Design of A Fault Tolerant Embedded Control System

Aiswarya B, Dr. A. A Powly Thomas and Dr.Indumathi.G

Abstract: When a fault occurs in modern systems which are safety critical, the main problem to be addressed is to raise an alarm, ideally diagnose what fault has occurred, and then decide how to deal with it. The problem of detecting a fault, finding the source/location and then taking appropriate action is the basis of fault tolerant control. When physical redundancy of components is not present in the plant, fault detection and isolation (FDI) is a prerequisite for fault tolerant control architecture.

Here a study on engine control system covering engine speed and temperature sensors as well as the position sensors is conducted. Here, a Full Authority Digital Engine Control System is used as an application. Three of the sensors used in its digital control unit and their respective signal processing circuits are modelled after which fault detection and isolation of the faulty sensor is performed.

Keywords: Full Authority Digital Electronic Control Unit (FADEC), Fault Detection and Isolation, Failure Mode Effect Analysis (FMEA), Fault Tolerant Control.

I. INTRODUCTION

Fault detection and isolation [1][2] is a subfield of control engineering which concerns itself with monitoring a system, identifying when a fault has occurred, and pinpointing the type of fault and its location. Sensor faults/failures can occur due to malfunctions in the components in the sensor unit, loose mounting of the sensors and loss of accuracy due to wear and tear.

Fault detection approaches can be classified as model free and model-based paradigms. Model-free fault diagnosis includes all the techniques that do not rely upon models of the underlying system, while model-based methods try to diagnose faults using the redundancy of some mathematical description of the dynamics. The sensor FDI subsystem [3] performs the tasks of failure detection and identification by continuously monitoring the outputs of the sensors.

Under nominal conditions, these measurements follow predictable patterns, within a tolerance determined by the amount of uncertainties introduced by random system disturbances and measurement noise in the sensors. Usually, sensor FDI tasks are accomplished by observing when the output of a failed sensor deviates from its predicted pattern.

FTC is a complex combination of three major research fields, FDI, robust control, and reconfigurable control. The monitoring of faults in feedback control system components is known as fault detection and isolation (FDI). The procedure of generating a control action which has a low dependency on the presence of certain faults is known as fault tolerant control.

For most FTC schemes, when a fault/failure occurs either in an actuator or sensor [4], the FDI scheme will detect and locate the source of the fault. This information is then passed to a mechanism to initiate reconfiguration. The reconfigurable controller will try to adapt to the fault, therefore providing stability and some level of performance. Both the FDI and the reconfigurable controller need to be robust against uncertainties and disturbances. Reconfiguration in these cases usually consists in isolating the faulty sensor and using the other sensors to get the best possible estimation of all the parameters involved.

II. MODELLING OF FAULTS

An engineering model of something that could go wrong in the construction or operation of a piece of equipment is called a fault model. From the model, the designer or user can then predict the consequences of this particular fault. The classical approaches are limit or trend checking of some measurable output variables. Because they do not give a deeper insight and usually do not allow a fault diagnosis, model-based methods [2] of fault detection were developed by using input and output signals and applying dynamic process models. These methods are based, e.g., on parameter estimation, parity equations or state observers. Also signal model approaches were developed. The goal is to generate several symptoms indicating the difference between nominal and faulty status.

Based on different symptoms fault diagnosis procedures follow, determining the fault by applying classification or inference methods. The task consists of the detection of faults in the processes, actuators and sensors by using the dependencies between different measurable signals. These dependencies are expressed by mathematical process models.

Aiswarya B, Asst.Proffessor, Department of Electrical &ElectronicsEngineering, HKBKCE;
Dr. A. A Powly Thomas, Prof & HOD, Dept of Electrical&ElectronicsEngineering ,HKBKCE ;
Dr.Indumathi.G, Prof &HOD, Department of Electronics & Communication,CMRIT.

