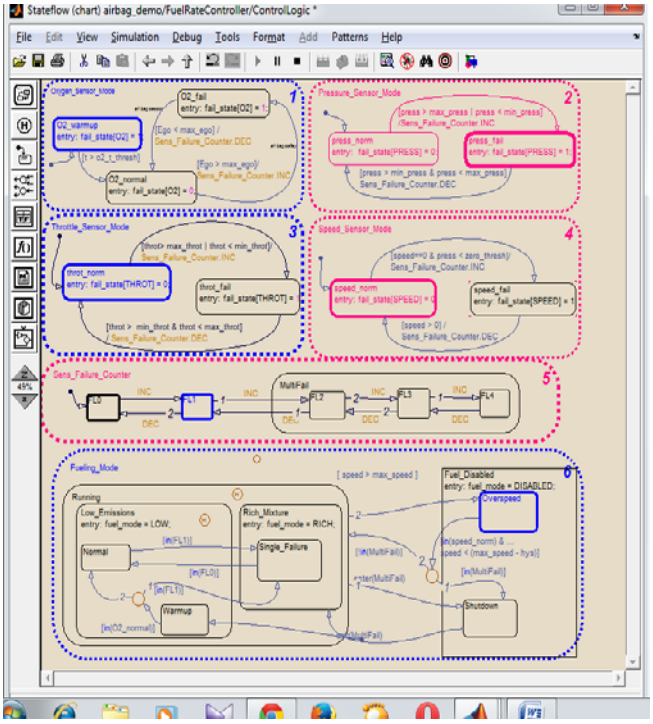

Figure 8. Control Flow Logic of Safety Sensor

Limitations: One of the limitations of this paper is considering inputs as speed of the car, threshold value and frontal distance of the car. Based on these inputs we are calculating the distance and speed of the car. The threshold value is between 0.3 to 0.55 the sensor one is calculating to ignite airbag. Otherwise it is more than the range another sensor will ignite the airbag because of first sensor failure. At the same time we are simulating the same process in matlab considering speed and velocity as inputs through

with safety and without safety. In with safety simulation particular range of speed is considered (300- 1000). If the rangeis crossed we are showing the bypassing flow to another safety sensor.

V. CONCLUSION

Airbag system is a vehicle safety device designed to protect occupant from accidents. Although airbag system saves 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.The failure of a safety-critical system can lead to injuries and even loss of life it isextremel y important to provide designers with safety assessment met hods that help to minimise the risk of the occurrence of such disastrous events. The safety analysis methods are failure mode and effect analysis (FMEA) and fault tree analysis (FTA). Considering speed and velocity of the vehicle as inputs of the airbag system to activate airbag during impact. The Results of this safety airbag system has simulated using C# with Window Forms and MATLAB-Simulink.Thetriggering unit, measures the deceleration recorded by one or several acceleration sensors during an impact and calculates physical parameters such as the deceleration, change in speed. The airbag is triggered when a threshold value is exceeded which is determined by thecollision conditions, the seat position and the passenger compartment.The safing sensor is used as a safety switch to prevent an unintentional triggering. Its switching thresholds are set so that no closure is possible in normal driving conditions. This sensor only switches early in the event of a crash and thus enables triggering.

VI. 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 201 3(Ref.No:20/ AICTE/ RIFD/RPS(Policy-1) 49/2013-14) 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 Analys is", 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.

