INVITED PAPER

SYSTEM SAFETY APPROACH IN ACCIDENT PREVENTION

Kanchan Biswas* and J.K. Sharma**

Introduction and Definitions

A **System** can be defined as a composite, at any level of complexity, of personnel, procedures, materials, tools, equipments, facilities and software. The elements of this composite entry are used together in the operational or support environment to perform a given task or achieve a specific mission.

Safety on the other hand indicates 'freedom from harm'. One can then immediately ask the question 'Is flying safe?' Well, we all know and accept that flying is always 'risky'. This again raises the question 'Is safe equivalent to 'risk free'?' US Supreme Court has accepted that they are not. Any activity for that matter will be associated with certain amount of risk, small or big. **Risk threshold** will be the boundary of safety beyond which accidents are likely to occur. 'Flight Safety' is essentially an activity to estimate the potential risk of each operational element of flying and take appropriate measures that the risk thresholds are not exceeded.

System Safety as defined in MIL - STD 882B reads, 'The conservation of human life and its effectiveness, and the prevention of damage to items, consistent with mission requirements'. In a simpler term, in aviation, it implies the application of engineering and management principles, criteria and techniques to prevent accidents over the life cycles of the air vehicle system, within the constraints of available skill, resources, cost and time.

The **Hazard Rate** or the acceptable levels of probability of loss of human lives as envisaged by a safety professional is to be less than one per million per year. This indirectly will call for a very low probability of failure of an individual product, which is a very difficult proposition. This has lead to the concept of System Safety rather than Product Safety as a means of elimination of accidents.

Flight Safety and Accident Prevention

Flight Safety Directorates of civil and military organiations usually maintain data bank on defects, flying incidences and accident reports along with their investigations or inquiry reports. The data is utilized to get an insight on probable deficiencies of a system. The analyses as shown at Fig.1, below bring out design improvement as a close loop solution.

While the analysis gives a trend toward safety status, but more often than not, one becomes knowledgeable only after the accident takes place. The flight safety group also takes measures to improve flight safety by taking appropriate measures on technical disciplines; human trainings, bird menace and other safety related issue based on the various defect and accident investigations.

Modern System Theory, at least with regards to safety, on the other hand emphasizes the need to examine all elements, which may have a bearing on the task at hand a priori. Indeed, a critical first step in any safety analysis is to carefully define the system under consideration and its interface with other systems. The safety problem has mostly been seen at the interface between two or more systems rather than within a system itself.

Human Factor in Accident Prevention (Shel Concept)

A system can be considered as the outcome of technological development of engineering and physical sciences for the use of human benefit. Edwards (1972) and Hawkins (1984) studied the inter connectivity of the four elements of the building block of a system namely **S**oftware,-**H**ardware, **E**nvironment and the **L**iveware in the famous **SHEL Concept**. In the center of the model is the Liveware (man), which is the most valuable but flexible and subjective component. As the liveware is the hub of the SHEL model, all other components must be adapted and matched to this central component.

The **L-H** interface addresses all issues related to Man Machine Interface (MMI). This includes design and locations of displays, seats, controls, operating switches etc., taking note of human capability and the natural instincts. The **L-S** interface design encompasses all non-physical aspects of systems like procedures, manuals and checklist

* Associate Director (Aircraft) ** Chief Executive (Airworthiness)
Centre for Military Airworthiness and Certification (CEMILAC), Defence Research and Development Organisation (DRDO)
Marathahalli Post, Bangalore-560 037, India