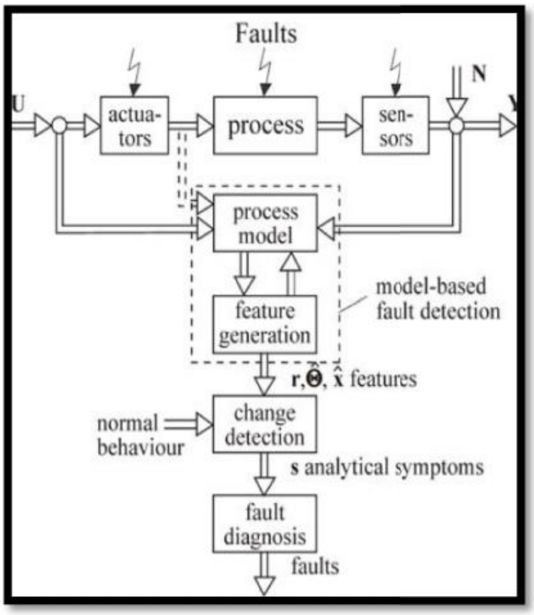

FIG 1: GENERAL SCHEME OF PROCESS MODEL-BASEDFAULT DETECTION AND DIAGNOSIS

FIG 1 shows the basic structure of model-based fault detection. Based on measured input signals **U** and output signals **Y**, the detection methods generate residuals **r**, parameter estimates **Θ** or state estimates ˆ*x,* which are called features. By comparison with the normal features, changes of features are detected, leading to analytical symptoms.

III. FAILURE MODE EFFECT ANALYSIS (FMEA)

A Failure Mode Effect Analysis (FMEA) [5] is often the first step of a system reliability study. It involves reviewing as many components, assemblies, and subsystems as possible to identify failure modes, and their causes and effects. For each component, the failure modes and their resulting effects on the rest of the system are recorded in a specific FMEA worksheet. There are numerous variations of such worksheets. A FMEA is mainly a qualitative analysis. A few different types of FMEA analysis exist, like Functional, Design and Process FMEA.

FMEA is an established reliability engineering activity that also supports fault tolerant design, testability, safety, logistic support, and related functions [6]. The technique has its roots in the analysis of electronic circuits made up of discrete components with well-defined failure modes. A successful FMEA activity helps to identify potential failure modes based on experience with similar products and processes or based on common physics of failure logic. Effects analysis refers to studying the consequences of failures on different system levels. FMEAs can be performed at the system, subsystem, assembly, subassembly or part level. The FMECA should be a living document during development of a hardware design. It should be scheduled and completed concurrently with the design.

Procedure

- Define the system and its performance requirements
- State all assumptions and ground rules that will be used in the analysis
- Develop block diagrams of the system and identify possible failure modes.[i.e., breaking, cracking, leaking, etc.]
- Identify cause of each failure mode
- Determine impact of every possible failure mode on the operation of affected items, items of subsequent assemblies, and the total system.
- List the possible symptoms of all failures and the means used to detect the failure.
- Assign a severity ranking to each failure mode.
- Evaluate and recommend any corrective actions and improvements to the design.

IV. FULL AUTHORITY DIGITAL ELECTRONIC CONTROL SYSTEM

Full Authority Digital Electronic Control system is common in all modern jet engines. The simplest engine control system is one that produces desired engine thrust by changing the fuel flow. As shown in FIG 2, FADEC System consists of either a dual redundant architecture or a quadruple control with two more Digital Engine Control Units (DECU). Engine inputs are duplicated, to suit the two controllers. Each controller drives a dual wound fuel metering unit, nozzle actuation systems, compressor inlet guide vanes actuation system, Engine spools rotational acceleration control, Engine spools rotational speed governing, Limiting pressure ratios, Limiting turbine entry temperature, Surge protection, Independent limiting of over speed and over temperature.