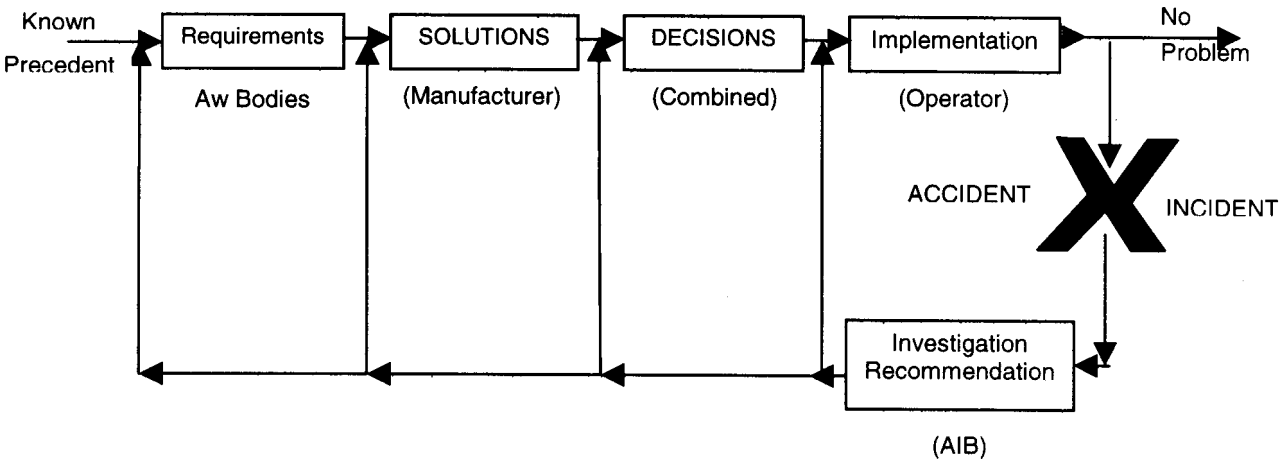


Fig.1 Closed loop solution of system improvement

layout, symbology and the other computer programmes. The **L-E** interface tries to take all measures aimed to adapting man to match the environment. For example, helmets to protect against noise, flying suits against cold, goggles against airstreams and sunlight, oxygen masks against the effect of altitude and 'g' suits against acceleration loads and so on. And finally the **L-L** interface discusses the synergy amongst pilots, crewmembers, and ground stations or with pilots on other flying aircraft (formation flights).

Evolution of System Safety

Explosive handled haphazardly in the post World War-I (WW-I) era and catastrophic fires drew the attention towards safety measures needed. Until WW-II, accidents were thought to be people oriented. It was believed that 'luck' was against those who were killed in accidents.

However, during the war period, statistics tragically indicated that more aircraft and pilots were lost in normal flight operations than in combat. For example, in 1943, in US, 5000 aircraft were lost in normal operation compared to 3800 in combat. This brought in focus the concept of system safety in the post war period. The landmark paper in this regard, entitled, 'The Organization and Utilisation of Aircraft Manufacturer's Air Safety Programme' by AL Wood of the Boeing Company in January 1946. The paper emphasized **'continuous focus of safety in design', 'advance analysis and post accident analysis', 'importance of near accident analysis'** and **'accident preventive design to minimize personnel errors'**.

In the fifties, when the supersonic aircraft appeared with many complexities including powered flight control system, the **Flight Safety Engineering** at aircraft companies became important. Human factor subjects were included in flight safety studies. The term **'System Safety'** was used for the first time in 1954 at a **Flight Safety Foundation Seminar**. In 1960 the 'System Safety' got further boost, driven largely by the new order of magnitude hazards associated with ballistic missiles and other space vehicles with their high energy and toxic rocket propulsion fuels. **'System Safety Programme for System and Associated Subsystems and Equipments'** (Mil-Std-882) first appeared in July 15, 1969. The Mil standard has gone through two revisions first in 1977 and finally in 1984.

System Safety Concepts

The system safety engineering is the process of applying scientific and engineering principles, criteria and techniques so as to develop products that are immune to component failures and human errors. The basic principles are to avoid accidents or mishaps. The essential condition for mishaps to happen is primarily, that a **hazardous situation** should exist and a **trigger event** will take it to the accident. Thus, if either the hazard or the trigger event can be prevented, then the accident would be avoided. The generic cause of an accident is shown at Fig.2. Most accidents normally occur as a consequence of any or a combination of inadequate design verification, improper maintenance or operations. The relationship amongst the contributory factors is shown in Fig.3.