Each control unit is an embedded controller with its set of engine sensors and external interfaces. Both control units communicate with each other in a limited way so that any one lane takes control of the engine while the other will be in hot standby mode. If the controlling lane detects a fault with its interfaces, or within itself detected by its Built-In Test Equipment (BIT), a lane change must occur to the other control unit (DECU). The BIT within the system should perform checks at regular intervals and transfer the control from one lane to the other when a fault is detected. Thus, it prevents the system from behaving abnormally.

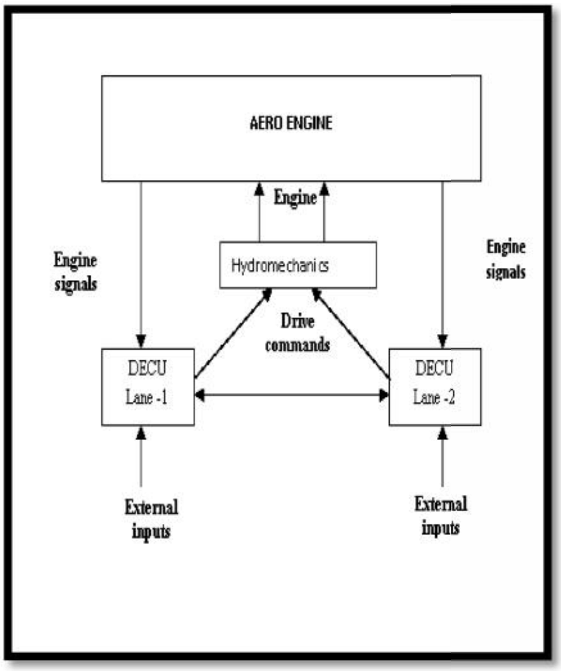

FIG 2: DUAL REDUNDANT ARCHITECTURE OF THE CONTROL SYSTEM

V. SIMULATION OF FAULT ANALYSIS ON POSITION SENSOR IN FADEC SYSTEM USING SIMULINK

Basic principle

The LVDT (Linear Variable Differential Transformer) is an electromagnetic device that produces an electrical voltage proportional to the displacement of a movable Magnetic Core. The LVDT is an electro-mechanical transducer, the input to which is a physical movement of the transducer core, and the output a change in magnetic coupling between the internal windings which can be measured using suitable conditioning electronics. Usually, the output of the conditioning electronics is a stable, DC voltage which is proportional to the core position.

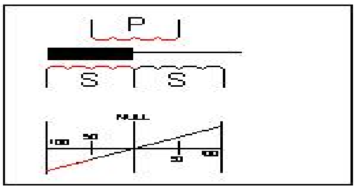

FIG 3: BASIC PRINCIPLE OF LVDT

It consists of the following parts as shown in the FIG 4:

- A ***coil winding assembly*** consisting of a Primary Coil and two Secondary Coils symmetrically spaced on a tubular center.
- A ***cylindrical case*** which encloses and protects the Coil Winding Assembly.
- A rod shaped ***magnetic core*** which is free to move axially within the Coil Winding Assembly.
- A separate shield is used for ***electromagnetic shielding.***

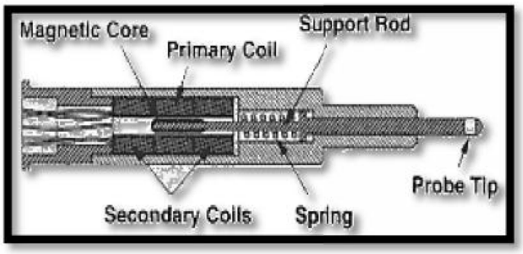

FIG 4: LVDT CONSTRUCTION

Detailed description of LVDT

The primary coil is connected to a sinusoidal signal of fixed amplitude and frequency, and the core electrically couples the resultant magnetic flux onto the secondary windings. An electronic circuit measures the differential signal across the two secondary coils. This usually takes the form of a difference amplifier with a suitable passive filter at the input.
FIG 5 shows the electrical connections to the LVDT.