It can be appreciated that the system safety process is a risk management process developed to the highest degree. The steps in the process would be:

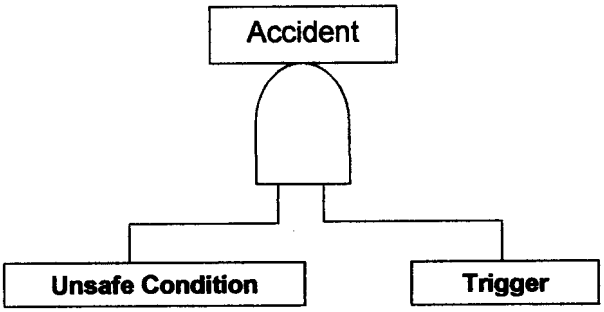
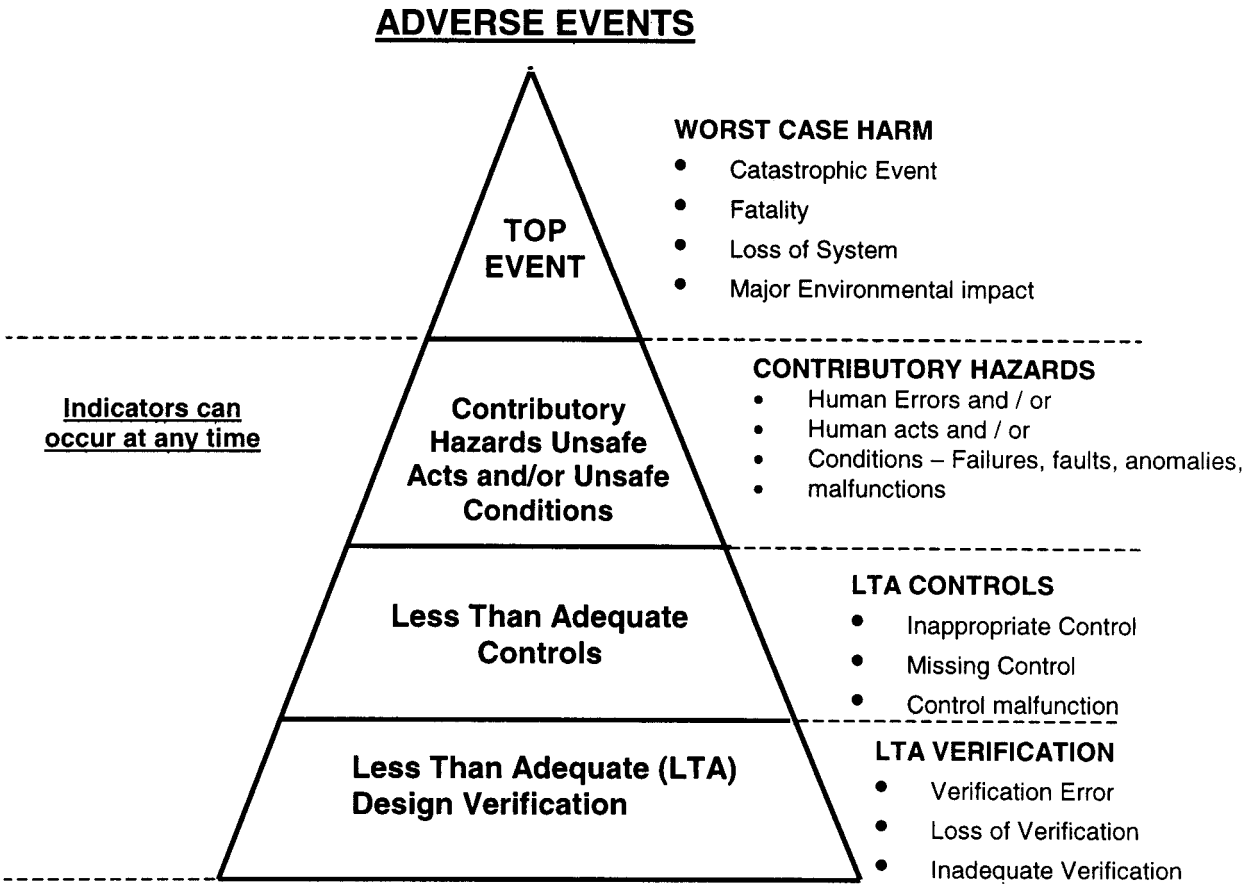


Fig.2 Genetic causes of an accident

- Identify the risks using hazard analysis techniques as early as possible in the system life cycle
- Develop options to eliminate, control, or avoid the hazard
- Provide for timely resolution of hazards
- Implement the best strategy
- Control the hazards through a close loop solution

System safety is not only a function of engineering but is an integral part of **top management activities**. Participation of management can assure the timely identification and resolution of hazards. Therefore a major requirement



- **Risk is associated with the adverse event, the potential accident**
- **RISK = (worst case severity of the event) (likelihood of the event)**
- **Accidents are the result of multi-contributors, unsafe acts and/ or conditions; failures, errors, malfunctions, inappropriate functions, normal functions that are out of sequence, faults, anomalies**

Fig.3 Relationship between contribution of hazards and adverse events

of system safety is that it must be institutionalized. Thus the system safety concepts aim at looking at safety as global perspectives of the management including man, machine and environment to perform the mission. To apply it as a modern method of accident prevention following must be conceptualized:

- Safety must be designed and built into the airplanes, just as are performance, stability and structural integrity.
- A safety group must be as important a part of an aircraft manufacturer's organization like stress, aerodynamics or controls group.
- A safety program should address all interface related issues like material compatibility, electromagnetic interference etc.
- Safety is a specialized subject as are other branches of aviation engineering.
- Every engineer cannot be expected to be thoroughly familiar with all the developments in the fields of safety any more than he can be expected to be an expert aerodynamicist.
- The evaluation of safety work in positive terms is extremely difficult. For example, when an accident does not occur, it is impossible to prove that some particular design feature prevented it.

On the human side the activities should address:

- Personnel planning, selection, assignment and performance assessment
- Design and build the aircraft in terms of human engineering of controls and displays and other system biomedical considerations
- Procedures and training to be considered
- Operational personnel situational awareness and motivation

System Safety Task

'System Safety Program Requirements' as defined in US DOD document MIL-STD-882 B, 1984, defines the task under two broad categories namely the, **'Program Management and control'** and the **'Design and Evaluation'**. At the proposal stage for a new aircraft, the contractor can and actually use ingenuity to submit specifics on how the tasks of system safety are to be accomplished. Eventually agreement is reached on the scope and direction of the program, which then gets monitored as the time progressed.

The various tasks as per the system safety program are shown below:

(a) Program Management and Control (MIL-STD-882B)

Task No.	Short Title
100	System Safety Program
101	System Safety Program Plan
102	Integration Management of Prime Contractors and Architect and Engineering Firms
103	System Safety Program Reviews
104	System Safety Group/Working Group Support
105	Hazard Tracking and Risk Resolution
106	Test and Evaluation Safety
107	System Safety Progress Summary
108	Qualification of System Safety Personnel

(b) Design and Evaluation (MIL-STD-882B)

Task No.	Short Title
201	Preliminary Hazard List
202	Preliminary Hazard Analysis
203	Sub System Hazard Analysis
204	System Hazard Analysis
205	Operating and Support Hazard Analysis
206	Operating Health Hazard Analysis
207	Safety Verification
208	Training
209	Safety Assessment
210	Safety Compliance Assessment
211	Software Hazard Analysis
212	Safety Re view of Engineering Change Deviations/Waivers
213	GFE/GFP System Safety Analysis

System Safety Matrix

(a) Severity Categories of Risk (MIL-STD-882B)

Severity Category	Description
Catastropic (I)	Death or System Loss
Critical (II)	Severe Injury, severe occupational illness or minor system damage
Marginal (III)	Minor Injury, minor occupational illness or minor system damage
Negligible (IV)	Less than minor Injury, occupational illness or system damage

(b) Probability Classifications from (MIL-STD-882B)

		Frequency of Occurrence	
Description	Level	Individual Items	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequency
Occasional	C	Likely to occur sometimes in life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be expected	Unlikely to occur, but possible

(c) Hazard Policy Guideline (MIL-STD-882B)

Hazard Risk Index	Acceptance Criteria
IA, IB, IC, IIA, IIB, IIIA	Hazard unacceptable
ID, IIC, IID, IIIB, IIIC	Hazard undesirable (higher management decision required)
IE, IIE, IIID, IIIE, IVA, IVB	Acceptable with review by management
IVC, IVD, IVE	Acceptable without review

System Safety Design Evaluations

System safety design concept tries to evaluate the risk associated with any event or existence of any unsafe conditions with an aim to estimate the safety margins available and ensure that that appropriate actions are taken to see that triggering action is avoided.