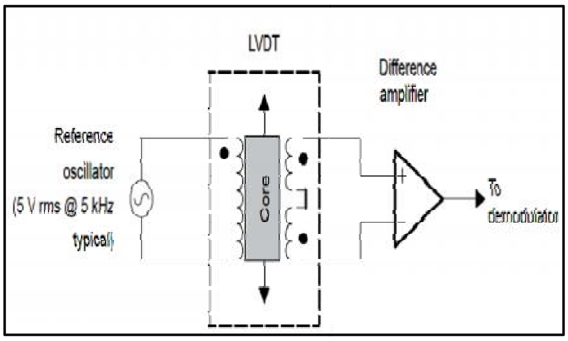

FIG 5: ELECTRICAL CONNECTIONS TO THE TRANSDUCER

With the core in its central position (shown above), magnetic flux is coupled equally onto both secondary windings and the output of the difference amplifier is theoretically zero. If the core is displaced a small amount from the null point, flux coupling to one secondary winding increases, while that to the other winding falls, and a net differential voltage is seen at the output of the difference amplifier. The resulting signal is a sinusoidal waveform of the same frequency as the input oscillator, and has amplitude proportional to the displacement of the core from the null point. The signal is either fully in phase or fully in anti-phase with the signal applied to the primary, depending on the direction of core displacement. Signal conditioning thus becomes a matter of determining the amplitude of the return signal from the secondary windings and its phase relative to the reference oscillator.

Signal conditioning circuit

The return signals from the two secondary windings are usually connected to an instrumentation amplifier (IA) which measures the differential voltage. This is filtered to remove unwanted noise by a band-pass filter tuned to extract the oscillator frequency. The filter output is passed through a synchronous demodulator circuit which yields a full-wave rectified signal, the polarity of which depends on the phase of the return signal relative to the oscillator. The signal is then smoothed and scaled to produce a stable DC voltage proportional to core position. FIG 6 shows a block diagram of the oscillator and signal conditioning electronics and FIG 7 is the simulated model of LVDT signal conditioning circuit using Simulink. The output of the model gives the voltages corresponding to various positions of the core.