The various design evaluations that are carried out are discussed below:

- Preliminary Hazard Analysis (PHA)
- Sub System Hazard Analysis (SSHA)
- Failure Mode Effect and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- System Hazard Analysis (SHA)
- Operating and Support Hazard Analysis (OSHA)
- Maintenance Engineers Safety Analysis (MESA)
- Occupational and Health Hazard Analysis (OHHA) and finally
- Safety Margin Assessment

These analyses are carried out during the various phases of development and operation of the product as shown in Fig.4.

Preliminary Hazard Analysis - PHA is done at concept stage so that safety considerations are included in trade off studies during early design. The objective of PHA is to identify the hazards. The hazards that will impede the mission objectives will also to be identified. The various hazards that are to be identified are:

i) Hardware Hazards
ii) Software Hazards

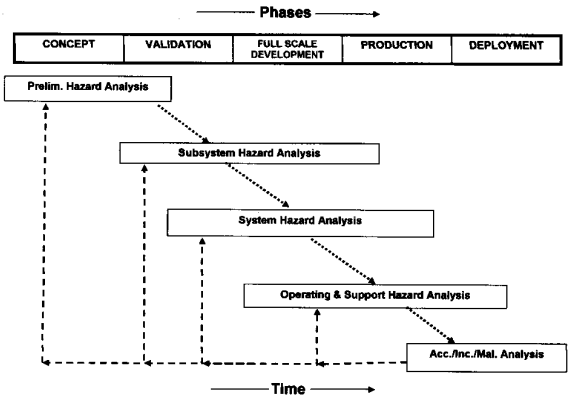


Fig.4 System Safety Analyses during product life cycle

iii) Procedural Hazards
iv) Human Factors
v) Interface Hazards
vi) Environmental Hazards including Health Hazard

The PHA tries to identify the hazards, both cause and effect of the hazard, criticality of the hazard and thus the recommendations and final actions. Example

Preliminary Hazard Analysis					
Hazard	Cause	Effect	Critic.	Recomnd	Final Action
Temp too high	Gauge Malfunction	Gas Leak	I	Provide cooling jacket	Provide cooling jacket
Leak thru pipeline	Vibration corrosion	Gas Leak	I	Instal St less Pipe	Install SS pipe with flexible joint

Sub System Hazard Analysis - SSHA is an extension of PHA. SSHA is based on the premise that an accident is a result of at least two events (a hazard state and a trigger) and can be prevented as long as either of them is controlled. These considerations are included in trade off studies during early design. The objective of PHA is to identify the hazards and the hazards that will impede the mission objectives. The analysis steps are:

i) Identify hazard
ii) Identify the trigger event leading to an accident
iii) Classify the criticality
iv) Identify the hazard and trigger control action

Fuel Sys.	**Sub System Hazard Analysis**				
Pt Name	Hazard	Trigger Event	Crit.	Recom.	Rev. crit.
Fuel Tank	Tank Rupture	Diff. pressure bet inside and outside the tank	IB	20 years life limit	IIIE
	Failure of tank seal	Any flame or spark	IB	Provide double seal	IIC

Failure Mode Effect Criticality Analysis - FMECA evaluates the effect of component failure and is usually done by reliability engineers as per Mil-STD- 1629. However a team of safety engineers, design engineers and reliability engineers would do it better. The difference lies in the outlook. For example a reliability engineer will not consider a failure critical if redundancy is present while a safety engineer may still consider the failure critical. For example, if an aircraft device has a redundant circuit board, a failure may not be critical if only one CB fails. But if the failure is not detectable and replaced immediately, the second failure could be catastrophic.

Fault Tree Analysis - FTA is an inductive process especially useful for analyzing cat II and I hazards, when the hazards have not been resolved. FTA is used to identify cause of hazard so that an effect can be made to eliminate as many causes as possible. FTA is a cause and effect diagram which uses the standard symbols of and, or, condition, diamond etc. It is top to bottom diagram. It also uses various tools like computing techniques for estimating the probability of accidents; cut set analysis to identify all single point failures and other paths, which lead to a failure. This helps to identify the weaknesses where a single event or component that can cause the system to fail.