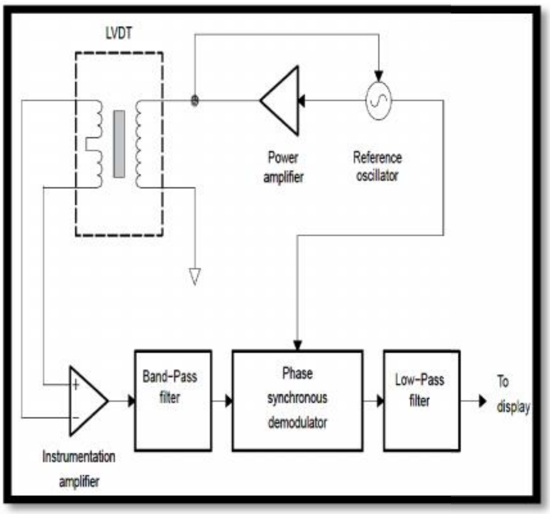

FIG 6: SIGNAL CONDITIONING BLOCK DIAGRAM

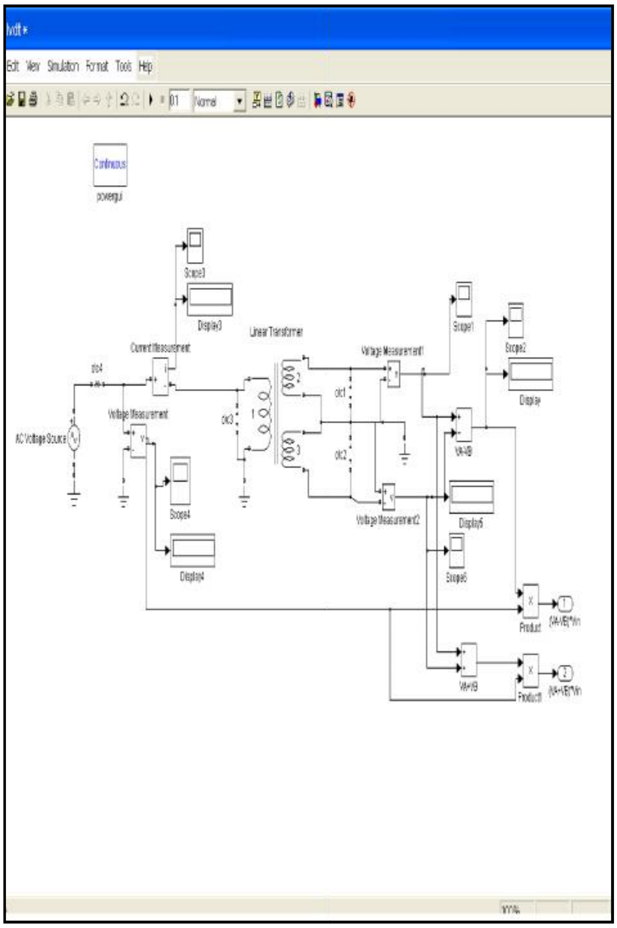

FIG 7: SIMULATED MODEL OF LVDT SIGNAL CONDITIONER

VI. SIMULATION RESULTS

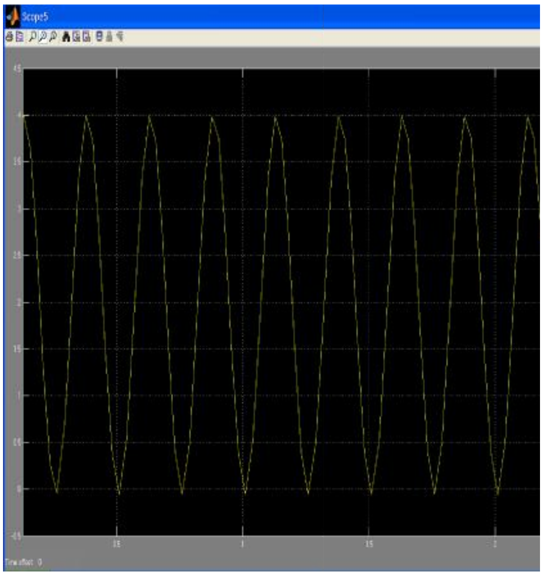

FIG 8: RECTIFIED OUTPUT OBTAINED FRON THE LVDT SIGNAL CONDITIONER MODEL

POSITION(mm)	V_a	V_b	V_{dc}
12	2.272	1.438	3.98
11	2.2025	1.5075	3.3
10	2.133	1.577	2.7
9	2.0635	1.6465	2
8	1.994	1.716	1.33
7	1.9245	1.7855	0.67
6	1.855	1.855	0
5	1.7855	1.9245	-0.67
4	1.716	2.0635	-1.33
3	1.6465	2.0635	-2
2	1.577	2.133	-2.7
1	1.5075	2.2025	-3.3
0	1.438	2.272	-3.98

TABLE I: SIMULATION RESULT

The position of the core must be limited between 0mm to 12mm and in order to perform this check, the output voltage obtained from this model must be subjected to rate and range check.

Rate check and range check using Simulink

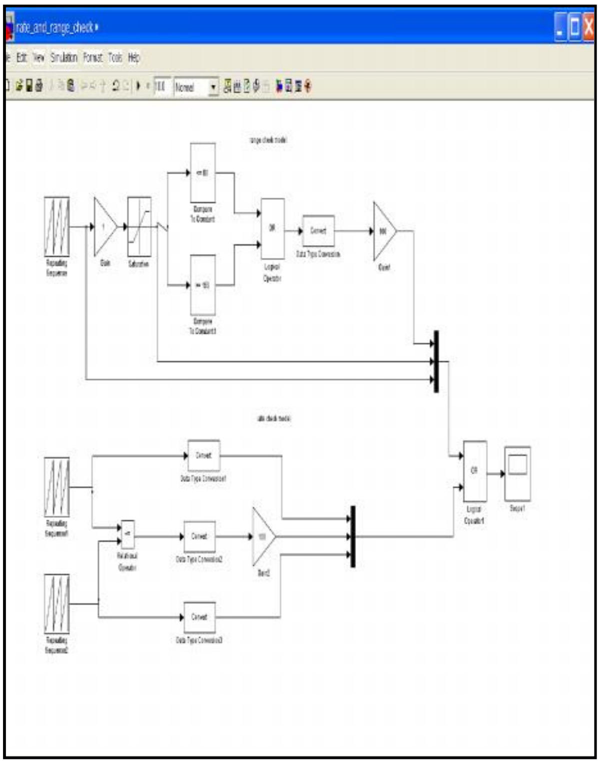

FIG 9: RANGE AND RATE CHECK MODEL

Outputs:

1. ***Range check***

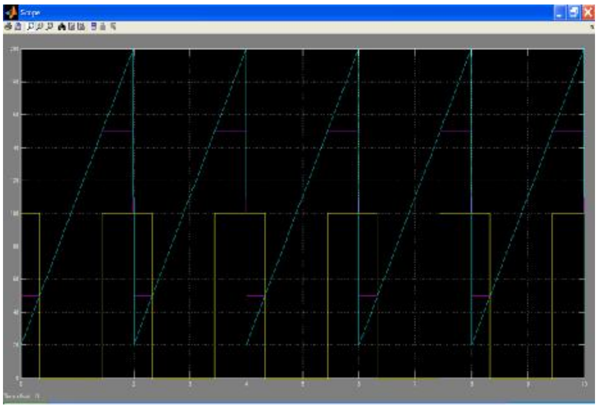

FIG 10: RANGE CHECK OUTPUT

It can be observed in FIG 10 that outputs that go out of range are detected. The yellow colored signal goes high whenever outputs from signal conditioner circuits go out of range.

2. ***Rate check***

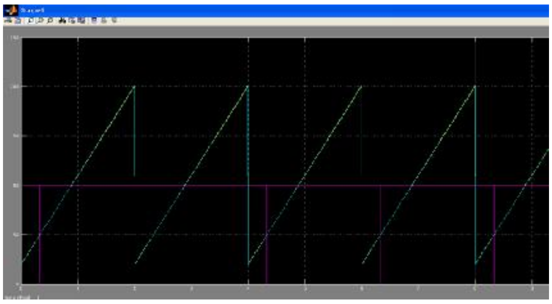

FIG 11: RATE CHECK OUTPUT

An output that varies at an undesirable rate is detected. It can be observed in FIG 11 that the pink colored signal goes high when output from signal conditioner circuits vary at an undesirable rate and the signal goes low when it varies within the limits.

3. ***Combined rate and range check output***

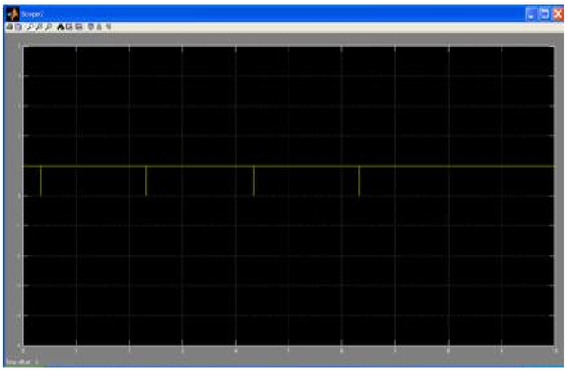

FIG 12: COMBINED OUTPUT OF BOTH RATE AND RANGE CHECK

The FIG 12 shows outputs from sensors are validated for any rate error as well as range errors.

Whenever there is a rate error or range error, this signal goes high.