System Hazard Analysis - SHA is the analysis of interface effects and interface integration. Results of subsystem hazard analysis are evaluated to assess impact on other subsystem and on the total system. The various interfaces that are to be considered are: hardware-to-hardware, hardware to software, and software to software. Human interfaces are also to be equally considered. Interface integration usually involves merger of the supplier system with that of the customer. There is no standard method, and the format for reporting varies according to the needs of the system.

In the beginning of the project, PHA serves as a rough SHA. PHA is then replaced by complete and detailed analysis. Techniques similar to SSHA can be used for SHA. Inputs from FMECA and SCA are especially valuable because they affect the entire system. FTA can also be a very efficient tool for the SHA.

Operating and Support Hazard Analysis - O & SHA is done for operating procedures and support functions such as

i) Production, Testing and Deployment

ii) Storage, Handling and Disposal
iii) Modification, Demilitarisation and Emergency Actions

The inputs for this analysis come from previously mentioned analyses where operating hazards are identified. Other inputs come from prototype tests, mock installations, emergency procedures and interviews with operating and maintenance personnel. The analyses bring out:

- Activities, which occur under hazardous conditions, their durations and actions, required to minimize their risk.
- Changes required in functional or design requirements for system hardware/software, facilities, tooling or support/test equipment to eliminate hazards or reduce associated risks.
- Requirements for safety devices and equipment including personnel safety and life support equipment.
- Warning, cautions and special emergency procedures (e.g. egress, rescue, back-out).
- Requirements for handling, storage, transportation, maintenance and disposal of hazardous materials.
- Requirements for safety training and personnel certification.

Maintenance Engineers Safety Analysis - MESA consists of writing the procedure in logical tasks and then treating each task as a component for hazard analysis. During the early part of the design procedures are not available. However a rough draft of the potential procedures is constructed with the help of maintenance personnel who have worked on similar systems. A method called **THERP** (Technique of Human Error Rate Prediction) is used where maintenance safety is analyzed on the basis of interviews of the maintenance and operating personnel on similar systems. The best time to do this analysis is during preliminary design and study must be completed before critical design review.

Occupational Health Hazard Assessment - OHHA identifies health hazard so that engineering control can be placed, rather than make short- term fixes or depend entirely on persons to protect themselves. Items to be considered are:

- Toxic material such as poisons, carcinogens and respiratory irritants
- Physical environments such as noise, heat and radiation
- Explosion hazards such as concentrations of fine metal particles, gaseous mixtures and combustibles
- Adequacy of protective means such as goggles and protective clothing
- Facility environment such as ventilation and combustible materials

Conclusion

While design evaluations help discover potential hazards, the residual hazards must have adequate safety margins. These evaluations should be continued and management actions to bring the safety within acceptable limits must continue.

Close Loop Hazard Management - the effort to resolve hazards permanently must go on. Hazard should be reported even if they did not result in an accident. The recommendations form defect, and incident investigations must be integrated in a close loop system so that never again similar occurrences take place. The task cards or the operating procedures must be upgraded incorporating these changes. Future audits should ensure their compliance.

Integrity of the procedures - in no case any one should be allowed to violate the safety procedures. A separate audit should be carried out to check their validity and that they are adhered to.

Configuration Control - changes in product design and manufacture should be controlled or administered through a Configuration Control Board. Configuration control means preserving the functional integrity of the product and not merely control of documents. Changes in manufacturing processes are to be properly evaluated before acceptance. In the change analysis the new procedure is written and compared side by side with the old procedure.

The differences are identified and are evaluated for their effect.

Accident Investigation - if mishaps already occurred, failure analysis laboratories are utilized for establishing the failure mode.

System Safety Goal - To a question ‘How safe is safe’, Flight safety foundation responded ‘It is as safe as our societal capabilities and determination allow it to be’. However as system safety engineers, ‘we are never happy with any safety record. We are always striving to do better’.

References

1. Earl L. Wiener and David C Nagel., "Human Factors in Aviation", Academic Press, Inc., USA, 1988.

2. Frank H Hawkins., "Human Factors in Flight", Himalayan Books, New Delhi, 1989.

3. Dev G. Raheja., "Assurance Technologies- Principles and Practices", McGraw Hill, Inc.

4. Shari Stamford Krause., "Aircraft Safety- Accident Investigations, Analyses and Applications", McGraw Hill Inc, 2003.