Result analysis

The rate and range check model monitors the output of the LVDT signal conditioner model. Whenever its output goes above 3.98V which corresponds to 12mm position or below -3.98V which corresponds to 0mm position, the output signal (yellow colored signal) goes high showing the occurrence of range error as shown in FIG 10. Similarly, when the rate of change of output goes beyond the threshold, it can be seen in the FIG 11 that, the pink signal goes high. FIG 13 shows the combined output of both the rate and range check. The signal goes high whenever a rate or range error occurs.

VII. CONCLUSION

The main aim is to achieve the pilot demanded thrust. In this project, the main purpose was to detect fault in three sensors present in the control system which are, temperature sensor, position sensor and speed sensor. The three sensors and their signal conditioning circuits were modeled using Simulink and fault analysis is conducted using FMEA. The analysis was tabulated as per the FMEA worksheet format.

For fault detection, a BIT circuitry was developed that performs rate checks and range checks. Fault is isolated and fault accommodation is done by building the property of reconfiguration within the control system. The control system behaves according to a particular algorithm built in whenever a fault is detected in any part of the system, such that reliability and safety is always assured.

ACKNOWLEDGEMENT

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and co-operation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped me in carrying out this work. I would like to take this opportunity to thank them all.

I extend my sincere and heartfelt thanks to **Dr. A. A Powly Thomas,** Professor & Head of the Department, EEE, HKBKCE & **Dr. Indumathi.G**, Professor & Head of the Department, ECE, CMRIT for their constant encouragement. I also extend my sense of gratitude and sincere thanks to Principal **Dr. T.C. Manjunath** and management of HKBKCE, Bengaluru.

REFERENCES

[1] "A Fault Detection and Isolation Model Based on Conditional Finite State Machine for Gas Turbine", Liu Yongbao; Ma Liangli; Huang Shuhong Natural Computation, 2009. ICNC '09. Fifth International Conference on, 2009

[2] "Fault Diagnosis and Isolation Process of Gas Turbine Based on Fault Dependency", Liu Yongbao; Ma Liangli; Huang Shuhong Computational Intelligence and Natural Computing, 2009. CINC '09. International Conference on, 2009

[3] "Damage propagation modeling for aircraft engine run-to-failure simulation", Saxena, A.; Goebel,K.; Simon,D.; Eklund, N. Prognostics and Health Management, 2008. PHM 2008. International Conference

[4] "Semantic sensor fusion for fault diagnosis in aircraft gas turbine engines", Sarkar,S.; Singh,D.S.; Srivastav,A.; Ray,A. American Control Conference (ACC), 2011

[5] "Failure analysis of FMEA", Bluvban,Z.;Grabov,P. Reliability and Maintainability Symposium, 2009. RAMS 2009. Annual.

[6] "FMEA-Based Control Mechanism for Embedded Control Software", HongZhe Shi; Xuejing Wang; Guoqi Li; Hong Zhang, Information Technology, Computer Engineering and Management Sciences (ICM), 2011 International Conference on, 2011.

Mrs.Aiswarya.B, Assistant Professor, EEE Department, HKBK College of Engineering, Bangalore. Pursued B.E in Electrical and Electronics from Visvesvaraya Technological University and completed M.Tech in VLSI & Embedded System Design from Visvesvaraya Technological University.

Dr. A. A. Powly Thomas, Professor and HOD, EEE Department, HKBK College of Engineering, Bangalore. Pursued B.Tech in Electrical Engineering from University of Calicut in 1986 and M.Tech in Control Systems from University of Kerala, in 1988 and Completed PhD in Control Systems from Department of Aerospace Engineering, Indian Institute of Science, Bangalore in the year 2004. At present is member of Board of Studies (BOS) and Board of Examinations (BOE) in VTU. Also Working as the Head of VTU Research Centre in EEE Dept. , HKBKCE, Bangalore.

Dr. Indumathi. G, Professor and HOD, Electronics and Communication Department, CMRIT.